



**Hewlett Packard
Enterprise**

HPE ProLiant DL20 Gen10 Server User Guide

Abstract

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

Part Number: P04759-001
Published: November 2018
Edition: 1

Notices

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

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

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

Acknowledgments

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

Linux[®] is the registered trademark of Linus Torvalds in the U.S. and other countries.

Red Hat[®] Enterprise Linux is a registered trademark of Red Hat, Inc. in the United States and other countries.

VMware[®] ESXi[™] and VMware vSphere[®] are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

Contents

- Component identification..... 7**
 - Front panel components.....7
 - Serial number/iLO information pull tab..... 9
 - Front panel LEDs and buttons.....9
 - UID button functionality.....10
 - Front panel LED power fault codes..... 10
 - Rear panel components.....11
 - Rear panel LEDs.....12
 - System board components.....13
 - System maintenance switch descriptions.....15
 - DIMM slot locations.....15
 - DIMM label identification.....16
 - PCIe riser board slot definitions.....17
 - Drive LED definitions.....18
 - Low profile LFF drive LED definitions.....18
 - Hot-plug drive LED definitions.....19
 - Drive bay numbering.....20
 - Fan locations.....22

- Setup.....23**
 - Optional service.....23
 - Setting up the server.....23
 - Operational requirements.....26
 - Space and airflow requirements.....26
 - Temperature requirements.....27
 - Power requirements.....27
 - Electrical grounding requirements.....27
 - Server warnings and cautions.....28
 - Rack warnings and cautions.....28
 - Electrostatic discharge.....29
 - Configuring the server.....30
 - Operating system.....30
 - Installing the operating system with Intelligent Provisioning.....31

- Operations.....32**
 - Removing the security bezel (optional).....32
 - Installing the security bezel (optional).....32
 - Powering down the server.....33
 - Powering up the server.....33
 - Extending the server from the rack.....34
 - Removing the server from the rack.....35
 - Removing the access panel.....36
 - Installing the access panel.....37
 - Removing the riser cage.....38
 - Installing the riser cage.....39
 - Installing the server into the rack.....40

Hardware options installation.....	44
Introduction.....	44
Rack rail option.....	44
Installing the rack rail option.....	44
Installing the rack rail hook-and-loop strap.....	48
Drive options.....	49
Drive installation guidelines.....	49
Drive support information.....	49
Installing an LFF non-hot-plug drive.....	49
Installing an LFF hot-plug drive.....	52
Installing an SFF hot-plug drive.....	53
Power supply options.....	54
Hot-plug power supply calculations.....	54
Power supply warnings and cautions.....	55
Installing a hot-plug power supply in redundant power supply bay.....	55
Optical drive enablement option.....	56
Installing the optical drive option for LFF configuration.....	56
Installing the optical drive enablement option for SFF configuration.....	59
Two-bay SFF hot-plug drive enablement option.....	61
Installing the two-bay SFF hot-plug drive enablement drive cage.....	62
Memory options.....	63
DIMM population information.....	63
Installing a DIMM.....	63
Expansion board options.....	64
Installing an expansion board.....	65
Installing the M.2 SATA SSD expansion board and M.2 SATA cables.....	67
Storage controller options.....	69
Smart Array modular controller (AROC) option.....	69
Installing a Smart Array modular controller (AROC).....	69
External type-P and type-E Smart Array SR Gen10 controller option.....	71
Smart Storage Battery option.....	71
Installing the Smart Storage Battery.....	71
M.2/dedicated iLO/serial port option.....	72
M.2/dedicated iLO/serial port option kit content.....	73
M.2 SSD system board connectors.....	74
Installing the M.2/dedicated iLO/serial port enablement board.....	74
M.2 SSD module option.....	78
Installing the M.2 SSD on the system board.....	78
Installing an M.2 SSD module on M.2/dedicated iLO/serial port enablement board....	81
Installing the Serial Port.....	83
Enabling the dedicated iLO management module.....	84
FlexibleLOM riser option.....	85
Installing the FlexibleLOM riser assembly.....	85
Transceiver option.....	86
Transceiver warnings and cautions.....	86
Installing a transceiver.....	87
Chassis Intrusion detection option.....	88
Installing the Chassis Intrusion Detection switch.....	88
HPE Trusted Platform Module 2.0 Gen10 option.....	89
Overview.....	89
HPE Trusted Platform Module 2.0 Guidelines.....	90
Installing and enabling the HPE TPM 2.0 Gen10 Kit.....	90
Installing the Trusted Platform Module board.....	90
Enabling the Trusted Platform Module.....	93

Cabling..... 95

Cabling guidelines..... 95

Storage cabling..... 96

 Non-hot-plug drive cabling..... 96

 Hot-plug drive cabling..... 97

 Two-bay LFF hot-plug drive cabling..... 97

 Four bay SFF hot-plug drive cabling..... 98

 4+2 bay SFF hot-plug drive cabling..... 99

 M.2 SATA SSD cabling..... 100

Smart Storage Battery cabling..... 101

Storage controller backup power cabling..... 102

Optical drive cabling..... 103

Fan cabling..... 104

Chassis Intrusion detection cabling..... 104

M.2/dedicated iLO/serial port cabling..... 105

Power supply cabling..... 105

Software and configuration utilities..... 107

Server mode..... 107

Product QuickSpecs..... 107

Active Health System Viewer..... 107

 Active Health System..... 107

 Active Health System data collection..... 108

 Active Health System Log..... 108

HPE iLO 5..... 108

 iLO Federation..... 109

 iLO Service Port..... 109

 iLO RESTful API..... 110

 RESTful Interface Tool..... 110

 iLO Amplifier Pack..... 110

Integrated Management Log..... 110

Intelligent Provisioning..... 110

 Intelligent Provisioning operation..... 111

Management Security..... 111

Scripting Toolkit for Windows and Linux..... 112

UEFI System Utilities..... 112

 Selecting the boot mode 112

 Secure Boot..... 113

 Launching the Embedded UEFI Shell 114

HPE Smart Storage Administrator..... 114

USB support..... 115

 External USB functionality..... 115

Redundant ROM support..... 115

 Safety and security benefits..... 115

Keeping the system current..... 115

 Updating firmware or system ROM..... 115

 Service Pack for ProLiant..... 116

 Updating firmware from the System Utilities 117

 Updating the firmware from the UEFI Embedded Shell 118

 Online Flash components..... 118

 Drivers..... 118

 Software and firmware..... 118

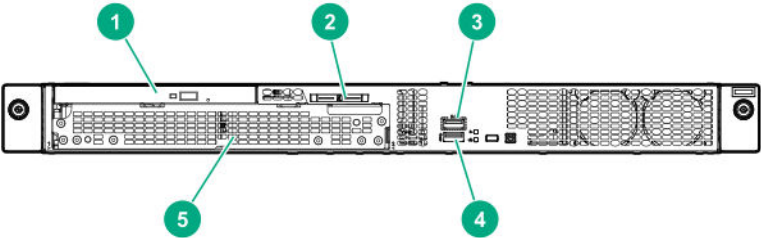
Operating system version support.....	119
HPE Pointnext Portfolio.....	119
Proactive notifications.....	119
Troubleshooting.....	120
NMI functionality.....	120
Troubleshooting resources.....	120
System battery replacement.....	121
Removing and replacing the system battery.....	121
Specifications.....	122
Environmental specifications.....	122
Mechanical specifications.....	123
Power supply specifications.....	123
ATX 290W Non-Hot-plug Power Supply.....	123
HPE 500W Flex Slot Platinum Hot-plug Low Halogen Power Supply.....	124
HPE 800W Flex Slot -48VDC Hot plug Low Halogen Power Supply.....	124
Safety, warranty, and regulatory information.....	126
Regulatory information.....	126
Local representative information.....	126
Turkey RoHS material content declaration.....	127
Ukraine RoHS material content declaration.....	127
GS Gloss declaration.....	127
Websites.....	128
Warranty information.....	128
Support and other resources.....	129
Accessing Hewlett Packard Enterprise Support.....	129
ClearCARE technical support.....	129
Accessing updates.....	129
Customer self repair.....	130
Remote support.....	130
Documentation feedback.....	131
Acronyms and abbreviations.....	132

Component identification

This chapter describes the external and internal server features and components.

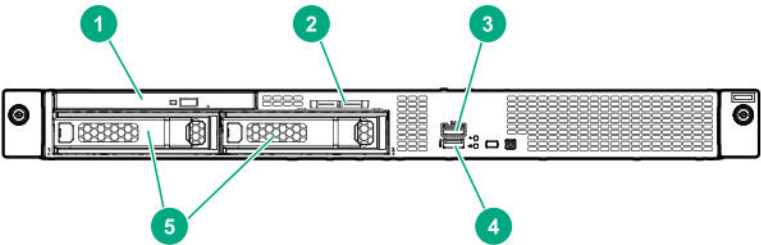
Front panel components

Two-bay LFF non-hot-plug drive model



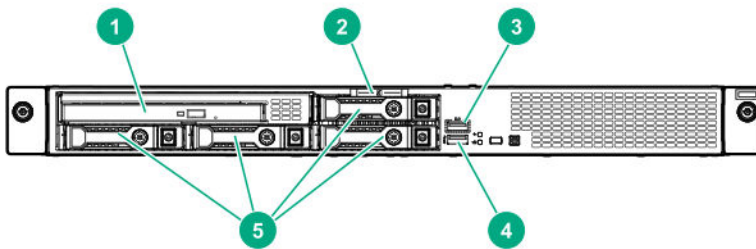
Item	Description
1	Optical drive (optional)
2	<u>Serial number/iLO information pull tab</u>
3	iLO Service Port
4	USB 3.0 port
5	Two-bay LFF non-hot-plug drive cage

Two-bay LFF hot-plug drive model



Item	Description
1	Optical drive (optional)
2	Serial number/iLO information pull tab
3	iLO Service Port
4	USB 3.0 port
5	Two-bay LFF hot-plug drive bays

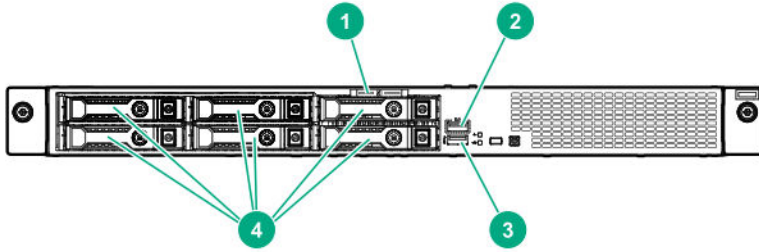
Four-bay SFF hot-plug drive model



Item	Description
1	Media drive bay ¹
2	Serial number/iLO information pull tab
3	iLO Service Port
4	USB 3.0 port
5	Four-bay SFF hot-plug drive bays

¹ The media drive bay supports an optical drive assembly or a two-bay SFF drive cage assembly.

Six-bay SFF hot-plug drive model



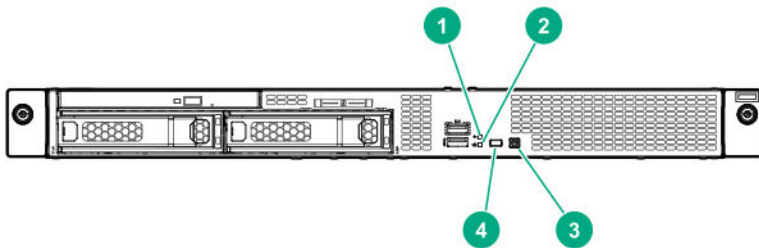
Item	Description
1	<u>Serial number/iLO information pull tab</u>
2	iLO Service Port
3	USB 3.0 port
4	Six-bay SFF hot-plug drive bays

Serial number/iLO information pull tab

The serial number/iLO information pull tab is double-sided. One side shows the server serial number and the customer asset tag label. The other side shows the default iLO account information and QR code label.

Use a mobile device to scan the QR code label to display the server mobile product page (<http://www.hpe.com/qref/dl20gen10>). This page contains links to server setup information, spare part numbers, QuickSpecs, troubleshooting resources, and other useful product links.

Front panel LEDs and buttons



Item	Description	Status	Definition
1	Health LED ¹	Solid Green	Normal
		Flashing Green	iLO is rebooting
		Flashing amber	System degraded ²
		Flashing Red	System critical ²
2	NIC status LED ¹	Solid green	Link to network
		Flashing green	Network active
		Off	No network activity
3	Power On/ Standby button and system power LED ¹	Solid green	System on
		Flashing green	Performing power-on sequence
		Solid amber	System in standby
		Off	No power present ³
4	UID button/LED ¹	Solid blue	Activated
		Flashing blue	<ul style="list-style-type: none"> • 1 flash per second = Remote management or firmware upgrade in progress • 4 flashes per second = iLO manual reboot sequence initiated • 8 flashes per second = iLO manual reboot sequence in progress
		Off	Deactivated
		Off	Deactivated

¹ When the LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see **Front panel LED power fault codes** on page 10.

² If the health LED indicates a degraded or critical state, review the system IML or use iLO to review the system health status.

³ Facility power is not present, power cord is not attached, no power supplies are installed, or power supply failure has occurred.

UID button functionality

The UID button can be used to display the Server Health Summary when the server will not power on. For more information, see the iLO user guide on the Hewlett Packard Enterprise website (<http://www.hpe.com/support/ilo-docs>).

Front panel LED power fault codes

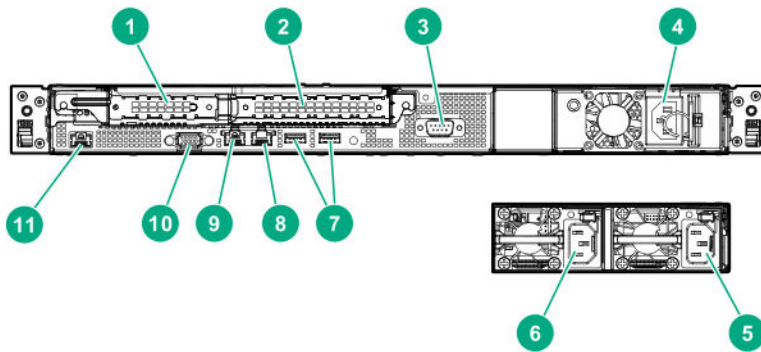
The following table provides a list of power fault codes, and the subsystems that are affected. Not all power faults are used by all servers.

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

Rear panel components

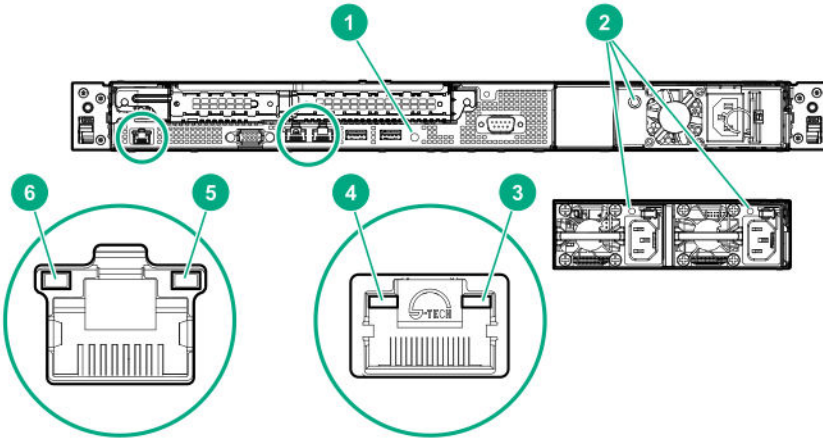


Item	Description
1	Slot 1 PCIe3 x8 (8, 4, 1)/FlexibleLOM ¹
2	Slot 2 PCIe3 x8 (8, 4, 1) ¹
3	Serial port (optional)
4	Non-hot-plug power supply
5	Hot-plug power supply bay 1 (optional)
6	Hot-plug power supply bay 2 (optional)
7	USB 3.0 ports (2)
8	NIC port (1Gb)
9	NIC port (1Gb) /iLo port ²
10	VGA port
11	Dedicated iLO Management port (optional)

¹ For more information, see [PCIe riser board slot definitions](#).

² If FlexibleLOM is installed in the server, the shared iLO port behavior will be default to port 1 of the FlexibleLOM card.

Rear panel LEDs

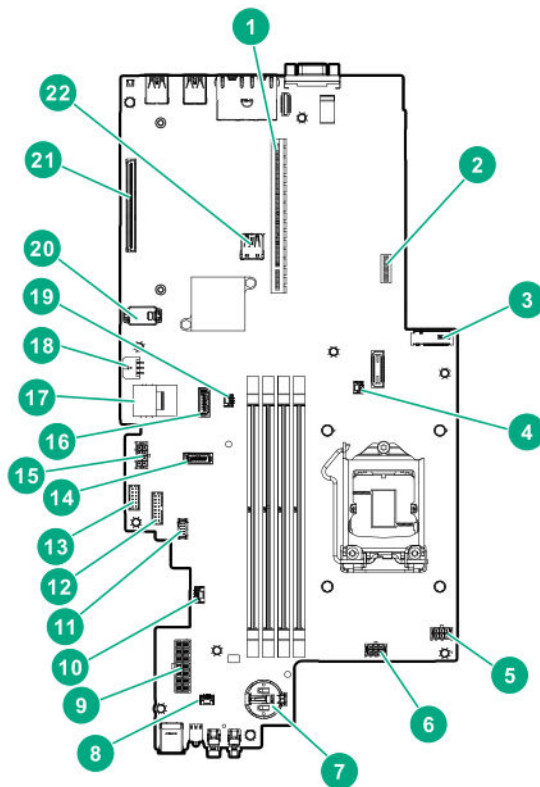


Item	LED	Status	Definition
1	UID	Solid blue	Activated
		Flashing blue	<ul style="list-style-type: none"> 1 flash per second = Remote management of firmware upgrade in progress 4 flashes per second = iLO manual reboot sequence initiated 8 flashes per second = iLO manual reboot sequence in progress
		Off	Deactivated
2	Power supply	Solid green	Normal
		Off	One or more of the following condition exists: <ul style="list-style-type: none"> Power is unavailable Power supply failed Power supply is in standby mode Power supply error
3	NIC/iLO status	Solid green	Link to network

Table Continued

Item	LED	Status	Definition
		Flashing green	Network active
		Off	No network activity
4	NIC link	Solid green	Network link
		Off	No network link
5	iLO status	Solid green	Link to network
		Flashing green	Network active
		Off	No network activity
6	iLO link	Solid green	Network link
		Off	No network link

System board components



Item	Description
1	PCIe riser connector ¹
2	<u>System maintenance switch</u> ²
3	Onboard M.2/Dedicated iLO management connector
4	Storage backup power connector for slot 1
5	Fan connector 2
6	Fan connector 1
7	System battery
8	Chassis Intrusion Detection switch
9	Standard or Flexible Slot power supply connector
10	Two-bay SFF drive sideband connector
11	Smart Storage Battery connector
12	Standard or Flexible Slot power supply sideband connector
13	Flexible slot power supply connector
14	x1 SATA port 2
15	Drive backplane and optical drive power connector
16	x1 SATA port 1
17	x4 SATA port (Mini-SAS connector)
18	Fan connector 3
19	Storage backup power connector for slot 2
20	TPM connector
21	Smart Array modular controller connector (AROC)
22	Internal USB 3.0 connector

¹ For more information on the riser board slots supported by the onboard PCI riser connectors, see **PCIe riser board slot definitions** on page 17.

² For more information on the system maintenance switch , see **System maintenance switch descriptions** on page 15

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

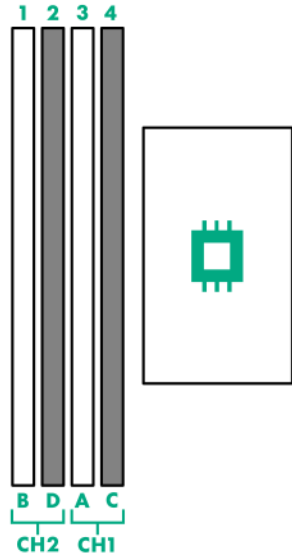
¹ To access the redundant ROM, set S1, S5, and S6 to On.

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 113.

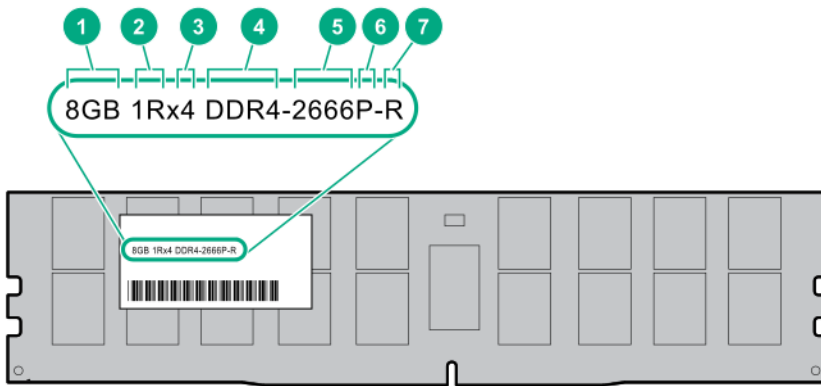
DIMM slot locations

The arrow in the illustration points to the front of the server.



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.



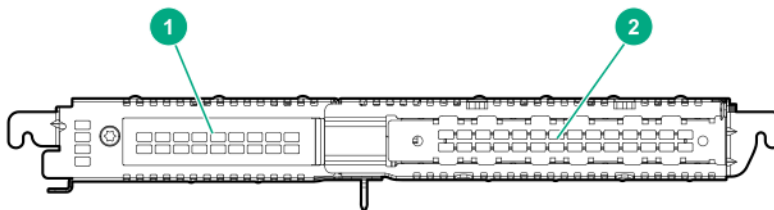
Item	Description	Example
1	Capacity	8 GB 16 GB 32 GB 64 GB 128 GB
2	Rank	1R = Single rank 2R = Dual rank 4R = Quad rank 8R = Octal rank

Table Continued

Item	Description	Example
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
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)
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 product QuickSpecs on the Hewlett Packard Enterprise website (<http://www.hpe.com/info/qs>).

PCIe riser board slot definitions



- FlexibleLOM riser board

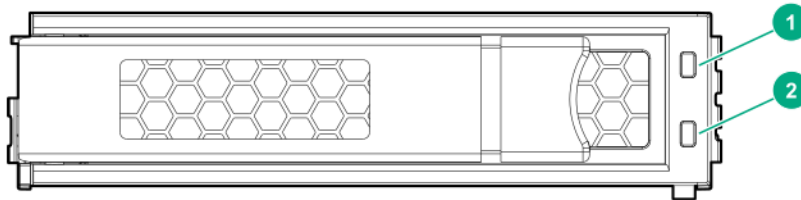
Item	Slot number	Form factor	Slot description
1	FlexibleLOM slot	FlexibleLOM	PCIe x8 (with NCSI)
2	2	Full-height, half-length	PCIe3 x16 (8,4,1)

- Two-slot PCIe riser board

Item	Slot number	Form factor	Slot description
1	1	Low-profile	PCIe3 x8 (8,4,1)
2	2	Full-height, half-length	PCIe3 x16 (8,4,1)

Drive LED definitions

Low profile LFF drive LED definitions

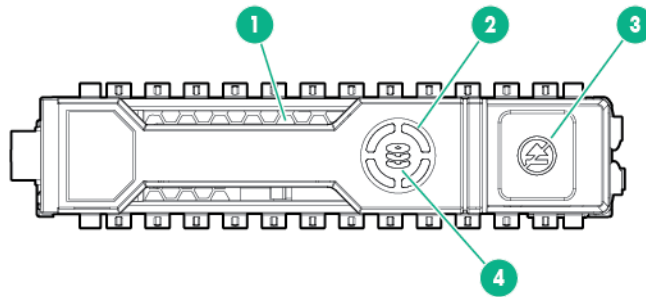


Item	LED	Status	Definition
1	Fault \Locate	Solid amber	The drive has failed.
		Solid blue	The drive is operating normally and being identified by a management application.
		Flashing amber/blue (1 flash per second)	The drive has failed, or a predictive failure alert has been received for this drive; it also has been identified by a management application.
		Flashing amber (1 flash per second)	A predictive failure alert has been received for this drive. Replace the drive as soon as possible.
2	Online Activity	Solid green	The drive is online and has no activity.
		Flashing green (4 flashes per second)	The drive is operating normally and has activity.

Table Continued

Item	LED	Status	Definition
		Flashing green (1 flash per second)	The drive is doing one of the following: <ul style="list-style-type: none"> • Rebuilding • Performing a RAID migration • Performing a strip size migration • Performing a capacity expansion • Performing a logical drive extension • Erasing • Spare part activation
		Off	The drive is not configured by a RAID controller or a spare drive.

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: <ul style="list-style-type: none"> • 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.

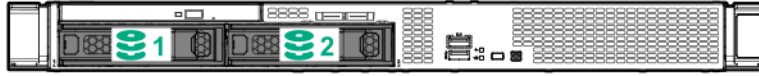
Drive bay numbering

The following images show the drive numbering for each of the supported drive configurations.

- Two-bay LFF non-hot-plug drive model



- Two-bay LFF hot-plug drive model



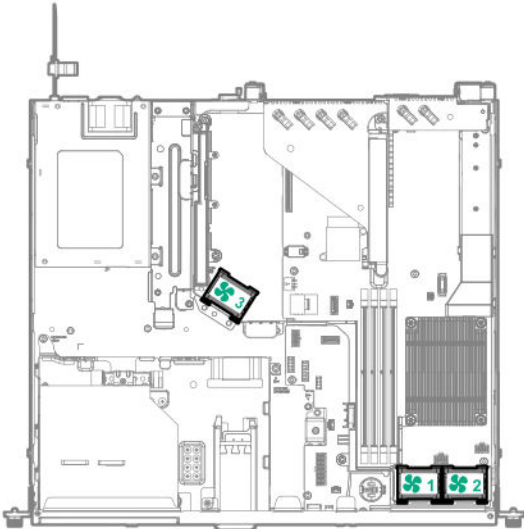
- Four-bay SFF hot-plug drive model



- Six-bay SFF hot-plug drive model



Fan locations



Setup

Optional service

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

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

- Foundation Care – Keep systems running.
 - 6-Hour Call-to-Repair¹
 - 4-Hour 24x7
 - Next Business Day
- Proactive Care – Help prevent service incidents and get you to technical experts when there is one.
 - 6-Hour Call-to-Repair¹
 - 4-Hour 24x7
 - Next Business Day
- Deployment service for both hardware and software
- Hewlett Packard Enterprise Education Services – Help train your IT staff.

