



**Hewlett Packard
Enterprise**

HPE ProLiant MicroServer Gen10 Troubleshooting Guide

Abstract

This document describes common procedures and solutions for troubleshooting the HPE ProLiant MicroServer Gen10. This document is intended for the person who installs, administers, and troubleshoots server or storage products. Hewlett Packard Enterprise assumes that you are qualified to service computer equipment, and trained in recognizing hazards in products with hazardous energy levels.

Part Number: 872948-001
Published: June 2017
Edition: 1

Notices

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

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

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

Acknowledgments

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

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

SD™ is a trademark or registered trademark of SD-3C in the United States, other countries, or both.

Contents

Getting started	7
Important safety information	7
Symbols on equipment.....	7
Server warnings and cautions.....	8
Electrostatic discharge.....	8
Preventing electrostatic discharge.....	8
Grounding methods to prevent electrostatic discharge.....	9
Component identification	10
Front panel components.....	10
Front panel LEDs and buttons.....	11
Health LED warning conditions.....	12
Rear panel components.....	12
Rear panel LEDs.....	14
System board components.....	14
DIMM slot locations.....	15
Basic operations	17
Power up the server.....	17
Power down the server.....	17
Remove the front bezel.....	17
Removing a locked front bezel.....	17
Removing an unlocked front bezel.....	18
Install the front bezel.....	19
Remove the chassis cover.....	20
Install the chassis cover.....	21
Install the chassis cover.....	21
Install the system board assembly.....	21
Install the system board assembly.....	21
Remove the system board assembly.....	22
Remove the system board assembly.....	23
Troubleshooting preparation	25
Preparing to troubleshoot.....	25
Symptom information.....	25
Preparing the server for diagnosis.....	26
Minimum hardware configuration.....	26
Breaking down the server to minimum hardware configuration.....	26
DIMM installation and configuration guidelines.....	26
DIMM handling guidelines.....	26
DIMM installation guidelines.....	27
Hardware issues	28
General hardware issues.....	28
Loose connections.....	28

New hardware issues.....	28
Third-party device issues.....	29
Testing the device.....	29
Power issues.....	30
Server does not power on.....	30
Power supply issues.....	30
Power source issues.....	31
UPS issues.....	31
UPS is not working properly.....	31
Low battery warning is displayed on the UPS.....	32
Internal system issues.....	32
Fan and thermal issues.....	32
Fans are not working.....	32
Fans are running at a higher than expected speed.....	33
Excessive fan noise (low speeds).....	33
Server shuts down or reboots without warning.....	34
Trusted Platform Module issues.....	34
HP Trusted Platform Module installation guidelines.....	34
TPM fails or is not detected.....	35
Memory issues.....	35
General memory issues.....	35
DIMM configuration errors.....	36
Server is out of memory.....	36
Server does not recognize new memory.....	37
Server does not recognize existing memory.....	37
Correctable memory error threshold exceeded.....	38
Uncorrectable memory error.....	38
System board issues.....	39
System battery is low or has lost power.....	39
Drive issues (hard drives and solid state drives).....	39
Drives do not display.....	39
Data is inaccessible.....	40
Server response time is slow.....	41
USB drive key issues.....	41
System does not boot from the USB drive key.....	41
CD-ROM and DVD drive issues.....	42
System does not boot from the CD-ROM or DVD drive.....	42
Data from the CD-ROM or DVD is inconsistent, or CD-ROM or DVD cannot read data.....	42
Drive is not detected.....	43
Tape drive issues.....	43
Tape drive does not eject.....	43
Read/write issues are occurring.....	44
Tape drive backup fails.....	44
Media issues.....	45
External device issues.....	45
Video issues.....	45
Screen is blank for more than 60 seconds after powering up the server.....	45
Monitor does not function properly with energy saver features.....	46
Video colors do not display correctly.....	46
Slow-moving horizontal lines are displayed.....	47
Mouse and keyboard issues.....	47
Network controller issues.....	48
Network controller has stopped working.....	48
Network controller is installed but not working.....	48
Network controller stopped working when an expansion board was added.....	49
Expansion board issues.....	49

System requests recovery method during expansion board replacement.....	49
Error messages during system bootup.....	50
Software issues.....	52
Operating system issues and resolutions.....	52
Operating system issues.....	52
Operating system locks up.....	52
Errors are displayed in the error log.....	52
Updating the operating system.....	52
Restoring a backup version.....	52
Prerequisites for reconfiguring or reloading software.....	53
Linux resources.....	53
Linux tools (sosreport and supportconfig).....	53
Application software issues.....	54
Software locks up.....	54
Errors occur after a software setting is changed.....	54
Errors occur after the system software is changed.....	54
Errors occur after an application is installed.....	55
ROM issues.....	55
System requests recovery method during a firmware update.....	55
Updating firmware.....	56
Software tools and solutions.....	57
Server mode.....	57
Product QuickSpecs.....	57
Aptio Setup Utility.....	57
Using the Aptio Setup Utility	57
Boot option control.....	58
Boot option.....	58
Selecting the boot mode	58
Restoring and customizing configuration settings.....	58
Clearing the BIOS configuration settings.....	58
Clearing the BIOS settings by using the Aptio Setup Utility.....	59
Clearing the BIOS settings by using the CMOS header.....	59
Embedded UEFI Shell	60
Secure Boot configuration	61
Enabling the Trusted Platform Module.....	61
Utilities and features.....	61
HPE Smart Storage Administrator	61
Marvell Storage Utility	62
Marvell BIOS Utility.....	62
Accessing the Marvell BIOS Utility under legacy boot mode.....	62
Accessing the Marvell BIOS Utility under UEFI boot mode.....	62
USB support	62
Keeping the system current.....	63
Firmware	63
Firmware update.....	63
Updating the system ROM using the EFI tool from within the Embedded UEFI Shell	64
Online Flash components	64
Drivers, firmware, and software updates	64
Operating System Version Support.....	64
HPE Pointnext Portfolio.....	65
Change control and proactive notification.....	65

Resources for troubleshooting.....	66
Online resources.....	66
Hewlett Packard Enterprise Information Library.....	66
Service notifications, advisories, and notices.....	66
Subscription services.....	66
White papers.....	66
Product installation resources.....	66
Registering the server.....	66
Power capacity.....	66
Spare part numbers.....	66
Teardown or removal and replacement procedure videos.....	66
DDR4 memory configuration.....	67
Device driver information.....	67
 Support and other resources.....	 68
Accessing Hewlett Packard Enterprise Support.....	68
Accessing updates.....	68
Customer self repair.....	68
Warranty information.....	69
Regulatory information.....	69
Documentation feedback.....	69
 Acronyms and abbreviations.....	 70

Getting started

Important safety information

Familiarize yourself with the safety information in the following sections before troubleshooting the system.



