Hewlett Packard
Enterprise

HPE ProLiant Thin Micro TM200 Server User Guide

Abstract

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

Part Number: 868923-002a
Published: October 2017
Edition: 3

Notices

Acknowledgments

Intel® and Xeon® are trademarks of Intel Corporation in the U.S. and other countries.

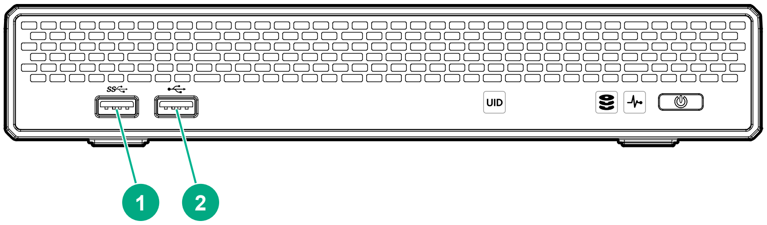
Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Windows® is either a registered trademark or trademark of the Microsoft Corporation in the Unites States and/or other countries.

Contents

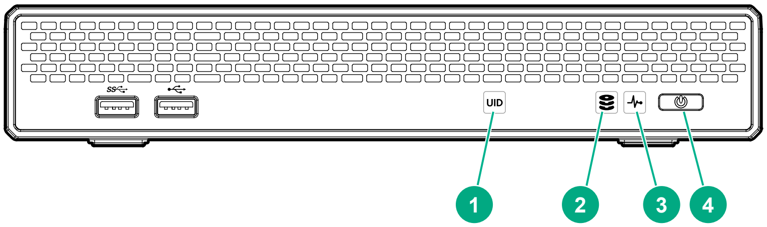
Component identification

Front panel components



Item	Description
1	USB 3.0 port
2	USB 2.0 port

Front panel LEDs and button



Item	Description	Status
1	UID LED	Solid blue = Activated Flashing blue = Remote management or firmware upgrade in progress Off = Deactivated
2	Drive LED	Flashing white = Ongoing drive activity Off = No drive activity This LED reflects the status of the drives installed in the server and in the storage expansion unit.

Table Continued

Item	Description	Status
3	Health LED	Solid white = Normal Flashing amber = System degraded Flashing red (1 flash per second) = System critical
4	Power On/Standby button/LED	Solid white = System on Flashing white = Performing power on sequence Solid red = System in standby Flashing red = Unsuccessful power on sequence. When the 120 W power adapter is connected to a server that is attached to a storage expansion unit, the system power LED flashes red. Replace the 120 W power adapter with the 180 W power adapter that shipped with the storage expansion unit option kit. Off = No power present If the system power LED is off, verify the following conditions: • Facility power is present. • The power adapter is connected to the server. • The power cord is attached to the adapter and is plugged into a power source.

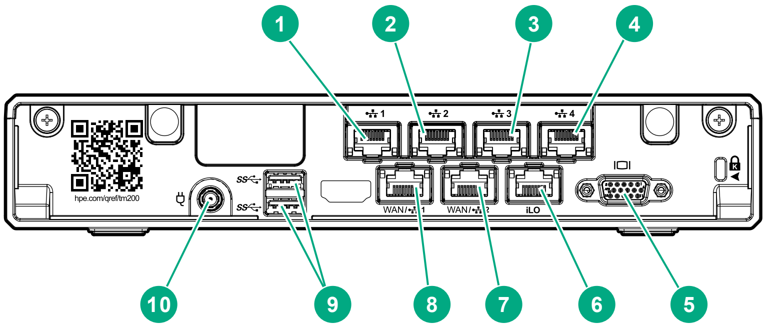
When all LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see **Front panel LED power fault codes**.

Front panel LED power fault codes

The following table provides a list of power fault codes, and the subsystems that are affected.

Subsystem	Front panel LED behavior
System board	1 flash
Processor	2 flashes
Memory	3 flashes

Rear panel components

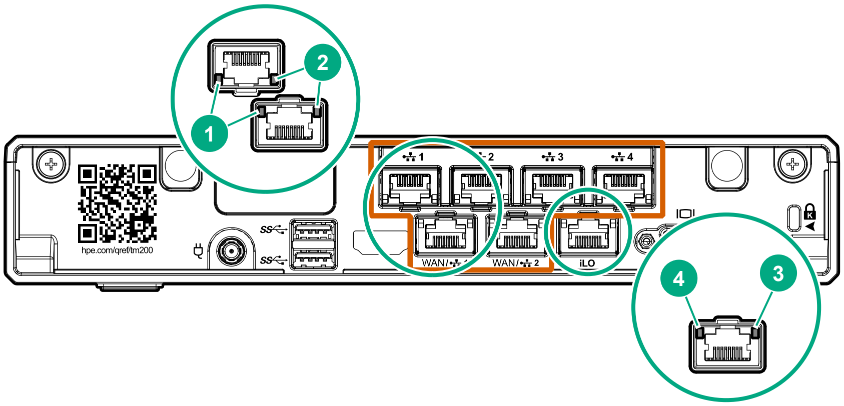


Item	Description
1	LAN port 1[1]
2	LAN port 2[1]
3	LAN port 3[1]
4	LAN port 4[1]
5	VGA port
6	iLO Management Port[2]
7	WAN/LAN port 2[2]
8	WAN/LAN port 1[2]
9	USB 3.0 ports (2)
10	Power adapter jack

[1] *This connector is on the communication board.*

[2] *This connector is on the system board.*

Rear panel LEDs and button



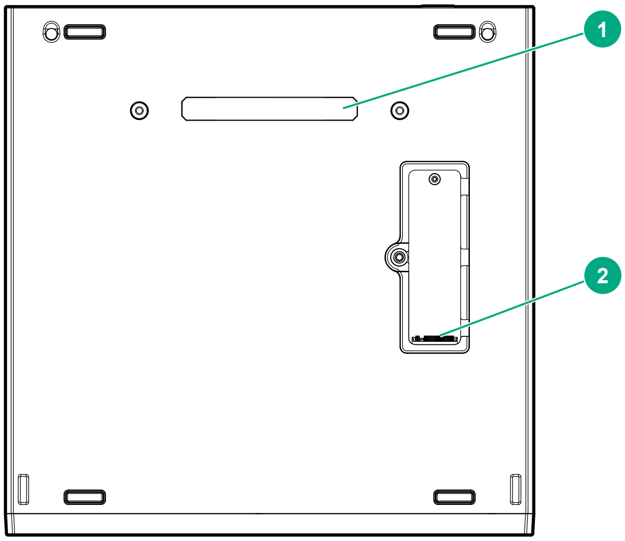
Item	Description	Status
1	NIC link LED	Solid green = Link exists Off = No link exists
2	NIC status LED	Solid green = Linked to network Flashing green = Network active Off = No network activity

Table Continued

Item	Description	Status
3	iLO status LED	Solid green = Linked to network Flashing green = Network active Off = No network activity

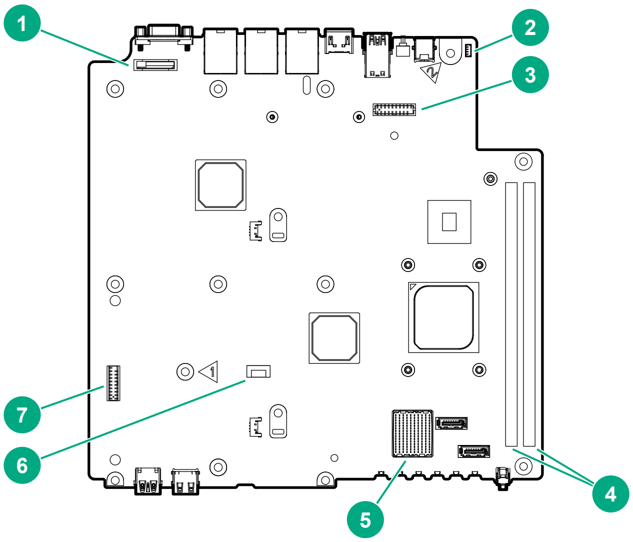
4	iLO link LED	Green = Network link
		Off = No network link

Bottom components



Item	Description
1	Dock connector (for storage expansion unit installation)
2	M.2 SSD compartment

System board components



Item	Description
1	System battery
2	Fan connector
3	TPM connector
4	DIMM slots
5	Communication board connector
6	Ambient temperature sensor connector
7	System maintenance switch

System maintenance switch

Position	Default	Function

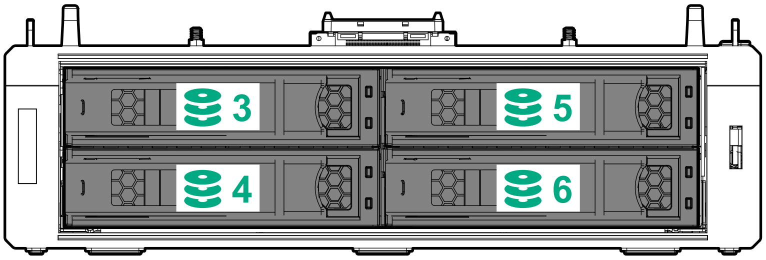
S1	Off	Off = iLO 4 security is enabled.
		On = iLO 4 security is disabled.

S2	Off	Off = System configuration can be changed. On = System configuration is locked.
S5	Off	Off = Power-on password is enabled. On = Power-on password is disabled.
S6	Off	Off = No function On = ROM reads system configuration as invalid.
S3, S4, S7, S8, S9, S10, S11, and S12	—	Reserved

You can access the redundant ROM by setting S1, S5, and S6 to On.

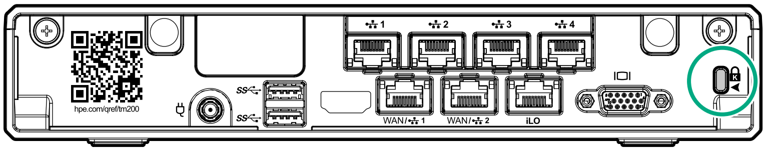
When the system maintenance S6 switch is set to the On position, the system will erase all system configuration settings from both CMOS and NVRAM on the next reboot. Clearing CMOS, NVRAM, or both delete configuration information. Be sure to configure the server properly to prevent data loss.

Storage expansion unit drive numbering

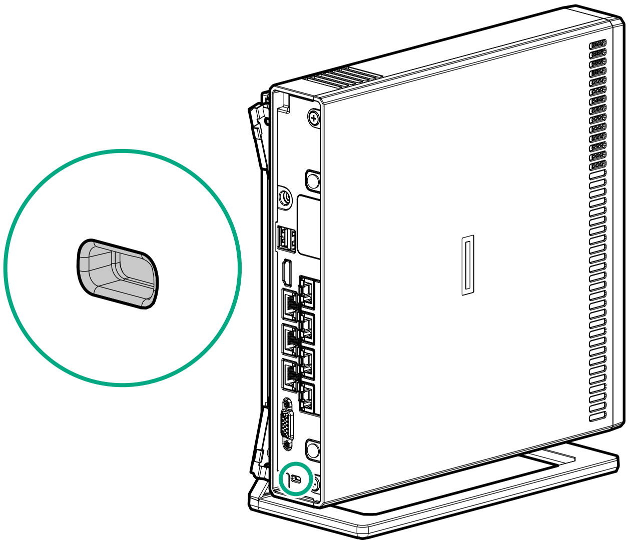


Kensington security slot locations

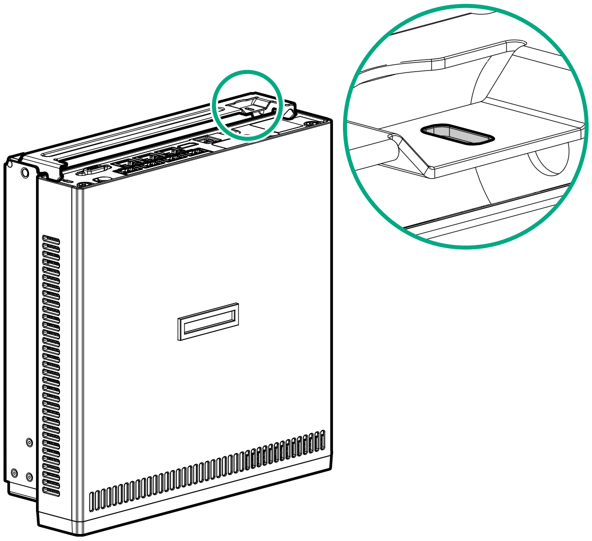
- Kensington security slot in a server in the desktop position – Use a Kensington cable lock.



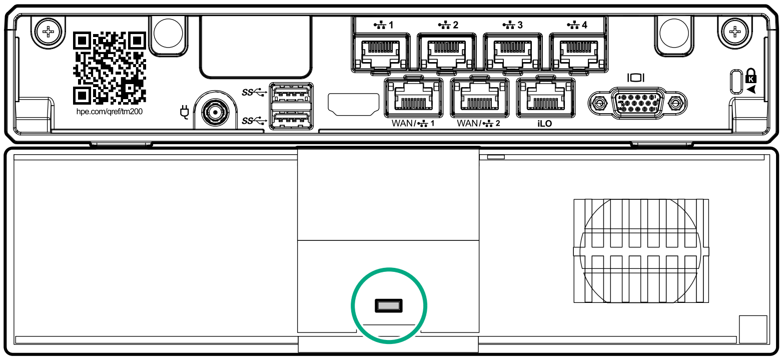
- Kensington security slot in a server installed in the cradle – Use a Kensington cable lock.



- Kensington security slot in the wall mount – Use a Kensington noncable lock or a cable lock that includes a wall mount anchor.

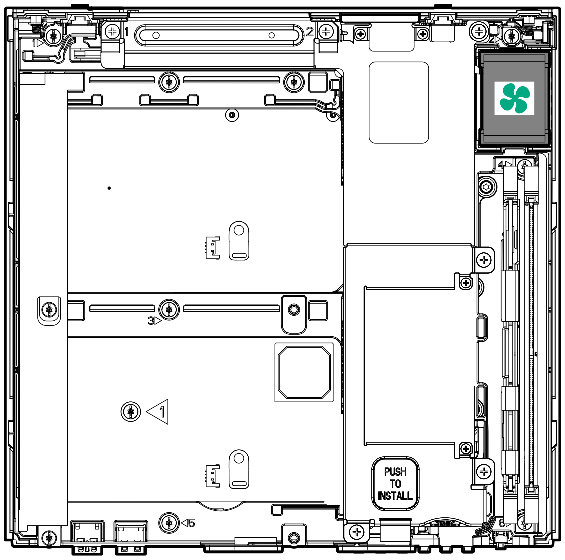


- Kensington security slot in the storage expansion unit – Use a Kensington cable lock.

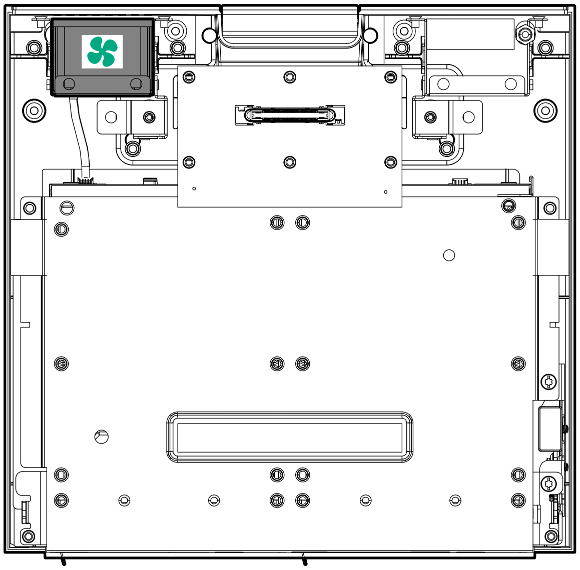


Fan locations

- Fan location in the server



- Fan location in the storage expansion unit



Setup

Optional service

Delivered by experienced, certified engineers, HPE support services help you keep your servers up and running with support packages tailored specifically for HPE ProLiant systems. HPE 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.

HPE 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 HPE support services for hardware, software or both are:

- Foundation Care – Keep systems running.
  - 6-Hour Call-to-Repair[1]
  - 4-Hour 24x7
  - Next Business Day
- Proactive Care – Help prevent service incidents and get you to technical experts when there is one.
  - 6-Hour Call-to-Repair[1]
  - 4-Hour 24x7
  - Next Business Day
- Deployment service for both hardware and software
- HPE Education Services – Help train your IT staff.

[1]The 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 **HPE support center**.