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

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

Setting up the server

Prerequisites

Before setting up the server, be sure to read the following:

- Download the latest SPP:
<http://www.hpe.com/servers/spp/download>
Support validation required
- Verify that your OS or virtualization software is supported:
<http://www.hpe.com/info/ossupport>
- Read the operational requirements for the server:
Operational requirements on page 26
- Read the safety and compliance information on the HPE website:
<http://www.hpe.com/support/safety-compliance-enterpriseproducts>

- Obtain the storage driver if needed:
 - Download it from the HPE Support Center website:
<http://www.hpe.com/support/hpesc>
 - Extract it from the SPP.
- Read the rack warnings and cautions:
Rack warnings and cautions on page 28
- Read the server warnings and cautions:
Server warnings and cautions on page 28

Procedure

Unbox the server

1. Unbox the server and verify the contents:
 - Server
 - Power cord
 - Rack-mounting hardware (optional)
 - Documentation

Install the hardware options

2. (Optional) Install hardware options. For installation instructions, see **Hardware options installation** on page 44.
3. **Install the server into the rack.**
4. Decide how to manage the server:
 - Locally: Use a KVM switch or a connect a keyboard, monitor, and mouse.
 - Remotely: Connect to the iLO web interface and run a remote console:
 - a. Verify the following:
 - iLO is licensed to use the remote console feature.
If iLO is not licensed, visit
<http://www.hpe.com/info/ilo>.
 - The iLO Management Port is connected to a secure network.
 - b. Using a browser, navigate to the iLO web interface, and then log in.
`https://<iLO hostname or IP address>`
Note the following:
 - The iLO hostname is located on the serial number/iLO information label located on the top of the chassis.
 - If a DHCP server assigns the IP address, the IP address appears on the boot screen.

- If a static IP address is assigned, use that IP address.
 - The default login credentials are located on the serial number/iLO information pull tab.
- c. In the side navigation, click the **Remote Console & Media** link, and then launch a remote console.
5. Press the Power On/Standby button.
For remote management, use the iLO virtual power button.
6. Using the SPP, **update the following**:
- System ROM
 - Storage controller
 - Network adapters
 - Intelligent Provisioning

Set up the storage

7. Set up the storage. Do one of the following:
- To configure the server to boot from a SAN, see the following guide:
<https://www.hpe.com/info/boot-from-san-config-guide>
 - If an HPE Smart Array SR controller is installed:
 - For SR controllers, use the HPE Smart Storage Administrator to create arrays:
 - a. From the boot screen, press **F10** to run Intelligent Provisioning.
 - b. From Intelligent Provisioning, run **HPE Smart Storage Administrator**.
 - If no controller option is installed, do one of the following:
 - AHCI is enabled by default. You can deploy an OS or virtualization software.
 - Disable AHCI, enable software RAID, and then create an array:
 - a. From the boot screen, press **F9** to run UEFI System Utilities.
 - b. From the UEFI System Utilities screen, select **System Configurations > BIOS/Platform Configuration (RBSU) > Storage Options > SATA Controller Options > Embedded SATA Configuration > Smart Array SW RAID Support**.
 - c. Enable **Smart Array SW RAID Support**.
 - d. Save the configuration and reboot the server.
 - e. Create an array:
 - I. From the boot screen, press **F9** to run UEFI System Utilities.
 - II. From the UEFI System Utilities screen, select **System Configuration > Embedded Storage: HPE Smart Storage S100i SR Gen10 > Array Configuration > Create Array**.

Deploy an OS or virtualization software

8. Deploy an OS or virtualization software. Do one of the following:

- Press **F10** at the boot screen to run Intelligent Provisioning and deploy and OS.
- Manually deploy an OS.
 - a. Insert the installation media.

For remote management, click **Virtual Drives** in the iLO remote console to mount images, drivers, or files to a virtual folder. If a storage driver is required to install the OS, use the virtual folder to store the driver.
 - b. Press F11 at boot screen to select the boot device.
 - c. After the OS installed, **update the drivers**.

Register the server

9. To experience quicker service and more efficient support, register the server at the HPE website:
<https://myenterpriselicence.hpe.com>

Operational requirements

Space and airflow requirements

To allow for servicing and adequate airflow, observe the following space and airflow requirements when deciding where to install a rack:

- Leave a minimum clearance of 63.5 cm (25 in) in front of the rack.
- Leave a minimum clearance of 76.2 cm (30 in) behind the rack.
- Leave a minimum clearance of 121.9 cm (48 in) from the back of the rack to the back of another rack or row of racks.

Hewlett Packard Enterprise servers draw in cool air through the front door and expel warm air through the rear door. Therefore, the front and rear rack doors must be adequately ventilated to allow ambient room air to enter the cabinet, and the rear door must be adequately ventilated to allow the warm air to escape from the cabinet.

⚠ CAUTION: To prevent improper cooling and damage to the equipment, do not block the ventilation openings.

When vertical space in the rack is not filled by a server or rack component, the gaps between the components cause changes in airflow through the rack and across the servers. Cover all gaps with blanking panels to maintain proper airflow.

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

The 9000 and 10000 Series Racks provide proper server cooling from flow-through perforations in the front and rear doors that provide 64 percent open area for ventilation.

⚠ CAUTION: When using a Compaq branded 7000 series rack, install the high airflow rack door insert (PN 327281-B21 for 42U rack, PN 157847-B21 for 22U rack) to provide proper front-to-back airflow and cooling.

-
- ⚠ CAUTION:** If a third-party rack is used, observe the following additional requirements to ensure adequate airflow and to prevent damage to the equipment:
- Front and rear doors—If the 42U rack includes closing front and rear doors, you must allow 5,350 sq cm (830 sq in) of holes evenly distributed from top to bottom to permit adequate airflow (equivalent to the required 64 percent open area for ventilation).
 - Side—The clearance between the installed rack component and the side panels of the rack must be a minimum of 7 cm (2.75 in).
-

Temperature requirements

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

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

-
- ⚠ CAUTION:** To reduce the risk of damage to the equipment when installing third-party options:
- Do not permit optional equipment to impede airflow around the server or to increase the internal rack temperature beyond the maximum allowable limits.
 - Do not exceed the manufacturer's TMRA.
-

Power requirements

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

-
- ⚠ WARNING:** To reduce the risk of personal injury, fire, or damage to the equipment, do not overload the AC supply branch circuit that provides power to the rack. Consult the electrical authority having jurisdiction over wiring and installation requirements of your facility.
-
- ⚠ CAUTION:** Protect the server from power fluctuations and temporary interruptions with a regulating uninterruptible power supply. This device protects the hardware from damage caused by power surges and voltage spikes and keeps the system in operation during a power failure.
-


Electrical grounding requirements


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


Because of the high ground-leakage currents associated with multiple servers connected to the same power source, Hewlett Packard Enterprise recommends the use of a PDU that is either permanently wired to the building's branch circuit or includes a nondetachable cord that is wired to an industrial-style plug. NEMA


locking-style plugs or those complying with IEC 60309 are considered suitable for this purpose. Using common power outlet strips for the server is not recommended.


Server warnings and cautions


-  **WARNING:** To reduce the risk of personal injury, electric shock, or damage to the equipment, disconnect the power cord to remove power from the server. Pressing the Power On/Standby button does not shut off system power completely. 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.


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


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

 -  **CAUTION:** To avoid data loss, Hewlett Packard Enterprise recommends that you back up all server data before installing or removing a hardware option, or performing a server maintenance or troubleshooting procedure.

 -  **CAUTION:** Do not operate the server for long periods with the access panel open or removed. Operating the server in this manner results in improper airflow and improper cooling that can lead to thermal damage.
-

Rack warnings and cautions

-  **WARNING:** When all components are removed, the server weighs 6 kg (20.81 lb). When all components are installed, the server can weigh up to 9.46 kg (13.18 lb).
Before configuring your rack solution, be sure to check the rack manufacturer weight limits and specifications. Failure to do so can result in physical injury or damage to the equipment and the facility.

 -  **WARNING:** To reduce the risk of personal injury or damage to the equipment, be sure that:
 - The rack has anti-tip measures in place. Such measures include floor-bolting, anti-tip feet, ballast, or a combination as specified by the rack manufacturer and applicable codes.
 - The leveling jacks (feet) are extended to the floor.
 - The full weight of the rack rests on the leveling jacks (feet).
 - The stabilizing feet are attached to the rack if it is a single-rack installation.
 - The racks are coupled together in multiple rack installations.
-

⚠ WARNING: The chassis is heavy. To reduce the risk of personal injury or damage to the equipment, do the following:

- Observe local occupational health and safety requirements and guidelines for manual material handling.
- Get help to lift and stabilize the product during installation or removal, especially when the product is not fastened to the rails. The chassis weighs more than 6 kg (20.81 lb), so at least two people must lift the chassis into the rack together. An additional person may be required to help align the chassis if the chassis is installed higher than chest level.
- Use caution when installing the chassis into or removing the chassis from the rack.
- Adequately stabilize the chassis before extending a component outside the rack. Extend only one component at a time. The rack might become unstable if more than one component is extended.
- Do not stack anything on top of rail-mounted component or use it as a work surface when extended from the rack.

⚠ WARNING: The rack rails form only a shelf for the chassis to rest on. The chassis is not attached to the rails by any other means. Slipping and falling chassis will cause bodily injury or damage the chassis, so use extreme care when pulling the chassis out from the rack. Hewlett Packard Enterprise is not responsible for any injury or damage caused by the mishandling of the chassis.

⚠ CAUTION: Before installing the server into a rack, be sure to properly scope the limitations of the rack. Before proceeding with the installation, consider the following:

- You must fully understand the static and dynamic load carrying capacity of the rack and be sure that it can accommodate the maximum weight of the server.
- Be sure sufficient clearance exists for cabling, installation and removal of the server, and movement of the rack doors.

⚠ CAUTION: Always plan the rack installation so that the heaviest item is on the bottom of the rack. Install the heaviest item first, and continue to populate the rack from the bottom to the top.

Electrostatic discharge

Be aware of the precautions you must follow when setting up the system or handling components. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the system or component.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

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

For more information on static electricity or assistance with product installation, contact an authorized reseller.

Configuring the server

When the server is powered on, the POST screen is displayed. Use the following options to configure the server:

- **System utilities (F9)**
Use this option to configure UEFI, RBSU, or other boot settings.
- **Intelligent Provisioning (F10)**
Use this option to configure drives, access Smart Storage Administrator, or begin installing or deploying an operating system.
- **Boot order (F11)**
Use this option to select a boot device.
- **Network boot (F12)**
Use this option to PXE boot the server from the network.

Operating system

This ProLiant server does not ship with provisioning media. Everything required to manage and install the system software and firmware is preloaded on the server.

To operate properly, the server must have a supported operating system. Attempting to run an unsupported operating system can cause serious and unpredictable results. For the latest information on operating system support, see the [Hewlett Packard Enterprise website](#).

Failure to observe UEFI requirements for ProLiant Gen10 servers can result in errors installing the operating system, failure to recognize boot media, and other boot failures. For more information on these requirements, see the *HPE UEFI Requirements* on the [Hewlett Packard Enterprise website](#).

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

- **Intelligent Provisioning**—For single-server deployment, updating, and provisioning capabilities. For more information, see [Installing the operating system with Intelligent Provisioning](#) on page 31.
- **Insight Control server provisioning**—For multiserver remote OS deployment, use Insight Control server provisioning for an automated solution. For more information, see the Insight Control documentation on the [Hewlett Packard Enterprise website](#).

For additional system software and firmware updates, download the Service Pack for ProLiant from the [Hewlett Packard Enterprise website](#). Software and firmware must be updated before using the server for the first time, unless any installed software or components require an older version.

For more information, see [Keeping the system current](#) on page 115.

For more information on using these installation methods, see the [Hewlett Packard Enterprise website](#).

Installing the operating system with Intelligent Provisioning

Procedure

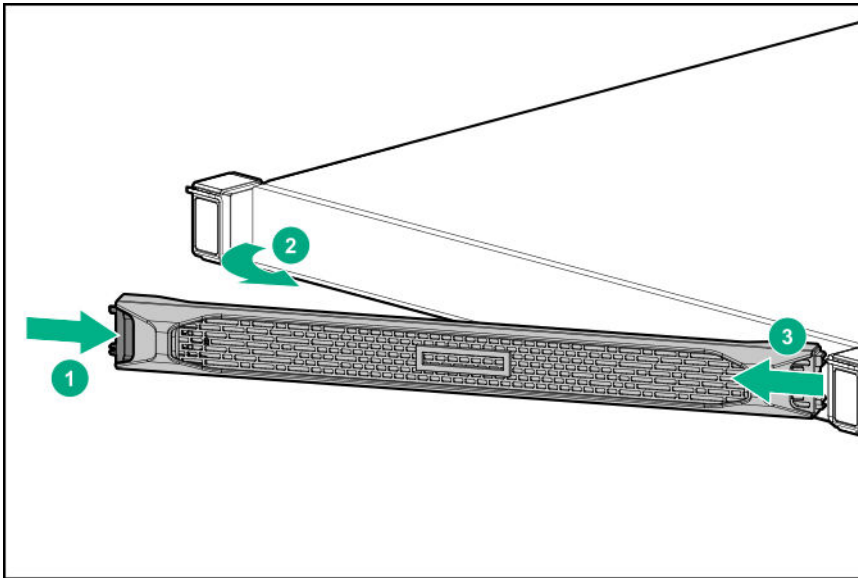
1. Connect the Ethernet cable between the network connector on the server and a network jack.
2. Press the Power On/Standby button.
3. During server POST, press **F10**.
4. Complete the initial Preferences and Registration portion of [Intelligent Provisioning](#).
5. At the 1 Start screen, click **Configure and Install**.
6. To finish the installation, follow the onscreen prompts. An Internet connection is required to update the firmware and systems software.

Operations

Removing the security bezel (optional)

Procedure

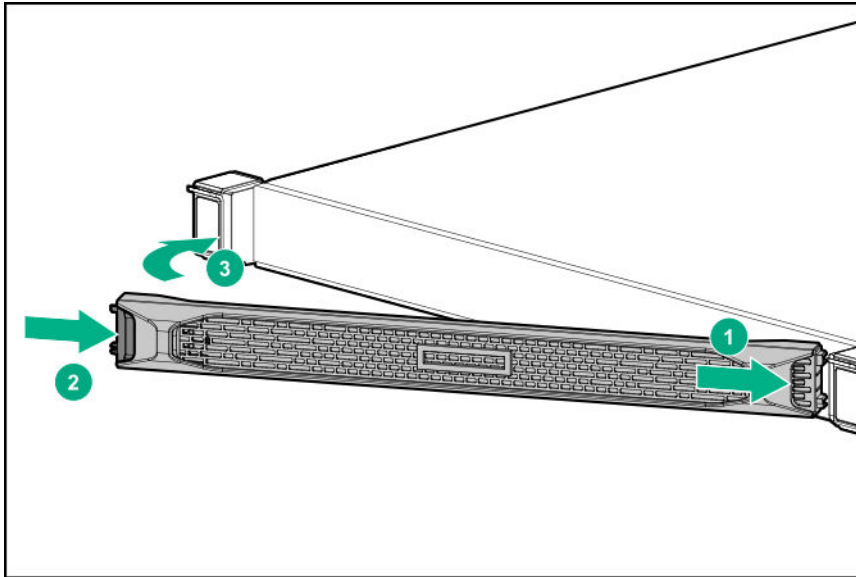
1. Press the latch.
2. Open the security bezel.
3. Detach the security bezel from the chassis ear.



Installing the security bezel (optional)

Procedure

1. Attach the security bezel to the latch ear.
2. Press the latch.
3. Close the security bezel.



4. Install the Kensington security lock.

For more information about the Kensington security lock, see the document with the component.

Powering down the server

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

⚠ **IMPORTANT:** When the server is in standby mode, auxiliary power is still being provided to the system.

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

- Press and release the Power On/Standby button.
This method initiates a controlled shutdown of applications and the OS before the server enters standby mode.
- Press and hold the Power On/Standby button for more than 4 seconds to force the server to enter standby mode.
This method forces the server to enter standby mode without properly exiting applications and the OS. If an application stops responding, you can use this method to force a shutdown.
- Use a virtual power button selection through iLO 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.

Powering up the server

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

Extending the server from the rack

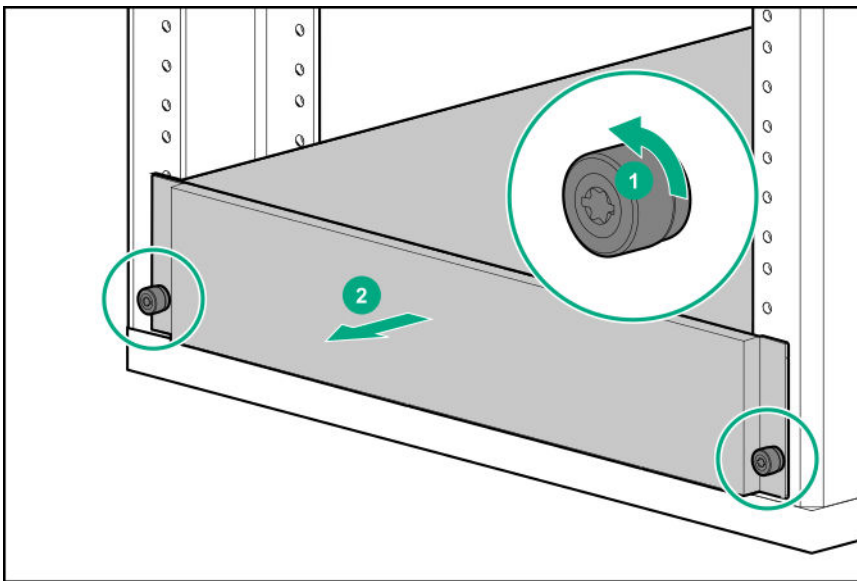
⚠ WARNING: To reduce the risk of personal injury or equipment damage, be sure that the rack is adequately stabilized before extending a component from the rack.

Prerequisites

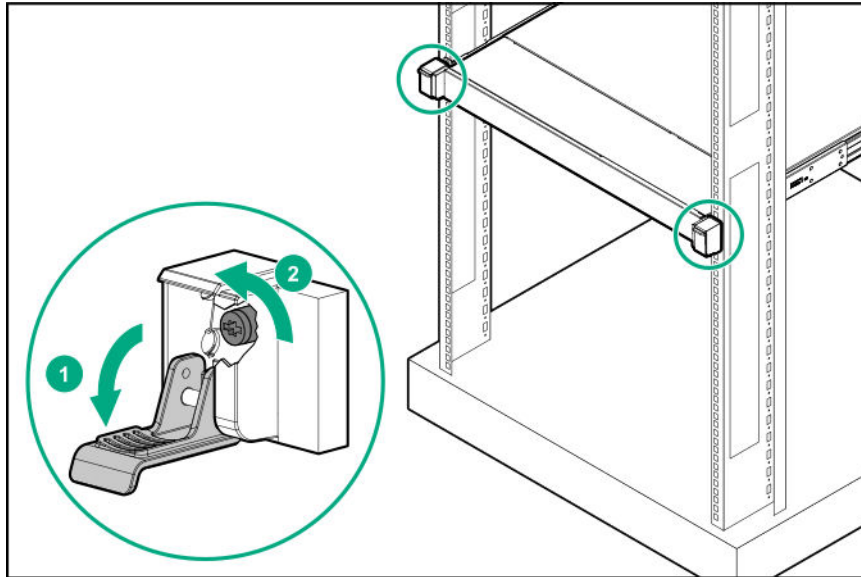
Before you perform this procedure, make sure that you have T-25 screwdriver available.

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Disconnect all peripheral cables from the server.
5. Do one of the following:
 - For server with thumbscrew ears:
 - a. Loosen the captive thumbscrews that secure the server to the rack.
 - b. Slide the server out of the rack.



- For server with quick-release latch ears:
 - a. Open the latches on both sides of the server.
 - b. If necessary, use a T-25 Torx screwdriver to loosen the shipping screws.



c. Slide the server out of the rack.

6. Extend the server on the rack rails until the server rail-release latches are engaged.

Removing the server from the rack



WARNING: This server is heavy. To reduce the risk of personal injury or damage to the equipment:

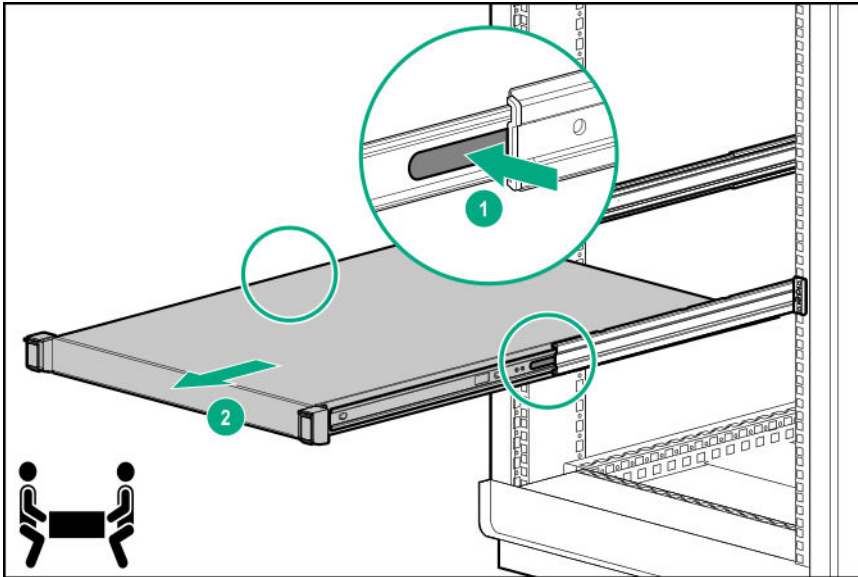
- Observe local occupational health and safety requirements and guidelines for manual material handling.
- Get help to lift and stabilize the product during installation or removal, especially when the product is not fastened to the rails.

Hewlett Packard Enterprise recommends that a minimum of two people are required for all rack server installations. If the server is installed higher than chest level, a third person may be required to help align the server.

- Use caution when installing the server in or removing the server from the rack. The server is unstable when not fastened to the rails.

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Disconnect all peripheral cables from the server.
5. **Extend the server from the rack.**
6. Press and hold both the safety release latches and remove the server from the rack.



7. Place the server on a sturdy, level surface.

Removing the access panel

-
- ⚠ 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, take the appropriate anti-static precautions before beginning any installation, removal, or replacement procedure. Improper grounding can cause electrostatic discharge.
-
- ⚠ CAUTION:** Do not operate the server for long periods with the access panel open or removed. Operating the server in this manner results in improper airflow and improper cooling that can lead to thermal damage.
-

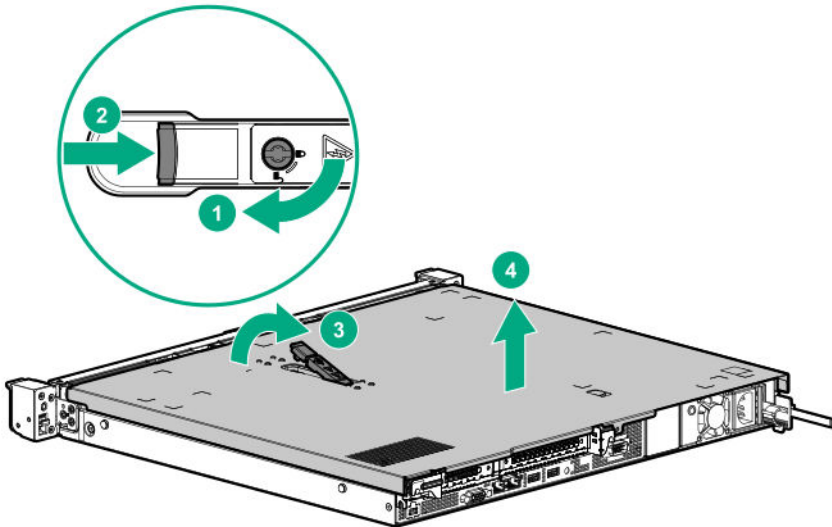
Prerequisites

Before you perform this procedure, make sure that you have a T-15 Torx screwdriver available.

Procedure

1. If installed, **remove the security bezel**.
2. **Power down the server**.
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:

- **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. Remove the access panel:
- a. If the locking latch is locked, use a T-15 Torx screwdriver to unlock the latch.
 - b. Press the release button and pull up the latch to disengage the access panel from the chassis.
 - c. Lift up the rear side of the access panel to remove the panel from the chassis.



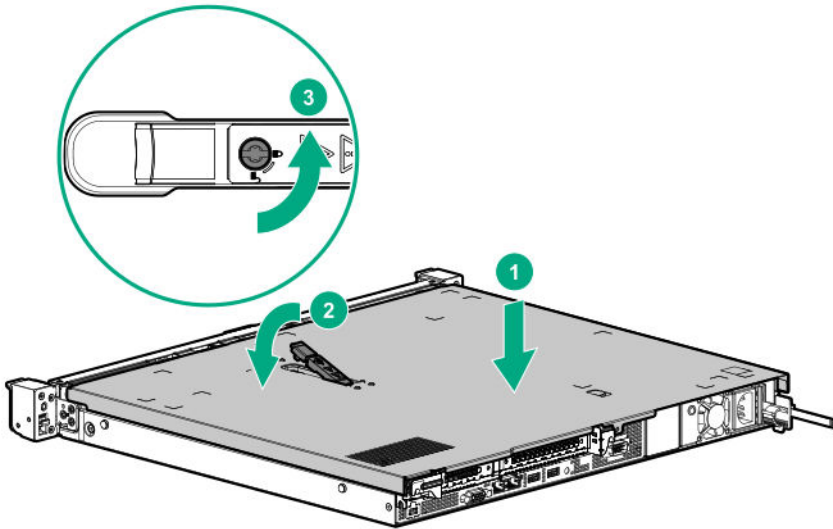
Installing the access panel

Prerequisites

Before you perform this procedure, make sure that you have a T-15 Torx screwdriver available.

Procedure

1. Place the access panel on top of the server with the latch open.
2. Insert the guide pin on the chassis through the hole on the access panel latch.
3. Press down the access panel latch.
The access panel slides to a closed position.
4. Tighten the access panel latch screw with a T-15 screwdriver and lock the access panel latch.

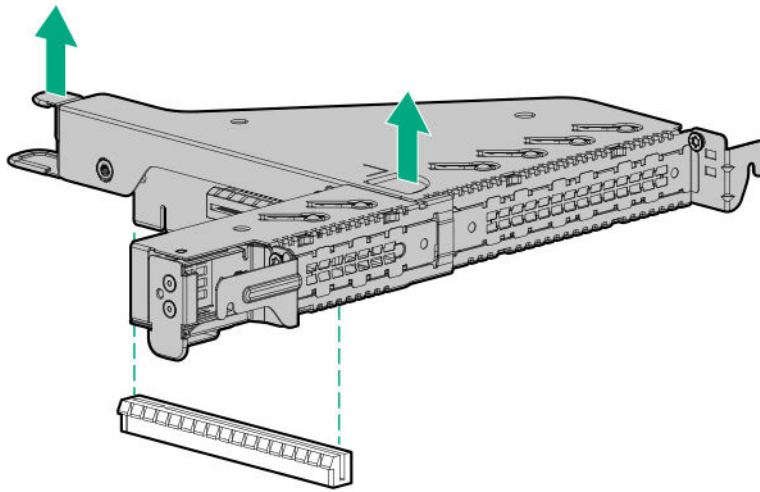


Removing the riser cage

-
- ⚠ 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 the server or expansion boards, power down the server, and disconnect all power cords before removing or installing the riser cage.
-

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. Disconnect all cables connected to existing expansion boards.
7. Remove the riser cage.