Important safety information

Before servicing this product, read *Safety and Compliance Information for Server, Storage, Power, Networking, and Rack Products* on the [Hewlett Packard Enterprise website](#).

Symbols on equipment

The following symbols might be found on the equipment to indicate the presence of potentially hazardous conditions.



This symbol indicates the presence of hazardous energy circuits or electric shock hazards. Refer all servicing to qualified personnel.

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



This symbol indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure.



This symbol on an RJ-45 receptacle indicates a network interface connection.

WARNING: To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.



This symbol indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



This symbol indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.



These symbols, on power supplies or systems, indicate that the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electric shock, remove all power cords to disconnect power from the system completely.

Server warnings and cautions



WARNING:

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



WARNING:

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



CAUTION:

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



CAUTION:

To prevent improper cooling and thermal damage, do not operate the server with the media bay blank, chassis cover, or the front bezel removed.



CAUTION:

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



CAUTION:

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

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.

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 \pm 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.

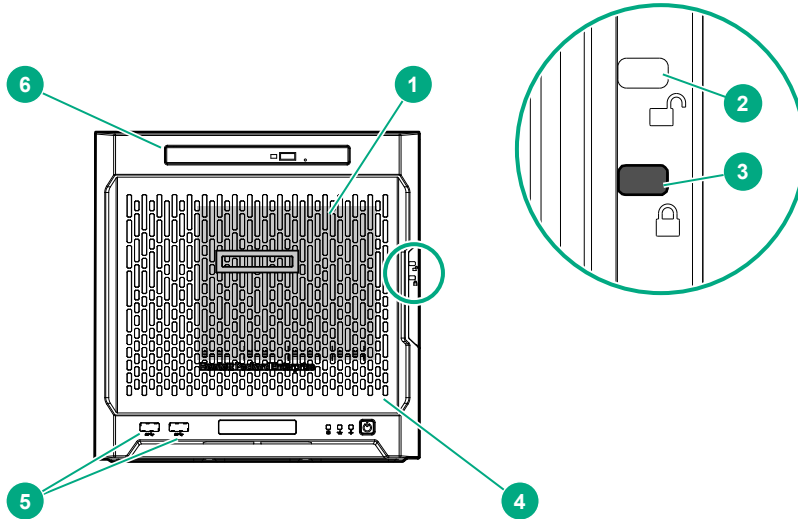
If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

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

Component identification

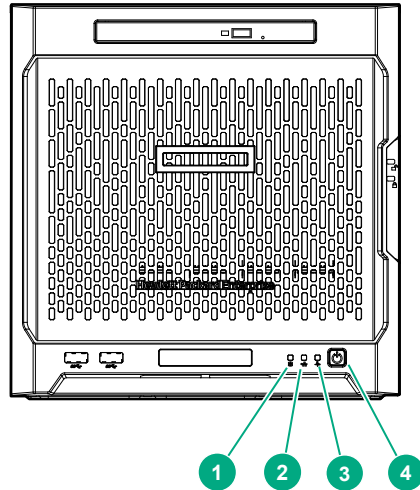
This chapter describes the external and internal server features and components.

Front panel components



Item	Component	Description
1	Drive bays (4, behind the front bezel)	By default, the drive bays support 3.5-inch LFF SATA drives. To support 2.5-inch SFF drives, install the SFF drive converter option.
2	Front bezel unlock indicator	To remove the front bezel from the chassis, this groove must show the blue indicator.
3	Front bezel lock indicator	To lock the front bezel in the chassis, this groove must show the blue indicator.
4	Front bezel	To access the front drive bays, remove this bezel.
5	USB 3.0 ports (2)	Connect USB 3.0 devices to these ports. USB 3.0 support after POST varies by operating system.
6	Media bay	When the relevant enablement options kits are installed, this bay supports either a slim-type optical disc drive or solid state drive option.

Front panel LEDs and buttons



Item	Description	Status
1	Drive activity LED	Flashing green = Ongoing drive activity Off = No drive activity This LED only reflects the status of LFF/SFF drives and SSD that are connected to the onboard SATA ports.
2	NIC status LED	Solid green = Linked to network Flashing green = Network active Off = No network activity This LED only reflects the status of Ethernet connections managed by the embedded Broadcom BCM5720 Gigabit Ethernet controller.
3	Health LED	Solid green = Normal Flashing amber = One or more components is in degraded condition. ¹ Flashing red = One or more components is in critical condition. ¹
4	Power on/Standby button and system power LED	Flashing green = Ongoing power-on sequence Solid green = System on and normal operation Amber = System in standby Off = No power present ²

¹ To identify which component is in the degraded or critical state, reboot the server. A POST error message screen showing the affected component will appear for about 30 seconds. Depending on how critical the component health status is, the system boot may or may not be completed. For troubleshooting information, see **Error messages during system bootup**.

² If the server does not power on, verify the following items:

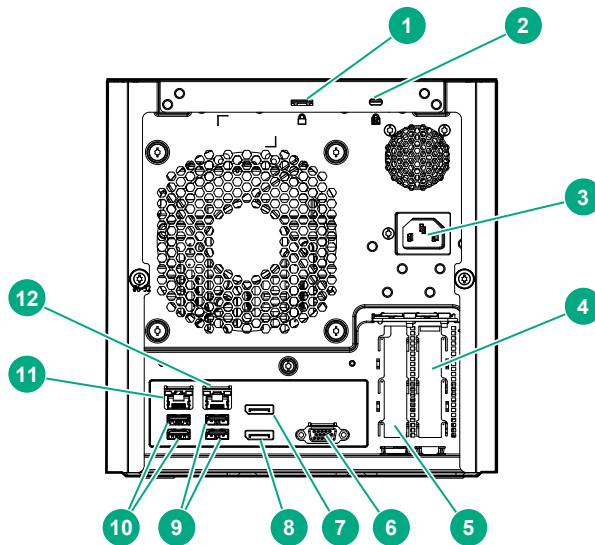
- The site power is available.
- The power cord is properly connected to the server power jack and to a working power source.
- The internal power supply cable is properly connected to the system board.

Health LED warning conditions

Health LED warning condition	Cause
Amber, blinking at 1 flash per second	Ambient temperature or server temperature is above the operating temperature range. ¹ See Fan and thermal issues .
Red, blinking at 1 flash per second	<ul style="list-style-type: none"> • A fan is not installed. • The fan has failed. • Ambient or server temperatures are above the operating temperature range.¹ See Fan and thermal issues .
Red, blinking at 1 flash per 4 seconds	System power problems exist. See Hardware issues .