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

Optimum environment

When installing theserver, select a location that meets the environmental requirements described in this section.

Operating environmental requirements

The server may be located in an office space or a purpose-made equipment room. The location must:

- Comply with local health and safety regulations.
- Be clean, tidy, and free of excessive dust and vibration and have an ambient temperature of between 10°C to 35°C (50°F to 95°F).
- Make sure that there is a minimum clearance of 30 cm (11.81 in) around the ventilation openings.

  The server draws in cool air through the ventilation openings on the left side, and expels warm air through the ventilation openings on right side. Do not block these openings. Failure to observe this caution will result in improper airflow and insufficient cooling that can lead to thermal damage.
- Offer space, ideally 1.00 m (3.28 ft) at the front and rear, for an authorized technician to access the server and cable it.
- Possess a reliable power source no more than 1.50 m (4.92 ft) from the server location or, ideally be protected by a UPS.
- Be in an area in which the server cannot easily be disconnected from their power source or by staff such as housekeeping.
- Not be adjacent to or underneath any area or piece of equipment where liquid is stored.
- Not be in a place where the server might be bumped, scratched, or disturbed.

- Be within an area that is ideally locked or at minimum not accessible by unauthorized personnel.
- Be within patching distance, directly or through cable management cross-patches, of the location of the WAN connection and the switch that supplies the office/room floor ports.

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 server. Consult the electrical authority having jurisdiction over wiring and installation requirements of your facility.

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

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

- Balance the server power load between available AC supply branch circuits.
- Do not allow the overall system AC current load to exceed 80% of the branch circuit AC current rating.
- Do not use common power outlet strips for this equipment.
- Provide a separate electrical circuit for the server.

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.

Prerequisites for preparing the server for installation

About this task

Before installation, the user must:

- **Verify that the optimum environmental requirements are satisfied**.
- Confirm that the installation engineer understands how to integrate the server into the user network, in particular from an IP addressing perspective and from a domain perspective.

- Prepare Ethernet cables of an appropriate length for each of the LAN, WAN, and remote management (iLO) connections.
- Verify that there are sufficient ports available on the devices to which the server will be connected (for example, router, LAN switch).

Identifying the contents of the server shipping carton

About this task

Unpack the server shipping carton and locate the materials and documentation necessary for installing the server.

The contents of the server shipping carton include:

- Server
- Power adapter (120 W)
- Power cord
- Printed setup documentation

Installing the server on the mounting/docking hardware

About this task

If you intend to set up the server in a cradle, wall mount, or storage expansion unit:

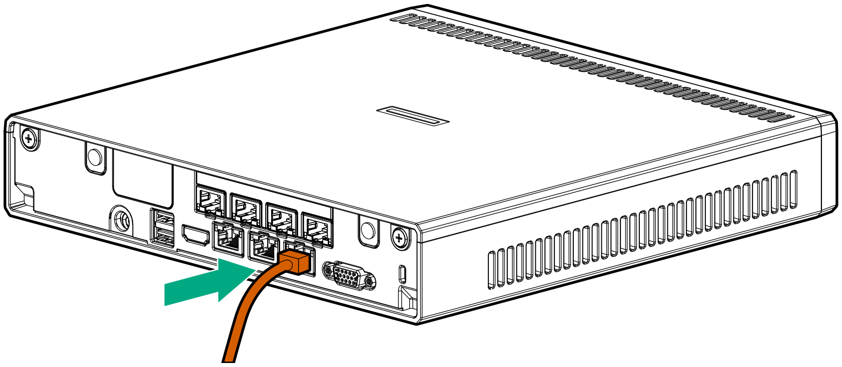
- **Install the server in the cradle**.
- **Install the server in the wall mount**.
- **Install the server on the storage expansion unit**.

Do not connect the power cord to the power source yet.

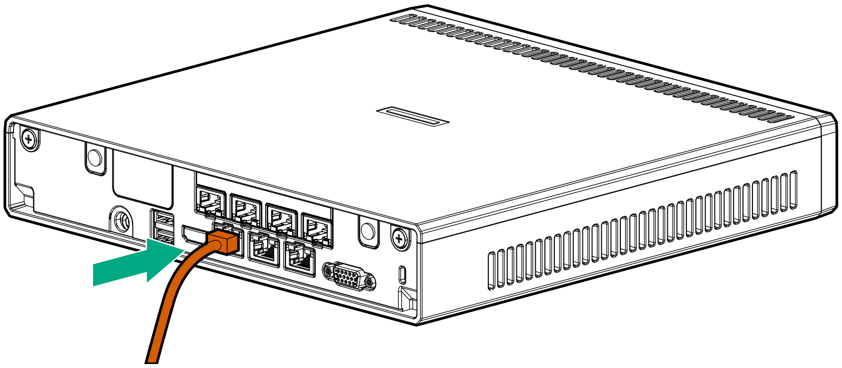
Connecting the network and peripheral cabling

Procedure

1. Connect the iLO cabling.



2. Connect the network cabling.

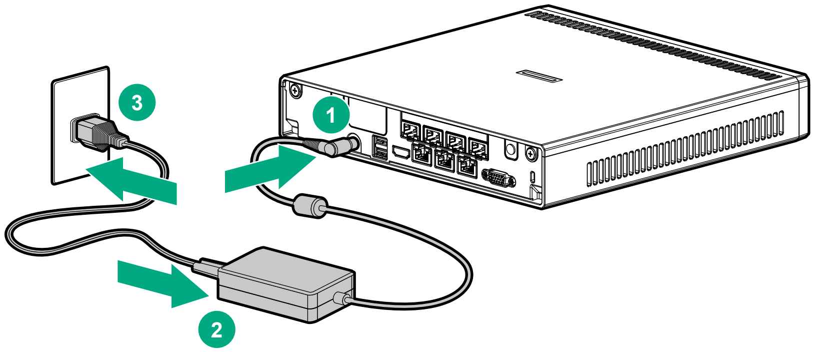


3. Connect all peripheral cabling to the server.

Connecting the power cord and powering on the server

Procedure

1. Connect the power cord:
   a. Connect the power adapter to the server.
   b. Connect the power cord to the adapter.
   c. Connect the power cord to the power source.



2. Secure the power cord and rear panel cables based on the standard cable management practices.
3. **Power up the server**.

Installing an operating system (OS)

About this task

To operate properly, the server must have a supported operating system. For information on supported operating systems, contact your authorized HPE representative.

This server supports Class 3 UEFI implementation. UEFI Class 3 implementation only supports UEFI Boot Mode; there is no support for Legacy BIOS Boot Mode. To prevent errors in installing the operating system, recognizing boot media, and other boot-related errors, observe the relevant UEFI requirements. For more information on these requirements, see *Important UEFI Requirements (for HPE ProLiant Thin Micro Servers)* on the **Hewlett Packard Enterprise website**.

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

Procedure

- Manual installation – Insert the operating system disc into a USB-attached DVD-ROM drive (user provided) and reboot the server.
- Remote deployment installation – Use Insight Control server provisioning for an automated solution to remotely deploy an operating system.

For additional system drivers, firmware, and software updates, download the Service Pack for ProLiant from the **Hewlett Packard Enterprise website**. Update the software and firmware before using the server for the first time, unless any installed software or components require an older version.

For more information on using these installation methods, see the **Hewlett Packard Enterprise website**.

Registering for HPE remote support

About this task

HPE remote support provides automatic submission of hardware events to Hewlett Packard Enterprise to prevent downtime and enable faster issue resolution. You can register directly to Hewlett Packard Enterprise or through an Insight RS Hosting Device. For more information, see the Insight Control documentation on the **Hewlett Packard Enterprise website**.

Operations

Server warnings and cautions

WARNING:
To reduce the risk of personal injury, electric shock, or damage to the equipment, remove power from the server by removing the power cord. The front panel Power On/Standby button does not shut off system power. Portions of the power supply and some internal circuitry remain active until AC power is removed.

WARNING:
To reduce the risk of electric, shock, fire, or damage to the equipment, only display devices that are qualified to be made of fire-retardant material must be connected to the VGA port on the rear panel.

WARNING:
To reduce the risk of any serious safety issues, do not install or remove the equipment. The installation and maintenance of this equipment must be carried out by qualified or approved personnel. Refer all maintenance, upgrades, and servicing to an authorized reseller or an authorized service provider.

WARNING:
請勿任意拆裝設備。任何未經授權或認證人員之設備拆裝可能造成嚴重的安全問題。任何問題，請洽您的銷售人員或經銷商尋求協助。

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 ESD.

CAUTION:
To prevent improper cooling and thermal damage, do not operate the server with the access panel and the M.2 SSD compartment cover open or removed.

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

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.

Electrostatic discharge

Preventing electrostatic discharge

About this task

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

To prevent electrostatic damage:

Procedure

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

Grounding methods to prevent electrostatic discharge

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

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

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

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

Power up the server

About this task

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

The server exits standby mode and applies full power to the system. **The system power LED changes from red to white**.

Power down the server

Prerequisites

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

Procedure

- 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 four 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.

A red system power LED means that the server is in standby mode. Auxiliary power is still present in the system in this mode. **Verify that the system power LED on the server is red**.

Prepare the server for hardware installation or removal

Prerequisites

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

Procedure

1. **Power down the server**.
2. Disconnect the power cord from the AC source, and then disconnect the power adapter from the server.
3. Disconnect all peripheral cables from the server.
4. If installed, unlock and remove the Kensington security lock.

   For more information, see the Kensington security lock documentation.

Prepare the server for operation

Procedure

1. If removed, install the Kensington security lock.

   For more information, see the Kensington security lock documentation.
2. Connect all peripheral cables to the server.
3. Connect the power adapter to the server, and then connect the power cord to the AC source.
4. Secure the power cord and rear panel cables based on the standard cable management practices.
5. **Power up the server**.

Remove the server from the mounting/docking hardware

About this task

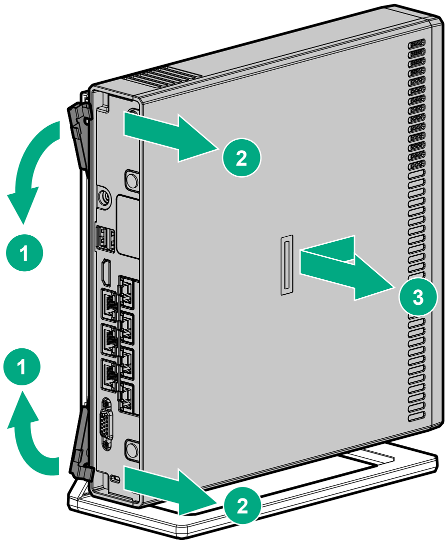
If the server is installed in a cradle, wall mount, or storage expansion unit:

- **Remove the server from the cradle**.
- **Remove the server from the wall mount**.
- **Remove the server from the storage expansion unit**.

Remove the server from the cradle

Procedure

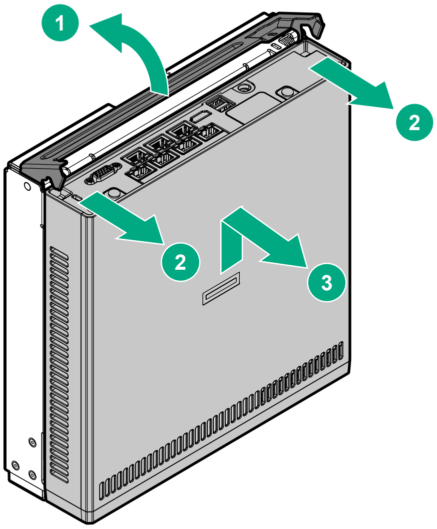
1. Open the latches on the cradle.
2. Remove the server from the cradle.



Remove the server from the wall mount

Procedure

1. Open the wall mount latch.
2. Remove the server from the wall mount.



Remove the server from the storage expansion unit

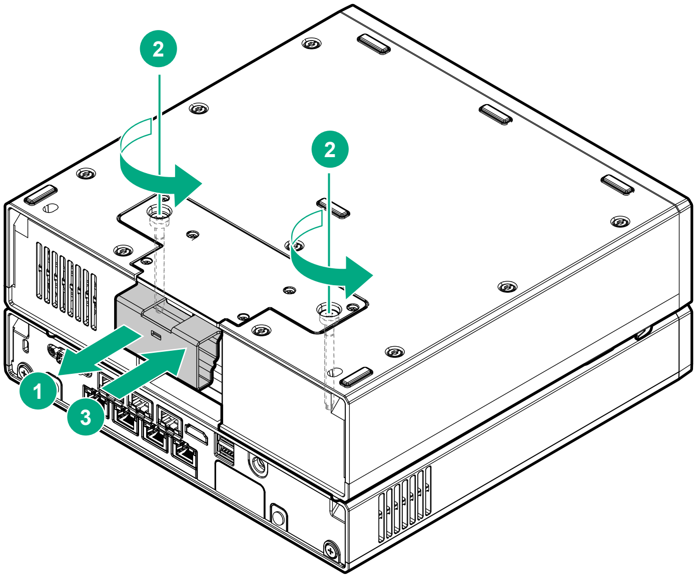
Prerequisites

Before you perform this procedure, make sure that you have a No. 2 Phillips screwdriver available.

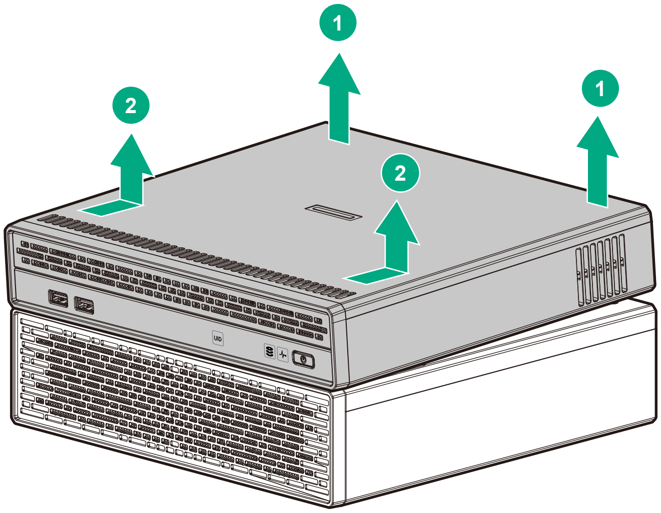
Procedure

1. Hold the top side of the server and the bottom side of the storage expansion unit, and then carefully turn the assembly over to access the bottom side of the storage expansion unit.
2. Remove the server from the storage expansion unit:

a. Pull the latch on the rear of the storage expansion unit.
b. Loosen the captive screws.
c. Push the latch back in place.



d. Return the assembly to an upright position.
e. Remove the server from the storage expansion unit.



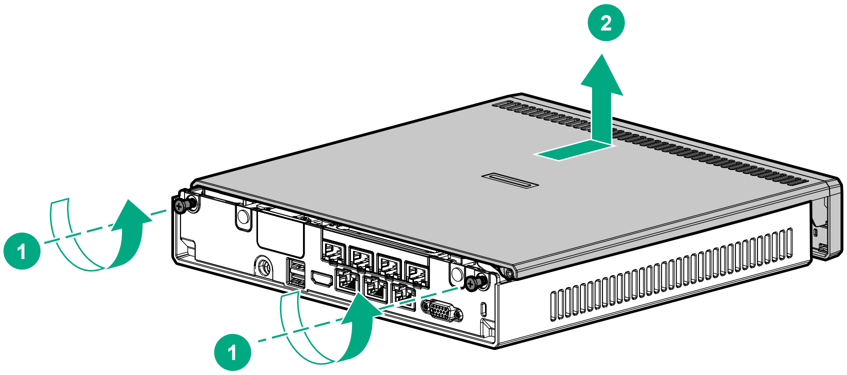
Remove the access panel

Prerequisites

Before you perform this procedure, make sure that you have a No. 2 Phillips screwdriver available.

Procedure

1. Loosen the captive screws.
2. Slide the access panel toward the front of the server, and then lift it from the server.