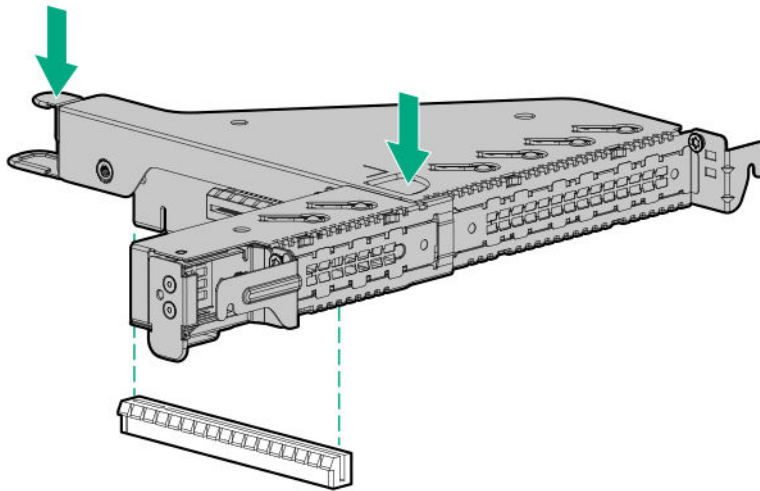


Installing the riser cage

⚠ CAUTION: To prevent damage to the server or expansion boards, power down the server, and disconnect all power cords before removing or installing the riser cage.

Procedure

1. Connect all necessary internal cabling to the expansion board.
2. Align the riser cage with the system board connector, then press down the riser cage.



3. Install the access panel.
4. Install the server into the rack.
5. Connect all peripheral cables to the server.
6. Power up the server.

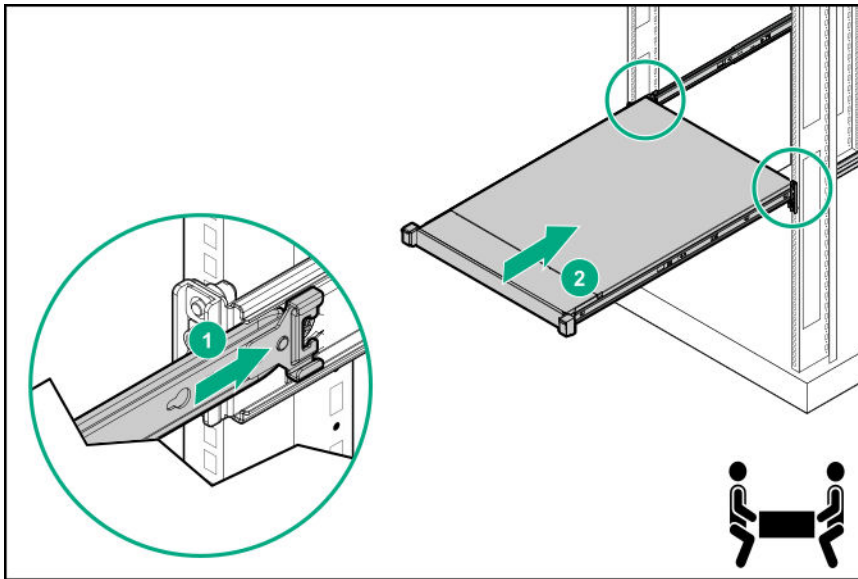
Installing the server into the rack

Prerequisites

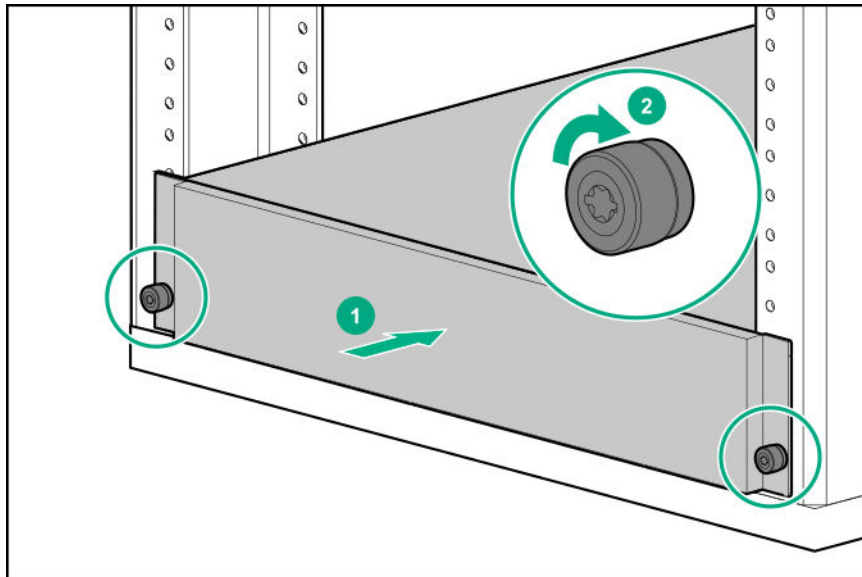
Before you perform this procedure, make sure you have the T-25 Torx screwdriver available.

Procedure

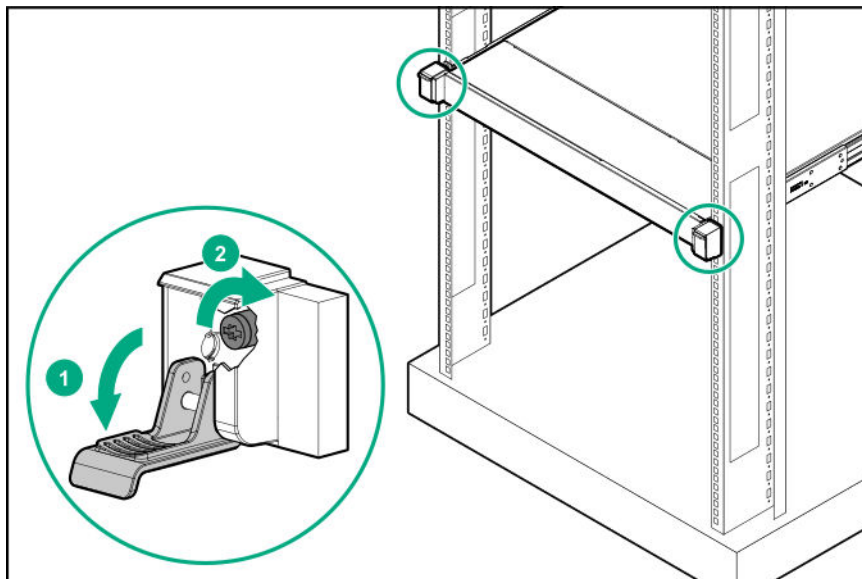
1. **Install the rack rail option.**
2. Do the following:
 - a. Align the mounting rail of the server with the rack rail.
 - b. Slide the server into the rack till the server ears engage with the rack column.



3. Do one of the following:
 - For server with thumbscrew ears, tighten the captive thumbscrews.



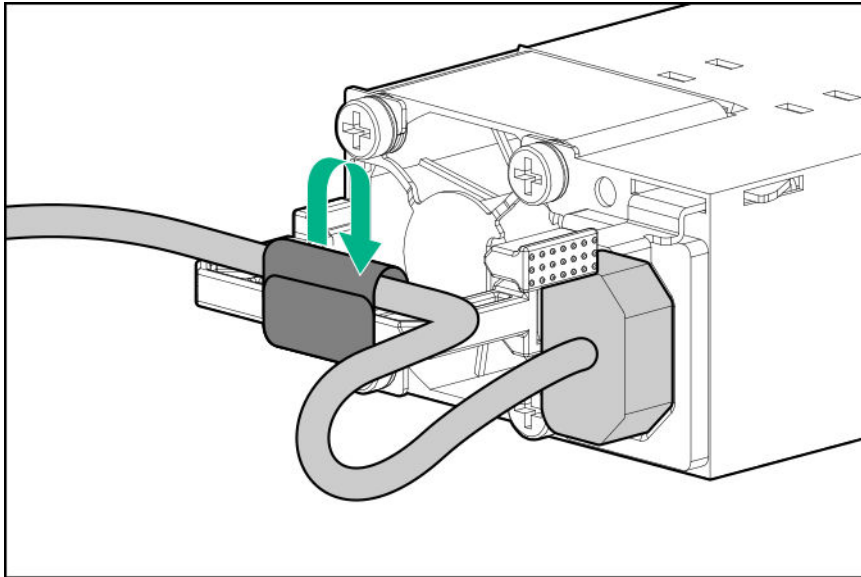
- For server with latch ears, if necessary, open the latches and tighten the screws.



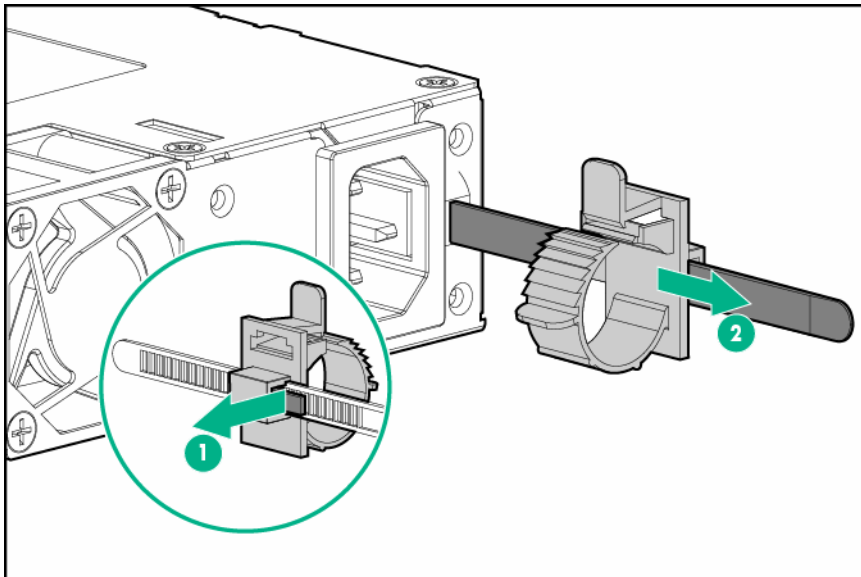
4. Connect peripheral devices to the server.
For information on identifying connectors, see **Rear panel components** on page 11.
5. Connect the power cord to the power supply.
6. **For hot-plug power supply:** To prevent accidental power cord disconnection when sliding the server in and out of the rack, secure the power cord in the strain relief strap attached to the power input module handle:
 - a. Unwrap the strain relief strap from the power input module handle.

⚠ CAUTION: Avoid tight bend radii to prevent damaging the internal wires of a power cord or a server cable. Never bend power cords and server cables tight enough to cause a crease in the sheathing.

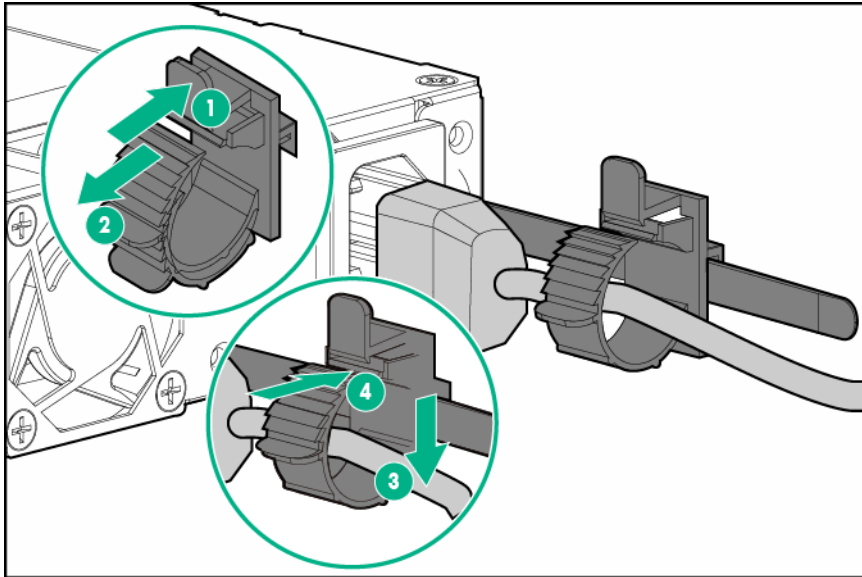
 - b. Secure the power cord with the strain relief strap.



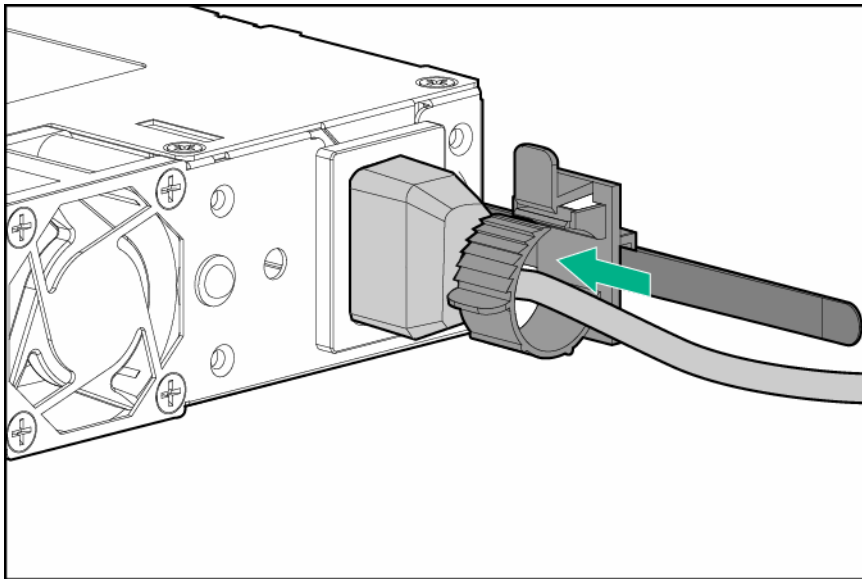
7. **For non-hot-plug power supply:** To prevent the accidental disconnection of the power cord when sliding the server into and from the rack, secure the power cord through the strain relief clip:
 - a. If the clip is positioned too near the power cord that it blocks the power cord plug connection, pull the release tab and then slide the clip backward.



- b. Connect the power cord to the server.
 - c. Press the top part of the clip, then pull the clip open.
 - d. Position the power cord inside the clip, and then close the clip.



- e. Slide the clip forward until it is flush against the edge of the power cord plug.



8. To secure the power cords and other rear panel cables to the rack rail, use the hook-and-loop strap. For detailed instructions, see **Installing the rack rail hook-and-loop strap** on page 48.
9. Connect the power cord to the power source.
10. **Power up the server.**

Hardware options installation

This chapter provides detailed instructions on how to install hardware options.

For more information on supported options, see the product QuickSpecs on the HPE ProLiant DL20 Gen10 Server website at:


<http://www.hpe.com/servers/dl20-gen10>


To view the warranty for your server and supported options, see [Warranty information](#) on page 128.

Introduction

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

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

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

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

Rack rail option

Installing the rack rail option

These rack rails can be installed in round-, square-, or threaded-hole racks.

Prerequisites

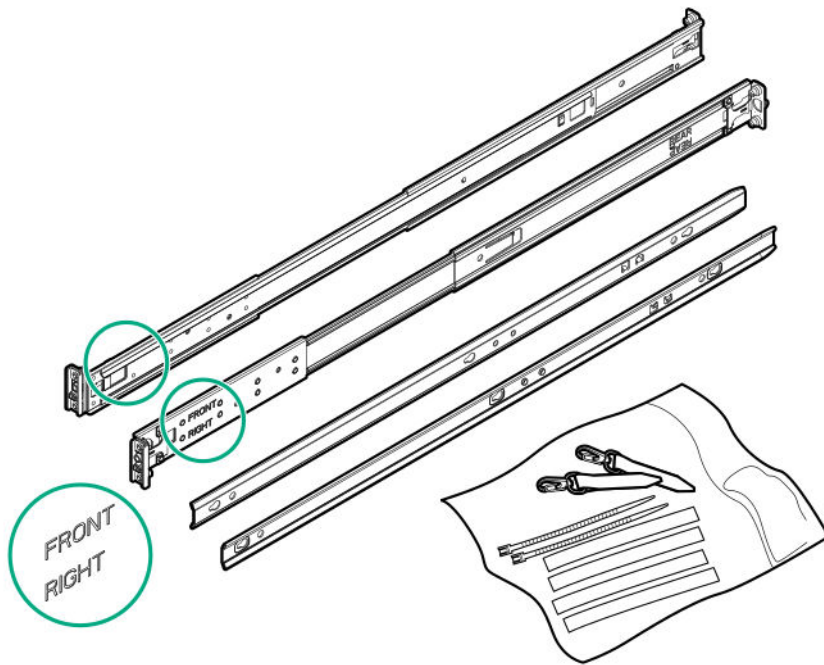
Before you perform this procedure, make sure you have the following items available:

- Left and right rack rail assemblies
- Server tray

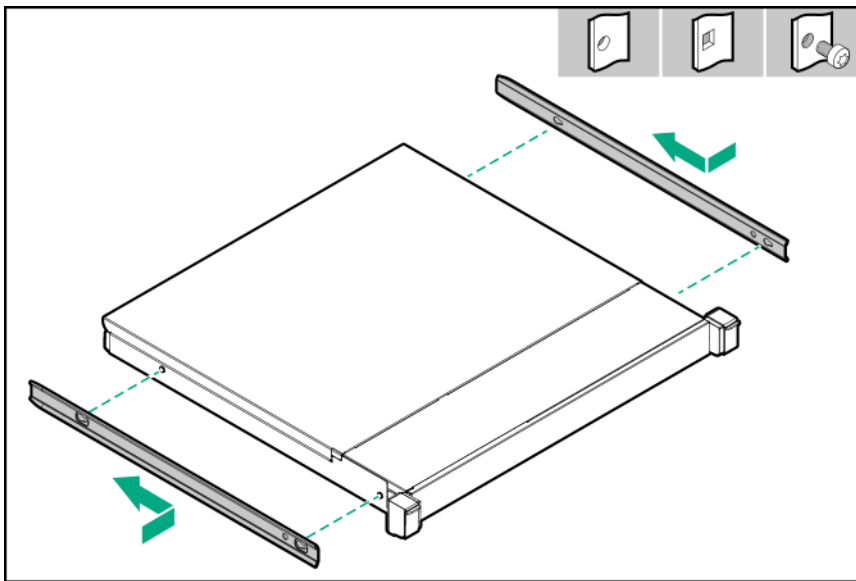
Procedure

1. Locate the orientation markers on the mounting rails.

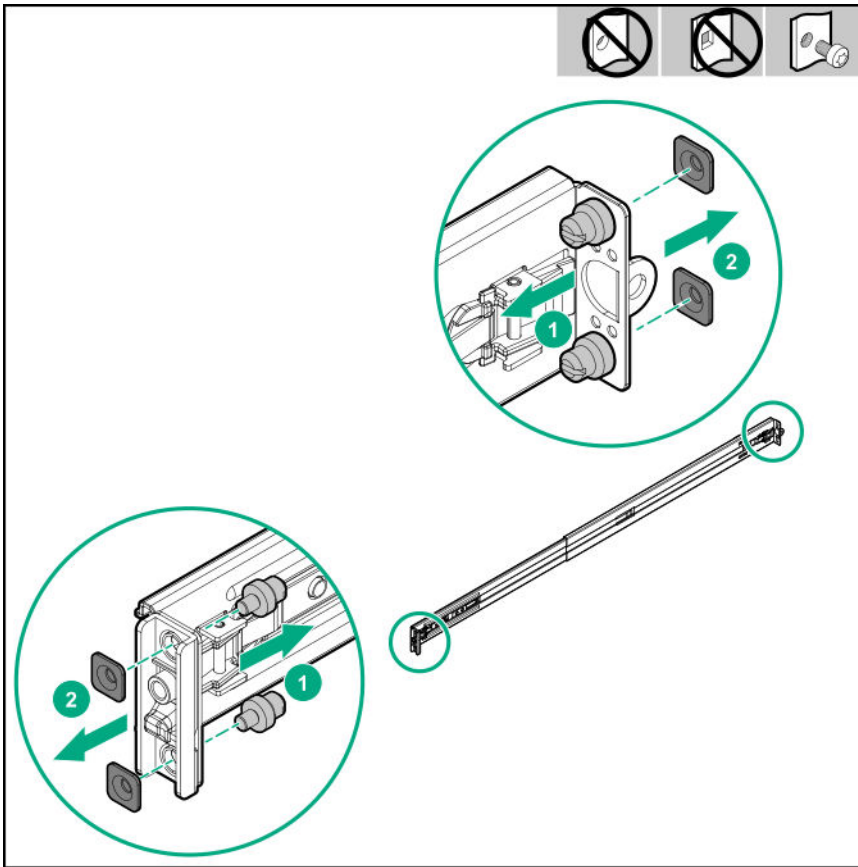
The front ends of the rails are marked 'Front left' and 'Front right'.



2. Install the sliding rails on the server tray.

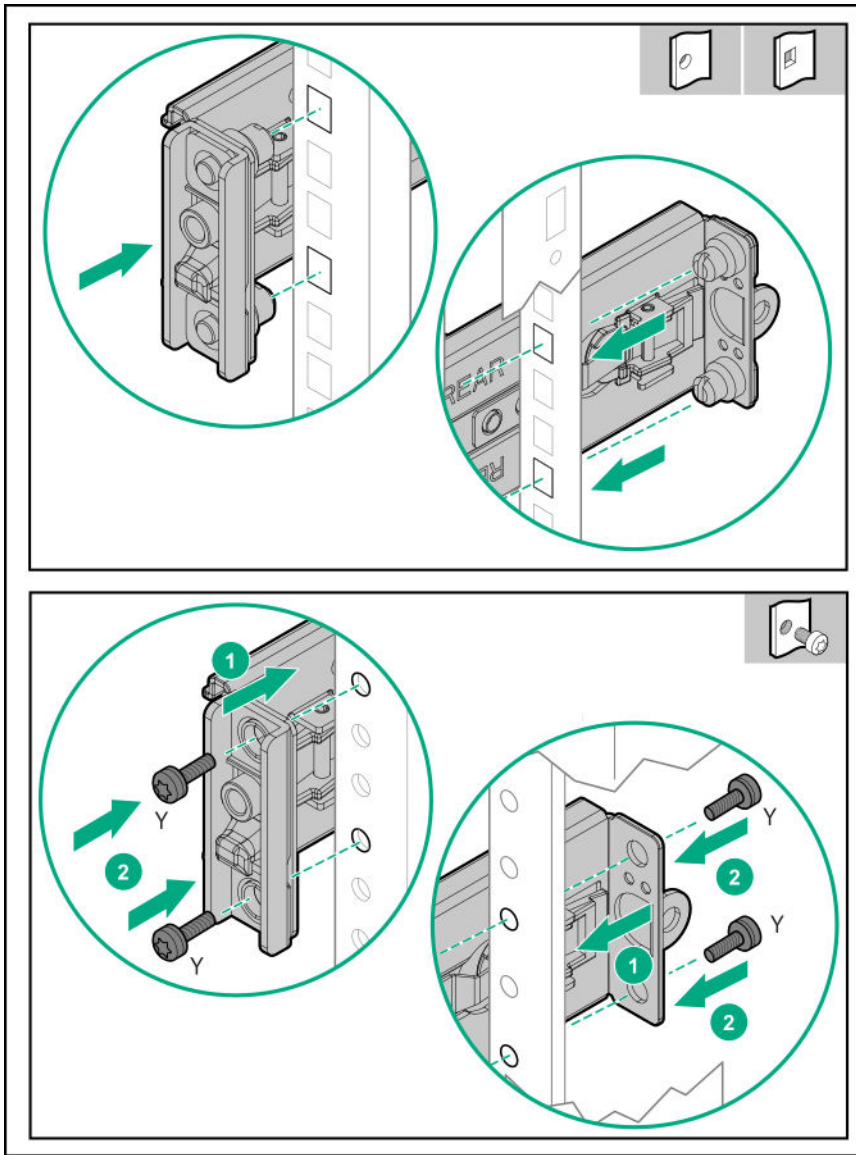


3. Remove the pins and also the pin nuts from the ends of the right and left rails.



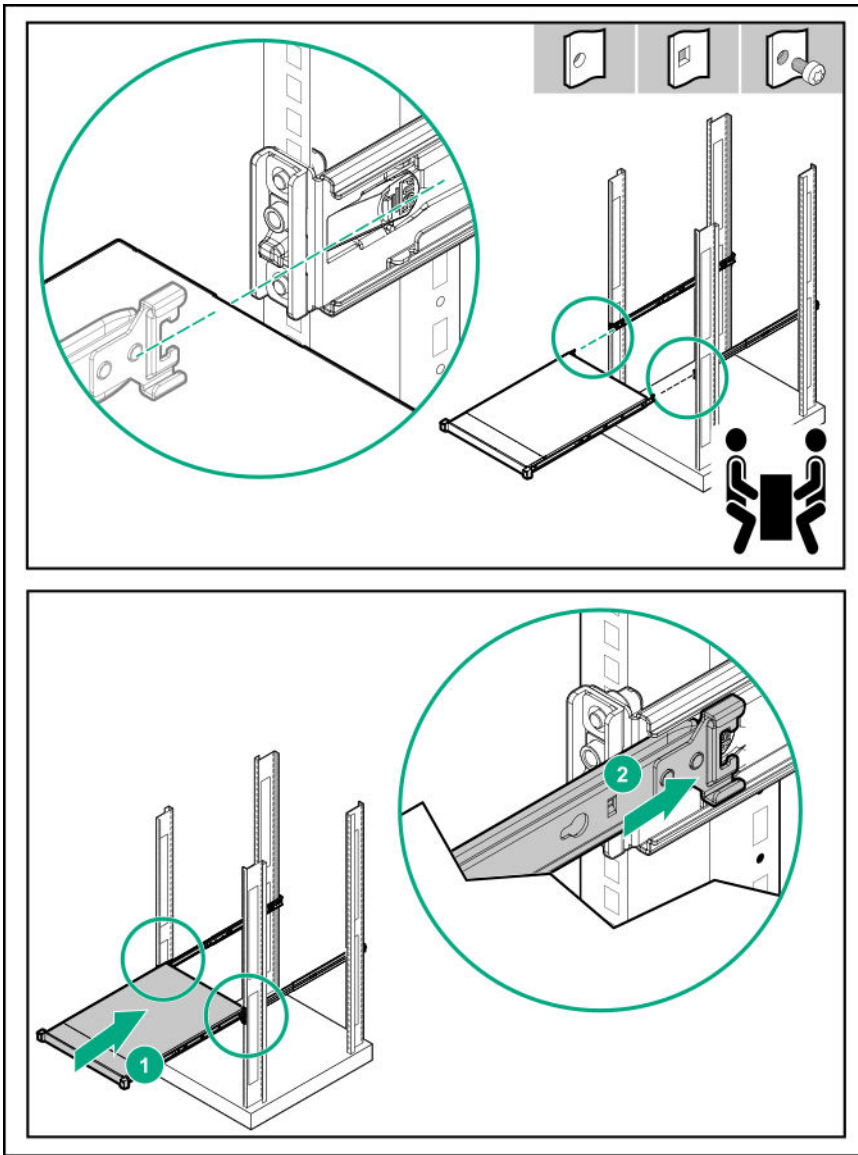
4. Fasten the mounting rails to the rack columns:

- For square hole racks: align the rail pins with the holes of the rack column and insert the pins.
- For round hole racks: align the rail pins with the holes of the rack column and mount the rails by fastening the screws.