¹ 10°C to 35°C (50°F to 95°F)

Rear panel components



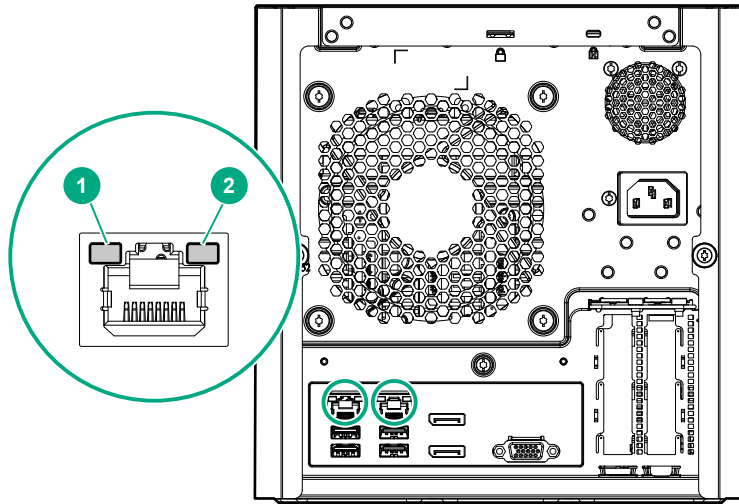
Item	Component	Description
1	Padlock eye	To lock the chassis cover and prevent access to the internal components, attach a padlock here.
2	Kensington security slot	To secure the server to a heavy or immovable object, connect an anti-theft security cable here.
3	Power jack	Connects the power cord.
4	Expansion slot 2, PCIe3 ×4 (1)	For additional hardware capabilities, install a compatible low-profile PCIe expansion board here. This expansion slot supports expansion boards with a physical connector link widths of up to ×16. ¹
5	Expansion slot 1, PCIe3 ×8 (8, 4, 1)	For additional hardware capabilities, install a compatible low-profile PCIe expansion board here. This expansion slot supports expansion boards with a physical connector link widths of up to ×16. ¹
6	Video port	Connects to an analog VGA monitor or projector.
7	Display port 1	Connects to a digital display device, such as a high-resolution set top boxes or TV displays. ²
8	Display port 2	Connects to a digital display device, such as a high-resolution set top boxes or TV displays. ²
9	USB 2.0 ports (2)	Connect USB 2.0 devices to these ports.
10	USB 3.0 ports (2)	Connect USB 3.0 devices to these ports. USB 3.0 support after POST varies by operating system.
11	NIC port 1 (1 Gb)	Connect an Ethernet cable here to connect the server to a wired network. ³
12	NIC port 2 (1 Gb)	Connect an Ethernet cable here to connect the server to a wired network. ³

¹ This expansion slot is open-ended, which enables down-plugging. Down-plugging means a larger-width expansion board can be installed in a smaller-width connector. For this server, the expansion slot supports low-profile expansion boards with a physical connector link width of up to ×16. The board operates at the highest common negotiable link width specified for the slot.

² To support 4K resolution at a full 60 Hz frame rate, this Display port requires dual-channel memory configuration. Single-channel memory configuration will only support up to 30 Hz frame rate.

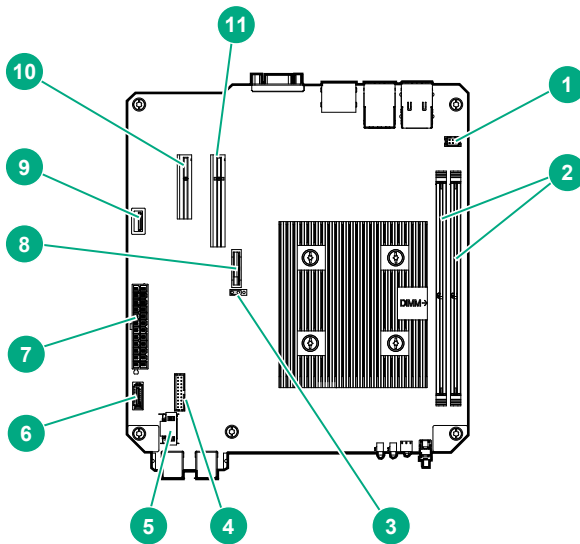
³ This NIC port supports 10/100/1000 Mbps data transfer rate per port.

Rear panel LEDs



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

System board components

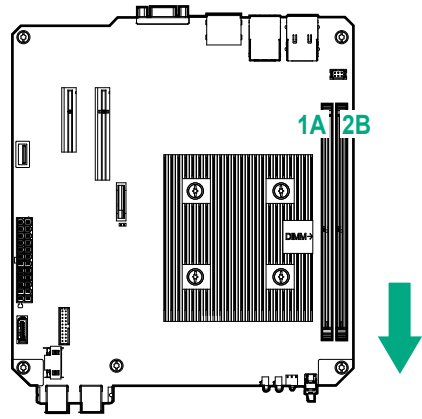


Item	Component	Description
1	Fan connector	Connects the fan cable.
2	DIMM slots	These slots support standard UDIMMs with ECC only.
3	CMOS header	Use the jumper on this header to clear the CMOS.
4	TPM connector	This connector supports the TPM 2.0 option for data security solution.
5	LFF/SFF drive SATA port	Connects the LFF/SFF drive SATA cable.
6	Optical drive or SSD SATA port	Connects the optical drive or SSD SATA cable.
7	System board power connector	Connects the power supply cable.
8	System battery	This battery provides power to the server real-time clock and BIOS settings.
9	Internal USB 2.0 port	Connect internal USB devices to this port.
10	Expansion slot 2, PCIe3 ×4 (1)	For additional hardware capabilities, install a compatible low-profile PCIe expansion board here. This expansion slot supports expansion boards with a physical connector link widths of up to ×16. ¹
11	Expansion slot 1, PCIe3 ×8 (8, 4, 1)	For additional hardware capabilities, install a compatible low-profile PCIe expansion board here. This expansion slot supports expansion boards with a physical connector link widths of up to ×16. ¹

¹ This expansion slot is open-ended, which enables down-plugging. Down-plugging means a larger-width expansion board can be installed in a smaller-width connector. For this server, the expansion slot supports low-profile expansion boards with a physical connector link widths of up to ×16. The board operates at the highest common negotiable link width specified for the slot.

DIMM slot locations

The DIMM slots are numbered 1 and 2. The arrow in the following illustration points to the front of the server.



Basic operations

Power up the server

About this task

Press the Power On/Standby button.

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

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 4 seconds to force the server to enter standby mode.

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

The system power LED changes to red indicating that the server is in standby mode. Auxiliary power is still present in the system in this mode.