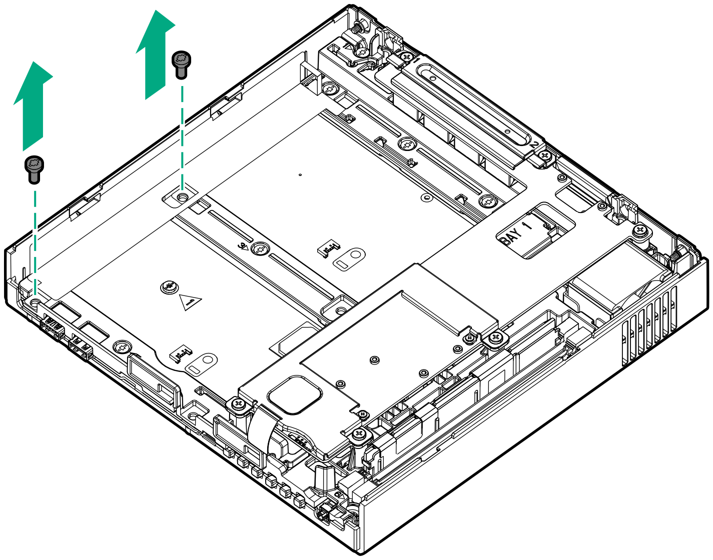
Remove the thermal sheet

Prerequisites

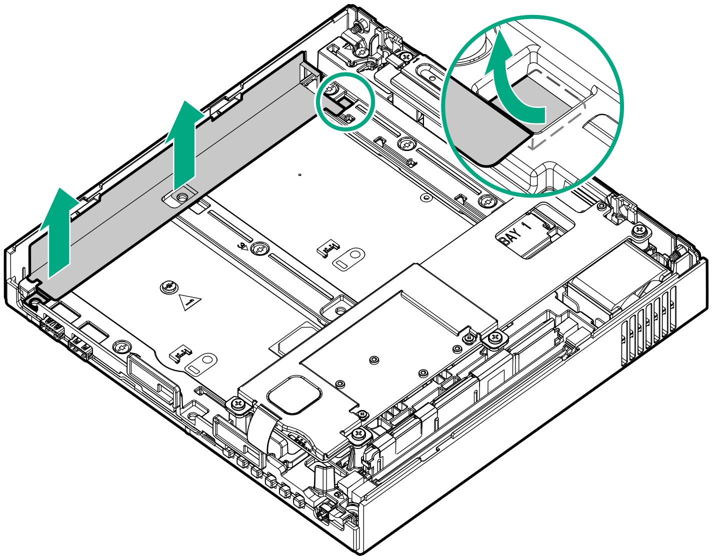
Before you perform this procedure, make sure that you have a T-15 Torx screwdriver available.

Procedure

1. Remove the thermal sheet screws.



2. Remove the thermal sheet.



Remove the communication board

Prerequisites

- Before you perform this procedure, make sure that you have a No. 2 Phillips screwdriver available.
- Before installing the hardware option, make sure that you understand the following warning and cautions.

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

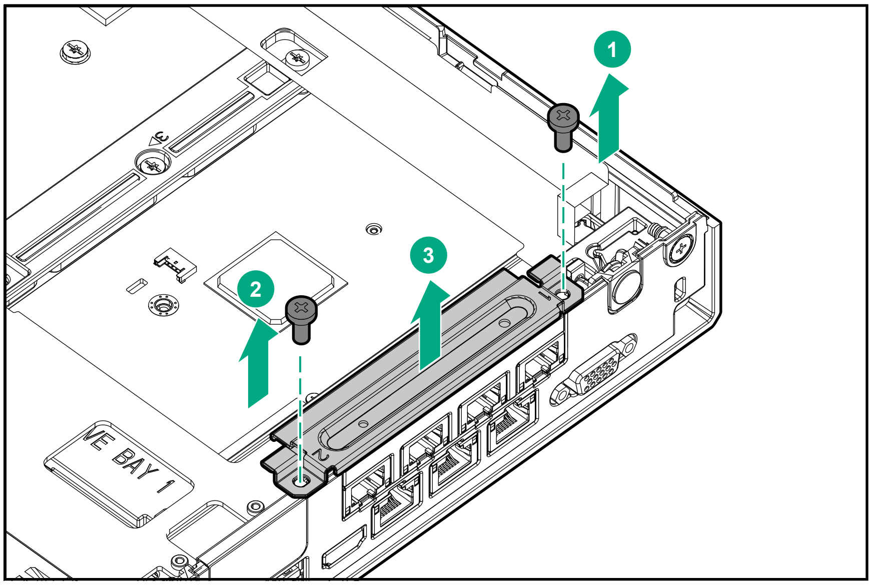
△ **CAUTION:**
To prevent damage to electrical components, properly ground the server before beginning any installation procedure. Improper grounding can cause ESD.

△ **CAUTION:**
To prevent improper cooling and thermal damage, do not operate the server with the access panel and the M.2 SSD compartment cover open or removed.

Procedure

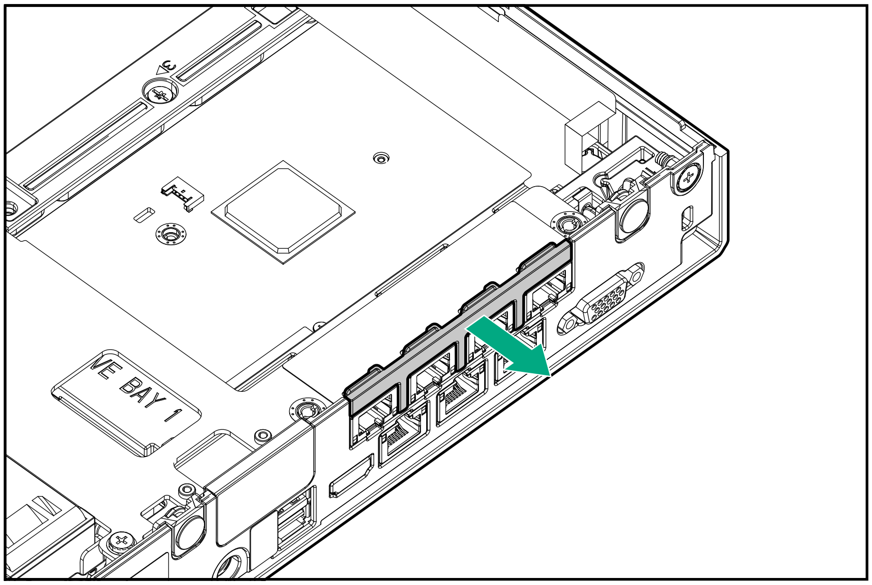
1. Remove the RJ-45 port bracket.

   Retain the screws for later use.

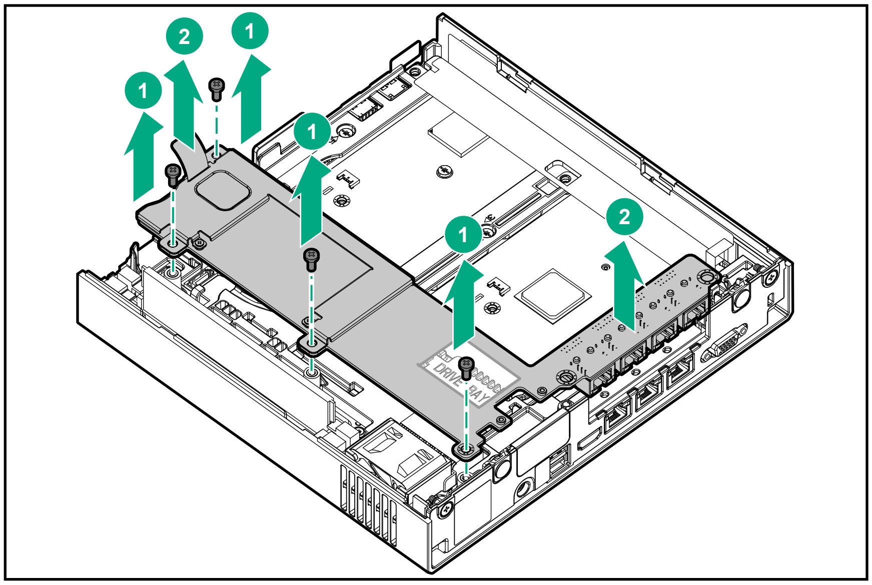


2. Remove the RJ-45 port spacer.

   Retain the blank for later use.



3. Remove the communication board.



Remove the middle frame

Prerequisites

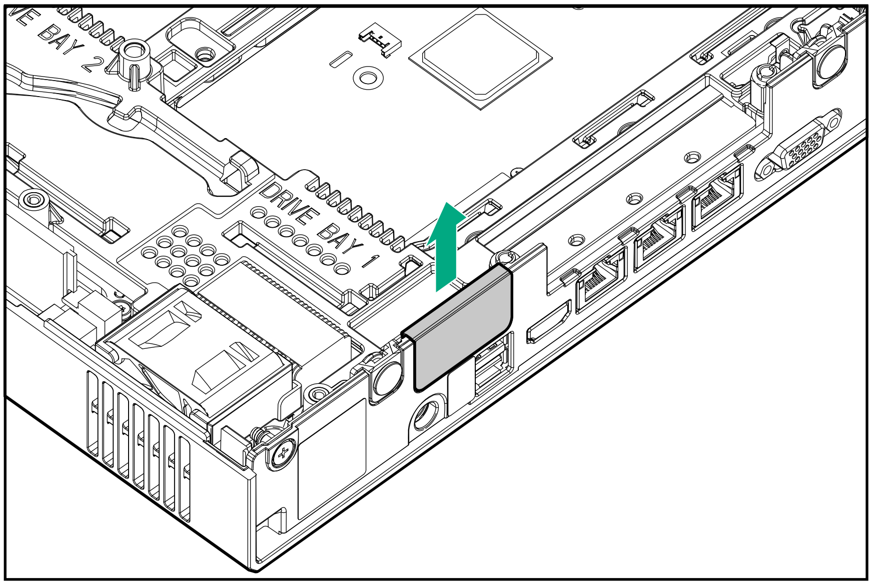
Before you perform this procedure, make sure that you have the following tools available:

- T-15 Torx screwdriver
- Flathead screwdriver

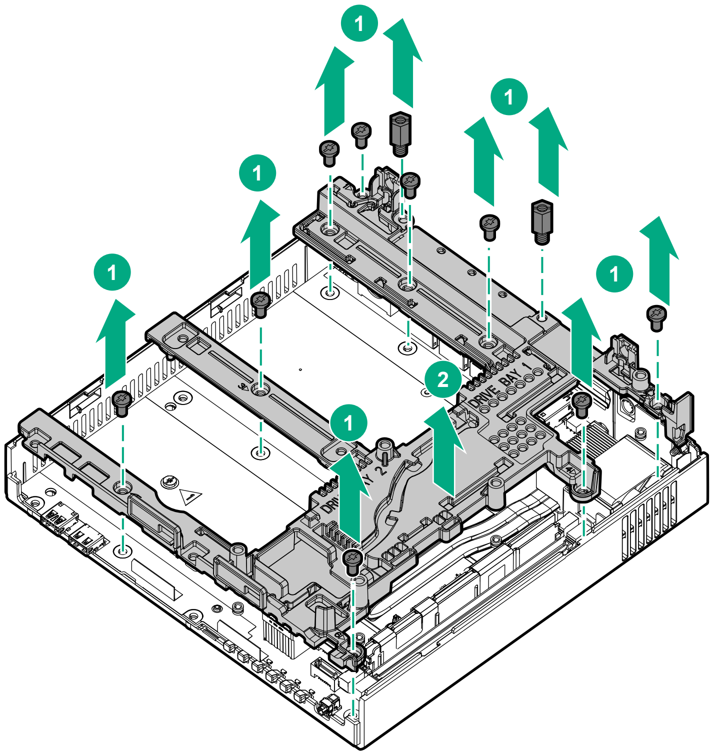
Procedure

1. Remove the RJ-11 port blank.

   Retain the blank for later use.



2. Remove the middle frame from the server:
   a. Remove the screws and standoffs securing the middle frame.
   b. Lift the middle frame from the system board.



Install the middle frame

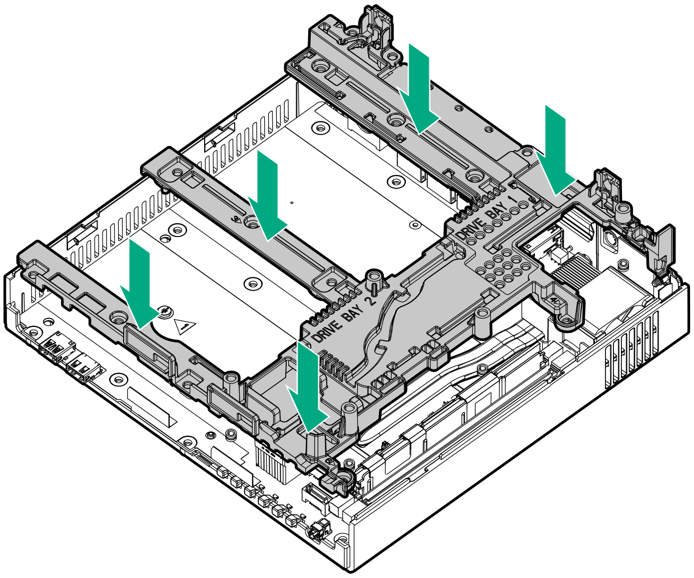
Prerequisites

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

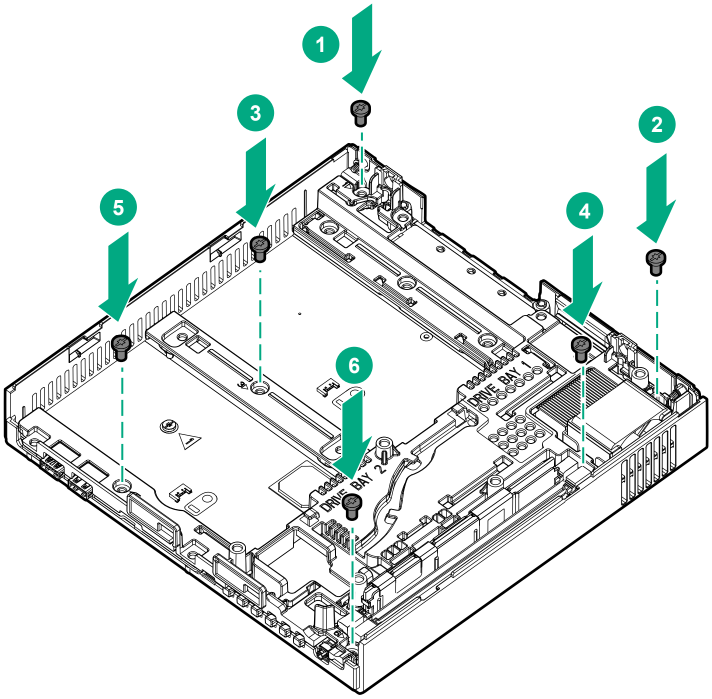
- T-15 Torx screwdriver
- Flathead screwdriver

Procedure

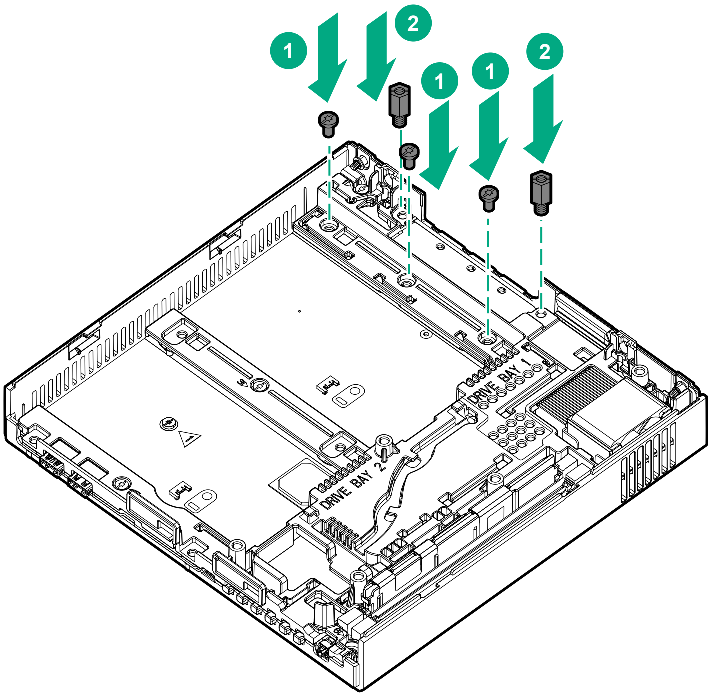
1. Align the middle frame with the system board.