5. Slide the server tray into the rack.

The rails will click and lock into place when the tray is properly engaged.

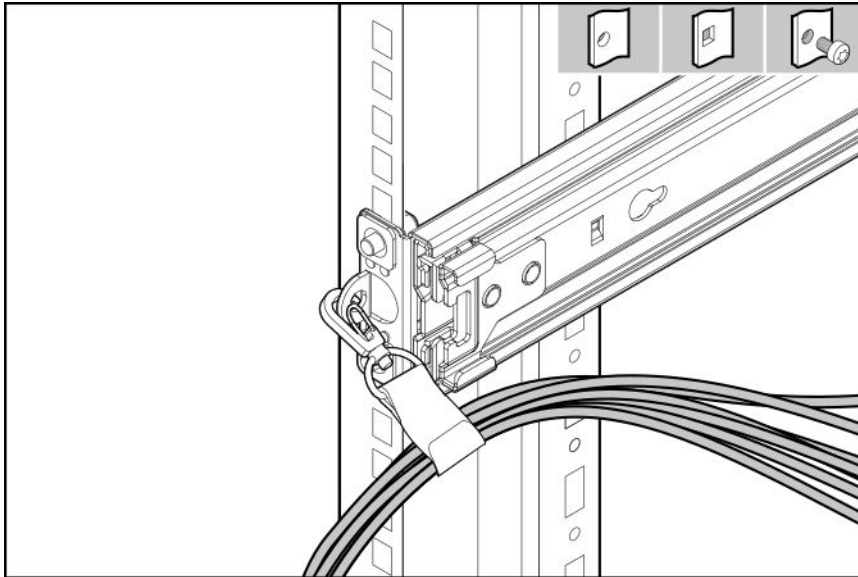


Installing the rack rail hook-and-loop strap

The rack rail hook-and-loop strap can be installed on either the left or right rack rail. Hewlett Packard Enterprise recommends installing it on the left rack rail for better cable management.

To install the rack rail hook-and-loop strap:

1. **Install the server into the rack.**
2. Install the rack rail hook-and-loop strap:
 - a. Lock the strap clip on the rack rail.
 - b. Hold the rear panel cables and then wrap the strap around the cables.



Drive options

Drive installation guidelines

Observe the following general guidelines:

- The system automatically sets all drive numbers.
- If only one drive is used, install it in the bay with the lowest drive number.
For drive numbering, see **Drive bay numbering** on page 20.
- Drives with the same capacity provide the greatest storage space efficiency when grouped into the same drive array.

Drive support information

Depending on the drive cage installed, the server supports the following drives:

- Non-hot plug LFF drives
- Hot-plug LFF drives
- Hot-plug SFF drives

The server supports up to six drives in SFF configuration and two drives in LFF configuration.

Installing an LFF non-hot-plug drive

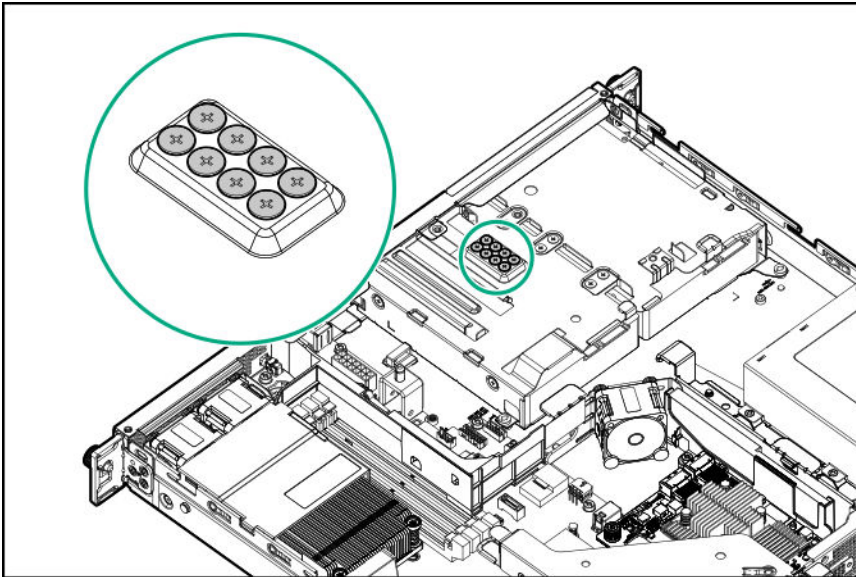
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

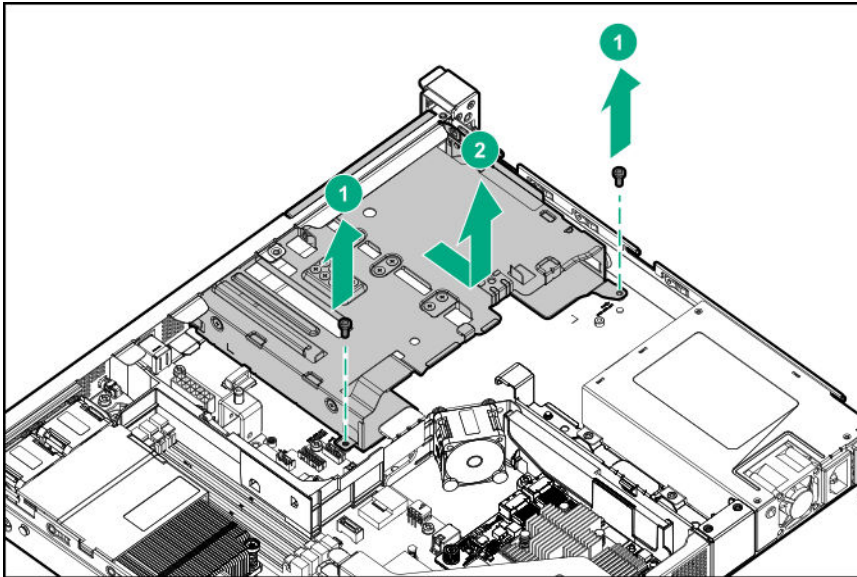
- T-15 Torx screwdriver
- Phillips screwdriver

Procedure

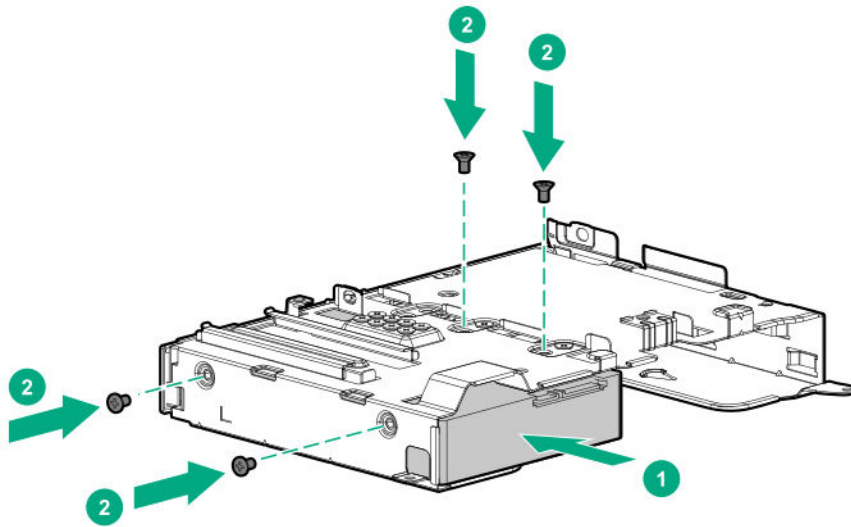
1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. Disconnect all existing drive cage cables.
7. Remove four Phillips screws from the drive cage.



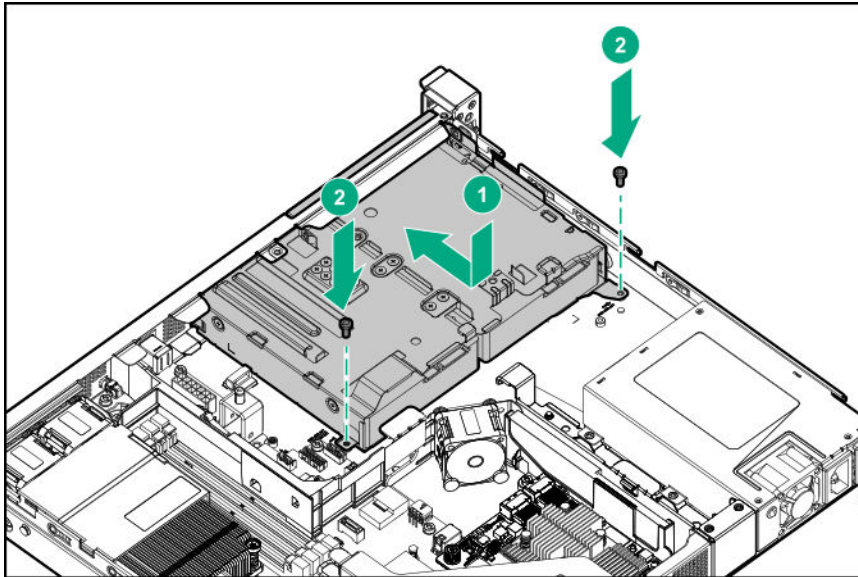
8. Remove the non-hot-plug drive cage.



9. Install the drive.



10. Install the non-hot-plug drive cage assembly.



11. **Connect all drive cables.**
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.**
17. If removed, **install the security bezel.**

The installation is complete.

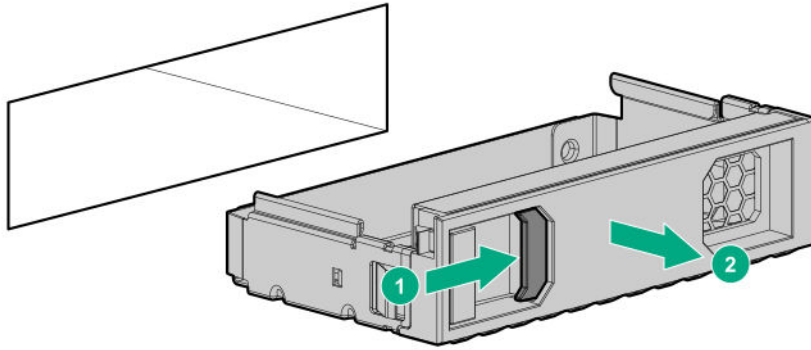
To configure arrays, see the *HPE Smart Array SR Gen10 Configuration Guide* at the **Hewlett Packard Enterprise website**.

Installing an LFF hot-plug drive

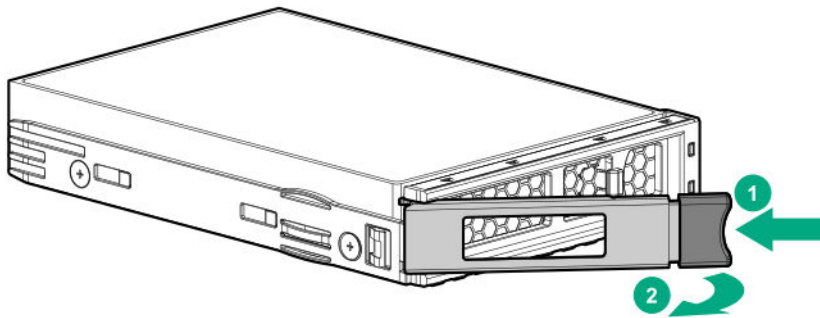
⚠ CAUTION: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

Procedure

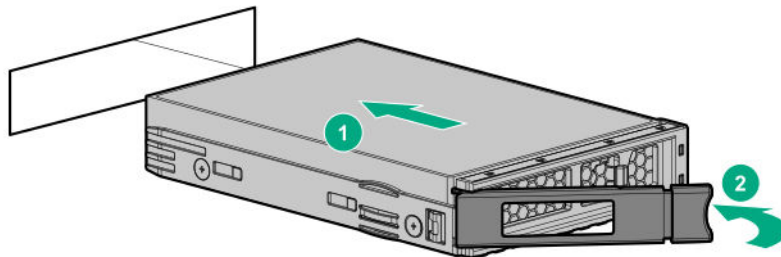
1. If installed, **remove the security bezel.**
2. Remove the drive blank.



3. Prepare the drive.



4. Install the drive.



5. **Determine the status of the drive from the drive LED definitions.**

The installation is complete.

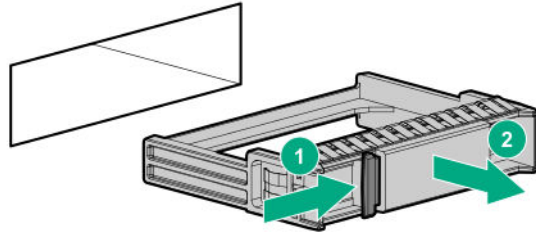
To configure arrays, see the *HPE Smart Array SR Gen10 Configuration Guide* at the [Hewlett Packard Enterprise website](#).

Installing an SFF hot-plug drive

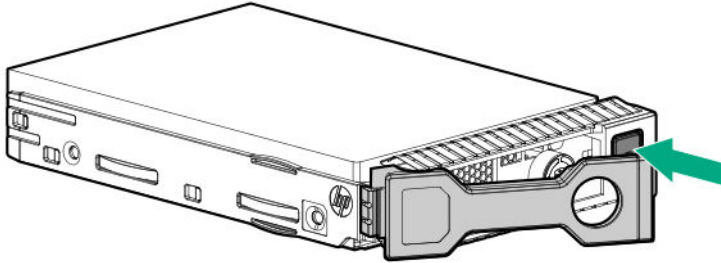
⚠ CAUTION: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

Procedure

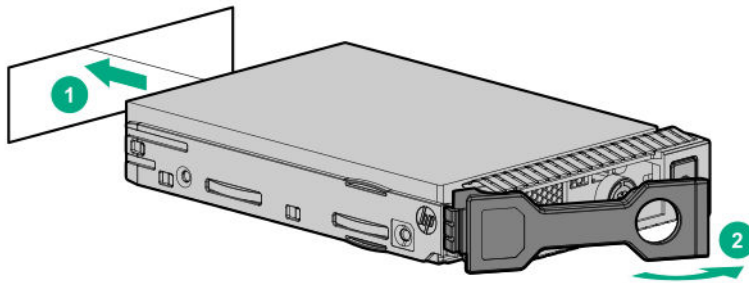
1. If installed, **remove the security bezel**.
2. Remove the drive blank.



3. Prepare the drive.



4. Install the SFF drive.



5. Determine the status of the drive from the drive LED definitions.

The installation is complete.

To configure arrays, see the *HPE Smart Array SR Gen10 Configuration Guide* at the [Hewlett Packard Enterprise website](http://www.hpe.com/enterprise).

Power supply options

Depending on the installed options and the regional location where the server was purchased, the server can be configured with one of the following **power supplies**.

Hot-plug power supply calculations

For more information on the hot-plug power supply and calculators to determine server power consumption in various system configurations, see the Hewlett Packard Enterprise Power Advisor website (<http://www.hpe.com/info/poweradvisor/online>).

Power supply warnings and cautions



WARNING: To reduce the risk of electric shock or damage to the equipment:

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
 - Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
 - Unplug the power cord from the power supply to disconnect power to the equipment.
 - Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.
-



WARNING: To reduce the risk of injury from electric shock hazards, do not open power supplies. Refer all maintenance, upgrades, and servicing to qualified personnel



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.



CAUTION: Mixing different types of power supplies in the same server might:

- Limit or disable some power supply features including support for power redundancy.
- Cause the system to become unstable and might shut down.

To ensure access to all available features, all power supplies in the same server should have the same output and efficiency ratings. Verify that all power supplies have the same part number and label color.

Installing a hot-plug power supply in redundant power supply bay



WARNING: To reduce the risk of personal injury from hot surfaces, allow the power supply or power supply blank to cool before touching it.

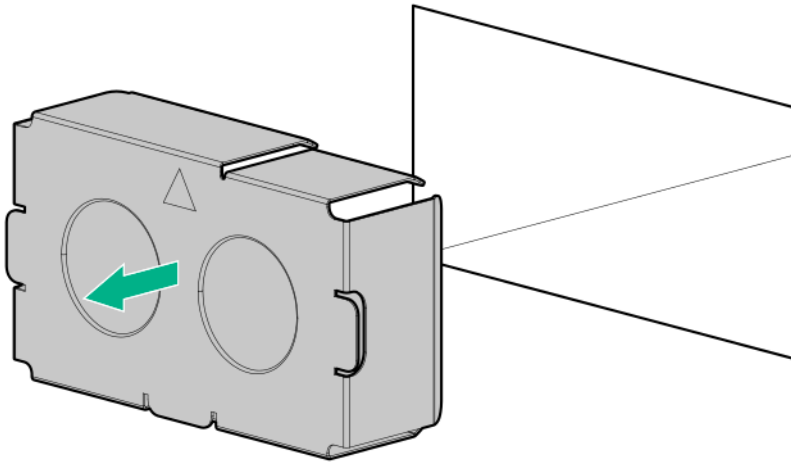


CAUTION: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

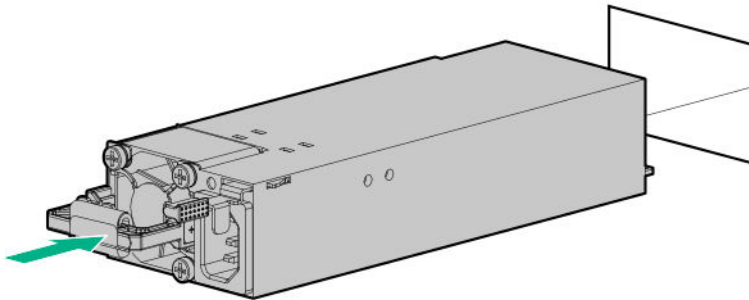
NOTE: Reboot the server if a second redundant power supply is installed in addition to the first redundant power supply.

Procedure

1. If you are installing a power supply in the power supply bay 2, remove the power supply blank.



2. Slide the power supply into the bay until it clicks into place.



3. Connect the power cord to the power supply.
4. **Secure the power cord in the strain relief strap attached to the power supply handle.**
5. Connect the power cord to the power source.
6. Make sure that the power supply LED is green.
7. Reboot the server.

The installation is complete.

Optical drive enablement option

The optical drive option can be installed for both LFF and SFF hot-plug configurations. For two-bay LFF configuration server, install the optical drive directly in the **optical drive bay**.

Installing the optical drive option for LFF configuration

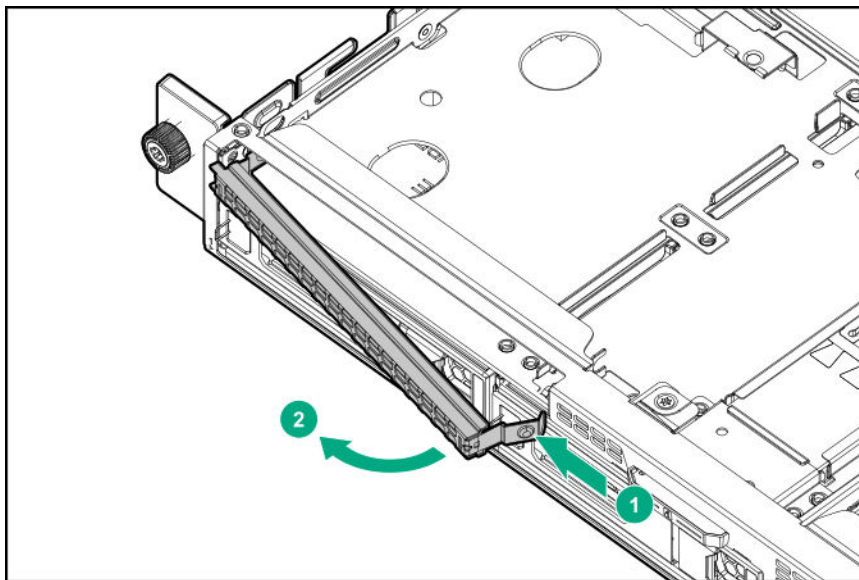
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

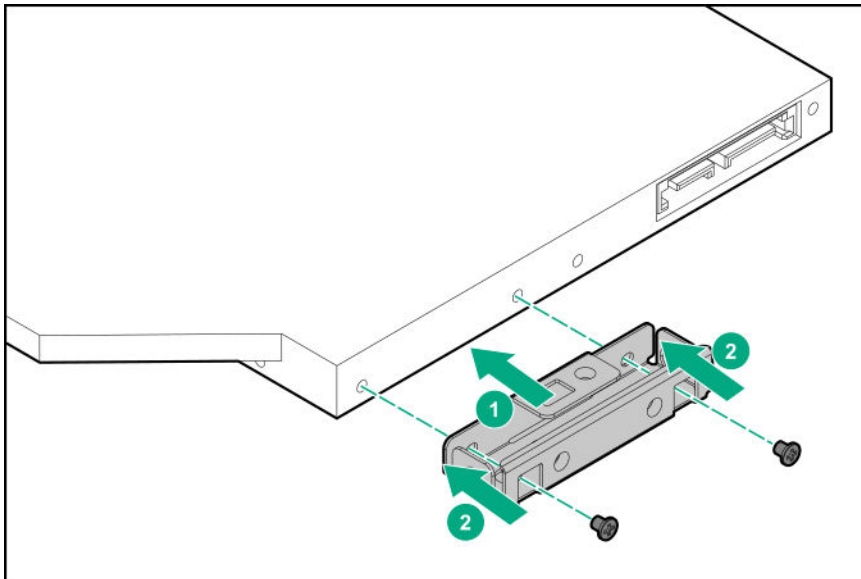
- Optical drive enablement kit
- T-10 Torx screwdriver
- Phillips screwdriver

Procedure

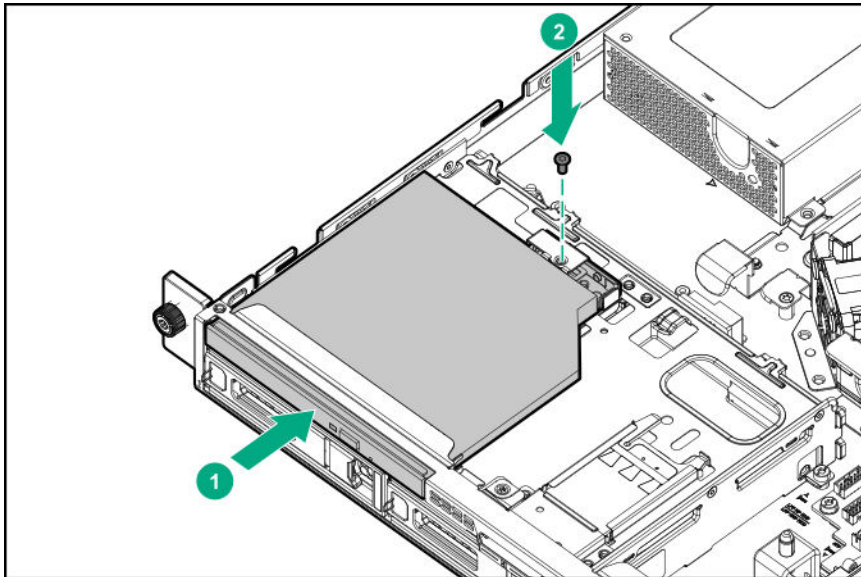
1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. Remove the optical drive bay blank.



7. Install the optical drive bracket.



8. Install the optical drive cage assembly in the server.



9. **Connect the SATA-power Y-cable.**
10. **Install the access panel.**
11. **Install the server into the rack.**
12. Connect each power cord to the server.
13. Connect each power cord to the power source.
14. **Power up the server.**
15. If removed, **install the security bezel.**

The installation is complete.

Installing the optical drive enablement option for SFF configuration

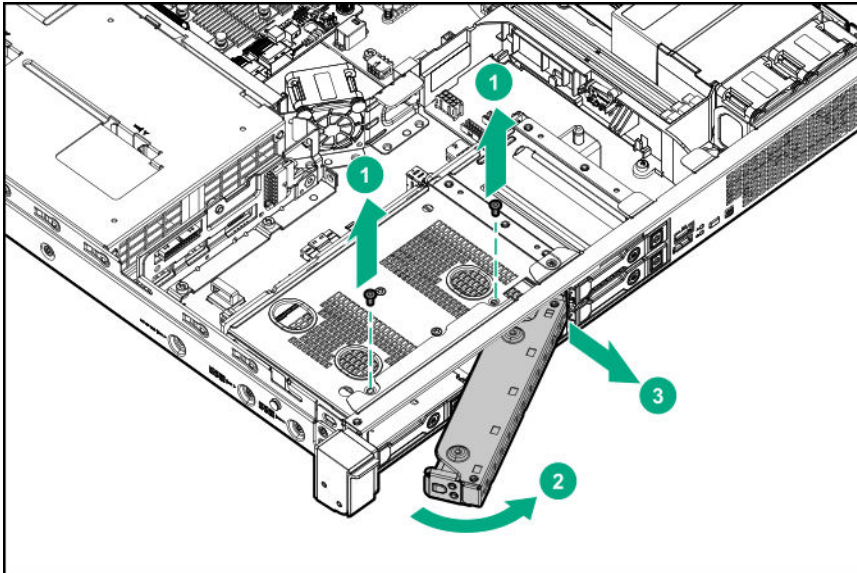
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

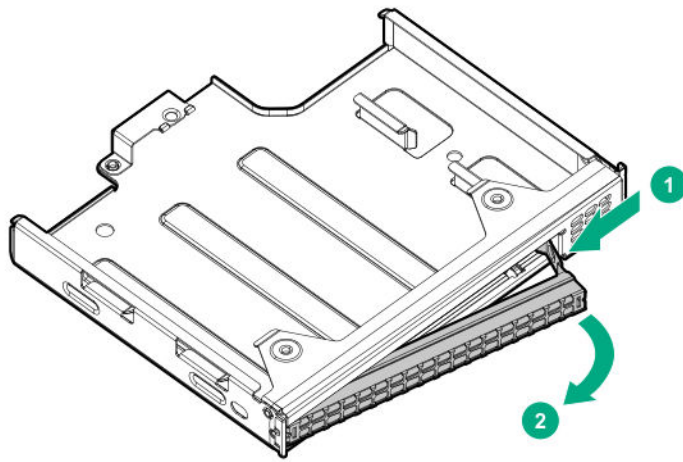
- Optical drive enablement kit
- T-10 Torx screwdriver
- Phillips screwdriver

Procedure

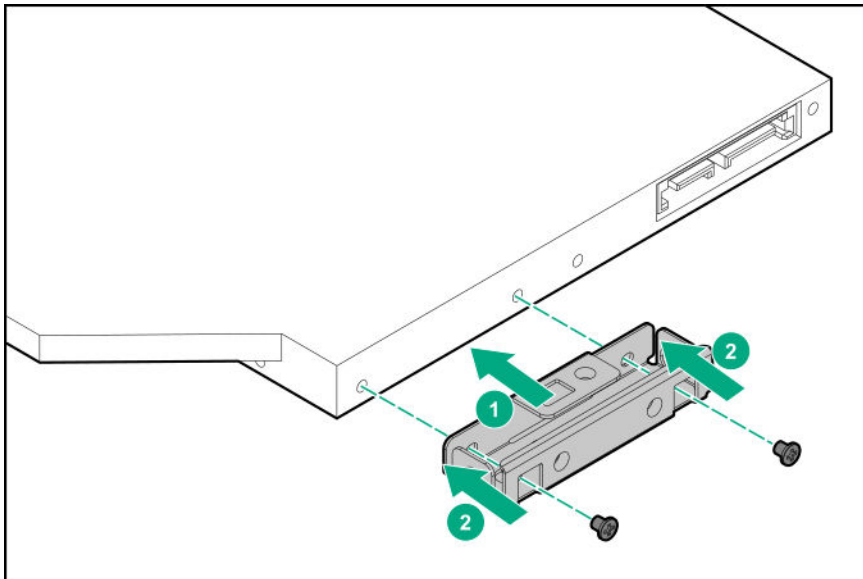
1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. Remove the media bay blank.
Retain the screws for installing the optical drive cage.