Remove the front bezel

To access the drive bays, remove the front bezel.

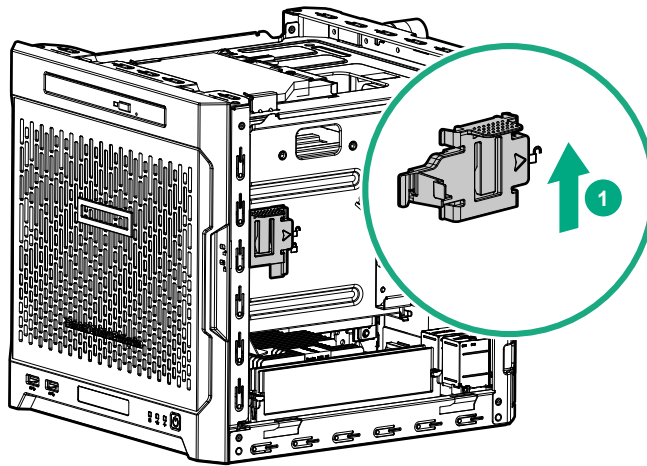
Removing a locked front bezel

Prerequisites

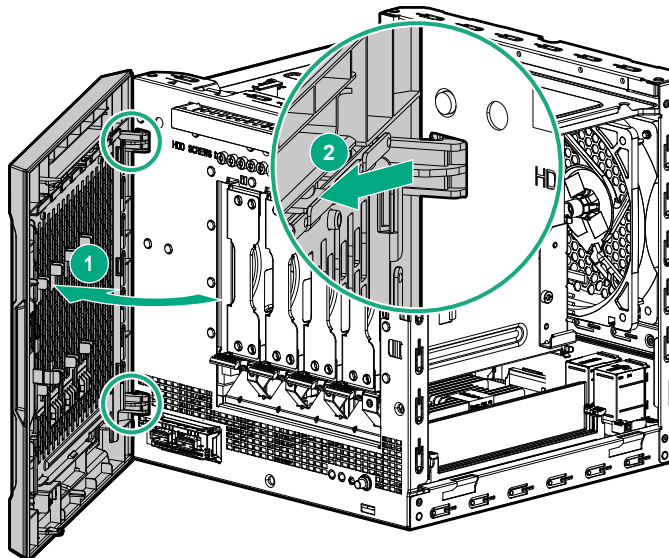
1. **Power down the server** on page 17.
2. Disconnect the power cord from the AC source, and then from the server.
3. Disconnect all peripheral cables from the server.
4. **Remove the chassis cover** on page 20.

Procedure

1. To unlock the front bezel from the chassis, slide the release tab upward.



2. Open the front bezel.
3. To completely detach the bezel from the front panel, release the bezel hinges from the chassis.
Retain the bezel for later use.



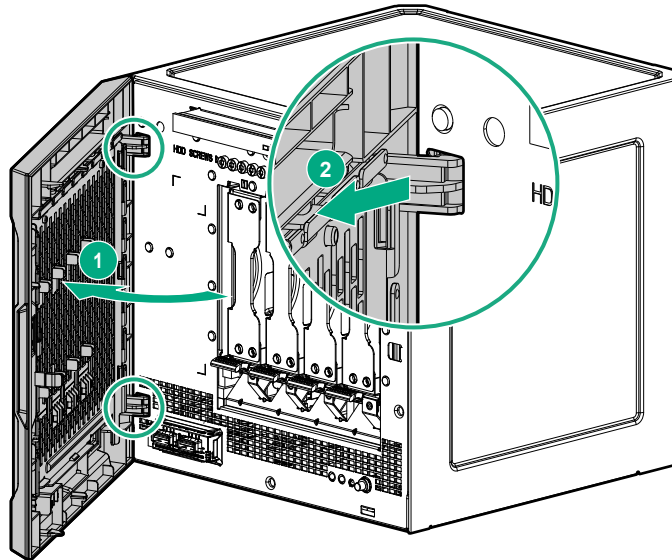
Removing an unlocked front bezel

Prerequisites

1. **Power down the server** on page 17.
2. Disconnect the power cord from the AC source, and then from the server.
3. Disconnect all peripheral cables from the server.

Procedure

1. Open the front bezel.
2. To completely detach the bezel from the front panel, release the bezel hinges from the chassis.
Retain the bezel for later use.



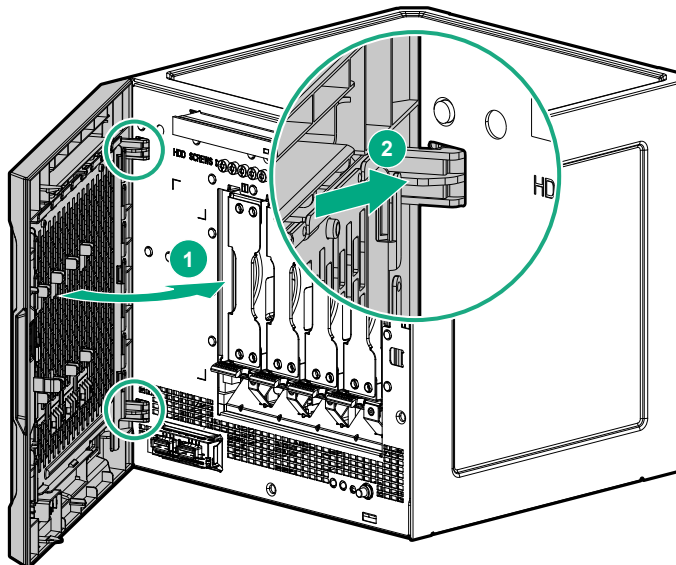
Install the front bezel

About this task

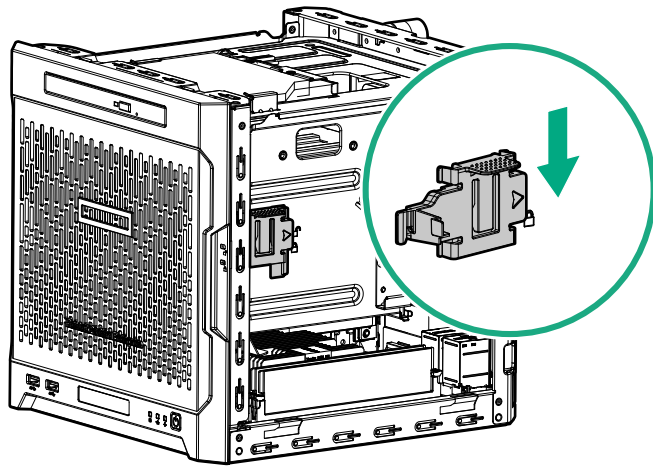
To cover the drive bays, install the front bezel.