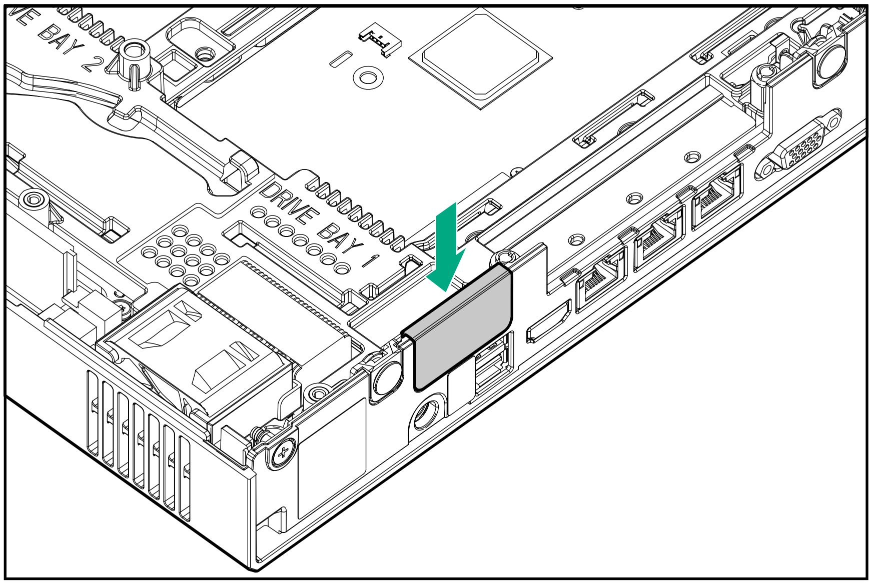
2. Install the first six screws according to the numbering indicated on the middle frame.



3. Install the remaining screws and standoffs on the middle frame.



4. Install the RJ-11 port blank.



Install the communication board

Prerequisites

- Before you perform this procedure, make sure that you have a No. 2 Phillips screwdriver available.
- Before installing the hardware option, make sure that you understand the following warning and caution.

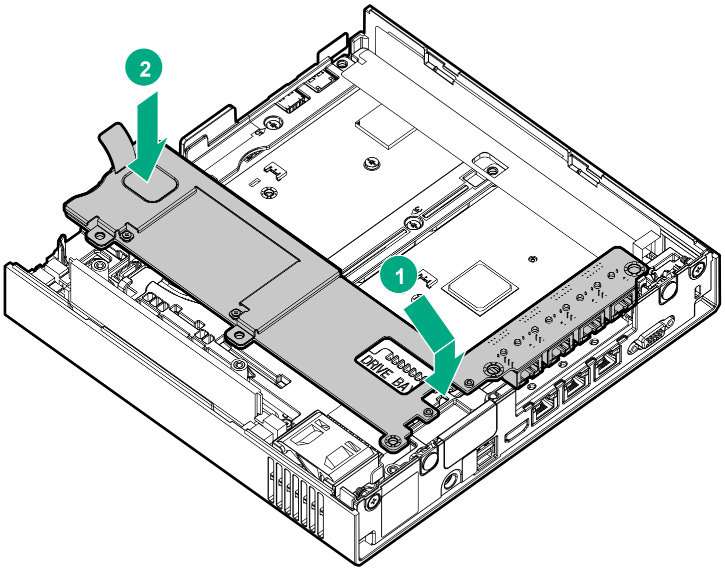
⚠ **WARNING:**
To reduce the risk of personal injury from hot surfaces, allow the drives and the internal system components to cool before touching them.

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

CAUTION:
To prevent improper cooling and thermal damage, do not operate the server with the access panel and the M.2 SSD compartment cover open or removed.

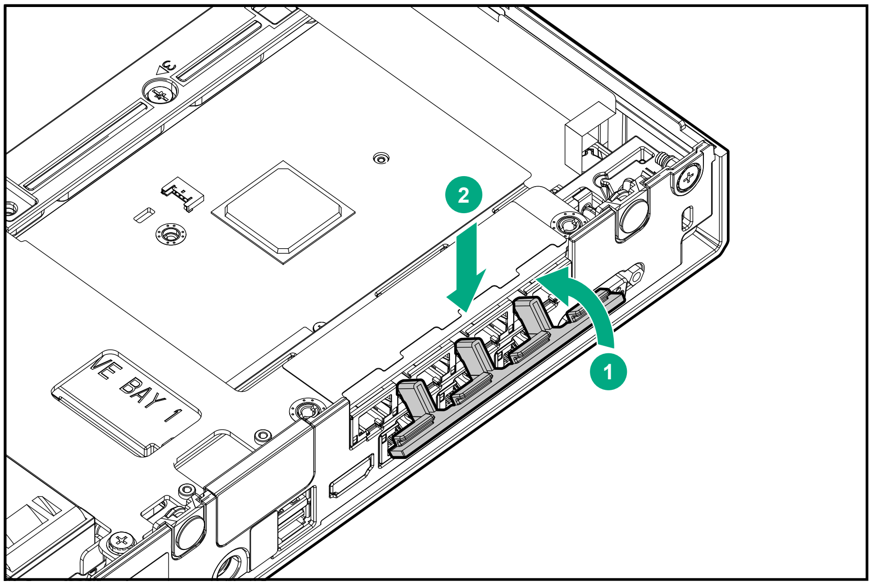
Procedure

1. Align the rear screw holes of the communication board to the middle frame.
2. Press the front end of the communication board until it clicks into place.

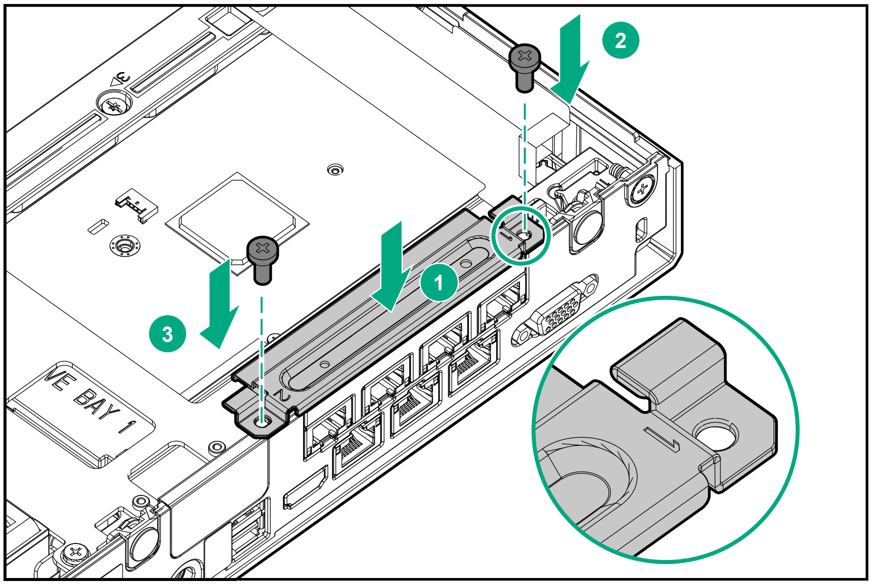


3. Install the RJ-45 port spacer.

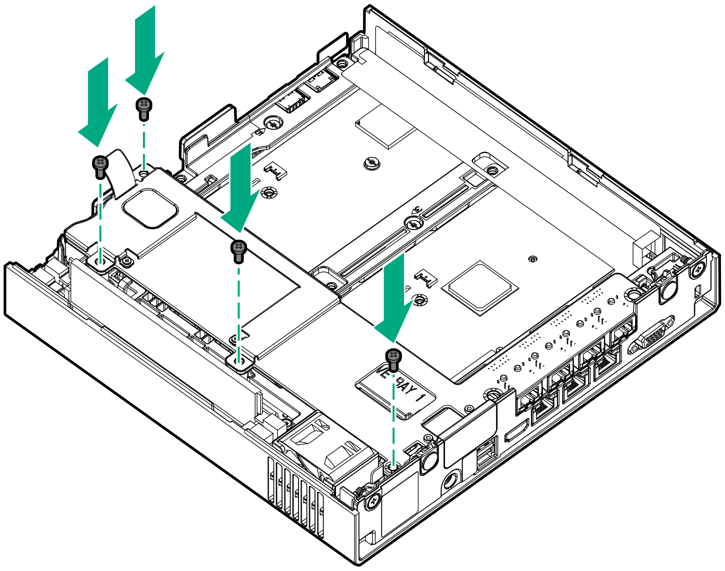
   Ensure that the spacer is flush against the rear panel surface.



4. Align the RJ-45 port bracket to the middle frame.
5. Install the RJ-45 port bracket screws according to the numbering indicated on the bracket.



6. Install the communication board screws.



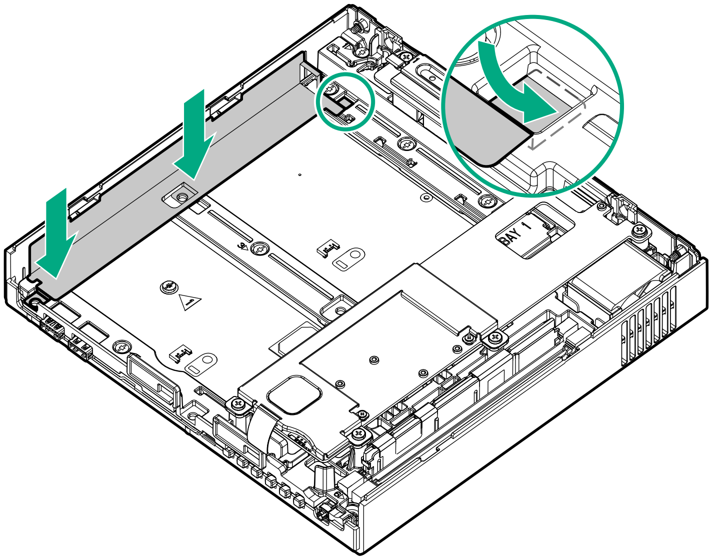
Install the thermal sheet

Prerequisites

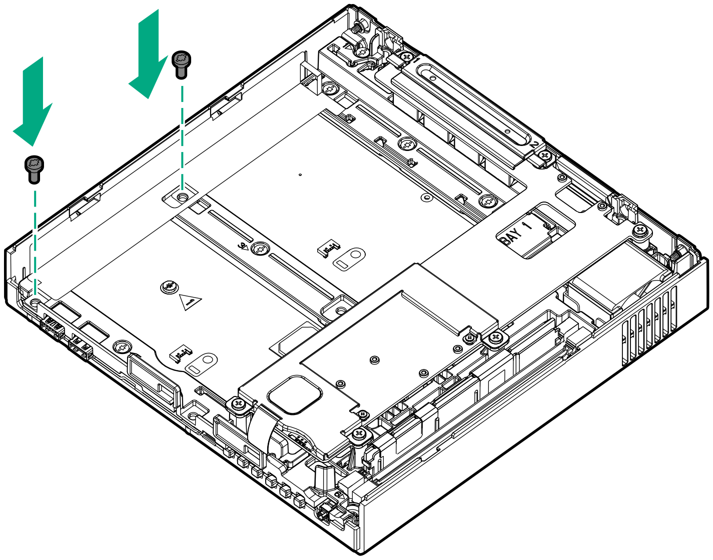
Before you perform this procedure, make sure that you have a T-15 Torx screwdriver available.

Procedure

1. Install the thermal sheet.



2. Install the thermal sheet screws.



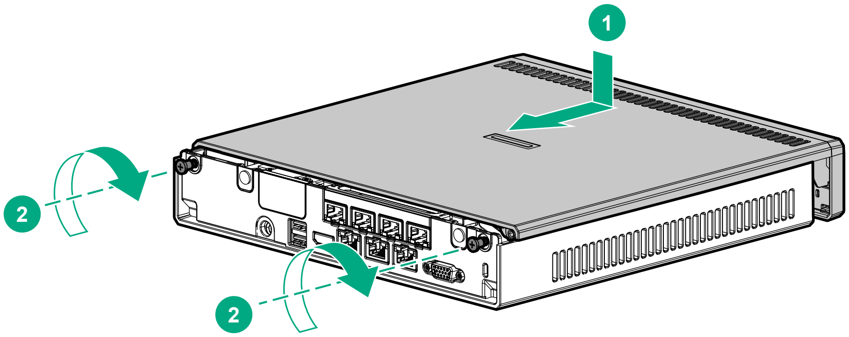
Install the access panel

Prerequisites

Before you perform this procedure, make sure that you have a No. 2 Phillips screwdriver available.

Procedure

1. Slide the access panel toward the rear of the server.
2. Tighten the captive screws.


1
2
2

Hardware options installation

Introduction

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

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

△ **CAUTION:**
To prevent damage to electrical components, take the appropriate anti-static precautions before beginning any installation, removal, or replacement procedure. Improper grounding can cause electrostatic discharge.

Installing the server in the cradle

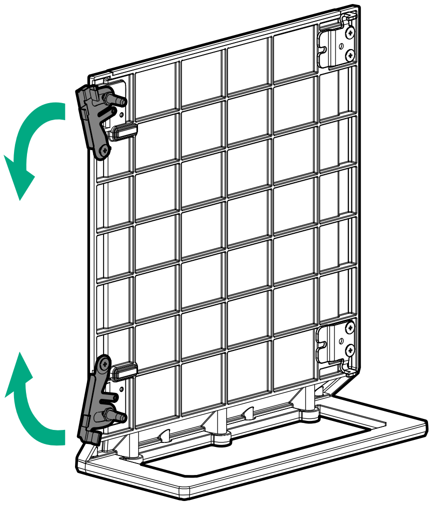
Procedure

1. **Prepare the server for hardware installation or removal**.
2. If the server is installed in a wall mount or on a storage expansion unit:
   - **Remove the server from the wall mount**.
   - **Remove the server from the storage expansion unit**.
3. **Install the server in the cradle**.
4. **Prepare the server for operation**.

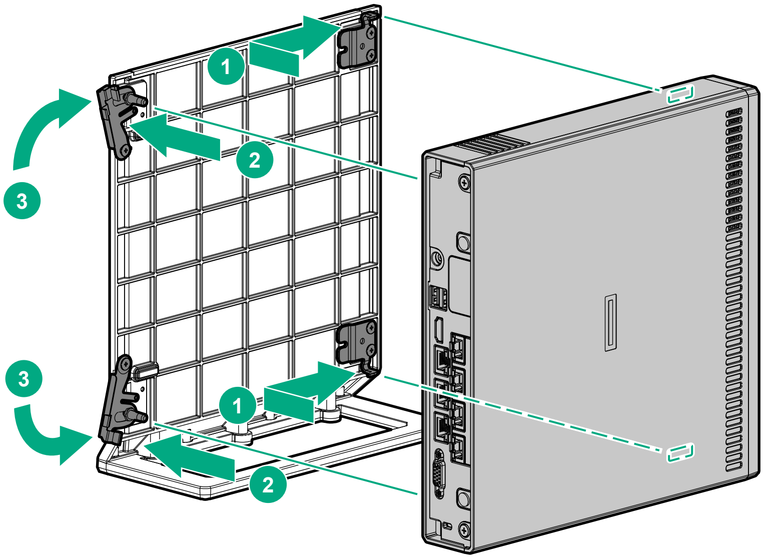
Install the server in the cradle

Procedure

1. Place the cradle on a level, sturdy surface.
2. Open the latches on the cradle.



3. Orient the server in a vertical position with the rear panel facing the cradle latches.
4. Install the server in the cradle:
   a. Insert the two hooks on the right side of the cradle into the corresponding openings on the bottom of the server.
   b. Align and insert the two posts on the cradle into the corresponding openings on the bottom of the server.
   c. Close the latches on the cradle.



Installing the server in the wall mount

Prerequisites

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

- Stud finder (if installing the wall mount on a hollow wall)
- Wall marker
- Level
- Electric drill
- Small wire brush (for cleaning the pilot holes)
- No. 2 Phillips screwdriver
- Hammer

Procedure

1. **Determine the location for the wall mount**.
2. **Prepare the server for hardware installation or removal**.
3. If the server is installed in a cradle or on a storage expansion unit:
   - **Remove the server from the cradle**.
   - **Remove the server from the storage expansion unit**.
4. **Install the wall mount**.
5. **Install the server in the wall mount**.
6. **Prepare the server for operation**.

Determine the location for the wall mount

About this task

Observe the following when determining the installation site for the wall mount:

- Make sure that there is a minimum clearance of 30 cm (11.81 in) around the ventilation openings.

  The server draws in cool air through the ventilation openings on the left side, and expels warm air through the ventilation openings on right side. Do not block these openings. Failure to observe this caution will result in improper airflow and insufficient cooling that can lead to thermal damage.
- Consider the effort required for installing and removing the server from the wall mount for servicing, as well as the rear panel cabling connections.
- Make sure that there is a reliable power source within 1.50 m (4.92 ft) of the server location.
- Do not install the wall mount where the combined weight of the server and the wall mount (5.89 kg, 12.99 lb) cannot be supported.