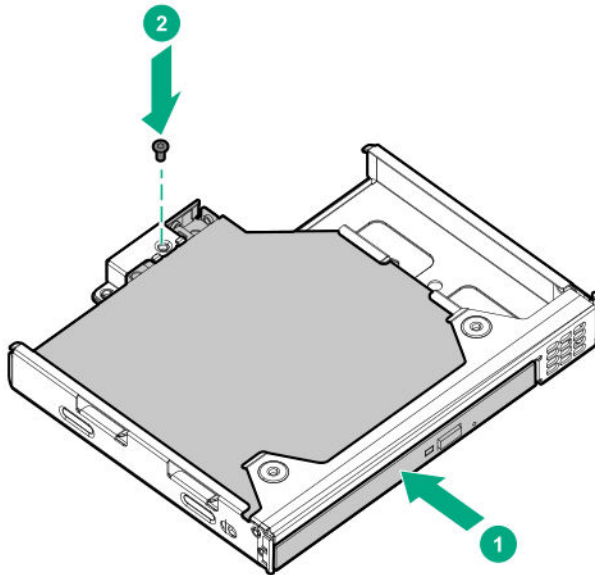
7. Remove the optical drive cage blank.



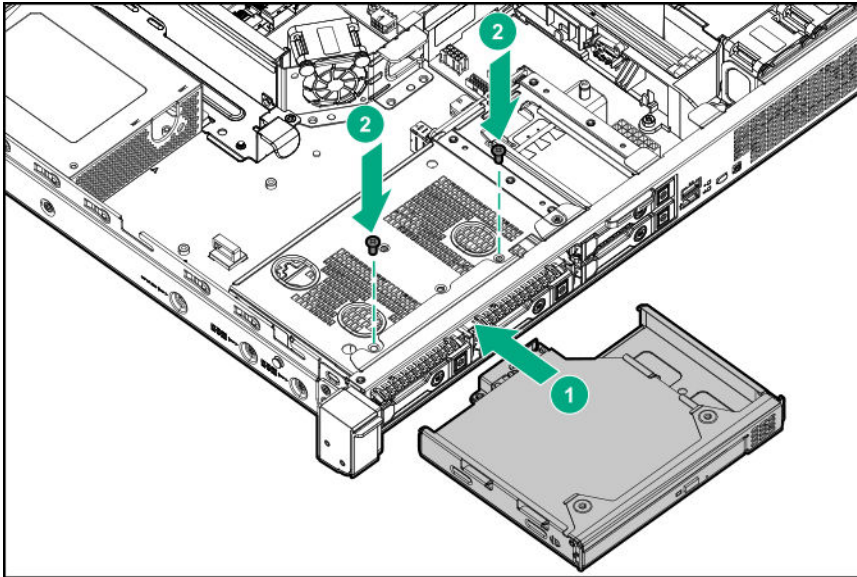
8. Install the optical drive bracket.



9. Install the optical drive in the optical drive cage.



10. Install the optical drive cage assembly in the server:



11. **Connect the SATA-power Y-cable.**
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.**
17. If removed, **install the security bezel.**

The installation is complete.

Two-bay SFF hot-plug drive enablement option

The server supports 4+2 SFF drive configuration.

Installing the two-bay SFF hot-plug drive enablement drive cage

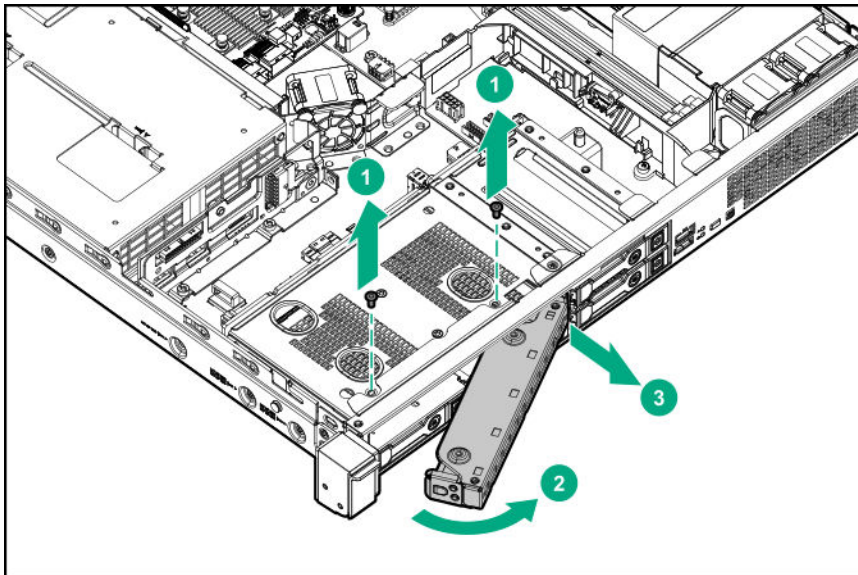
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

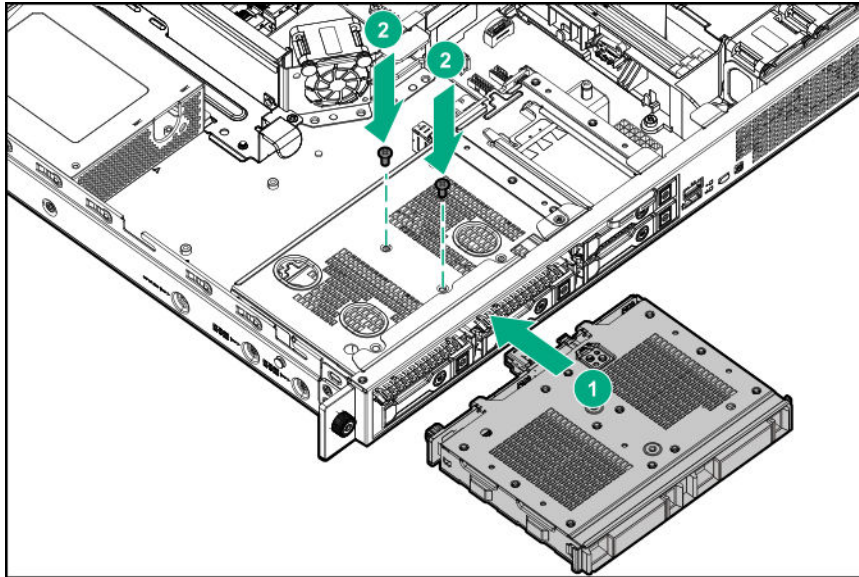
- Two-bay SFF drive enablement kit
- Two SFF drives
- T-10 screwdriver

Procedure

1. If installed, **remove the security bezel**.
2. **Power down the server**.
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack**.
 - **Remove the server from the rack**.
5. **Remove the access panel**.
6. Remove the media bay blank.
Retain the screws for installing the option.



7. Install the SFF drive cage.



8. **Install the SFF drives.**
9. **Connect the cables.**
10. **Install the access panel.**
11. **Install the server into the rack.**
12. Connect each power cord to the server.
13. Connect each power cord to the power source.
14. **Power up the server.**
15. If removed, **install the security bezel.**

The installation is complete.

Memory options

- ⓘ **IMPORTANT:** This server does not support mixing RDIMMs and UDIMMs. Attempting to mix these two types causes 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/standard-population-rules>).

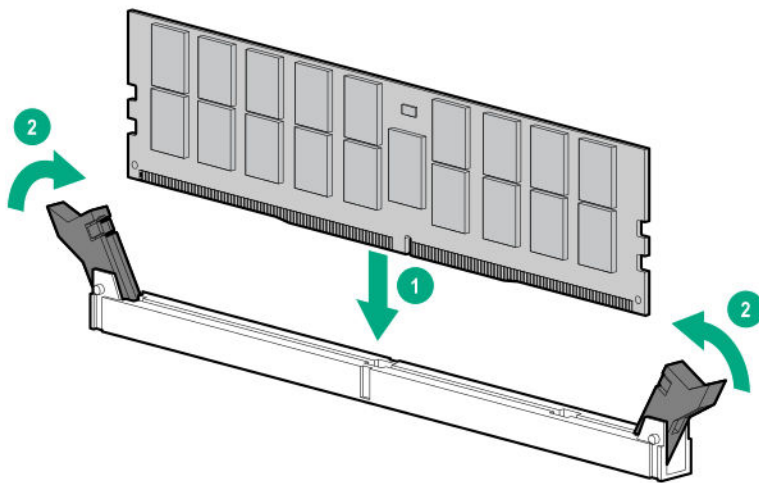
Installing a DIMM

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:

- a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
 5. **Remove the access panel.**
 6. Open the DIMM slot latches.
 7. Align the notch on the bottom edge of the DIMM with the keyed surface of the DIMM slot, and then fully press the DIMM into the slot until the latches snap back into place.

The DIMM slots are structured to ensure proper installation. If you try to insert a DIMM but it does not fit easily into the slot, you might have positioned it incorrectly. Reverse the orientation of the DIMM and insert it again.



8. **Install the access panel.**
9. **Install the server into the rack.**
10. Connect each power cord to the server.
11. Connect each power cord to the power source.
12. **Power up the server.**
13. If removed, **install the security bezel.**

The installation is complete.

After installing the DIMMs, use the **System Utilities > System Configuration > BIOS/Platform > Configuration (RBSU) > Memory Options** to configure the memory settings.

Expansion board options

For information on PCIe riser slot definitions, see **PCIe riser board slot definitions** on page 17.

Installing an expansion board

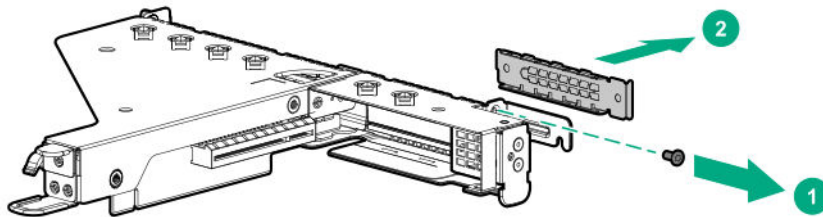
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

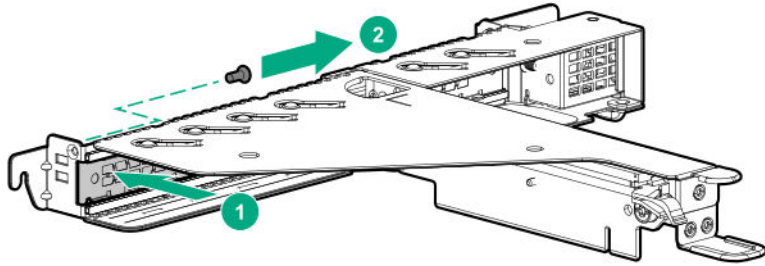
- Expansion board option kit
- External and internal cabling required by the expansion board
- T-10 Torx screwdriver

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. **Remove the PCIe riser cage.**
7. **Identify the expansion slot compatible with the option.**
8. Remove the blank from the PCIe riser cage slot.
 - Slot 1



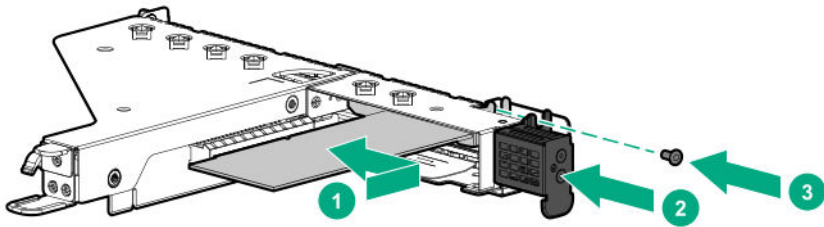
- Slot 2



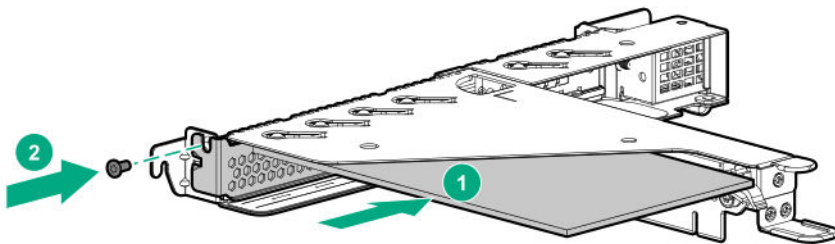
Retain the screw for future use.

9. Install the expansion board.

- Slot 1




- Slot 2



10. **Install the PCIe riser cage.**
11. Connect all necessary internal cabling to the expansion board.
For more information on the cabling requirements, see the documentation that ships with the option.
12. **Install the access panel.**
13. **Install the server into the rack.**
14. Connect all necessary external cabling to the expansion board.
For more information on the cabling requirements, see the documentation that ships with the option.
15. Connect each power cord to the server.
16. Connect each power cord to the power source.
17. **Power up the server.**
18. If removed, **install the security bezel.**

The installation is complete.

Installing the M.2 SATA SSD expansion board and M.2 SATA cables

 **IMPORTANT:** The M.2 SATA expansion board supports 2280 or 22110 M.2 SSDs only.

Prerequisites

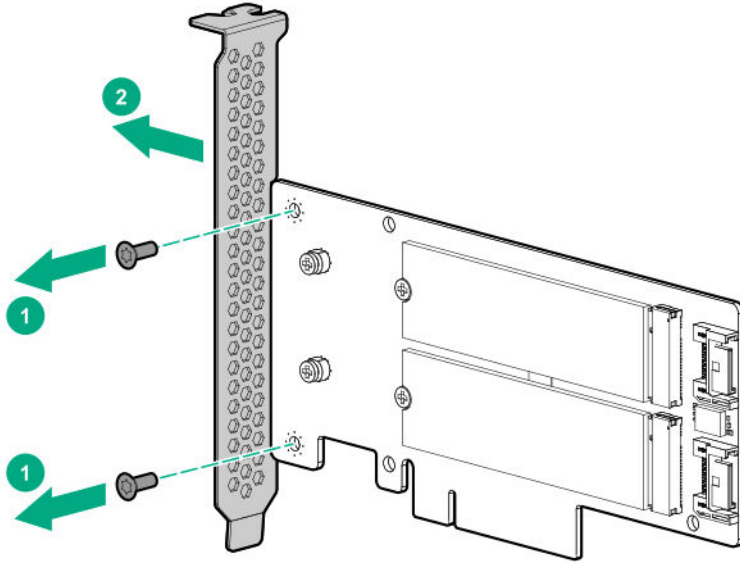
Before you perform this procedure, make sure that you have the following items available:

- M.2 SATA cable kit
- T-15 Torx screwdriver
- Phillip screwdriver

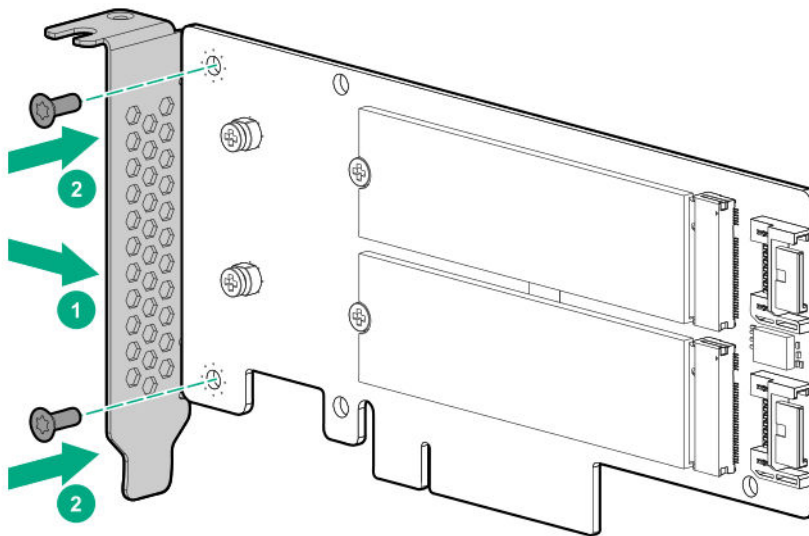
Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. **Remove the PCIe riser cage.**
7. **Identify the appropriate PCIe slot to install the M.2 SATA SSD expansion board.**

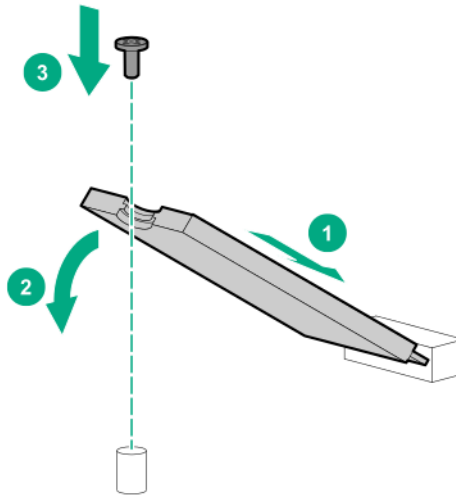
8. If installing the expansion board into slot 1 of the PCIe riser cage, do the following:
 - a. Remove the full-height bracket from the M.2 SATA SSD expansion board.



- b. Install the low-profile bracket onto the expansion board.



9. Install the M.2 SATA SSD module on the expansion board:
 - a. Insert the SSD into the SSD slot at a 45 degree angle.
 - b. Carefully press the SSD down to the horizontal position.
 - c. Install the SSD mounting screw.
 - d. Repeat the process if you are installing a second SSD module.



10. **Install the M.2 SATA SSD expansion board.**
11. **Install the PCIe riser cage.**
12. **Connect the M.2 SATA cables.**
13. **Install the access panel.**
14. **Install the server into the rack.**
15. Connect each power cord to the server.
16. Connect each power cord to the power source.
17. **Power up the server.**
18. If removed, **install the security bezel.**

The installation is complete.

Storage controller options

The server supports following controllers:

- **Type-a Smart Array modular controller (AROC)**
- **External type-P and type-E Smart Array SR Gen10 controllers**

Smart Array modular controller (AROC) option

Installing a Smart Array modular controller (AROC)

Prerequisites

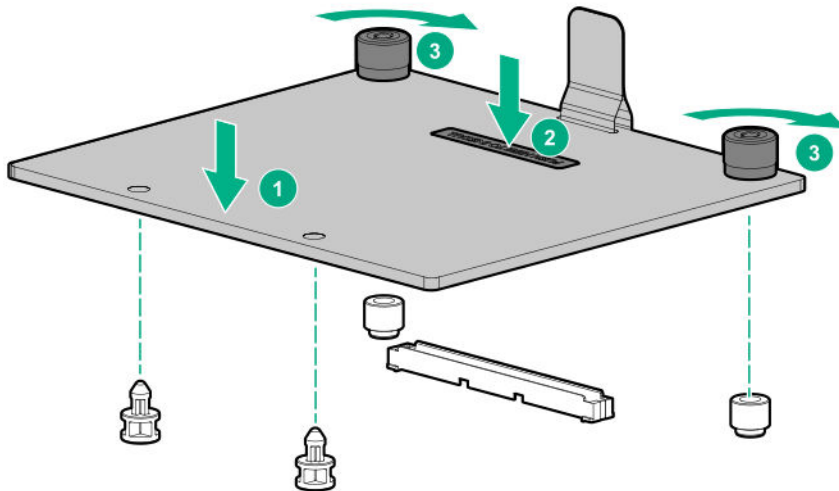
Before you perform this procedure, make sure that you have the following items available:

- Smart Array modular controller option (AROC)
- AROC Mini-SAS cable kit (optional, required only for two-bay LFF hot-plug drive cage)
- T-15 Torx screwdriver

- ⚠ CAUTION:** In systems that use external data storage, be sure that the server is the first unit to be powered down and the last to be powered back up. Taking this precaution ensures that the system does not erroneously mark the drives as failed when the server is powered up.

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. **Remove the PCIe riser cage.**
7. Install the Smart Array modular controller (AROC):
 - a. Insert the alignment pins on the system board through the holes on the controller board.
 - b. Press on the area of the controller board marked as PRESS TO INSTALL to ensure that the board is firmly seated on the slot.
 - c. Tighten the controller board thumbscrews.



8. **Connect the AROC Mini-SAS cables.**
9. **Install the PCIe riser cage.**
10. **Install the access panel.**
11. **Install the server into the rack.**

12. Connect each power cord to the server.
13. Connect each power cord to the power source.
14. **Power up the server.**
15. If removed, **install the security bezel.**

The installation is complete.

To configure arrays, see the *HPE Smart Array SR Gen10 Configuration Guide* at the **Hewlett Packard Enterprise website**.

External type-P and type-E Smart Array SR Gen10 controller option

The server supports the following external controllers:

- HPE Smart Array P408e-p SR Gen10 controller
- HPE Smart Array E208e-p SR Gen10 controller

These controllers are installed on the PCIe riser cage, for installation procedure see, **Installing an expansion board** on page 65.

Smart Storage Battery option

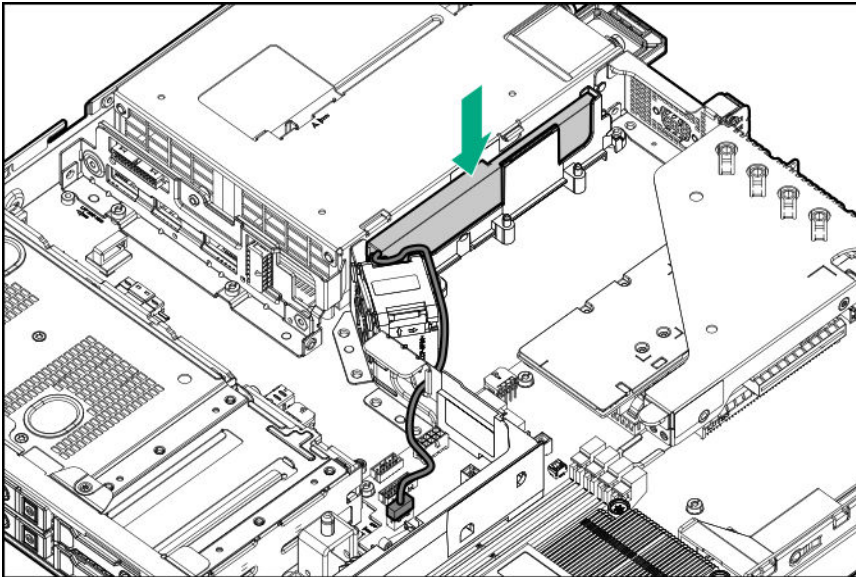
The Smart Storage Battery is a centralized backup source and is required to back up the write cache content onto flash memory on the Smart Array P-class Gen10 controllers in case of an unplanned server power loss. In this server, the 12 W, 230 mm battery supports up to two P-class Gen10 controllers.

After the battery is installed, it might take up to two hours to charge. Controller features requiring backup power are not enabled until the battery is capable of providing the backup power.

Installing the Smart Storage Battery

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. Install the Smart Storage Battery into the holder on the chassis.



7. Connect the cable.

When routing the Smart Storage Battery cable, make sure that it does not block the air flow of the fan and route the cable under the metal tab.

8. Install the access panel.

9. Install the server into the rack.

10. Connect each power cord to the server.

11. Connect each power cord to the power source.

12. Power up the server.

13. If removed, install the security bezel.

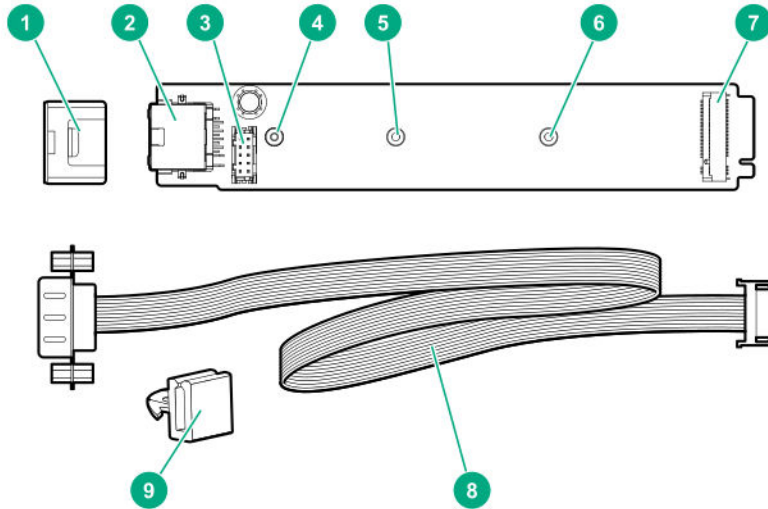
The installation is complete.

M.2/dedicated iLO/serial port option

This option provides support for the following:

- M.2 SSD installation
- serial port connection
- iLO management

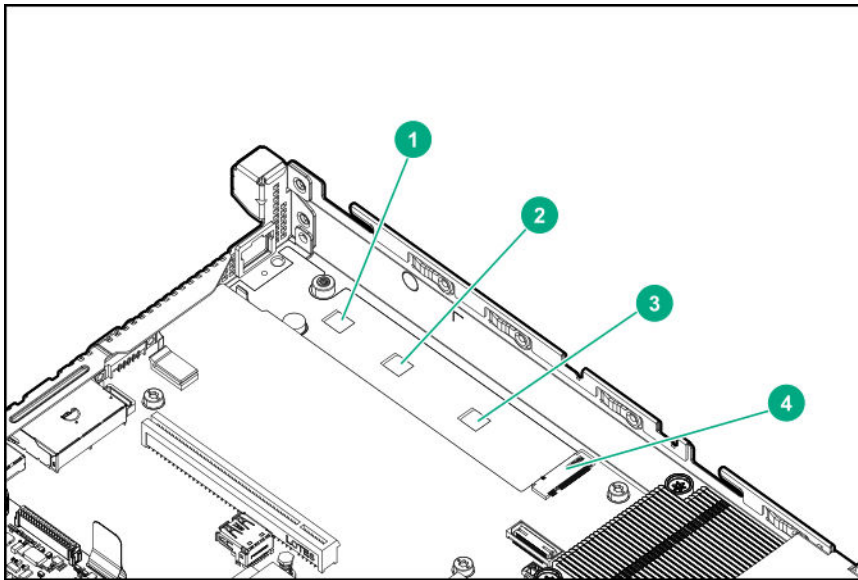
M.2/dedicated iLO/serial port option kit content



Item	Description
1	Enablement board stabilizer
2	Dedicated iLO (iLO Management Port)
3	Serial port cable connector
4	M.2 22110 SSD standoff position
5	M.2 2280 SSD standoff position
6	M.2 2242 SSD standoff position
7	M.2 SSD module connector
8	Serial port cable
9	Serial port cable clip

NOTE: Enablement board stabilizer and serial port cable clip are not used in HPE ProLiant DL20 Gen10 server.