Procedure

1. Attach the bezel to the front panel, and then close it.



2. If you prefer to secure the bezel to the chassis, do the following:
 - a. If installed, **remove the chassis cover**.
 - b. Slide the release tab downwards to lock the bezel to the chassis.



c. **Install the chassis cover** on page 21.

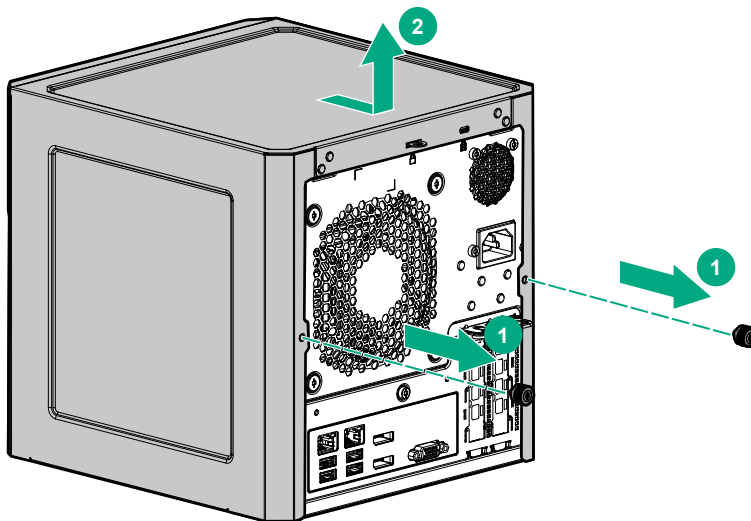
Remove the chassis cover

About this task

To access the front bezel lock and the internal components, remove the chassis cover.

Procedure

1. If installed, unlock and remove the security padlock and/or the Kensington security lock.
For more information, see the lock documentation.
2. Remove the chassis cover thumbscrews.
If the thumbscrews are too tight, use a T-15 screwdriver to remove it.
3. Slide the chassis cover toward the rear panel, and then lift it from the server.



Install the chassis cover

To prevent access to the front bezel lock and the internal components, install the chassis cover.

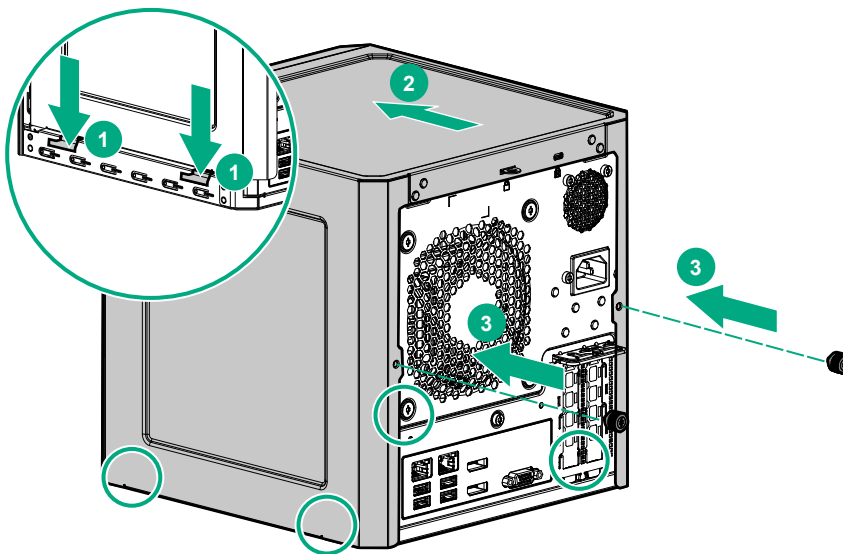
Install the chassis cover

Prerequisites

1. Verify that all internal cables are properly connected and are secured in their respective cable ties.
2. Verify that the drive cables are not blocking the fan blades.

Procedure

1. Insert the tabs on the bottom left and right sides of the chassis cover into the corresponding slots on the chassis.
2. Slide the chassis cover towards the front panel.
3. Install the chassis thumbscrews.



4. If removed, install the security padlock and/or the Kensington security lock.
For more information, see the lock documentation.

Install the system board assembly

To secure the system board inside the chassis, install the system board assembly.

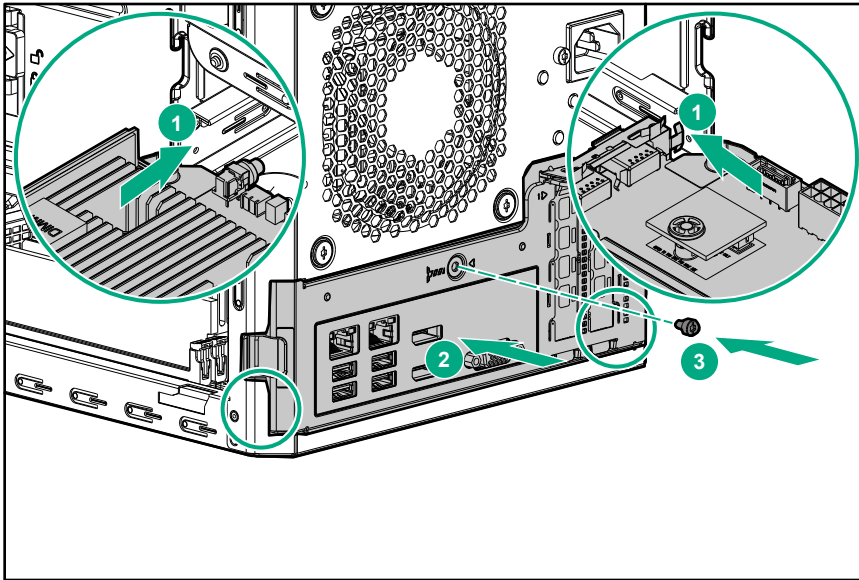
Install the system board assembly

Prerequisites

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

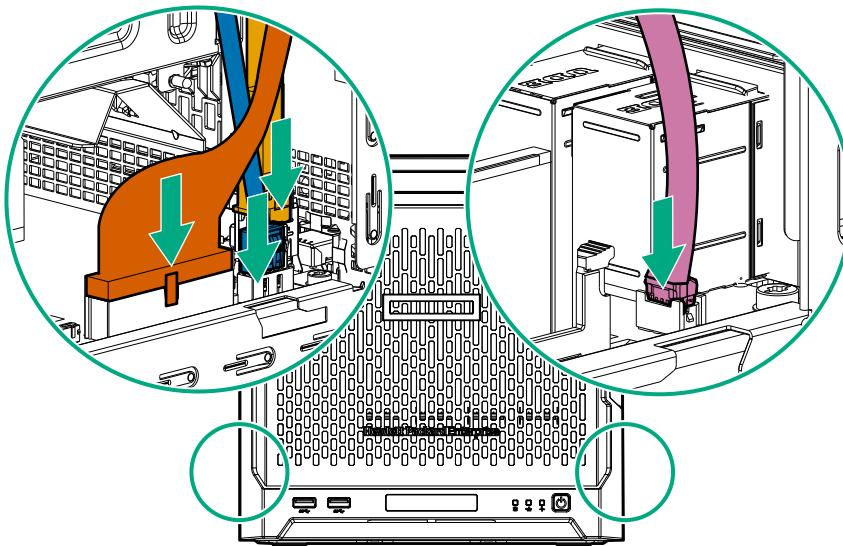
Procedure

1. Slide the system board assembly into the chassis.
2. Press against the system board assembly until it clicks into place.
3. Install the system board assembly screw.