Wall mount installation

This wall mount can only be installed in a single orientation—the retention latch on the top side of the wall mount must be facing upward. When the server is installed on the wall mount, the server rear panel will be facing upward as well.

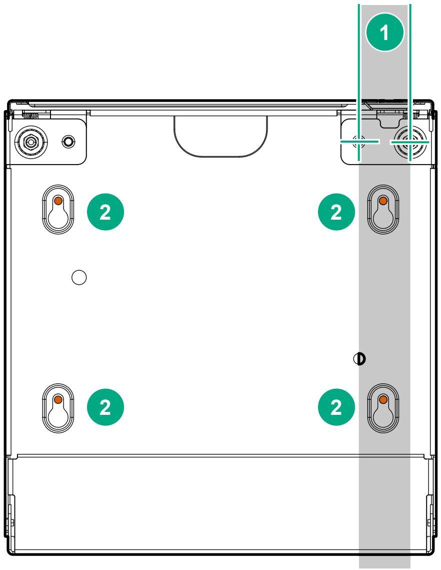
The fasteners included in this kit support wall mount installation on either a hollow wall (dry wall or gypsum over wood studs) or on a brick/concrete wall.

Install the wall mount on a hollow wall

Procedure

1. Use a stud finder to locate the internal wall studs on the selected mounting location and mark them accordingly.
2. Mark all four screw mounting positions:
   a. Align the right or left wall mount holes with the center of an internal wall stud.

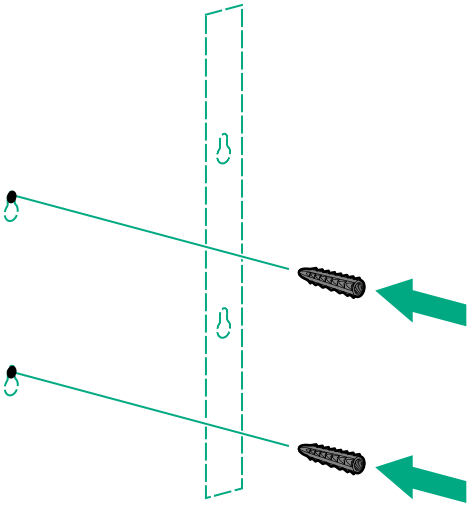
      The illustrations used in this section show the right wall mount holes aligned with an internal wall stud.
   b. Mark the screw mounting positions.



   c. Use a level to ensure that the mounting positions are perfectly straight.
3. Install the wall mount anchors on the left pilot holes:

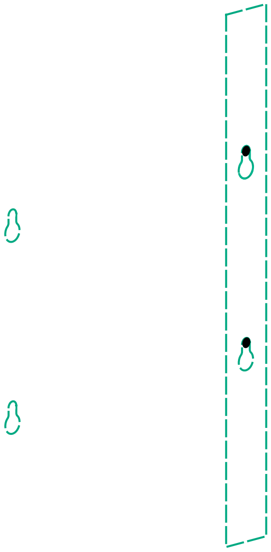
a. On the left mounting positions, use a drill to bore pilot holes with a diameter of 7.920 mm (0.312 in) and depth of at least 50.8 mm (2.00 in).

b. Use a hammer to install the anchors in the pilot holes.

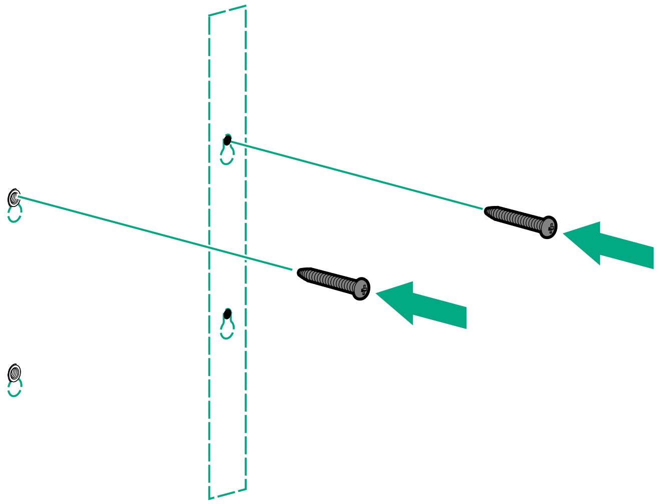


4. In the stud side mounting positions, use a drill to bore pilot holes with a diameter of 3.175 mm (0.125 in) and depth of at least 50.8 mm (2.00 in).

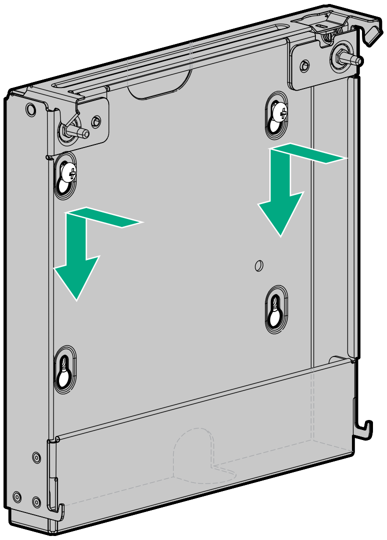
   Wall anchors are not required on these locations.



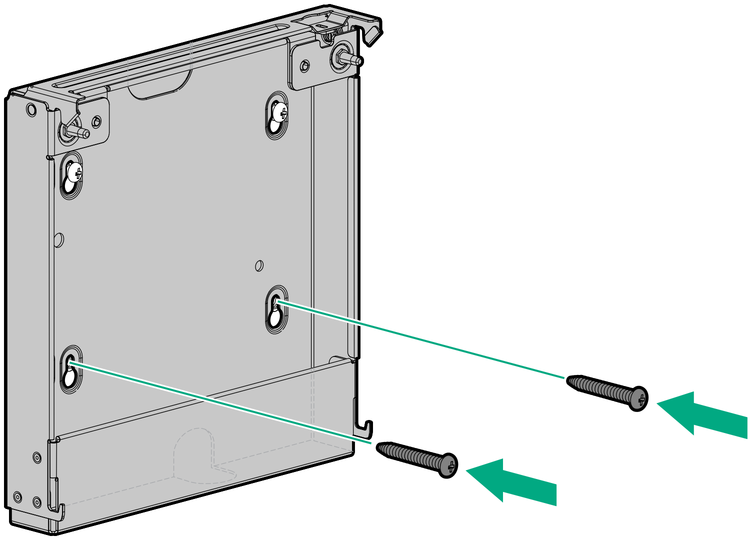
5. Use a small wire brush to clean the right pilot holes.
6. Install the wall mount screws halfway through into the top mounting positions.



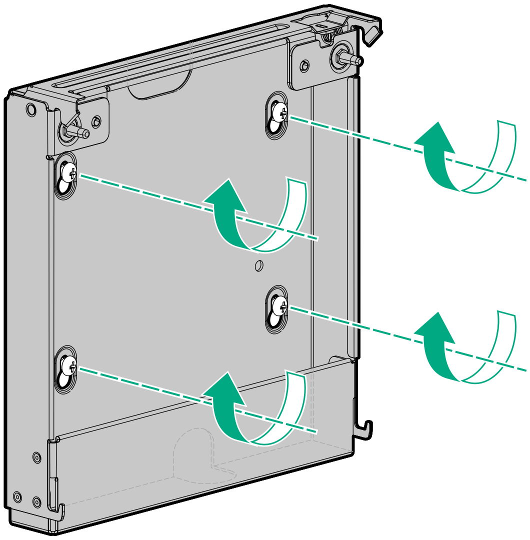
7. Install the wall mount.



8. Install the wall mount screws halfway through into the bottom mounting positions.



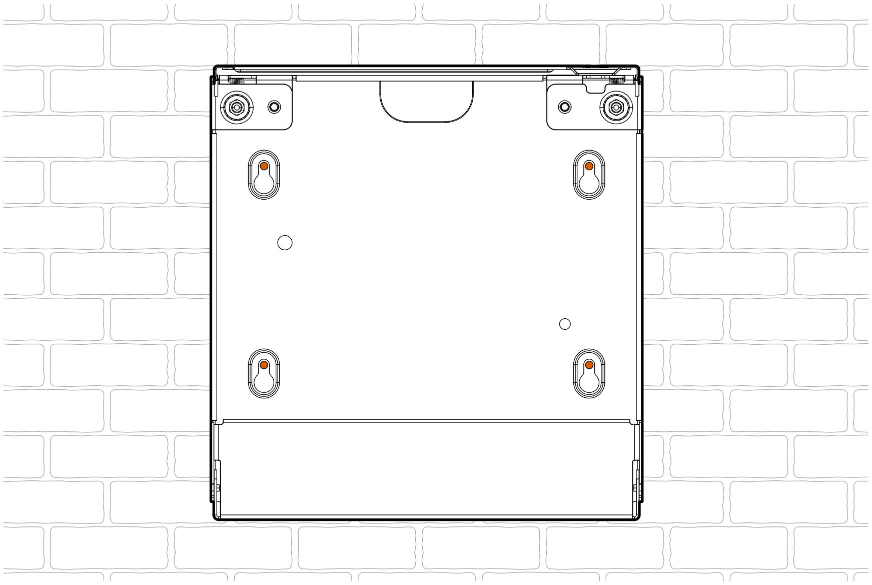
9. Completely tighten all four wall mount screws.



Install the wall mount on a brick/concrete wall

Procedure

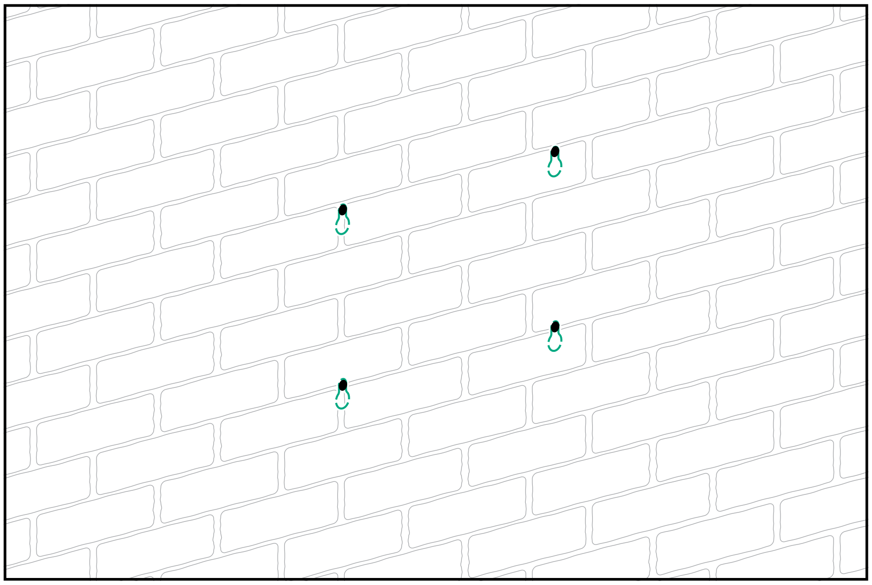
1. Mark all four screw mounting positions:
   a. Mark the screw mounting positions.



b. Use a level to ensure that the mounting positions are perfectly straight.

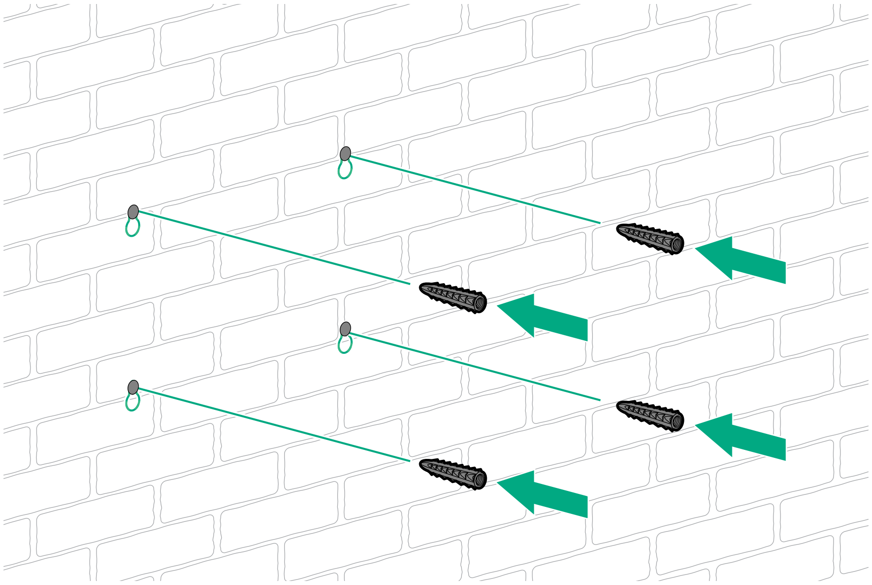
2. Install the wall mount anchors:

   a. On all four mounting positions, use a drill to bore pilot holes with a diameter of 7.920 mm (0.312 in) and depth of at least 50.8 mm (2.00 in).

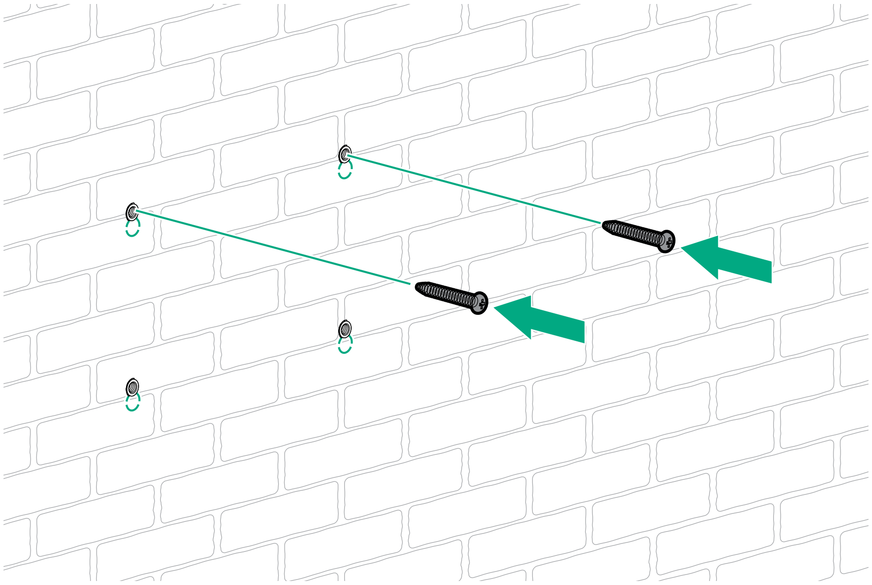


   b. Use a small wire brush to clean the pilot holes.

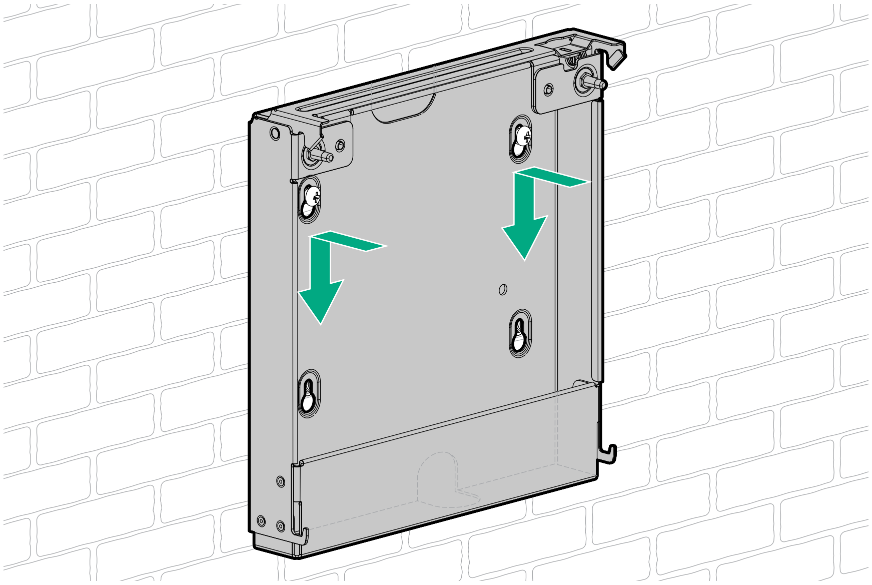
   c. Use a hammer to install the anchors in the pilot holes.