M.2 SSD system board connectors



Item	Description
1	Standoff position to secure the 22110 M.2 SSD module
2	Standoff position to secure the 2280 M.2 SSD module
3	Standoff position to secure the 2242 M.2 SSD module
4	M.2 SSD module connector

Installing the M.2/dedicated iLO/serial port enablement board

Prerequisites

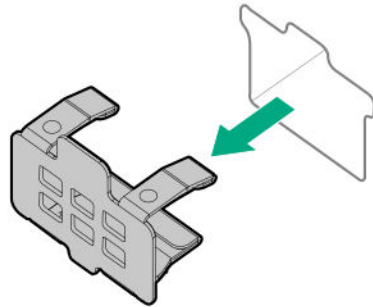
Before you perform this procedure, make sure that you have the following items available:

- T-15 Torx screwdriver
- Hex nut screwdriver
- Sleeve screwdriver

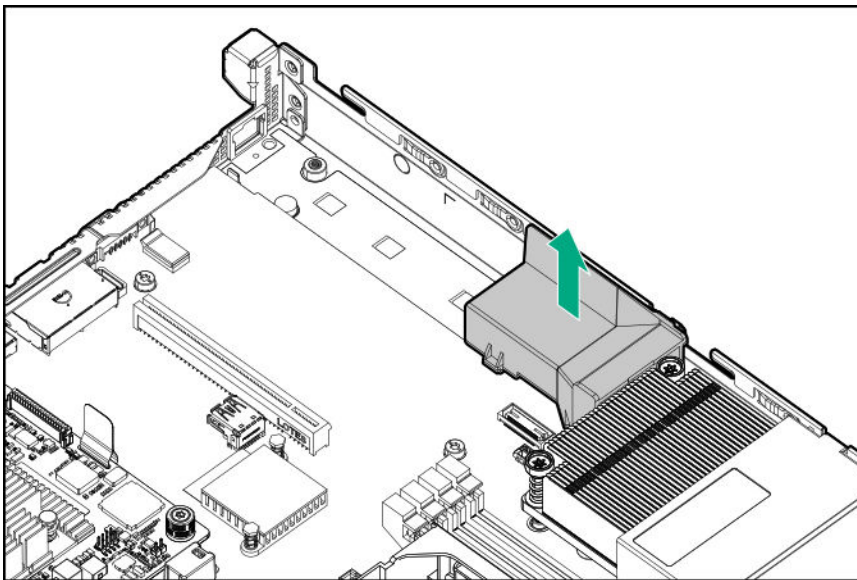
Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:

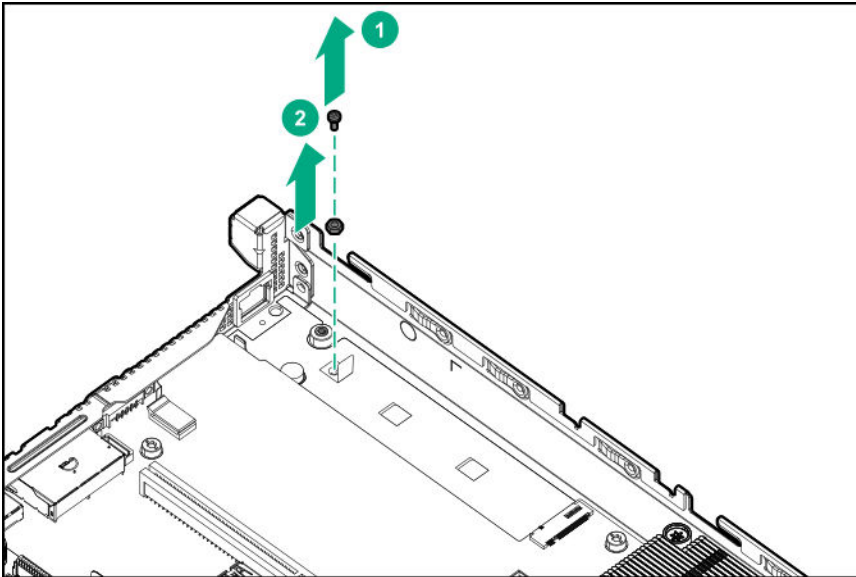
- Extend the server from the rack.
 - Remove the server from the rack.
5. Remove the access panel.
 6. Remove the PCIe riser cage.
 7. Remove the iLO port blank.



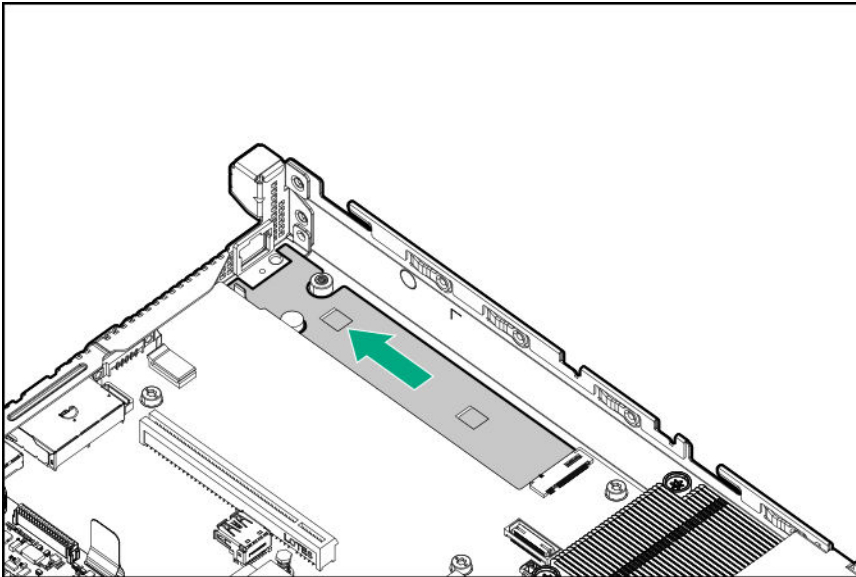
8. Remove the M.2 air guider.



9. Remove the screw and the standoff.

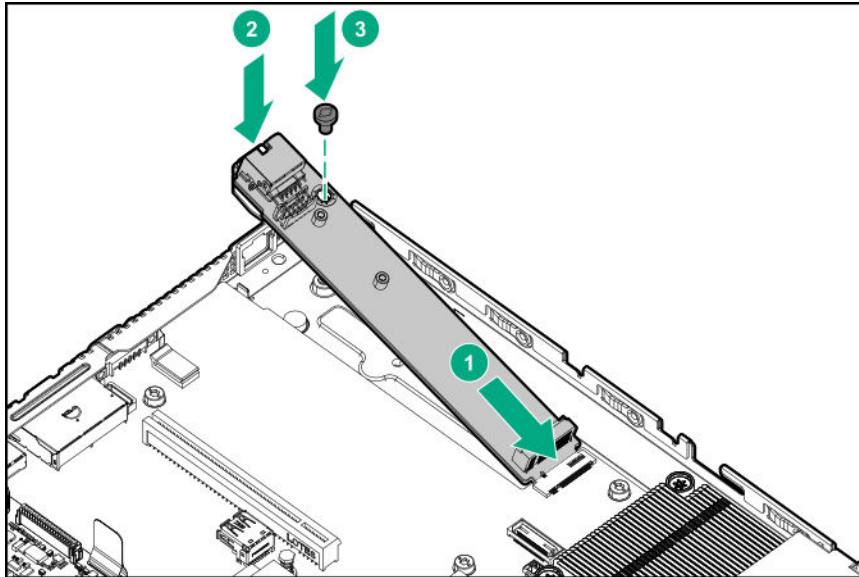


10. Smoothen the tape mylar on the system board.

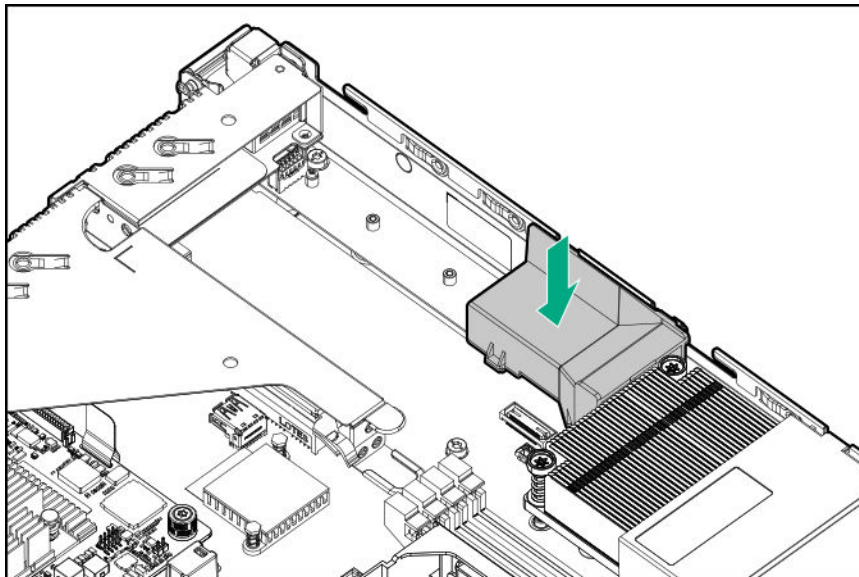


11. Install the M.2/ dedicated iLO/serial port enablement board:

- a. Insert the enablement board in the slot.
- b. Press down the other end of the board.
- c. Secure the board with screw.



12. **Identify the standoff position on the enablement board for securing the M.2 NVMe SSD** and install the standoff.
13. If you intend to install the M.2 SSD, **install it now**.
14. **Install the serial port**
15. **Install the PCIe riser cage**.
16. Install the M.2 air guider.



17. **Install the access panel**.
18. **Install the server into the rack**.
19. Connect each power cord to the server.
20. Connect each power cord to the power source.
21. Optional- **enable the dedicated iLO**.

22. **Power up the server.**
23. If removed, **install the security bezel.**

The installation is complete.

M.2 SSD module option

Use the M.2 connector on the system board or on the optional M.2/dedicated iLO/serial port enablement board to install an M.2 SSD on the server.

Installing the M.2 SSD on the system board

- ❗ **IMPORTANT:** When installing HPE 400GB NVMe x4 MU M.2 22110 DS SSD (875583-B21) and HPE 480GB NVMe x4 RI M.2 22110 DS SSD (875579-001) modules, the supporting ambient temperature should be under 30°C (86°F).
-

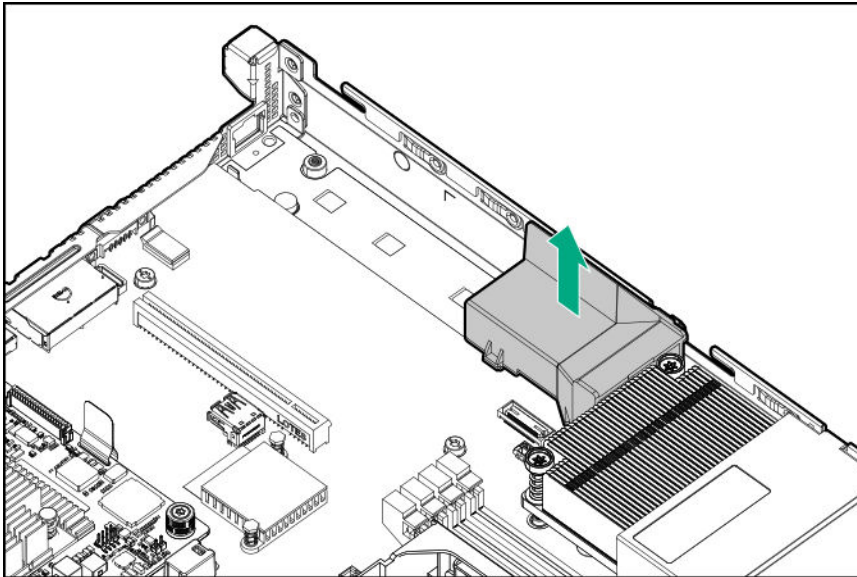
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

- T-15 Torx screwdriver
- Hex nut screwdriver
- Sleeve screwdriver

Procedure

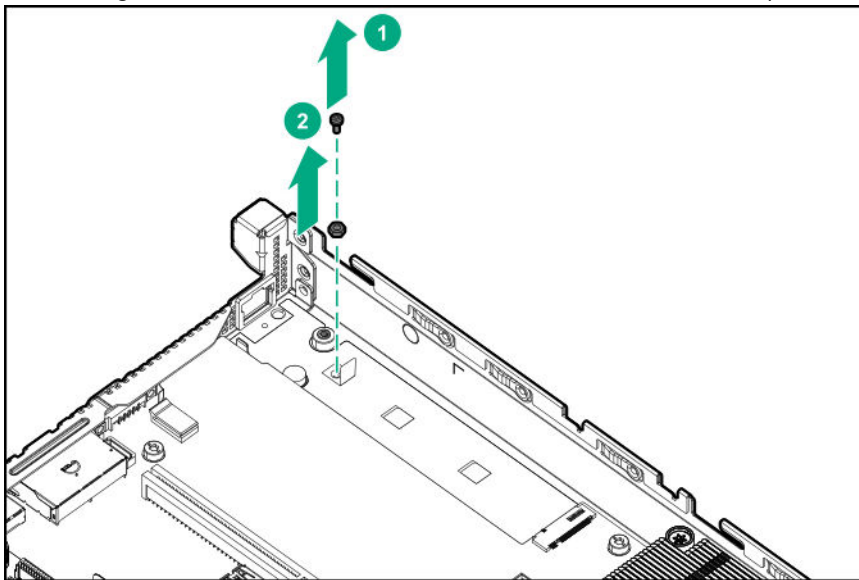
1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. Remove the M.2 air guider.



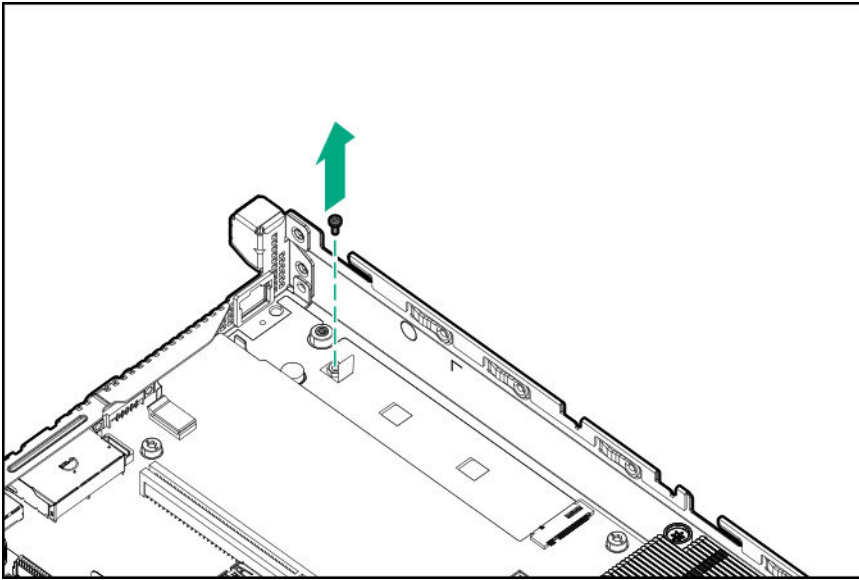
7. **Identify the standoff position on the system board for securing the M.2 NVMe SSD.**

8. Remove the alignment screws:

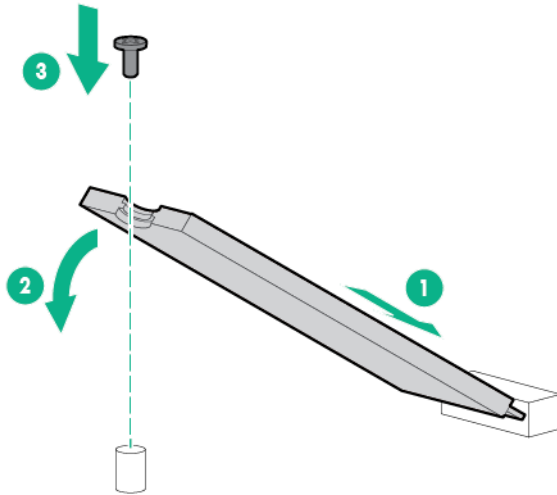
- If installing an M.2 2242 or 2280 SSD, remove both the standoff (Hex nut) screw and Phillips screw.



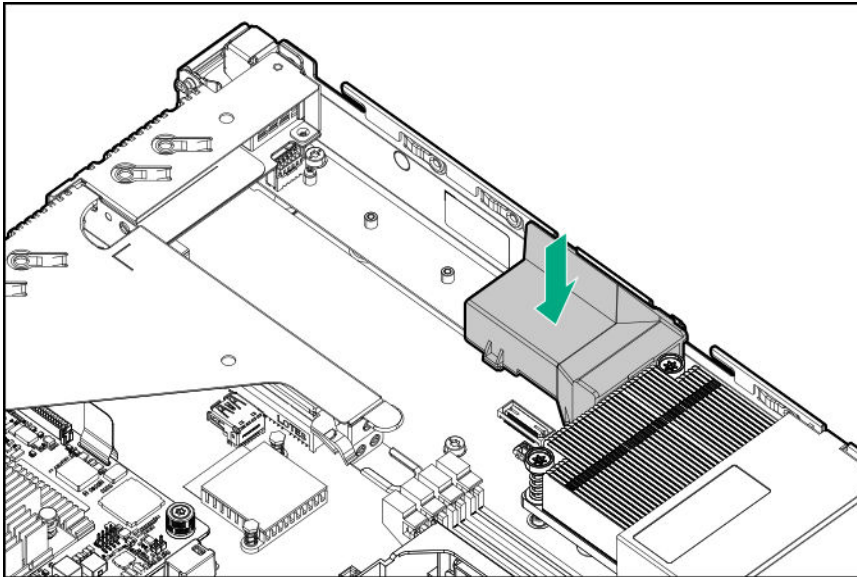
- If installing the M.2 22110, remove only the Phillips screw. Retain the standoff (Hex nut) screw.



9. Install the standoff (hex nut) screw on 2242 or 2280 standoff position on the system board.
10. Install the M.2 SSD module:
 - a. Insert the SSD into the M.2 slot at a 45° angle.
 - b. Carefully press the SSD down to the horizontal position.
 - c. Install the SSD mounting screw.



11. Install the M.2 air guider.



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.**
17. If removed, **install the security bezel.**

The installation is complete.

To configure the M.2 SSD, see the *HPE Smart Array SR Gen10 Configuration Guide* at the [Hewlett Packard Enterprise website](#).

Installing an M.2 SSD module on M.2/dedicated iLO/serial port enablement board

Prerequisites

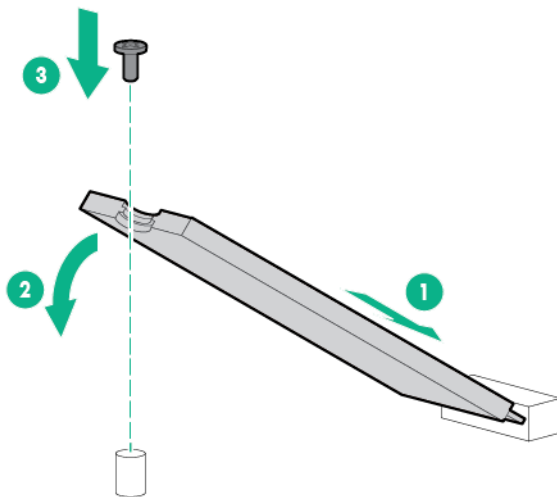
Before you perform this procedure, make sure that you have the following items available:

- T-15 Torx screwdriver
- Hex nut screwdriver
- Phillips screwdriver

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.

4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. **Remove the PCIe riser cage.**
7. **Install the M.2/ dedicated iLO/serial port enablement board.**
8. **Install the standoff (Hex nut) screw on either 2242, 2280 or 22110 standoff position on kit.**
9. Install the M.2 SSD:
 - a. Insert the SSD into the M.2 slot at a 45° angle.
 - b. Carefully press the SSD down to the horizontal position.
 - c. Install the SSD mounting screw.



10. **Install the PCIe riser cage.**
11. **Install the access panel.**
12. **Install the server into the rack.**
13. Connect each power cord to the server.
14. Connect each power cord to the power source.
15. **Power up the server.**
16. If removed, **install the security bezel.**

The installation is complete.

To configure the M.2 SSD, see the *HPE Smart Array SR Gen10 Configuration Guide* at the **Hewlett Packard Enterprise website**.

Installing the Serial Port

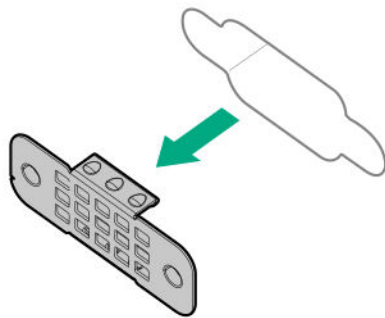
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

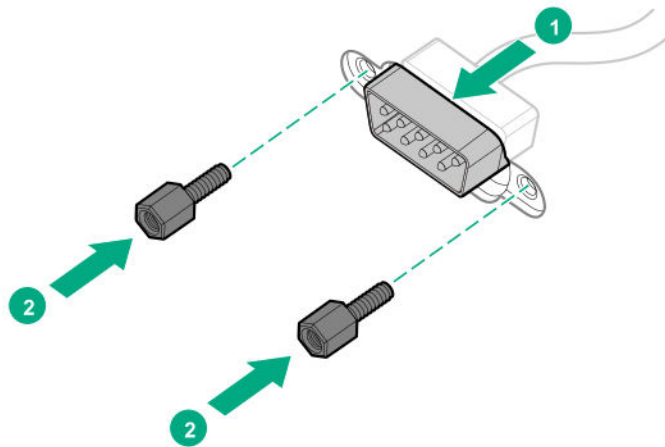
- T-15 Torx screwdriver
- Sleeve screwdriver

Procedure

1. If installed, **remove the security bezel.**
2. **Power down the server.**
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack.**
 - **Remove the server from the rack.**
5. **Remove the access panel.**
6. **Remove the PCIe riser cage.**
7. **Install the M.2/ dedicated iLO/serial port enablement board.**
8. Remove the serial port blank.



9. Install the serial port.



10. Connect the cable.

Route the serial cable between the chassis and above the rear I/O port.

11. Install the PCIe riser cage.

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.

17. If removed, **install the security bezel.**

The installation is complete.

Enabling the dedicated iLO management module

The onboard NIC 1/shared iLO connector is set as the default system iLO connector. To enable the dedicated iLO management module, use the iLO 5 Configuration Utility accessible within the HPE UEFI System Utilities.

For more information on the UEFI System Utilities, see the UEFI documentation on the Hewlett Packard Enterprise website (<http://www.hpe.com/servers/uefi>).

! **IMPORTANT:** If the iLO configuration settings are reset to the default values, remote access to the machine will be lost. Access the physical machine and repeat the procedure described in this section to re-enable the dedicated iLO management connector.

Procedure

1. During the server startup sequence after installing the module, press F9 in the POST screen.

The System Utilities screen appears.

2. Select System Configuration | iLO 5 Configuration Utility.

The iLO 5 Configuration Utility screen appears.

3. Select Network Options, and then press Enter.
The Network Options screen appears.
4. Set the Network Interface Adapter field to ON, and then press Enter.
5. Press F10 to save your changes.
A message prompt to confirm that the iLO settings reset appears.
6. Press Enter to reboot the iLO settings.
7. Press Esc until the main menu is displayed.
8. Select Reboot the System to exit the utility and resume the boot process.
The IP address of the enabled dedicated iLO connector appears on the POST screen on the subsequent boot-up. Access the Network Options screen again to view this IP address for later reference.

FlexibleLOM riser option

If FlexibleLOM is installed in the server, the **shared iLO port** behavior will be default to port 1 of the FlexibleLOM card. For more information, see the [Hewlett Packard Enterprise website](#).

Installing the FlexibleLOM riser assembly

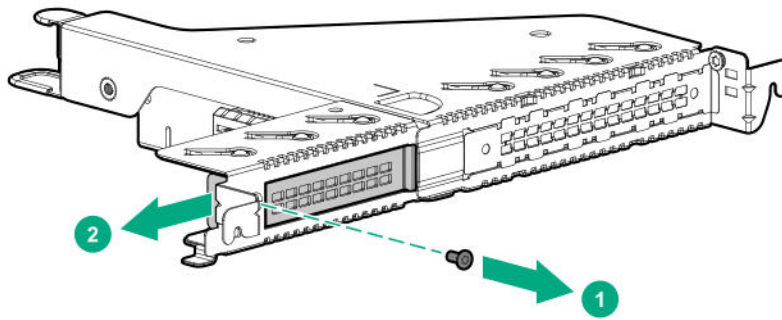
Prerequisites

Before you perform this procedure, make sure that you have the following items available:

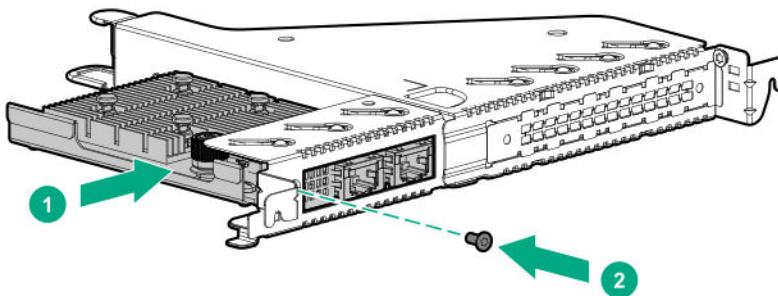
- FlexibleLOM riser kit
- T-10 Torx screwdriver

Procedure

1. If installed, **remove the security bezel**.
2. **Power down the server**.
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack**.
 - **Remove the server from the rack**.
5. **Remove the access panel**.
6. **Remove the PCIe riser cage**.
7. Remove blank from the FlexibleLOM slot of the riser cage.
Retain the screw for future use.



8. Install the component:
 - a. Firmly seat the FlexibleLOM riser into the slot.
 - b. Secure the FlexibleLOM riser with a screw.



9. **Install the FLOM riser cage.**
10. **Install the access panel.**
11. **Install the server into the rack.**
12. Connect all necessary external cabling.
13. Connect each power cord to the server.
14. Connect each power cord to the power source.
15. **Power up the server.**
16. If removed, **install the security bezel.**

The installation is complete.

Transceiver option

Transceiver warnings and cautions



WARNING: Fiber-optic transceivers and fiber-optic cables connected to transceivers emit laser light that can damage your eyes. To avoid eye injuries, avoid direct eye exposure to the beam from the fiber-optic transceiver or into the ends of fiber-optic cables when they are powered-up.