4. Connect the following system cables:

- Power supply cable
- Optical drive or SSD SATA cable (optional)
- LFF/SFF drive SATA cable – This cable can either be connected to the system board or to an installed HBA.
- Fan cable



5. If removed, install the internal USB device.

Remove the system board assembly

To install or remove hardware components on the system board or to access the CMOS header, remove the system board assembly.

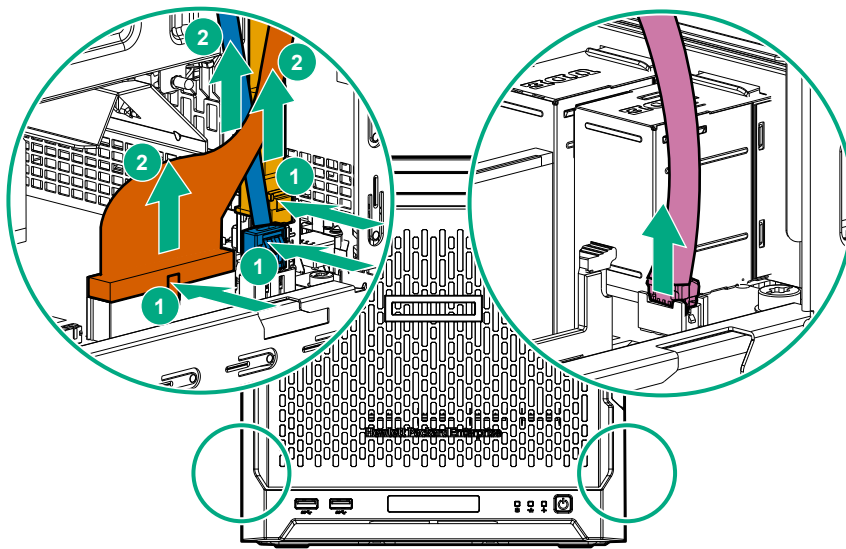
Remove the system board assembly

Prerequisites

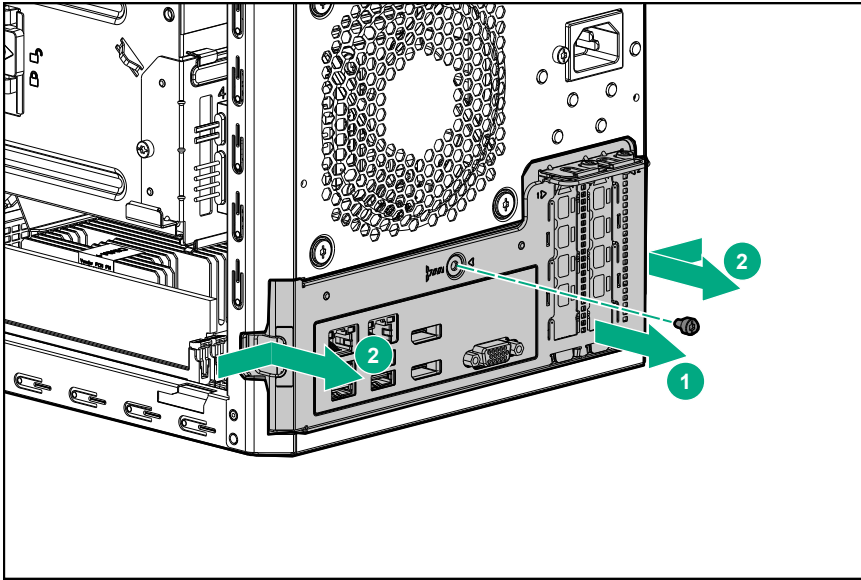
Before you perform this procedure, make sure that you have a T-15 Torx screwdriver available.

Procedure

1. If installed, remove the internal USB device.
2. To serve as a reference for system cable connections when the system board assembly is installed back into the server, take a picture of the current system board cable connections.
3. Disconnect the following system cables:
 - Power supply cable
 - Optical drive or SSD SATA cable (optional)
 - LFF/SFF drive SATA cable – This cable can either be connected to the system board or to an installed HBA.
 - Fan cable



4. Remove the system board assembly screw.
5. Place a finger in the notch on both sides of the system board assembly, and then pull out the assembly.



Troubleshooting preparation

Preparing to troubleshoot

Procedure

1. Review the **important safety information**.
2. Gather and record **symptom information**.
3. Gather all materials necessary to troubleshoot, such as a Torx screwdriver, loopback adapters, ESD wrist strap, and software utilities.

Symptom information

The following list of questions can help to identify a specific issue. Use these questions to identify the source of an issue prior to completing troubleshooting procedures. Once the symptom information has been gathered, use the appropriate sections of this guide to troubleshoot the issue. If you cannot solve the issue, or you need assistance, contact the **Hewlett Packard Enterprise Support Center**.

- Does the server power on?
- Does the server complete POST? If not, then what do the health LEDs indicate? Is the video display available?

If the server completes POST and video is available, do any POST error messages display? Record the text of the POST error message as displayed.
- Does the server successfully boot an operating system or hypervisor? If not, does the server display any of the following symptoms?
 - An uncorrectable machine check exception
 - Stop error or blue screen (Windows)
 - Purple diagnostic screen (Linux)
 - Linux kernel panic
 - A system "hang"
 - A system "freeze"
- If the problem occurs after an OS is installed:
 - Does the problem occur when a new application is loading?
 - What symptoms did the server display when the malfunction occurred? For example, did the server reboot? Were there LED codes, health logs, messages on the screen, and so forth?
- Are there any indicators present that show that the malfunction was reported as a memory error, PCI error, or so forth?
- When did the problem occur? Record exactly when the problem occurred. Include the date and time. If the issue happens multiple times, keep a list of all symptoms for each occurrence.
- What events preceded the failure? After which step does the problem occur?
- What has been changed since the last time the server was working?
- Did you recently add or remove hardware or software?
- How long has the server shown problem symptoms?
- If the problem occurs randomly, what is the duration or frequency?