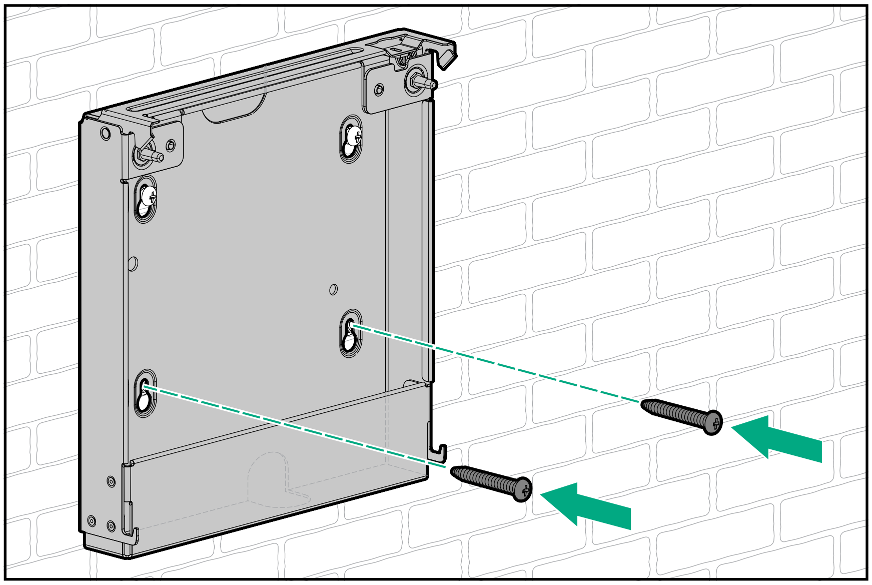
3. Install the wall mount screws halfway through into the top mounting positions.



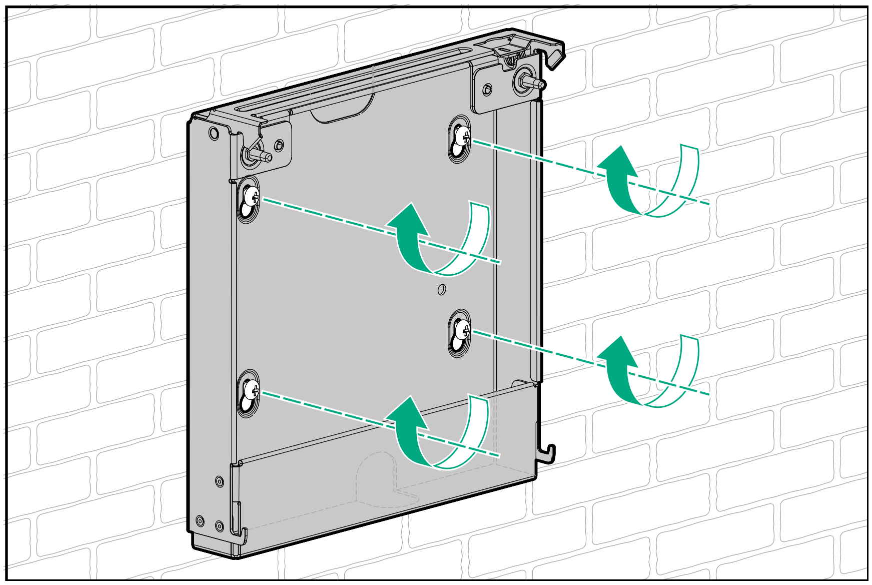
4. Install the wall mount.



5. Install the wall mount screws halfway through into the bottom mounting positions.



6. Completely tighten all four wall mount screws.

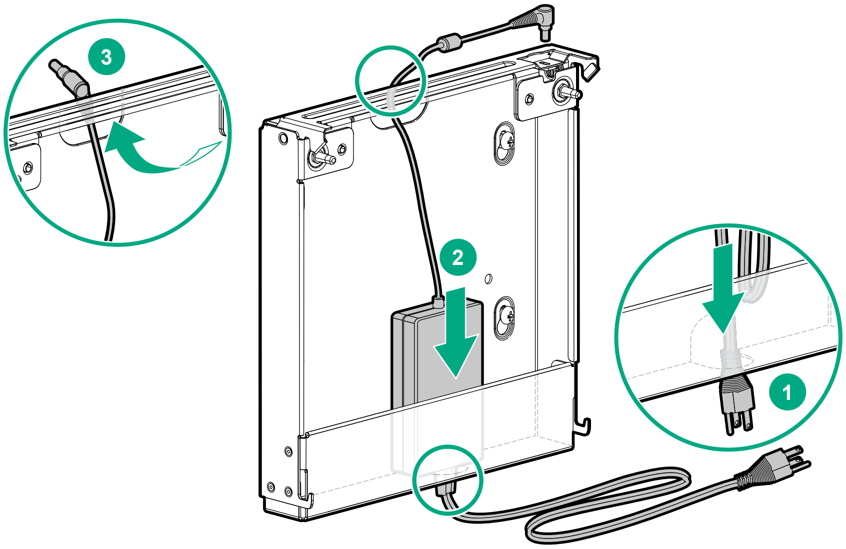


Install the server in the wall mount

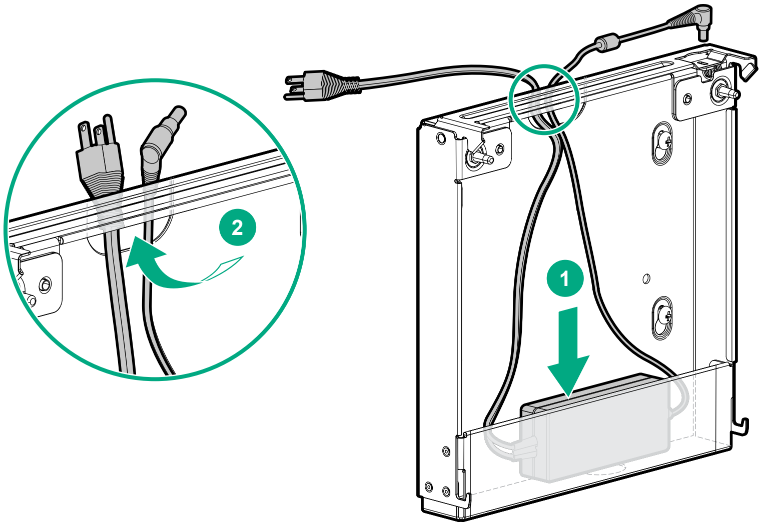
About this task

Procedure

1. If the power source location is lower than the wall mount, do the following to position the power adapter inside the wall mount:
   a. Route the power cord through the bottom opening of the wall mount.
   b. Place the power adapter inside the wall mount.
   c. Route the adapter cord through the top opening of the wall mount with the grommet extended out of the opening.

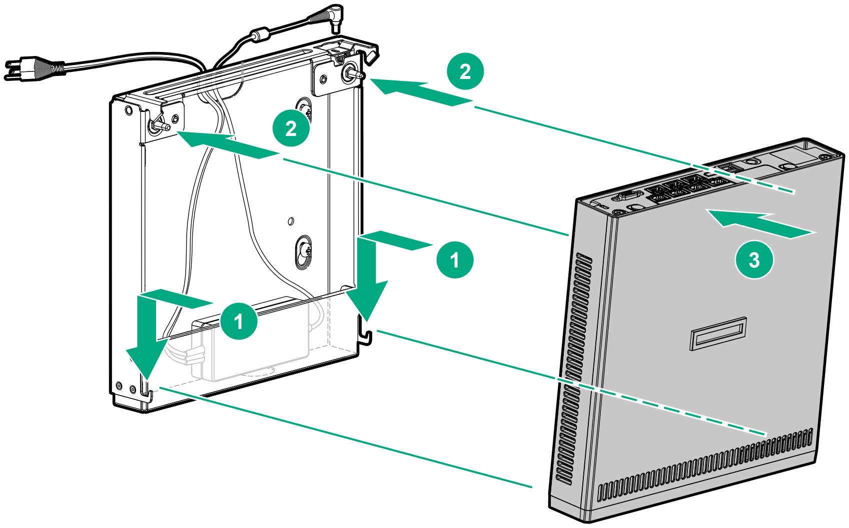


2. If the power source location is higher than the wall mount, do the following to position the power adapter inside the wall mount:
   a. Place the power adapter inside the wall mount.
   b. Route the power and adapter cords through the top opening of the wall mount, with the adapter cord grommet extended out of the opening.

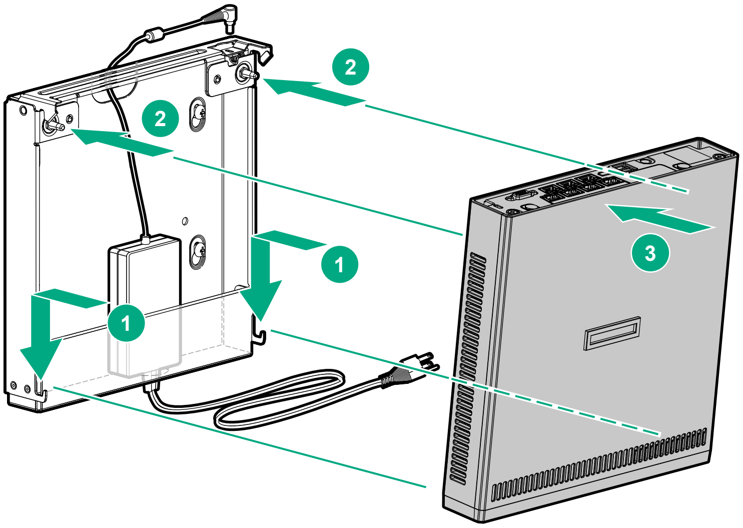


3. For cable management purposes, secure the extra length of the adapter cord that is not extended out of the wall mount inside the wall mount.
4. Depending on how far the power source is from the wall mount, store the extra length of the power cord inside the wall mount.
5. Install the server on the wall mount:
   a. Orient the server in a vertical position with the rear panel parallel to the retention latch.
   b. Insert the two hooks on the bottom side of the wall mount into the corresponding openings on the server.
   c. Align and insert the two posts on the wall mount into the corresponding openings on the server.
   d. To ensure that the retention latch fully engages with the server, push the back edge of the server against the wall mount.

      - Installing the server on the wall mount when the power source location is lower than the wall mount.



      - Installing the server on the wall mount when the power source location is higher than the wall mount.



Installing the server on the storage expansion unit

About this task

The storage expansion unit supports four LFF SATA 6Gb/s non-hot-plug hard drives. These drives are managed by the embedded SATA controller in the Intel Xeon D-1500 series processor.

This server only supports software RAID. For RAID configuration procedures, see the relevant OS documentation.

Procedure

1. **Prepare the server for hardware installation or removal.**
2. If the server is installed in a cradle or wall mount:
   - **Remove the server from the cradle**.
   - **Remove the server from the wall mount**.
3. **Install the server on the storage expansion unit**.
4. **Prepare the server for operation**.

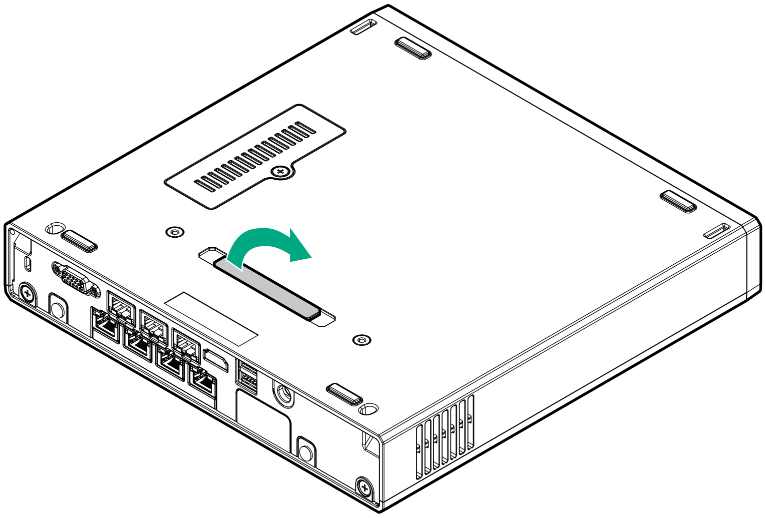
Install the server on the storage expansion unit

Prerequisites

Before you perform this procedure, make sure that you have a No. 2 Phillips screwdriver available.

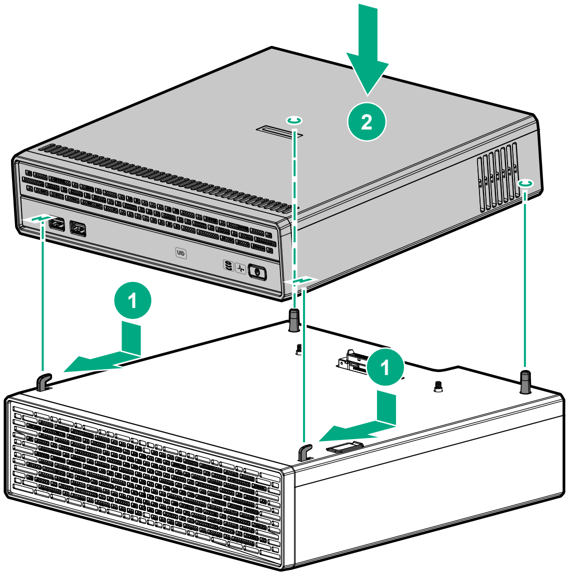
Procedure

1. Remove the cover from the server dock connector.



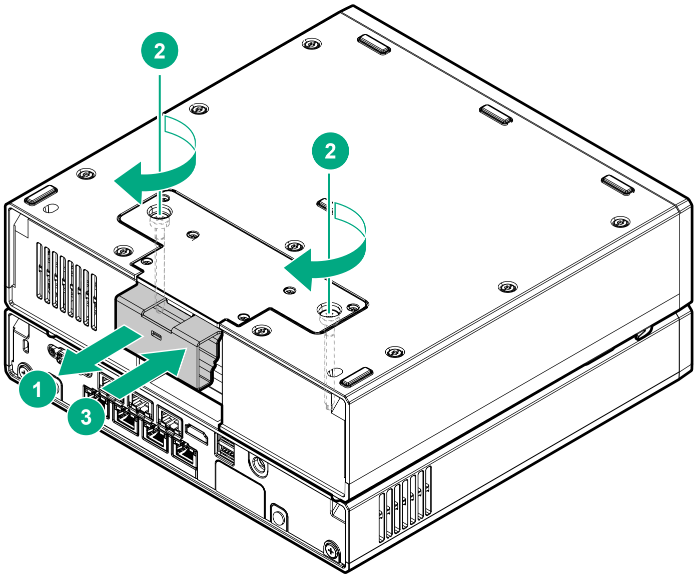
Keep the cover for future use.

2. Insert the two hooks on top of the storage expansion unit into the corresponding openings on the bottom of the server.
3. Tilt the server down until the two posts on top of the storage expansion unit seat into the corresponding openings on the bottom of the server.



This docking action attaches the server to the storage expansion unit. However, the assembly is **NOT** yet locked into place.

4. Hold the top side of the server and the bottom side of the storage expansion unit, and then carefully turn the assembly over to access the bottom side of the storage expansion unit.
5. Pull the latch on the rear of the storage expansion unit.
6. Tighten the captive screws.
7. Push the latch back in place.



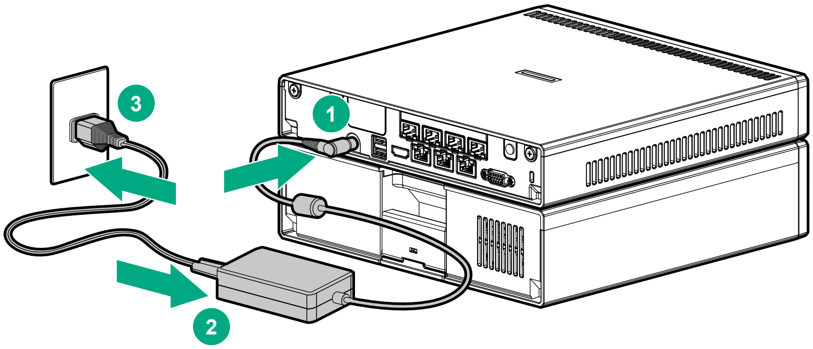
8. Return the assembly to an upright position.