-
- ⚠ **CAUTION:** The presence of dust in transceiver ports can cause poor cable connectivity. To prevent dust from entering, install a dust plug in an unused transceiver port.
-
- ⚠ **CAUTION:** Supported transceivers can be hot-swapped—removed and installed while the server is powered-on. However, to prevent potential damage to the transceiver or the fiber-optic cable, disconnect the cable from the transceiver before hot-swapping it.
-
- ⚠ **CAUTION:** Do not remove and install transceivers more often than is necessary. Doing so can shorten the useful life of the transceiver.
-
- ❗ **IMPORTANT:** When you replace a transceiver with another of a different type, the server might retain selected port-specific configuration settings that were configured for the replaced transceiver. Be sure to validate or reconfigure port settings as required.
-

Installing a transceiver

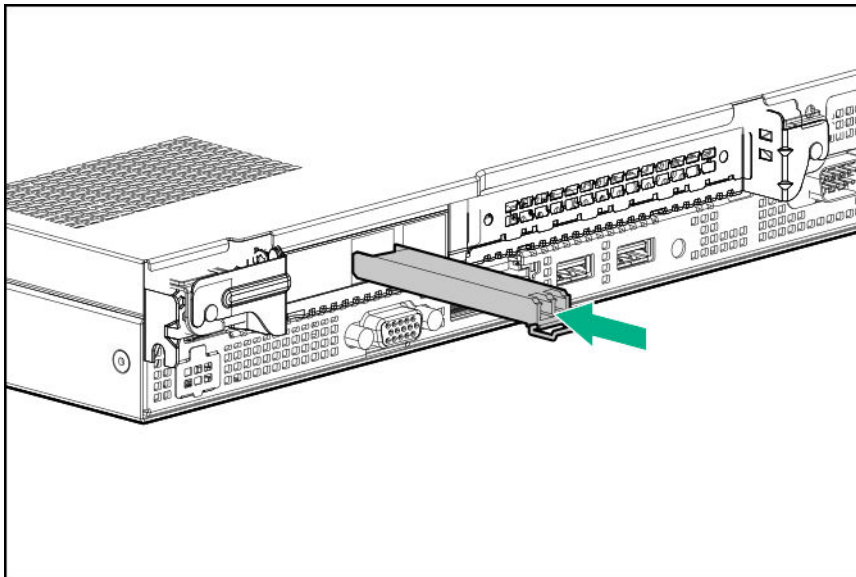
Prerequisites

Before installing a transceiver, be sure to read the following:

- [Transceiver warnings and cautions](#) on page 86
- Transceiver documentation for specific operational and cabling requirements

Procedure

1. **Install the FlexibleLOM.**
2. Hold the transceiver by its sides and gently insert it in slot 1 of the FlexibleLOM until it clicks into place.



Transceivers are keyed so that they can only be inserted in the correct orientation. If the transceiver does not fit easily into the port, you might have positioned it incorrectly. Reverse the orientation of the transceiver and insert it again.

3. Remove the dust plug or protective cover from the transceiver.

4. Connect a compatible network cable to the transceiver.
5. If needed, see the transceiver documentation for the model-specific fastening mechanism applicable to the transceiver.

The installation is complete.

Chassis Intrusion detection option

The chassis intrusion detection option detects if the chassis access cover is opened or closed. The iLO management processor monitors the switch and if there is a change (if the access cover is either opened or closed), it creates a log entry noting the intrusion. You can set various alerting mechanisms (Remote SysLog, SNMP, AlertMail, and so on) to be notified of the intrusion. The switch and the iLO reporting occur as long as the server is plugged in, regardless of whether the server is powered on or off.

The iLO 5 chipset helps in detecting any intrusions. It provides an unprecedented level of hardware security with its silicon root of trust. The silicon root of trust:

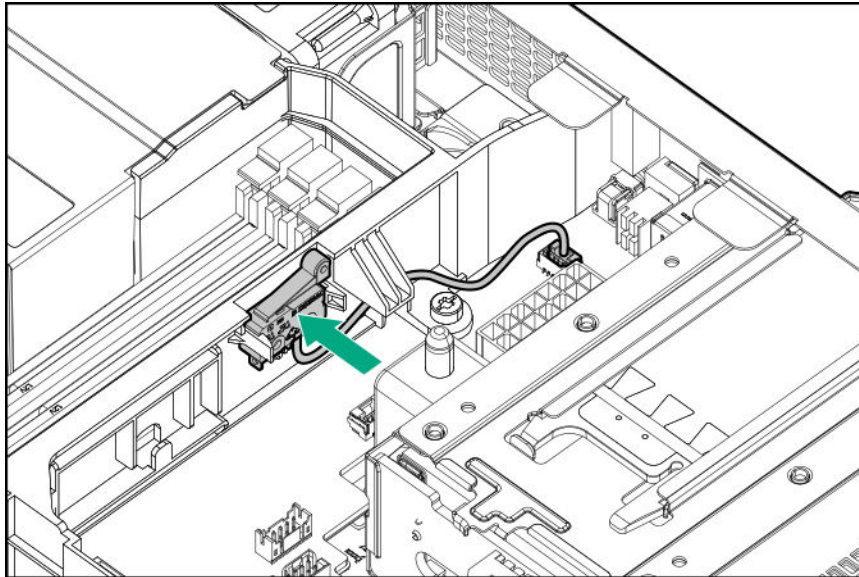
- Is based in the silicon chip hardware itself
- Is impossible to alter
- Enables firmware to be authenticated as far back as the supply chain
- Provides a secure startup process

The iLO 5 chipset acts as a silicon root of trust and includes an encrypted hash embedded in silicon hardware at the chip fabrication facility. Thus making it virtually impossible to insert any malware, virus, or compromised code that would corrupt the boot process. Rather than the iLO firmware checking the integrity of the firmware every time it boots, the iLO 5 hardware determines whether to execute the iLO firmware, based on whether it matches the encryption hash that is permanently stored in the iLO chipset silicon. These improvements help ensure that, if iLO 5 is running, your server is trusted.

Installing the Chassis Intrusion Detection switch

Procedure

1. If installed, **remove the security bezel**.
2. **Power down the server**.
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack**.
 - **Remove the server from the rack**.
5. **Remove the access panel**.
6. Install the chassis intrusion detection switch on the DIMM guard.



7. **Connect the cable.**
8. **Install the access panel.**
9. **Install the server into the rack.**
10. Connect each power cord to the server.
11. Connect each power cord to the power source.
12. **Power up the server.**
13. If removed, **install the security bezel.**

The installation is complete.

HPE Trusted Platform Module 2.0 Gen10 option

Overview

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

This procedure includes three sections:

1. Installing the Trusted Platform Module board.
2. Enabling the Trusted Platform Module.
3. Retaining the recovery key/password.

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

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

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

HPE Trusted Platform Module 2.0 Guidelines

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

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

- Do not remove an installed TPM. Once installed, the TPM is bound to the system board. If an OS is configured to use the TPM and it is removed, the OS may go into recovery mode, data loss can occur, or both.
- When installing or replacing hardware, Hewlett Packard Enterprise service providers cannot enable the TPM or the encryption technology. For security reasons, only the customer can enable these features.
- When returning a system board for service replacement, do not remove the TPM from the system board. When requested, Hewlett Packard Enterprise Service provides a TPM with the spare system board.
- Any attempt to remove the cover of an installed TPM from the system board can damage the TPM cover, the TPM, and the system board.
- If the TPM is removed from the original server and powered up on a different server, data stored in the TPM including keys will be erased.
- When using BitLocker, always retain the recovery key/password. The recovery key/password is required to complete Recovery Mode after BitLocker detects a possible compromise of system integrity or system configuration.
- Hewlett Packard Enterprise is not liable for blocked data access caused by improper TPM use. For operating instructions, see the TPM documentation or the encryption technology feature documentation provided by the operating system.

Installing and enabling the HPE TPM 2.0 Gen10 Kit

Installing the Trusted Platform Module board

Preparing the server for installation

Procedure

1. Observe the following warnings:

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

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

For rack and tower servers, remove the power cord.

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

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

2. Update the system ROM.

Locate and download the latest ROM version from the [Hewlett Packard Enterprise Support Center website](#). Follow the instructions on the website to update the system ROM.

3. Power down the server ([Powering down the server](#) on page 33).

4. If installed, [remove the security bezel](#).

5. Remove all power:

- a. Disconnect each power cord from the power source.
- b. Disconnect each power cord from the server.

6. Do one of the following:

- [Extend the server from the rack](#).
- [Remove the server from the rack](#).

7. [Remove the access panel](#).

8. Proceed to [Installing the TPM board and cover](#) on page 91.

Installing the TPM board and cover

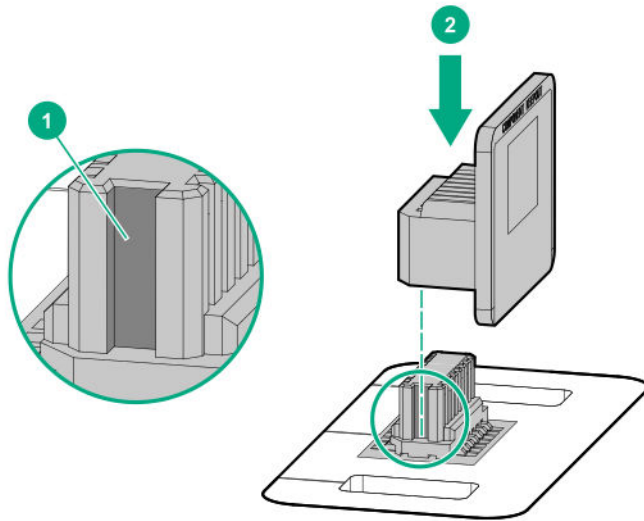
Procedure

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.

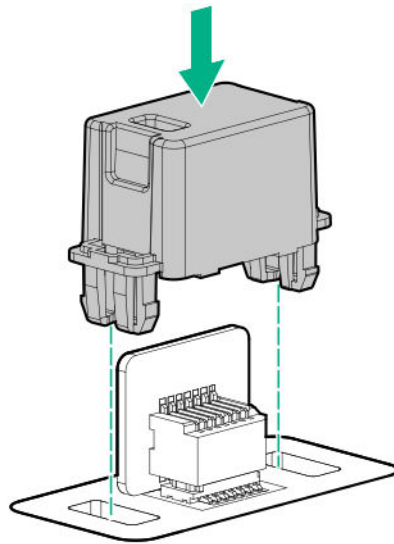
⚠ CAUTION: The TPM is keyed to install only in the orientation shown. Any attempt to install the TPM in a different orientation might result in damage to the TPM or system board.

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 92.

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. **Install the server into the rack.**
4. Connect each power cord to the server.

5. Connect each power cord to the power source.
6. **Power up the server.**
7. If removed, **install the security bezel.**

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

Cabling guidelines

The cable colors in the cabling diagrams used in this chapter are for illustration purposes only. Most of the server cables are black.

Observe the following guidelines when working with server cables.

Before connecting cables

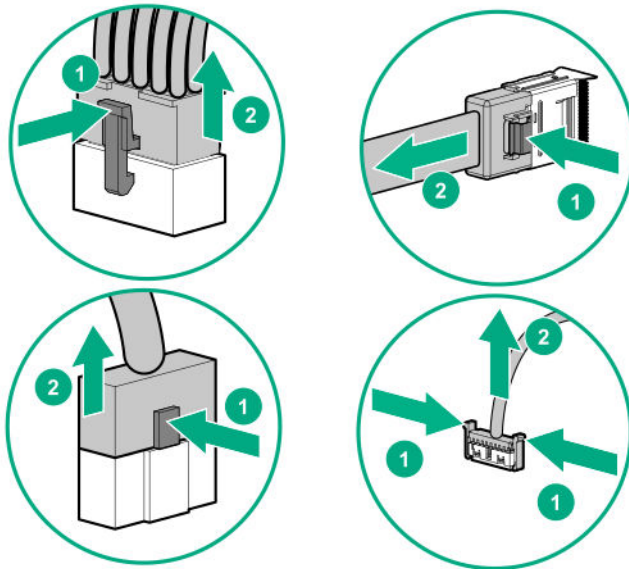
- Note the port labels on the PCA components. Not all of these components are used by all servers:
 - System board ports
 - Drive and power supply backplane ports
 - Expansion board ports (controllers, adapters, expanders, risers, and similar boards)
- Note the label near each cable connector. This label indicates the destination port for the cable connector.
- Some data cables are pre-bent. Do not unbend or manipulate the cables.
- To prevent mechanical damage or depositing oil that is present on your hands, and other contamination, do not touch the ends of the connectors.

When connecting cables

- Before connecting a cable to a port, lay the cable in place to verify the length of the cable.
- Use the internal cable management features to properly route and secure the cables.
- When routing cables, be sure that the cables are not in a position where they can be pinched or crimped.
- Avoid tight bend radii to prevent damaging the internal wires of a power cord or a server cable. Never bend power cords and server cables tight enough to cause a crease in the sheathing.
- Make sure that the excess length of cables are properly secured to avoid excess bends, interference issues, and airflow restriction.
- To prevent component damage and potential signal interference, make sure that all cables are in their appropriate routing position before installing a new component and before closing up the server after hardware installation/maintenance.

When disconnecting cables

- Grip the body of the cable connector. Do not pull on the cable itself because this action can damage the internal wires of the cable or the pins on the port.
- If a cable does not disconnect easily, check for any release latch that must be pressed to disconnect the cable.

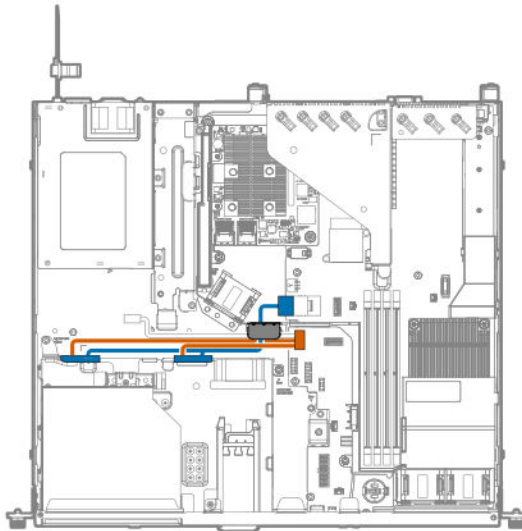


- Remove cables that are no longer being used. Retaining them inside the server can restrict airflow. If you intend to use the removed cables later, label and store them for future use.

Storage cabling

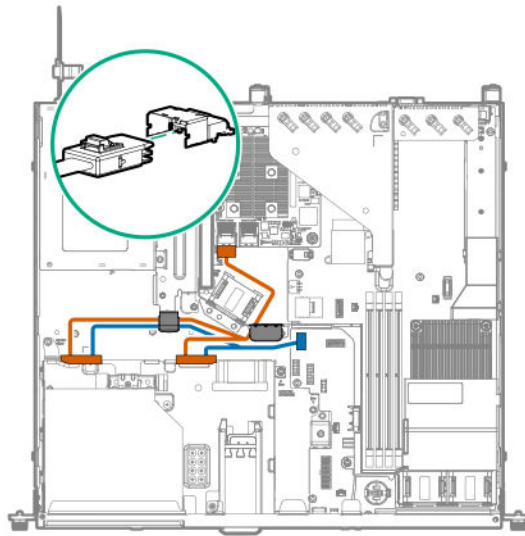
Non-hot-plug drive cabling

Two-bay LFF non-hot-plug drive embedded controller cabling



Cable color	Description
Orange	Non-hot-plug drive power cable
Blue	SATA cable

Two-bay LFF non-hot-plug drive Smart Array modular controller (AROC) cabling

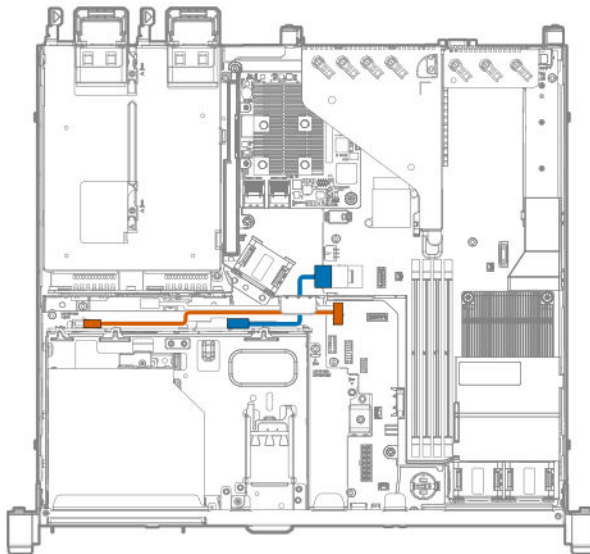


Cable color	Description
Orange	Mini-SAS cable from drive backplane to modular controller (AROC) port 1
Blue	Drive backplane power cable

Hot-plug drive cabling

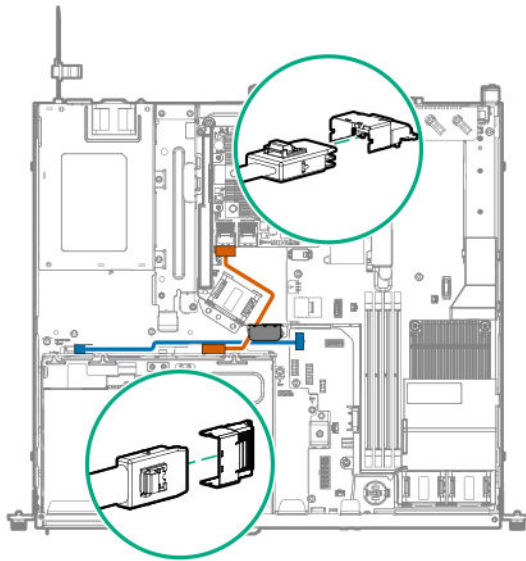
Two-bay LFF hot-plug drive cabling

Two-bay LFF hot-plug drive embedded controller cabling



Cable color	Description
Orange	Two-bay LFF drive backplane power cable
Blue	Mini-SAS cable

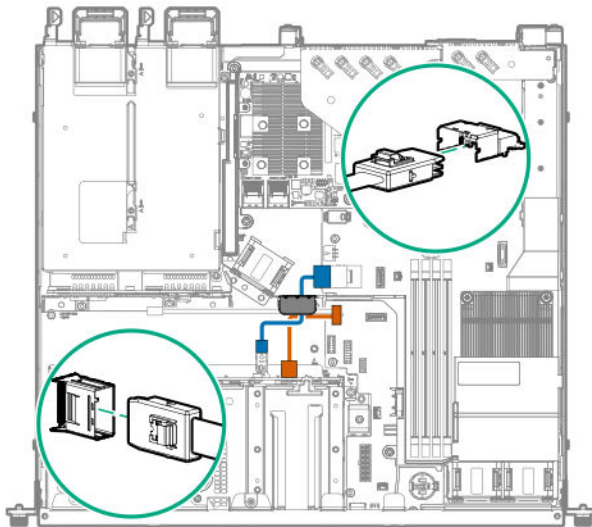
Two-bay LFF hot-plug drive Smart Array modular controller (AROC) cabling



Cable color	Description
Blue	Drive backplane power cable
Orange	Min-SAS cable from drive backplane to AROC port 1

Four bay SFF hot-plug drive cabling

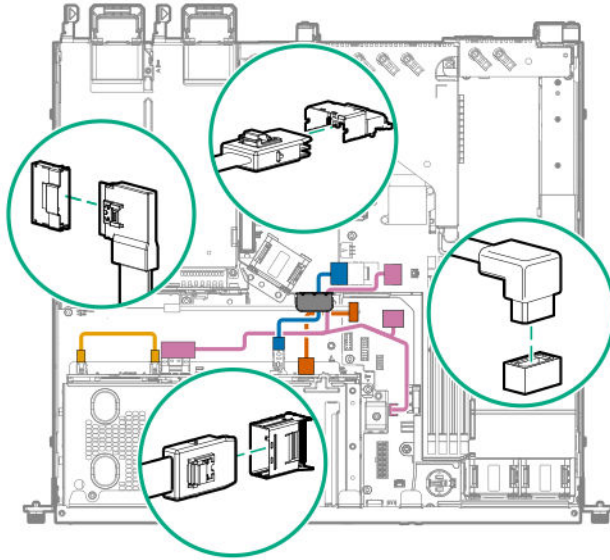
Four-bay SFF hot-plug drive embedded controller cabling



Cable color	Description
Orange	Four-bay SFF drive backplane power cable
Blue	SATA cable

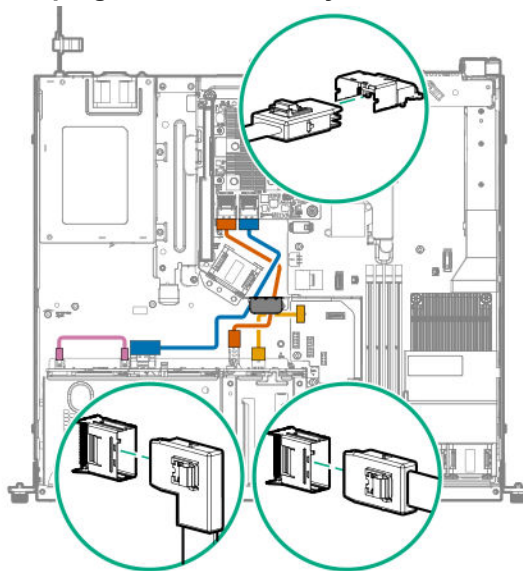
4+2 bay SFF hot-plug drive cabling

4+2 bay SFF hot-plug drive embedded controller cabling



Cable color	Description
Orange	Four-bay SFF drive backplane power cable
Blue	Mini-SAS cable
Gold	Two-bay SFF to four-bay SFF drive backplane power cable
Pink	SATA cable and drive sideband cable

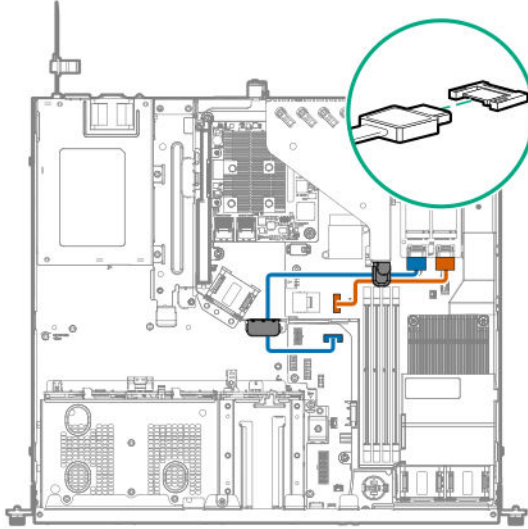
4+2 bay SFF hot-plug drive Smart Array modular controller (AROC) cabling



Cable color	Description
Blue	Mini-SAS cable from two-bay SFF drive backplane to AROC port 2
Orange	Mini-SAS cable from four-bay SFF drive backplane Mini-SAS cable to AROC port 1
Gold	Four-bay SFF drive backplane power cable
Pink	Two-bay to four-bay SFF drive backplane power cable

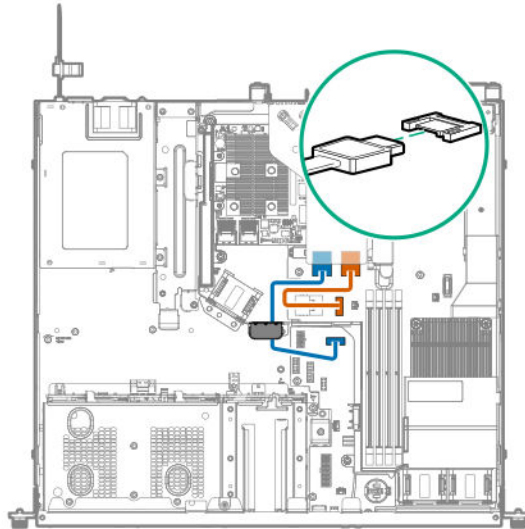
M.2 SATA SSD cabling

M.2 SATA SSD in slot 1



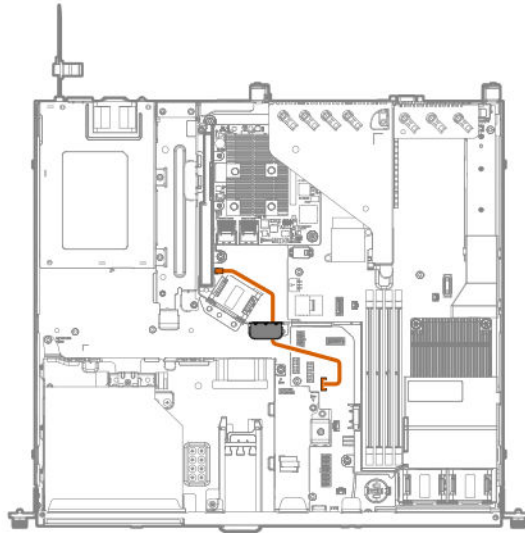
Cable color	Description
Orange	SATA cable to x1 SATA port 1
Blue	SATA cable to x1 SATA port 2

M.2 SATA SSD in slot 2



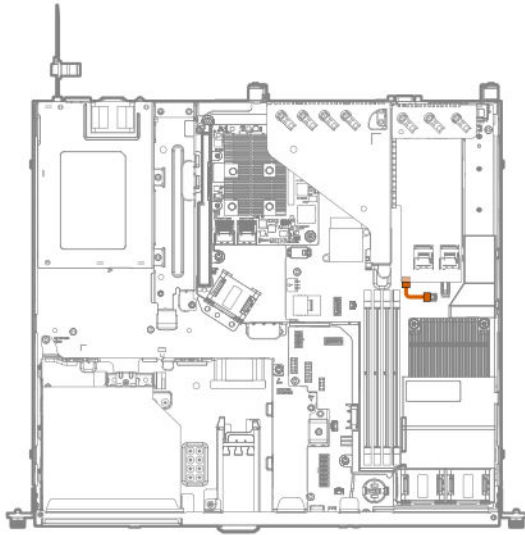
Cable color	Description
Orange	SATA cable to x1 SATA port 2
Blue	SATA cable to x1 SATA port 1

Smart Storage Battery cabling



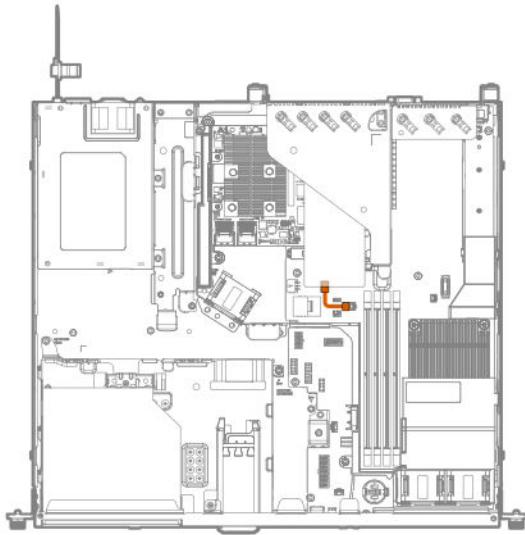
Storage controller backup power cabling

Smart Array P-class storage controller in slot 1



Cable color	Description
Orange	Slot 1 storage controller backup power cable

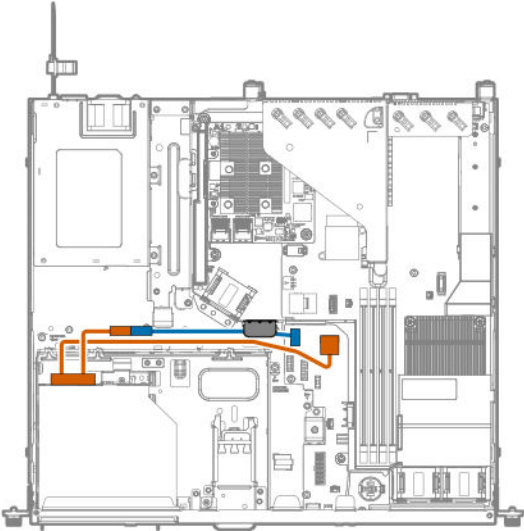
Smart Array P-class storage controller in slot 2