Preparing the server for diagnosis

Prerequisites

- Verify that the appropriate software is installed on the server.
- Hewlett Packard Enterprise recommends that you access the server documentation in the [Hewlett Packard Enterprise Information Library](#).

Procedure

1. Verify that the server is in the proper operating environment with adequate power, air conditioning, and humidity control.

For the required environmental conditions, see the server user guide in the [Hewlett Packard Enterprise Information Library](#).

2. Record all error messages displayed by the system.
3. Remove all CD-ROMs, DVD-ROMs, USB drive keys, or SD cards that are not bootable devices.

Minimum hardware configuration

During the troubleshooting process, you might be asked to reduce the server to its minimum hardware configuration. This configuration consists of only the components required to boot the server and successfully pass POST.

When reducing the server to its minimum hardware configuration, keep in mind the following:

- Before removing any components, determine the minimum configuration for each component and follow all guidelines in the server user guide.
- The processor is embedded into the system board. If an issue occurs with the processor, replace the system board.

Breaking down the server to minimum hardware configuration

Procedure

1. Determine the minimum configuration for each component.
2. If installed, uninstall the following components based on the removal guidelines described in the server maintenance and service guide, which can be found in the [Hewlett Packard Enterprise Information Library](#).

- Additional DIMMs

Leave only the minimum number of DIMMs required to boot the server. For more information, see the memory guidelines in the Gen10 memory user guide.

- Hard drives and solid-state drives
- Optical drives (DVD-ROM, CD-ROM, and so forth)
- Expansion boards

DIMM installation and configuration guidelines

DIMM population order and configuration are critical in maximizing performance for the system. For more information, see the Gen10 memory user guide on the [Hewlett Packard Enterprise website](#).

DIMM handling guidelines

When handling a DIMM, observe the following guidelines:

- Avoid electrostatic discharge.
- Always hold DIMMs by the side edges only.
- Avoid touching the connectors on the bottom of the DIMM.
- Never wrap your fingers around a DIMM.
- Avoid touching the components on the sides of the DIMM.
- Never bend or flex the DIMM.



CAUTION:

Failure to properly handle DIMMs can cause damage to the components on the DIMM, as well as the system board connector.

DIMM installation guidelines

When installing a DIMM, observe the following guidelines:

- Before seating the DIMM, open the DIMM slot and align the DIMM with the slot.
- To align and seat the DIMM, use two fingers to hold the DIMM along the side edges.
- To seat the DIMM, use two fingers to apply gentle pressure along the top of the DIMM.

For more information, see the [**Hewlett Packard Enterprise website**](#).

Hardware issues

General hardware issues

Loose connections

The first step to troubleshooting any issue is to verify that no loose connections exist. Verify the following:

- The power cord and internal power supply cable is securely connected.
- All cables are properly routed and securely connected for all internal and external components.
- No data or power cables are damaged. Remove and check each data and power cable for damage. Verify that no cables have bent pins or damaged connectors.
- If a device has latches, verify that they are closed and locked. If screws are integrated into the latch, verify that the screws are properly tightened.
- Each device is properly seated. Avoid bending or flexing circuit boards when reseating components.

If problems continue to occur, remove and reinstall each device, checking the connectors and sockets for bent pins or other damage.

New hardware issues

Cause

- The hardware is not supported.
- A memory bank is not fully populated.
- The data cable of a new device is connected, but the power cable is not connected.

Action

Procedure

1. Verify that the hardware being installed is supported on the server.

If the hardware is not supported, remove the hardware.

For more information on supported hardware, see the product QuickSpecs on the HPE ProLiant MicroServer Gen10 website:

<http://www.hpe.com/server/microserver>

2. Verify that a change to the hardware release did not cause the issue.

For more information, see the release notes included with the hardware. If no documentation is available, see the **Hewlett Packard Enterprise Information Library**.

3. Verify that the new hardware is properly installed.
4. Verify that no conflicts or interrupt exist with the memory or I/O device.
5. Verify that no loose connections exist. For more information, see **Loose connections**.
6. Verify that all cables are connected to the correct locations and are the correct lengths.

For more information, see the server user guide in the **Hewlett Packard Enterprise Information Library**.

7. Verify that other components were not unseated during the installation of the new hardware component.
8. Verify that all necessary software updates, such as device drivers, ROM updates, and patches, are installed and current. Additionally, verify that the correct version for the hardware is installed.

For example, if you are using a Smart Array controller, verify that the latest Smart Array Controller device driver is installed. Uninstall any incorrect drivers before installing the correct drivers.

9. After installing or replacing boards or other options, verify that the system recognizes all changes to the hardware in the **Aptio Setup Utility**. If the new hardware is not configured properly, a POST error message might display, indicating a configuration error.
10. Verify that all switch settings are correct.
For more information about required switch settings, see the server user guide in the **Hewlett Packard Enterprise Information Library**.
11. Verify that all boards are properly installed in the server.
12. Uninstall the new hardware.

Third-party device issues

Procedure

1. Verify that the server and operating system support the device.

For more information, see the server and operating system documentation.

2. Verify that the latest device drivers are installed.
3. Verify that the device is properly installed.

For more information on which PCIe technology is supported and for the slot PCIe bus width, see **Rear panel components**.

For more information about a particular device, see the device documentation.

Testing the device

Procedure

1. Uninstall the device.

If the server works when the device is removed, then one of the following issues exists:

- An issue exists with the device.
 - The server does not support the device.
 - The device conflicts with another device.
2. If there is only one device on a bus, verify that the bus works by installing a different device on the bus.
 3. To determine if the device is working, install the device:
 - a. In a PCIe slot on a different bus.
 - b. In the same slot in another working server of the same or similar design.

Restart the server each time the device is reinstalled.

If the board works in any of these slots, either the original slot is bad or the board was not properly seated. Reinstall the board into the original slot to verify.

4. If you are testing a board (or a device that connects to a board):
 - a. Test the board with all other boards removed.
 - b. Test the server with only that board removed.
5. Clear the CMOS.

For more information, see **Clearing the BIOS configuration settings**.

6. Verify that the PCIe device or graphics controller does not need additional power to operate. For more information, see the device documentation.

Power issues

Server does not power on

Symptom

The server will not power on.

Cause

- The power cord or internal power supply cable might not be securely connected.
- Issues might exist with the power supply or power source.
- The circuit breaker is in the off position.
- There is not enough power allocated to support the server.
- The line voltage is not sufficient for the load.