Prepare the server for operation after storage expansion unit installation

Procedure

1. If removed, install the Kensington security lock.

   For more information, see the Kensington security lock documentation.
2. Connect all peripheral cables to the server.
3. The server-storage expansion assembly requires a higher wattage rating than the 120 W provided by the power adapter that shipped with the server. Use the 180 W power adapter included in the option kit instead:
   1. Connect the power adapter to the server.
   2. Connect the power cord to the adapter.
   3. Connect the power cord to the power source.



4. Secure the power cord and rear panel cables based on the standard cable management practices.
5. **Power up the server**.
6. Determine the status of the storage expansion unit drives from the **drive LED definitions**.

HP Trusted Platform Module information

The TPM is a hardware-based system security feature. It can store information securely, such as passwords and encryption keys, which can be used to authenticate the platform.

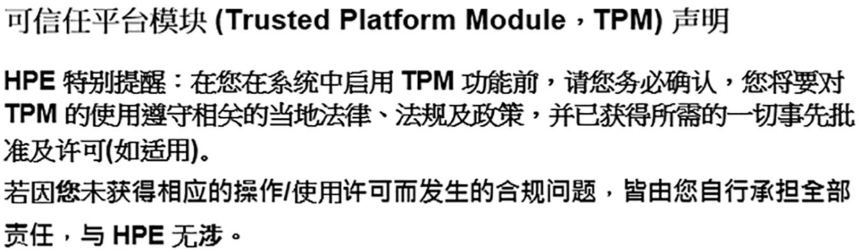
TPM installation requires the use of drive encryption technology, such as the Microsoft Windows BitLocker Encryption feature. BitLocker is a data protection feature available in Microsoft Windows Server 2008 R2 SP1 and later operating systems. It helps protect user data and ensure that a server running Windows Server has not been tampered with while the system was offline. For more information on BitLocker, see the **Microsoft website**.

This server supports TPM 1.2 and TPM 2.0. However, once the TPM version 1.2 is installed on the system board, it can no longer be upgraded to the TPM version 2.0.

Trusted Platform Module (TPM) — China Import Restrictions

HPE Special Reminder: Before enabling TPM functionality on this system, you must ensure that your intended use of TPM complies with relevant local laws, regulations and policies, and approvals or licenses must be obtained if applicable.

For any compliance issues arising from your operation/usage of the TPM which violates the above mentioned requirement, you shall bear all the liabilities wholly and solely. HPE will not be responsible for any related liabilities.



可信任平台模块 **(Trusted Platform Module，TPM)** 声明

HPE 特别提醒：在您在系统中启用 TPM 功能前，请您务必确认，您将要对 TPM 的使用遵守相关的当地法律、法规及政策，并已获得所需的一切事先批准及许可(如适用)。

若因您未获得相应的操作/使用许可而发生的合规问题，皆由您自行承担全部责任，与 HPE 无涉。

HP Trusted Platform Module installation 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 becomes a permanent part of the system board.
- 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, HPE Service provides a TPM with the spare system board.
- Any attempt to remove an installed TPM from the system board breaks or disfigures the TPM security rivet. Upon locating a broken or disfigured rivet on an installed TPM, administrators should consider the system compromised and take appropriate measures to ensure the integrity of the system data.
- 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.
- HPE is not liable for blocked data access caused by improper TPM use. For operating instructions, see the encryption technology feature documentation provided by the operating system.

Installing the Trusted Platform Module

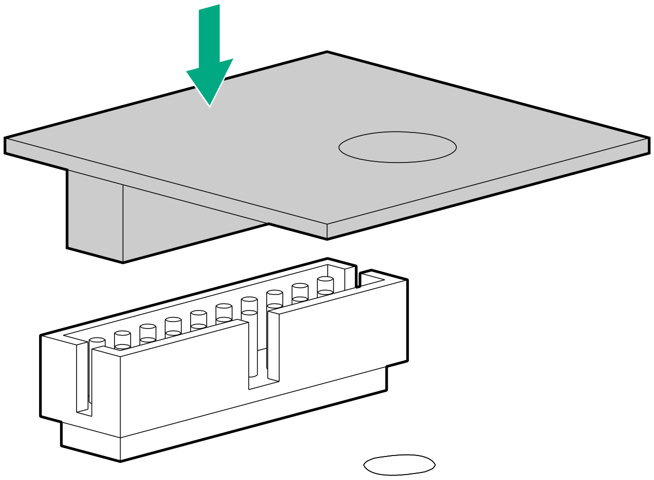
Procedure

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

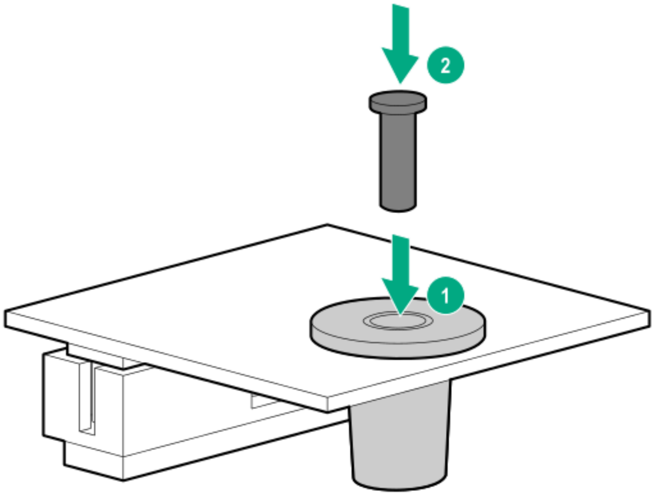
Installing the Trusted Platform board

Procedure

1. **Prepare the server for hardware installation or removal**.
2. If the server is installed in a cradle, wall mount or storage expansion unit:
   - **Remove the server from the cradle**.
   - **Remove the server from the wall mount**.
   - **Remove the server from the storage expansion unit**.
3. **Remove the access panel**.
4. **Remove the thermal sheet**.
5. **Remove the communication board**.
6. **Remove the middle frame**.
7. **Locate the TPM connector on the system board**.
8. Install the TPM board.



9. Install the TPM security rivet by pressing the rivet firmly into the system board.



10. **Install the middle frame**.
11. **Install the communication board**.

12. **Install the thermal sheet**.
13. **Install the access panel**.
14. If the server was removed from a cradle, wall mount, or storage expansion unit:
    - **Install the server in the cradle**.
    - **Install the server in the wall mount**.
    - **Install the server on the storage expansion unit**.
15. **Prepare the server for operation**.

Retaining the recovery key/password

About this task

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.

Enabling the Trusted Platform Module

About this task

> **CAUTION:**
> When a TPM is installed and enabled on the server, data access is locked if you fail to follow the proper procedures for updating the system or option firmware, replacing the system board, replacing a hard drive, or modifying OS application TPM settings.

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**.
3. Select **Trusted Platform Module Options**, and press the **Enter** key**.**
4. To set the TPM operational state:
    - If TPM 1.2 is installed, then select **No Action, Enable, Disable,** or **Clear**.
    - If TPM 2.0 is installed, then select **No Action** or **Clear**.
5. Select **Visible** to set the TPM Visibility, if necessary.
6. Press the **F10** key to save your selection.
7. When prompted to save the change in System Utilities, press the **Y** key.
8. Press the **ESC** key to exit System Utilities. Then, press the **Enter** key when prompted to reboot the compute module.

    The compute module then reboots a second time without user input. During this reboot, the TPM setting becomes effective.
9. Enable TPM functionality in the OS, such as Microsoft Windows BitLocker or measured boot.

    For more information on adjusting TPM usage in BitLocker, see the Microsoft website (**http://support.microsoft.com**).

For more information on the UEFI System Utilities, see the *UEFI System Utilities User Guide for HPE ProLiant Gen9 and Synergy Servers* in theUEFI Information Library (**http://www.hpe.com/info/ProLiantUEFI/docs**).

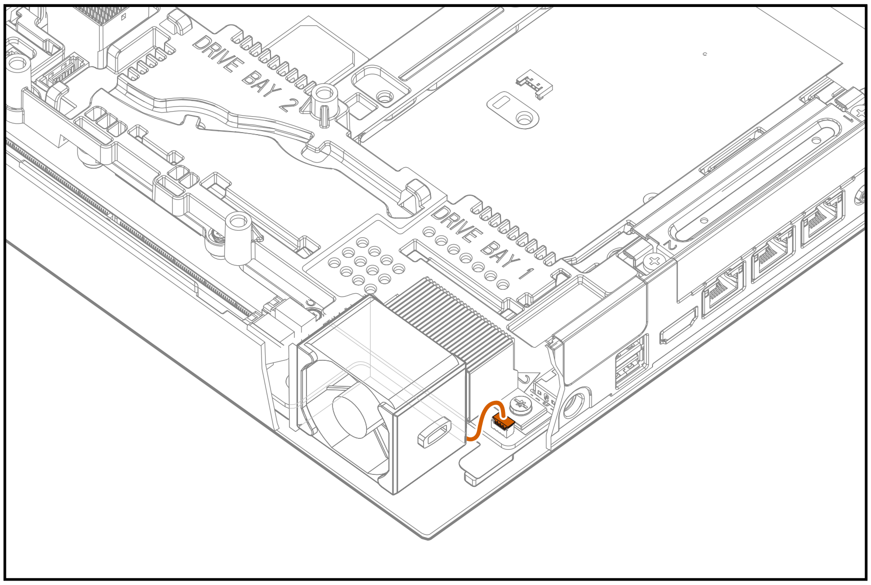
Cabling

Cabling overview

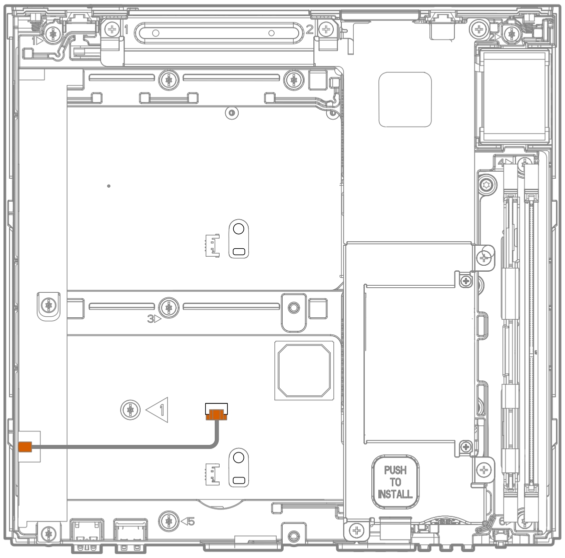
This section provides guidelines that help you make informed decisions about cabling the server and hardware options to optimize performance.

CAUTION:
When routing cables, always be sure that the cables are not in a position where they can be pinched or crimped.

Server fan cabling



Ambient temperature sensor cabling



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
HPE iLO	Online and Offline
Integrated Management Log	Online and Offline
Insight Diagnostics	Online and Offline
Scripting Toolkit for Windows and Linux	Online
Service Pack for ProLiant	Online and Offline
Smart Update Manager	Online and Offline
UEFI System Utilities	Offline
FWUPDATE utility	Offline

HPE iLO

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

Features that enhance server administrator productivity are licensed. For more information, see the iLO 4 documentation on the **Hewlett Packard Enterprise website**.

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 operating system-specific IML viewers:
  - For Windows: IML Viewer
  - For Linux: IML Viewer Application
- From within the iLO web interface
- From within Insight Diagnostics

Insight Diagnostics

Insight Diagnostics provides a comprehensive suite of offline system and component tests, providing in-depth testing of critical hardware components for devices such as processors, memory, and hard drives. Insight Diagnostics captures system configuration information and provides detailed diagnostic testing capabilities.

The Insight Diagnostics Offline Edition is available through SPP.

Insight Diagnostics simplifies the process of effectively identifying, diagnosing, and isolating hardware issues. System availability is maintained through the following key features:

- Surveying the current configuration, with various levels and categories
- Testing and diagnosing apparent hardware failures
- Documenting system configurations for upgrade planning, standardization, inventory tracking, disaster recovery, and maintenance
- Sending configuration information to another location for more in-depth analysis
- Managing the Integrated Management Log (IML)

In addition to system management tools, service tools can resolve system problems quickly. To streamline the service process and resolve problems quickly, you must have the right information available at the time that a service call is placed. This combination of features simplifies the service process and minimizes downtime.

Insight Diagnostics survey functionality

Insight Diagnostics provides survey functionality that gathers critical hardware and software information on ProLiant servers.

This functionality supports operating systems that the server supports.

If a significant change occurs between data-gathering intervals, the survey function marks the previous information and overwrites the survey data files to reflect the latest changes.

Survey functionality is installed with every Intelligent Provisioning-assisted Insight Diagnostics installation, or it can be installed through the SPP.

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**.

Service Pack for ProLiant

The SPP is a comprehensive systems software (drivers and firmware) solution delivered as a single package with major server releases. This solution uses SUM as the deployment tool and is tested on all supported ProLiant servers including HPE ProLiant Gen8 and later servers.

SPP allows the following operating modes:

- Online mode – The installation occurs while the host processor is running in the normal server environment.
- Offline mode – Boots a small Linux kernel and enables updates to occur on a single server.

For more information or to download SPP, see one of the following pages on the Hewlett Packard Enterprise website:

- **Service Pack for ProLiant download page**
- **Smart Update: Server Firmware and Driver Updates page**

Smart Update Manager

SUM is a product used to install and update firmware, drivers, and systems software on ProLiant servers. SUM provides a GUI, a command-line scriptable interface, and an interactive command-line scriptable interface. The interfaces allow you to deploy firmware, drivers, and software for supported servers.

For more information about SUM, see the product page on the **Hewlett Packard Enterprise website**.

To download SUM, see the **Hewlett Packard Enterprise website**.

To access the *Smart Update Manager User Guide*, see the **Hewlett Packard Enterprise Information Library**.

UEFI System Utilities

Most servers have a UEFI Class 2 implementation and support both UEFI Boot Mode (default) and Legacy BIOS Boot Mode. The boot mode is configured through the Boot Mode setting in UEFI System Utilities. Note that servers with a UEFI Class 3 implementation support UEFI Boot Mode only and do not have a Boot Mode setting in UEFI System Utilities.

The UEFI System Utilities is embedded in the system ROM. The UEFI System Utilities 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
- Configuring memory options
- Selecting a language
- Launching other preboot environments such as the Embedded UEFI Shell

For more information, see the UEFI System Utilities user guide on the **Hewlett Packard Enterprise website**.

To access mobile-ready online help for the UEFI System Utilities and UEFI Shell, scan the QR code at the bottom of the screen. For on-screen help, press the **F1** key.

Using UEFI System Utilities

To use the System Utilities, use the following keys.

Action	Key
Access System Utilities	F9 during server POST
Navigate menus	Up and Down arrows
Select items	Enter
Save selections	F10
Access Help for a highlighted configuration option[1]	F1

[1] *Scan the QR code on the screen to access online help for the UEFI System Utilities and UEFI Shell.*

Default configuration settings are applied to the server at one of the following times:

- Upon the first system power-up
- After defaults have been restored

Default configuration settings are sufficient for typical server operations; however, you can modify configuration settings as needed. The system prompts you for access to the UEFI System Utilities each time the system is powered up.

Flexible boot control

This feature enables you to do the following:

- Add Boot Options:
  - Browse all FAT16 and FAT32 file systems.
  - To add a new UEFI boot option, select an X64 UEFI application with an .EFI extension. For example, adding an OS boot loader or other UEFI application as a new UEFI boot option.

    The new boot option is appended to the boot-order list. When you select a file, you are prompted to enter the boot option description. This description, and any optional data to be passed to an .EFI application, is then displayed in the boot menu.
- Boot to System Utilities

  After pre-POST, the boot options screen appears. During this time, you can access the UEFI System Utilities by pressing the **F9** key.

For more information, see the UEFI System Utilities user guide for your product on the **Hewlett Packard Enterprise Information Library**.

Restoring and customizing configuration settings

You can reset all configuration settings to the factory default settings, or you can restore and use the system default configuration settings.

You can also configure default settings as necessary, and then save the configuration as the custom default configuration. When the system loads the default settings, it uses the custom default settings instead of the factory defaults.

Secure Boot configuration

Secure Boot is integrated in the UEFI specification on which the Hewlett Packard Enterprise implementation of UEFI is based. Secure Boot is implemented in the BIOS and does not require special hardware. Secure Boot ensures that each component launched during the boot process is digitally signed. Secure Boot also ensures 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 enabled, only firmware components and operating systems with boot loaders that have an appropriate digital signature can execute during the boot process. Only operating systems that support Secure Boot and have an EFI boot loader signed with one of the authorized keys can boot. For more information about supported operating systems, see the UEFI System Utilities and Shell release notes for your server on the **Hewlett Packard Enterprise website**.