Cable color	Description
Orange	Slot 2 storage controller backup power cable

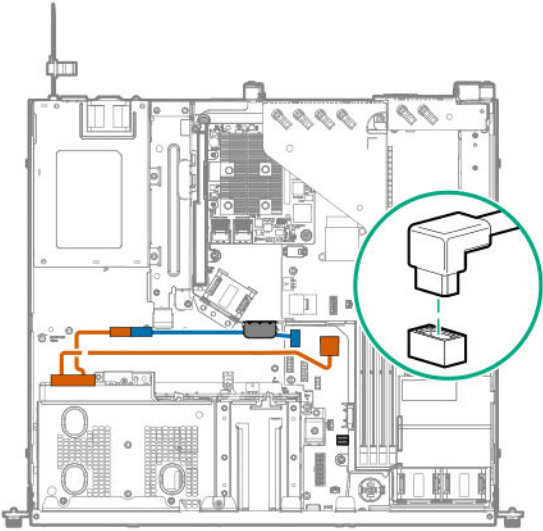
Optical drive cabling

LFF configuration



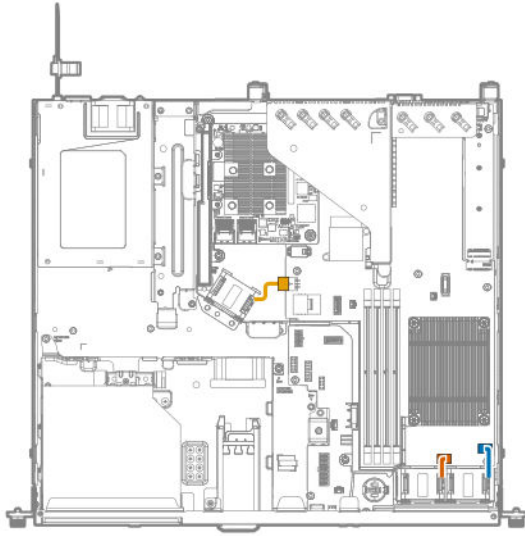
Cable color	Description
Orange	SATA-power Y-cable to x1 SATA port 2
Blue	Power extension cable

SFF configuration



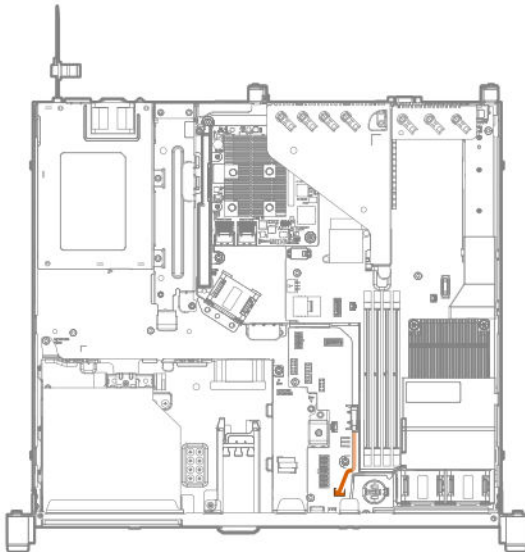
Cable color	Description
Orange	SATA-power-Y cable to x1 SATA port 2
Blue	Power extension cable

Fan cabling

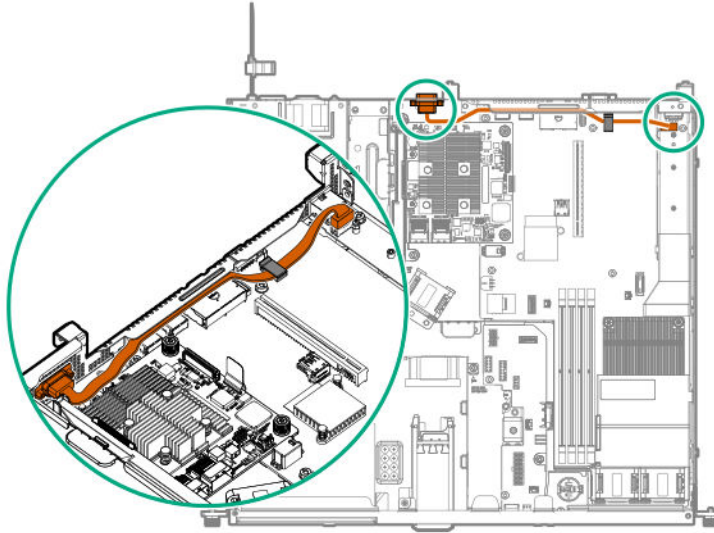


Cable color	Description
Orange	Fan 1 cable
Blue	Fan 2 cable
Gold	Fan 3 cable

Chassis Intrusion detection cabling

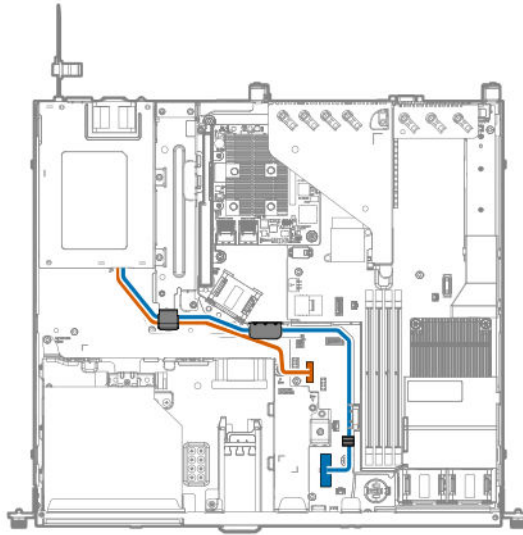


M.2/dedicated iLO/serial port cabling



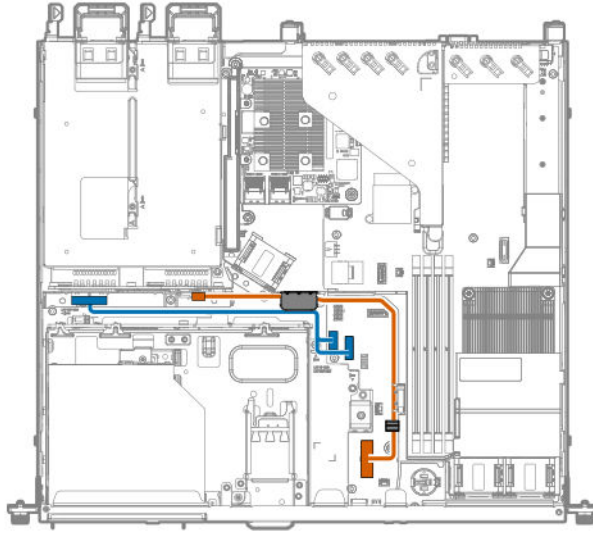
Power supply cabling

- Non-hot-plug



Cable color	Description
Orange	16-pin power supply sideband cable
Blue	14-pin power supply cable

- Hot-plug



Cable color	Description
Orange	14-pin power supply cable
Blue	Redundant power supply sideband cable

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 107	Online and Offline
HPE iLO 5 on page 108	Online and Offline
HPE Smart Storage Administrator on page 114	Online and Offline
iLO RESTful API on page 110	Online and Offline
Intelligent Provisioning on page 110	Online and Offline
Scripting Toolkit for Windows and Linux on page 112	Online
Service Pack for ProLiant on page 116	Online and Offline
Smart Update Manager on page 116	Online and Offline
UEFI System Utilities on page 112	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

Active Health System is the 24/7 control center for your server. With fast diagnostic data collection and the richest, most relevant data, it is the fastest way to get your system back online and keep it running optimally.

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

The Active Health System provides:

- Continuous health monitoring of over 1600 system parameters
- Logging of all configuration changes
- Consolidated health and service alerts with precise time stamps
- Agentless monitoring that does not affect application performance

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

Active Health System data collection

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

Examples of information that is collected:

- Server model and serial number
- Processor model and speed
- Storage capacity and speed
- Memory capacity and speed
- Firmware/BIOS and driver versions and settings

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

Active Health System Log

The data collected by the Active Health System is stored in the Active Health System Log. The data is logged securely, isolated from the operating system, and separate from customer data.

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>.

HPE iLO 5

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

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

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

iLO Federation

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

When configured for iLO Federation, iLO uses multicast discovery and peer-to-peer communication to enable communication between the systems in 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 at the following website: <http://www.hpe.com/support/ilo-docs>.

iLO Service Port

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.

When you use the iLO Service Port:

- Actions are logged in the iLO Event Log.
- The server UID flashes to indicate the Service Port status.
You can also retrieve the Service Port status by using a REST client and the iLO RESTful API.
- You cannot use the Service Port to boot any device within the server, or the server itself.
- You cannot access the server by connecting to the Service Port.
- You cannot access the connected device from the server.

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

iLO RESTful API

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

To learn more about the iLO RESTful API, see the Hewlett Packard Enterprise website (<http://www.hpe.com/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, firmware and driver update solution that enables rapid discovery, detailed inventory reporting, firmware, and driver updates by leveraging iLO advanced functionality. The iLO Amplifier Pack performs rapid server discovery and inventory for thousands of supported servers for the purpose of updating firmware and drivers at scale.

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

Integrated Management Log

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

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

- From within HPE SIM
- From within the UEFI System Utilities
- From within the Embedded UEFI shell
- From within the iLO web interface

Intelligent Provisioning

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

Intelligent Provisioning 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.

Intelligent Provisioning operation

Intelligent Provisioning includes the following components:

- Critical boot drivers
- Active Health System (AHS)
- Erase Utility
- Deployment Settings

❗ **IMPORTANT:**

- Although your server is pre-loaded with firmware and drivers, you should update the firmware upon initial setup to ensure you have the latest versions. Also, downloading and updating the latest version of Intelligent Provisioning ensures the latest supported features are available.
 - For ProLiant servers, firmware is updated using the Intelligent Provisioning Firmware Update utility.
 - Do not update firmware if the version you are currently running is required for compatibility.
-

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

Intelligent Provisioning provides installation help for the following operating systems:

- Microsoft Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware ESXi/vSphere Custom Image

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

Management Security

HPE ProLiant Gen10 servers are built with some of the industry's most advanced security capabilities, out of the box, with a foundation of secure embedded management applications and firmware. The management security provided by HPE embedded management products enables secure support of modern workloads,

protecting your components from unauthorized access and unapproved use. The range of embedded management and optional software and firmware available with the iLO Advanced and iLO Advanced Premium Security Edition licenses provides security features that help ensure protection, detection, and recovery from advanced cyber-attacks. For more information, see the *HPE Gen10 Server Security Reference Guide* on the Hewlett Packard Enterprise Information Library at <http://www.hpe.com/support/gen10-security-ref-en>.

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

Scripting Toolkit for Windows and Linux

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

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

For more information or to download the STK, see the [Hewlett Packard Enterprise website](#).

UEFI System Utilities

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

- Configuring system devices and installed options.
- Enabling and disabling system features.
- Displaying system information.
- Selecting the primary boot controller or partition.
- Configuring memory options.
- Launching other preboot environments.

HPE servers with UEFI can provide:

- Support for boot partitions larger than 2.2 TB. Such configurations could previously only be used for boot drives when using RAID solutions.
- Secure Boot that enables the system firmware, option card firmware, operating systems, and software collaborate to enhance platform security.
- UEFI Graphical User Interface (GUI)
- An Embedded UEFI Shell that provides a preboot environment for running scripts and tools.
- Boot support for option cards that only support a UEFI option ROM.

Selecting the boot mode

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

- Secure Boot, UEFI Optimized Boot, Generic USB Boot, IPv6 PXE Boot, iSCSI Boot, and Boot from URL
- Fibre Channel/FCoE Scan Policy

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

Prerequisite

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

Procedure

1. From the **System Utilities** screen, select **System Configuration > BIOS/Platform Configuration (RBSU) > Boot Options > Boot Mode**.
2. Select a setting.
 - **UEFI Mode** (default)—Configures the system to boot to a UEFI compatible operating system.
 - **Legacy BIOS Mode**—Configures the system to boot to a traditional operating system in Legacy BIOS compatibility mode.
3. Save your setting.
4. Reboot the server.

Secure Boot

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

- UEFI drivers loaded from PCIe cards
- UEFI drivers loaded from mass storage devices
- Preboot UEFI Shell applications
- OS UEFI boot loaders

When Secure Boot is enabled:

- Firmware components and operating systems with boot loaders must have an appropriate digital signature to execute during the boot process.
- Operating systems must support Secure Boot and have an EFI boot loader signed with one of the authorized keys to boot. For more information about supported operating systems, see <http://www.hpe.com/servers/ossupport>.

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

You can configure Secure Boot:

- Using the **System Utilities** options described in the following sections.
- Using the iLO RESTful API to clear and restore certificates. For more information, see the Hewlett Packard Enterprise website (<http://www.hpe.com/info/redfish>).
- Using the `secboot` command in the Embedded UEFI Shell to display Secure Boot databases, keys, and security reports.

Launching the Embedded UEFI Shell

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

Prerequisites

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

Procedure

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

The **Embedded UEFI Shell** screen appears.

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

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

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

The `Shell>` prompt appears.

4. Enter the commands required to complete your task.

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

HPE Smart Storage Administrator

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

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

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

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

- Accessing HPE SSA in the offline environment

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

Using one of multiple methods, you can run HPE SSA before launching the host operating system. In offline mode, users can configure or maintain detected and supported devices, such as optional Smart

Array controllers and integrated Smart Array controllers. Some HPE SSA features are only available in the offline environment, such as setting the boot controller and boot volume.

- Accessing HPE SSA in the online environment

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

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

USB support

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

External USB functionality

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

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

Redundant ROM support

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

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

Safety and security benefits

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

Keeping the system current

Updating firmware or system ROM

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

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

Service Pack for ProLiant

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

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

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

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

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

Smart Update Manager

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

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

Key features of SUM include:

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

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

Integrated Smart Update Tools

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

- **iSUT:** Polls iLO to check for requests from 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 iSUT. Performs inventory on target servers, stages deployment, deploys updates, and then reboots the servers.

- **iLO 5 with integrated Smart Update** (Gen10 servers only): Performs iLO Repository-based updates by downloading the components from iLO Repository when iLO Installation Queue has the components which can be updated by iSUT.
- **iLO Amplifier Pack**: Displays available updates for servers. Communicates with iSUT (or SUT 1.x) to initiate updates using the iLO Redfish interface. iSUT reports the status of updates to iLO Amplifier Pack via iLO Restful Interface.
- **HPE OneView**: Displays available updates for servers. Communicates with iSUT (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 system software components from the server product page in the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>).

Operating system version support

For information about specific versions of a supported operating system, refer to the [operating system support matrix](#).

HPE Pointnext Portfolio

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

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

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

Utilize the Advisory and Transformation Services in the following areas:

- Private or hybrid cloud computing
- Big data and mobility requirements
- Improving data center infrastructure
- Better use of server, storage, and networking technology

For more information, see the Hewlett Packard Enterprise website:

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

Proactive notifications

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

- Hardware, firmware, and software changes
- Bulletins
- Patches
- Security alerts

You can subscribe to proactive notifications on the [Hewlett Packard Enterprise website](#).

Troubleshooting

NMI functionality

An NMI crash dump enables administrators to create crash dump files when a system is hung and not responding to traditional debugging methods.

An analysis of the crash dump log is an essential part of diagnosing reliability problems, such as hanging operating systems, device drivers, and applications. Many crashes freeze a system, and the only available action for administrators is to cycle the system power. Resetting the system erases any information that could support problem analysis, but the NMI feature preserves that information by performing a memory dump before a hard reset.

To force the OS to invoke the NMI handler and generate a crash dump log, the administrator can use the iLO Virtual NMI feature.

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>).

System battery replacement

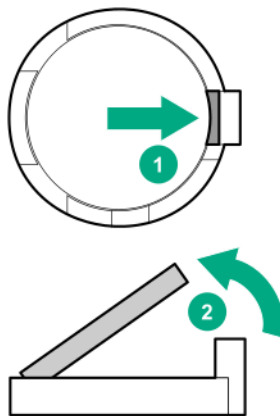
Removing and replacing the system battery

Prerequisites

Before you perform this procedure make sure that you have flat-headed, nonconductive tool.

Procedure

1. If installed, **remove the security bezel**.
2. **Power down the server**.
3. Remove all power:
 - a. Disconnect each power cord from the power source.
 - b. Disconnect each power cord from the server.
4. Do one of the following:
 - **Extend the server from the rack**.
 - **Remove the server from the rack**.
5. **Remove the access panel**.
6. **Locate the battery**.
7. Use a small flat-bladed, nonconductive tool to carefully lift the front of the battery from the socket.



8. To replace the component, reverse the removal procedure.
9. Properly dispose of the old battery.

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

Specifications

Environmental specifications

Specifications	Value
Temperature range*	—
Operating	10°C to 35°C (50°F to 95°F)
Nonoperating	-30°C to 60°C (-22°F to 140°F)
Relative humidity (noncondensing)	—
Operating	8% to 90% 28°C (82.4°F) maximum wet bulb temperature
Nonoperating	5 to 95% 38.7°C (101.7°F) maximum wet bulb temperature
Altitude	—
Operating	3050 m (10,000 ft). This value may be limited by the type and number of options installed. Maximum allowable altitude change rate is 457 m/min (1500 ft/min).
Nonoperating	9144 m (30,000 ft). Maximum allowable altitude change rate is 457 m/min (1500 ft/min).

Standard operating support

10°C to 35°C (50°F to 95°F) at sea level with an altitude derating of 1.0°C per every 305 m (1.8°F per every 1000 ft) above sea level to a maximum of 3050 m (10,000 ft), no direct sustained sunlight. Maximum rate of change is 20°C/hr (36°F/hr). The upper limit and rate of change may be limited by the type and number of options installed.

System performance during standard operating support may be reduced if operating above 30°C (86°F).

Extended ambient operating support

For approved hardware configurations, the supported system inlet range is extended to be: 5°C to 10°C (41°F to 50°F) and 35°C to 40°C (95°F to 104°F) at sea level with an altitude derating of 1.0°C per every 175 m (1.8°F per every 574 ft) above 900 m (2953 ft) to a maximum of 3050 m (10,000 ft). The approved hardware configurations for this system are listed at the [Hewlett Packard Enterprise website](#).

40°C to 45°C (104°F to 113°F) at sea level with an altitude derating of 1.0°C per every 125 m (1.8°F per every 410 ft) above 900 m (2953 ft) to a maximum of 3050 m (10,000 ft). The approved hardware configurations for this system are listed on the [Hewlett Packard Enterprise website](#).

System performance may be reduced if operating in the extended ambient operating range.

Mechanical specifications

Specification	Value
Height	4.32 cm (1.70 in)
Depth	38.22 cm (15.05 in)
Width	43.46 cm (17.11 in)
Weight, maximum	9.46 kg (20.85 lb)
Weight, minimum	6.0 kg (13.22 lb)

Power supply specifications

Depending on the installed options and the regional location where the server was purchased, the server can be configured with one of the following power supplies:

- **ATX 290W Non-hot-plug Power Supply**
- **HPE 500W Flex Slot Platinum Hot-plug Low Halogen Power Supply**
- **HPE 800W Flex Slot -48VDC Hot-plug Low Halogen Power Supply**

These are entry class power supply products for ProLiant Servers. For detailed power supply specifications, see the QuickSpecs on the [Hewlett Packard Enterprise website](#).

ATX 290W Non-Hot-plug Power Supply

Specification	Value
Input requirements	—
Rated input voltage	100 VAC to 240 VAC
Rated input frequency	50 Hz to 60 Hz
Rated input current	5.5 A
Maximum rated input power	550 W
Efficiency	No less than 88% at 100% load No less than 92% at 50% load No less than 88% at 20% load
Power supply output	—
Rated steady-state power	290 W
Maximum peak power	366 W
Rated output power	290 W

HPE 500W Flex Slot Platinum Hot-plug Low Halogen Power Supply

Specification	Value
Input requirements	—
Rated input voltage	100 VAC to 240 VAC 240 VDC for China only
Rated input frequency	50 Hz to 60 Hz Not applicable to 240 VDC
Rated input current	5.8 A at 100 VAC 2.8 A at 200 VAC 2.4 A at 240 VDC for China only
Maximum rated input power	557 W at 100 VAC 539 W at 200 VAC 537 W at 240 VDC for China only
BTUs per hour	1902 at 100 VAC 1840 at 200 VAC 1832 at 240 VDC for China only
Power supply output	—
Rated steady-state power	500 W at 100 VAC to 127 VAC input 500 W at 100 VAC to 240 VAC input 500 W at 240 VDC input for China only
Maximum peak power	500 W at 100 VAC to 127 VAC input 500 W at 100 VAC to 240 VAC input 500 W at 240 VDC input for China only

HPE 800W Flex Slot -48VDC Hot plug Low Halogen Power Supply

Specification	Value
Input requirements	—
Rated input voltage	-40 VDC to -72 VDC -48 VDC
Rated input current	24 A at -40 VDC
Rated input power (W)	874 W at -40 VDC
Rated input power (BTUs per hour)	2983 at -40 VDC

Table Continued

Specification	Value
Power supply output	—
Rated steady-state power (W)	800 W at -40 VDC to -72 VDC
Maximum peak power (W)	800 W at -40 VDC to -72 VDC
Maximum peak power	800 W at 200 VAC to 277 VAC 800 W at -40VDC to -72 VDC

⚠ WARNING: To reduce the risk of electric shock or energy hazards:

- This equipment must be installed by trained service personnel.
- Connect the equipment to a reliably grounded secondary circuit source. A secondary circuit has no direct connection to a primary circuit and derives its power from a transformer, converter, or equivalent isolation device.
- The branch circuit overcurrent protection must be rated 27 A.

⚠ CAUTION: This equipment is designed to permit the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment.

If this connection is made, all of the following must be met:

- This equipment must be connected directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus to which the DC supply system earthing electrode conductor is connected.
- This equipment must be located in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor, and also the point of earthing of the DC system. The DC system must be earthed elsewhere.
- The DC supply source is to be located within the same premises as the equipment.
- Switching or disconnecting devices must not be in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

Safety, warranty, and regulatory information

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

Local representative information

Local representative information Russian

Russia:

ООО «Хьюлетт Паккард Энтерпрайз», Российская Федерация, 125171, г. Москва, Ленинградское шоссе, 16А, стр.3, Телефон/факс: +7 495 797 35 00

Belarus:

ИООО «Хьюлетт-Паккард Бел», Республика Беларусь, 220030, г. Минск, ул. Интернациональная, 36-1, Телефон/факс: +375 17 392 28 20

Kazakhstan:

ТОО «Хьюлетт-Паккард (К)», Республика Казахстан, 050040, г. Алматы, Бостандыкский район, проспект Аль-Фараби, 77/7, Телефон/факс: +7 727 355 35 50

Local representative information Kazakh

Russia:

ЖШС "Хьюлетт Паккард Энтерпрайз" Ресей Федерациясы, 125171, Мәскеу, Ленинград тас жолы, 16А блок 3, Телефон/факс: +7 495 797 35 00

Belarus:

«HEWLETT-PACKARD Bel» ЖШС, Беларусь Республикасы, 220030, Минск қ.,
Интернациональная көшесі, 36/1, Телефон/факс: +375 17 392 28 20

Kazakhstan:

ЖШС «Хьюлетт-Паккард (К)», Қазақстан Республикасы, 050040, Алматы қ.,
Бостандық ауданы, Әл-Фараби даңғылы, 77/7, Телефон/факс: +7 727 355 35 50

Turkey RoHS material content declaration

Türkiye Cumhuriyeti: EEE Yönetmeliğine Uygundur

Ukraine RoHS material content declaration

Обладнання відповідає вимогам Технічного регламенту щодо обмеження використання деяких небезпечних речовин в електричному та електронному обладнанні, затвердженого постановою Кабінету Міністрів України від 3 грудня 2008 № 1057

GS Gloss declaration

The product is not suitable for use at visual display workplaces according to §2 of the German Ordinance for Work with Visual Display Units.

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Subscription Service/Support Alerts

www.hpe.com/support/e-updates

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 general support websites, see [Support and other resources](#).

Product websites

Product QuickSpecs

<http://www.hpe.com/servers/dl20-gen10>

HPE ProLiant DL20 Gen10 support page

<http://www.hpe.com/support/dl20gen10>

HPE ProLiant DL20 Gen10 user documents

<http://www.hpe.com/info/dl20gen10-docs>

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

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/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

ClearCARE technical support

Support for ClearOS and ClearVM is not provided by Hewlett Packard Enterprise. Support for ClearOS and ClearVM is purchased and delivered by ClearCenter. You can purchase single support incidents by submitting a support ticket to ClearCenter, or you can purchase a Bronze, Silver, Gold, or Platinum ClearCARE subscription. For more information, go to the ClearOS website:

<https://www.clearos.com/>

Several levels of professional technical support are available to licensed users. For more information, go to the ClearCARE support website:

<https://www.clearos.com/products/support/clearcare-overview>

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

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.

Acronyms and abbreviations

AHS

Active Health System

AHSV

Active Health System Viewer

API

application program interface

CAS

column address strobe

CSA

Canadian Standards Association

CSR

customer self repair

DDR4

double data rate-4

FCoE

Fibre Channel over Ethernet

HPE SSA

HPE Smart Storage Administrator

IEC

International Electrotechnical Commission

iLO

Integrated Lights-Out

IML

Integrated Management Log

ISO

International Organization for Standardization

iSUT

Integrated Smart Update Tools

LFF

large form factor

LRDIMM

load reduced dual in-line memory module

NMI

nonmaskable interrupt

NVMe

nonvolatile memory express

PCA

printed circuit assembly

PCIe

Peripheral Component Interconnect Express

PDU

power distribution unit

POST

Power-On Self-Test

PXE

Preboot eXecution Environment

QR code

quick response code

RBSU

ROM-Based Setup Utility

RDIMM

registered dual in-line memory module

REACH

Registration, Evaluation, Authorization, Restriction of Chemicals (European Union chemical regulatory framework)

REST

representational state transfer

RoHS

Restriction of Hazardous Substances

SAS

serial attached SCSI

SATA

serial ATA

SFF

small form factor

STK

scripting toolkit

SPP

Service Pack for ProLiant

SSD

solid state device

SUM

Smart Update Manager

SUT

Smart Update Tools

TMRA

recommended ambient operating temperature

TPM

Trusted Platform Module

UDIMM

unbuffered dual in-line memory module

UEFI

Unified Extensible Firmware Interface

UID

unit identification

UPS

uninterruptible power supply