A physically present user can customize the certificates embedded in the UEFI BIOS by adding or removing their own certificates.

When Secure Boot is enabled, the System Maintenance Switch does not restore all manufacturing defaults when set to the ON position. For security reasons, the following are not restored to defaults when the System Maintenance Switch is in the ON position:

- Secure Boot and remains enabled.
- The Secure Boot Database is not restored to its default state.
- iSCSI Software Initiator configuration settings are not restored to defaults.

Embedded UEFI shell

The system BIOS includes an Embedded UEFI Shell in the ROM. The UEFI Shell environment provides an API, a command-line prompt, and a set of CLIs that allow scripting, file manipulation, and system information. These features enhance the capabilities of the UEFI System Utilities.

For more information, see the following documents:

- UEFI Shell user guide on the **Hewlett Packard Enterprise website**
- UEFI Shell Specification on the **UEFI website**

Embedded Diagnostics option

The system BIOS includes an Embedded Diagnostics option in the ROM. The Embedded Diagnostics option can run comprehensive diagnostics of the server hardware, including processors, memory, drives, and other server components.

For more information on the Embedded Diagnostics option, see the UEFI System Utilities user guide for your server on the **Hewlett Packard Enterprise website**.

Re-entering the server serial number and product ID

About this task

After you replace the system board, you must re-enter the server serial number and the product ID:

Procedure

1. During the server startup sequence, press the **F9** key to access UEFI System Utilities.
2. Select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Advanced Options** > **Advanced System ROM Options** > **Serial Number**, and then press the **Enter** key.
3. Enter the serial number and press the **Enter** key.

   The following message appears:

   ```
   The serial number should only be modified by qualified service personnel. This
   value should always match the serial number located on the chassis.
   ```
4. To clear the warning, press the **Enter** key.
5. Enter the serial number and press the **Enter** key.
6. Select **Product ID**.

   The following warning appears:

   ```
   Warning: The Product ID should ONLY be modified by qualified service
   personnel. This value should always match the Product ID located on the
   chassis.
   ```
7. Enter the product ID and press the **Enter** key.
8. To confirm exiting System Utilities, press the **F10** key.

   The server automatically reboots.

Utilities and features

Automatic Server Recovery

ASR is a feature that causes the system to restart when a catastrophic operating system error occurs, such as a blue screen, ABEND, or panic. A system fail-safe timer, the ASR timer, starts when the System Management driver, also known as the Health Driver, is loaded. When the operating system is functioning properly, the system periodically resets the timer. However, when the operating system fails, the timer expires and restarts the server.

ASR increases server availability by restarting the server within a specified time after a system hang. You can disable ASR from the System Management Homepage or through UEFI System Utilities.

USB support

Hewlett Packard Enterprise servers support both USB 2.0 ports and USB 3.0 ports. Both port types support installing all types of USB devices (USB 1.0, USB 2.0, and USB 3.0), but might run at lower speeds in specific situations:

- USB 3.0 capable devices operate at USB 2.0 speeds when installed in a USB 2.0 port.
- In UEFI Boot Mode, Hewlett Packard Enterprise provides legacy USB support in the preboot environment before the operating system loading for USB 1.0, USB 2.0, and USB 3.0 speeds.

For maximum compatibility of USB 3.0 devices with all operating systems, Hewlett Packard Enterprise provides a configuration setting for USB 3.0 Mode. Auto is the default setting. This setting impacts USB 3.0 devices when connected to USB 3.0 ports in the following manner:

- **Auto (default)**—If configured in Auto Mode, USB 3.0 capable devices operate at USB 2.0 speeds in the preboot environment and during boot. When a USB 3.0 capable OS USB driver loads, USB 3.0 devices transition to USB 3.0 speeds. This mode is compatible with operating systems that do not support USB 3.0 while allowing USB 3.0 devices to operate at USB 3.0 speeds with state-of-the-art operating systems.
- **Enabled**—If Enabled, USB 3.0 capable devices operate at USB 3.0 speeds at all times (including the preboot environment) when in UEFI Boot Mode. Do not use this mode with operating systems that do not support USB 3.0.
- **Disabled**—If configured for Disabled, USB 3.0 capable devices function at USB 2.0 speeds at all times.

The pre-OS behavior and default operation of the USB ports is configurable in the UEFI System Utilities. For more information, see the UEFI System Utilities user guide for your product on the **Hewlett Packard Enterprise website**.

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

Multiple methods exist to update the firmware or System ROM:

- Service Pack for ProLiant
- FWUPDATE utility
- FWUpdate command from within the Embedded UEFI Shell
- Firmware Update application in the UEFI System
- Online Flash components

Product entitlement is required to perform updates.

FWUPDATE utility

The FWUPDATE utility enables you to upgrade the system firmware (BIOS).

To use the utility to upgrade the firmware:

1. Download the FWUPDATE flash component from the **Hewlett Packard Enterprise Support Center website**.
2. Save the FWUPDATE flash components to a USB key.
3. Set the boot order so that the USB key will boot first using one of the following options:
   - Configure the boot order so that the USB key is the first bootable device.
   - Press the **F11** key (Boot Menu) when prompted during system boot to access the **One-Time Boot Menu**. This menu allows you to select the boot device for a specific boot and does not modify the boot order configuration settings.
4. Insert the USB key into an available USB port.
5. Boot the system.

   The FWUPDATE utility checks the system and provides a choice (if more than one exists) of available firmware revisions.

To download the flash components, see the **Hewlett Packard Enterprise Support Center website**.

For more information about One-Time Boot Menu, see the UEFI System Utilities user guide for your product on the **Hewlett Packard Enterprise website**.

FWUpdate command from within the Embedded UEFI Shell

For systems configured in either boot mode, update the firmware:

1. Access the System ROM Flash Binary component for your server from the **Hewlett Packard Enterprise Support Center website**. When searching for the component, always select **OS Independent** to locate the binary file.
2. Copy the binary file to a USB media or iLO virtual media.
3. Attach the media to the server.
4. Boot to Embedded Shell.
5. To obtain the assigned file system volume for the USB key, enter the `Map -r` command.

For more information about accessing a file system from the shell, see the UEFI Shell user guide on the **Hewlett Packard Enterprise website**.

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 the **Enter** key.
7. Use the `cd` command to change from the current directory to the directory that contains the binary file.
8. Enter the `fwupdate -d BIOS -f <filename>` command to flash the system ROM.

   For help on the FWUPDATE command, enter the following command:

   ```
   help fwupdate -b
   ```
9. Reboot the server.

   A reboot is required after the firmware update for the updates to take effect, and for hardware stability to be maintained.

For more information about the commands used in this procedure, see the UEFI Shell user guide on the **Hewlett Packard Enterprise website**.

Firmware Update application in the UEFI System Utilities

For systems configured in either boot mode, update the firmware:

1. Access the System ROM Flash Binary component for your server from the **Hewlett Packard Enterprise Support Center website**. When searching for the component, always select **OS Independent** to locate the binary file.
2. Copy the binary file to a USB media or iLO virtual media.
3. Attach the media to the server.
4. During POST, press **F9** to enter System Utilities.
5. Select **Embedded Applications** > **Firmware Update** > **System ROM** > **Select Firmware File**.
6. Select the device containing the flash file.
7. Select the flash file. This step may take a few moments to complete.
8. Select **Start firmware update** and allow the process to complete.
9. Reboot the server. A reboot is required after the firmware update 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.

The server includes new hardware that may not have driver support on all OS installation media.

Drivers, ROM images, and value-add software can be downloaded as part of an SPP. If you are installing drivers from SPP, be sure that you are using the latest SPP version that your server supports. To verify that your server is using the latest supported version and for more information about SPP, see the **Hewlett Packard Enterprise website**.

To locate the drivers for a particular server, go to the **Hewlett Packard Enterprise Support Center website**. Under **Select your HPE product**, enter the product name or number and click **Go**.

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**.
- Download individual drivers, firmware, or other systems software components from the server product page in the **Hewlett Packard Enterprise Support Center website**.

Version control

The VCRM and VCA are web-enabled Insight Management Agents tools that SIM uses to schedule software update tasks to the entire enterprise.

- VCRM manages the repository for SPP. Administrators can do the following:
    - View the SPP contents
    - Configure VCRM to update the repository automatically with internet downloads of the latest software and firmware from Hewlett Packard Enterprise
- VCA compares installed software versions on the server with updates available in the VCRM managed repository. Administrators configure VCA to point to a repository managed by VCRM.

For more information about version control tools, see the following documents on the **Hewlett Packard Enterprise website**:

- Systems Insight Manager User Guide
- Version Control Agent User Guide
- Version Control Repository Manager User Guide

To locate the documents, do the following:

1. Select **Insight Management** from the available options in Products and Solutions.
2. Select **Version Control** from the available options in Models / Subcategories.
3. Locate and download the latest document.

HPE Technology Service Portfolio

HPE Technology Services deliver confidence, reduces risk and helps customers realize agility and stability. We help customers succeed through Hybrid IT by simplifying and enriching the on-premise experience, informed by public cloud qualities and attributes. HPE Support Services enables you to choose the right service level, length of coverage and response time to fit your business needs. Connect to HPE to help prevent problems and solve issues faster. By connecting, you will receive 24x7 monitoring, prefailure alerts, automatic call logging, and automatic parts dispatch. To learn more about getting connected, see the **HPE website**.

For more information about support services, see the **HPE website**.

Utilize our consulting expertise 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 **HPE website**.

Change control and proactive notification

Hewlett Packard Enterprise offers Change Control and Proactive Notification to notify customers 30 to 60 days in advance of the following:

- Upcoming hardware and software changes
- Bulletins
- Patches

Let us know what Hewlett Packard Enterprise commercial products you own and we will send you the latest updates to keep your business running smoothly.

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

Troubleshooting

Troubleshooting resources

The HPE ProLiant Gen9 Troubleshooting Guide, Volume I: Troubleshooting provides procedures for resolving common problems and comprehensive courses of action for fault isolation and identification, issue resolution, and software maintenance on ProLiant servers and server blades. To view the guide, select a language:

- **English**
- **French**
- **Spanish**
- **German**
- **Japanese**
- **Simplified Chinese**

The HPE ProLiant Gen9 Troubleshooting Guide, Volume II: Error Messages provides a list of error messages and information to assist with interpreting and resolving error messages on ProLiant servers and server blades. To view the guide, select a language:

- **English**
- **French**
- **Spanish**
- **German**
- **Japanese**
- **Simplified Chinese**

Specifications

Environmental specifications

Specification	Value
Temperature range	—
Operating	10°C to 35°C (50°F to 95°F)
Nonoperating	-30°C to 65°C (-22°F to 149°F)
Relative humidity (noncondensing)	—
Operating	Maximum wet bulb temperature of 28°C (82.4°F) = 10% to 90%
Nonoperating	Maximum wet bulb temperature of 38.7°C (101.7°F) = 0% to 95%

Mechanical specifications

Dimension	Value
Height with chassis rubber feet	4.85 cm (1.91 in)
Height without chassis rubber feet	4.50 cm (1.77 in)
Depth	25.40 cm (10.00 in)
Width	25.40 cm (10.00 in)
Weight (approximate values)	—
Server, minimum	1.55 kg (3.42 lb)
Server, maximum	3.69 kg (8.13 lb)
Server with storage expansion unit, minimum	4.09 kg (9.02 lb)
Server with storage expansion unit, maximum	8.92 kg (19.67 lb)
Server and the wall mount	5.89 kg (12.99 lb)

Warranty and regulatory information

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Belarus Kazakhstan Russia marking

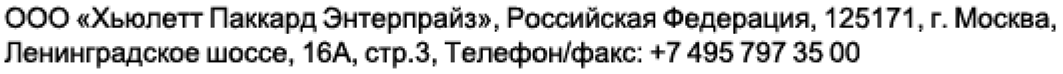
Manufacturer and Local Representative Information

Manufacturer information:

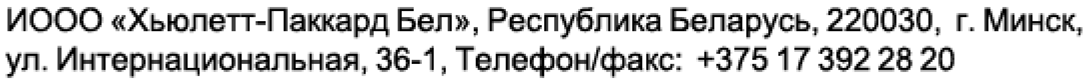
- Hewlett Packard Enterprise Company, 3000 Hanover Street, Palo Alto, CA 94304 U.S.

Local representative information Russian:

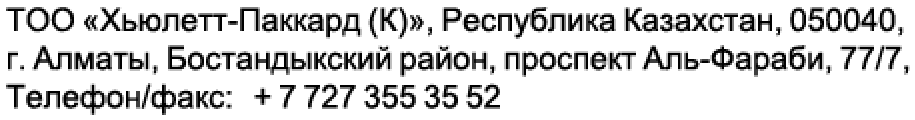
- Russia:


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

- Belarus:

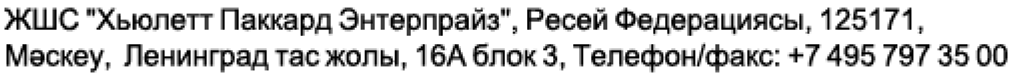

ИООО «Хьюлетт-Паккард Бел», Республика Беларусь, 220030, г. Минск,
ул. Интернациональная, 36-1, Телефон/факс: +375 17 392 28 20

- Kazakhstan:

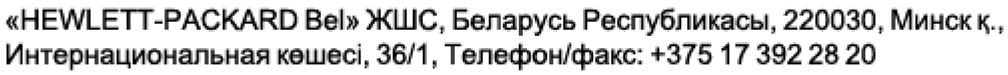

ТОО «Хьюлетт-Паккард (К)», Республика Казахстан, 050040,
г. Алматы, Бостандыкский район, проспект Аль-Фараби, 77/7,
Телефон/факс: + 7 727 355 35 52

Local representative information Kazakh:

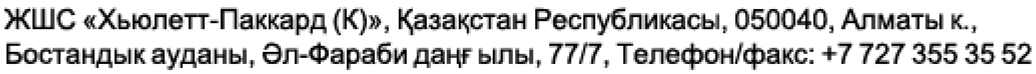
- Russia:


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 к.,
Бостандык ауданы, Әл-Фараби даңғылы, 77/7, Телефон/факс: +7 727 355 35 52

Manufacturing date:

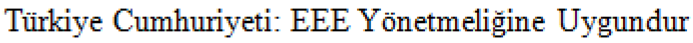
The manufacturing date is defined by the serial number.

CCSYWWZZZZ (serial number format for this product)

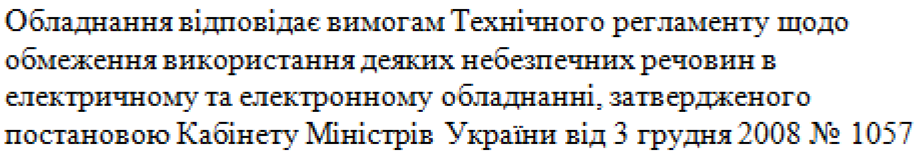
Valid date formats include:

- YWW, where Y indicates the year counting from within each new decade, with 2000 as the starting point; for example, 238: 2 for 2002 and 38 for the week of September 9. In addition, 2010 is indicated by 0, 2011 by 1, 2012 by 2, 2013 by 3, and so forth.
- YYWW, where YY indicates the year, using a base year of 2000; for example, 0238: 02 for 2002 and 38 for the week of September 9.

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

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

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

ABEND

abnormal end

API

application program interface

ASR

Automatic Server Recovery

CSA

Canadian Standards Association

CSR

Customer Self Repair

ESD

electrostatic discharge

FAT

file allocation table

HPE SIM

HPE Systems Insight Manager

IEC

International Electrotechnical Commission

iLO

Integrated Lights-Out

IML

Integrated Management Log

LFF

large form factor

NVRAM

nonvolatile memory

PDU

power distribution unit

POST

Power-On Self-Test

QR code

quick response code

RBSU

ROM-Based Setup Utility

REACH

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

RoHS

Restriction of Hazardous Substances

SATA

serial ATA

SPP

Service Pack for ProLiant

SSD

solid-state device

STK

scripting toolkit

SUM

Smart Update Manager

TPM

Trusted Platform Module

UEFI

Unified Extensible Firmware Interface

UID

unit identification

UPS

uninterruptible power supply

VC

Virtual Connect

VCA

Version Control Agent

VCRM

Version Control Repository Manager