Action

Procedure

1. Press the Power On/Standby button to verify that the server is powered on.
For more information, see [Front panel LEDs and buttons](#).
2. Verify that no loose connections exist.
For more information, see [Loose connections](#).
3. Verify that all components are properly seated.
4. Verify that the power supply is supported on the server.
For more information, see [Power supply issues](#).
5. Verify that the power source meets applicable standards.
6. Plug another device into the power outlet to verify that the outlet is working properly.
For more information, see [Power source issues](#).
7. Verify that the circuit breaker is in the On position.
8. Have a qualified electrician check the line voltage to verify that it meets the required specifications.

Power supply issues

Symptom

The server will not power on.

Cause

- The power supply cable is disconnected from the system board.
- AC power is unavailable.
- The power supply failed.
- The power supply is in standby mode.
- The power supply has exceeded the current limit.
- The power supply is not supported on the server.

Action

Procedure

1. Verify that no loose connections exist.

For more information, see **Loose connections**.

2. Verify that the power supply is supported on the server.
3. Check the system power LED to see if it indicates an issue.
 - a. If the system power LED is red, replace the power supply.
 - b. If the system power LED is amber, then the power supply is in standby mode.
 - c. If the system power LED is off, check the power source. Then, power on the server again.

If the power source is working properly, and the LED remains off, replace the power supply.

Power source issues

Symptom

The server will not power on.

Cause

- The grounded power outlet is not working.
- The power cord is not functional.
- The power strip is not functional.
- The circuit breaker is in the Off position.
- The line voltage is insufficient for the load.

Action

Procedure

1. Press the Power On/Standby button to verify that the server is powered on.

For more information, see **Front panel LEDs and buttons**.
2. Verify that no loose connections exist.

For more information, see **Loose connections**.
3. Plug another device into the grounded power outlet to verify that the outlet works. Also, verify that the power source meets applicable standards.
4. Replace the power cord with a known functional power cord to verify that it is working properly.
5. Replace the power strip with a known functional power strip to verify that it is working properly.
6. Verify that the proper circuit breaker is in the On position.
7. Have a qualified electrician check the line voltage to verify that it meets the required specifications.

UPS issues

UPS is not working properly

Cause

- The UPS switch is not in the On position.
- The UPS batteries are not charged to the proper level.
- The UPS software is not up-to-date.
- The UPS power cord is not connected.
- The UPS power cord is not the correct type for the UPS and the country/region in which the server is located.

Action

Procedure

1. Verify that the UPS batteries are charged to the proper level for operation. For more information, see the UPS documentation.
2. Verify that the UPS power switch is in the On position. For the location of the switch, see the UPS documentation.
3. Verify that the UPS software is updated to the latest version. Use the Power Management software on the **Hewlett Packard Enterprise website**.
4. Verify that the power cord is the correct type for the UPS and the country/region in which the server is located. For specifications, see the UPS reference guide.
5. Verify that the line cord is connected.
6. Verify that each circuit breaker is in the On position, or replace the fuse if needed. If this occurs repeatedly, contact an authorized service provider.
7. Check the UPS LEDs to verify that a battery or site wiring issue has not occurred. See the UPS documentation.
8. If the UPS sleep mode is initiated, disable sleep mode for proper operation. The UPS sleep mode can be turned off through the configuration mode on the front panel.
9. Change the battery to verify that the damage was not caused by excessive heat, particularly if a recent air conditioning outage has occurred.

Low battery warning is displayed on the UPS

Symptom

A low battery warning is displayed on the UPS.

Cause

- The batteries need to be charged.
- The batteries are failing to hold a charge.
- The batteries are faulty.

Action

Procedure

1. Plug the UPS into an AC grounded outlet for at least 24 hours to charge the batteries.
2. Test the batteries.
3. Replace the batteries if necessary.
4. Be sure the alarm is set appropriately by changing the amount of time given before a low battery warning. For more information, see the UPS documentation.

Internal system issues

Fan and thermal issues

Fans are not working

Symptom

The fans are not working.

Cause

- The fan airflow might be blocked.
- An air baffle or blank is missing or not installed properly, causing a disruption in the airflow.
- The fan cable is not properly connected.
- The server is not properly ventilated.

Action

Procedure

1. Verify that no loose connections exist.
For more information, see **Loose connections**.
2. Check the front panel LEDs to see if any LEDs indicate an issue.
For more information, see **Front panel LEDs and buttons**.
3. Verify that cables or other material are not blocking the fan airflow path.
4. Verify that no ventilation issues exist.

If the system has been operating for an extended period with the chassis cover removed, airflow might have been impeded. Fans operate at 100% when the chassis cover is removed.

Fans are running at a higher than expected speed

Symptom

The fans are running at a higher speed than expected.

Cause

- The system temperature sensor reading is high and within approximately 10°C of the maximum operating temperature.
- An air baffle or blank is missing or not installed properly, causing a disruption in the airflow.
- The processor heatsink is not installed properly.

Action

Procedure

1. Update the server to the latest firmware version, such as system BIOS, option firmware, etc.
For more information about updating the firmware, see **Keeping the system current**.
2. Check the temperature. If a temperature sensor is high and within approximately 10°C of the maximum operating temperature, fan speeds can be higher than normal.
3. Verify that all air baffles and required blanks, such as processor heatsink blanks, power supply blanks, etc., are installed.
4. Verify that the correct processor heatsink is installed.
5. If the system supports both standard and performance fans, verify that the correct fan is installed.

Excessive fan noise (low speeds)

Symptom

Abnormal/rattling noise is observed at low fan speeds.

Cause

An issue exists with the fan.

Action

Procedure

- Replace the fan.

For more information, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

Server shuts down or reboots without warning

Symptom

- The server shuts down or reboots without being prompted.
- The health LED is blinking amber.
- The server displays fan or thermal issues as the system is powering on.

Action

Procedure

1. Verify that the fan cable is securely and properly connected.
2. Verify that the ambient temperature meets operating requirements.
3. Verify that the chassis cover is properly installed on the server.
4. Verify that the processor heatsink is properly installed.

If issues continue to occur with the fan, replace the fan.

For more information, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

Trusted Platform Module issues

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.

TPM fails or is not detected

Symptom

The TPM has failed or is not detected.

Action

Procedure

- Leave the TPM installed and request a new system board and TPM from a Hewlett Packard Enterprise authorized service provider. For more information, see [Accessing Hewlett Packard Enterprise Support](#).

CAUTION:

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, consider the system compromised and take appropriate measures to ensure the integrity of system data.

Memory issues

General memory issues

Cause

- The DIMM does not meet server requirements.
- A DIMM has failed.
- Third-party memory is installed on the server.
- The DIMM is not properly seated.

Action

Procedure

1. Isolate and minimize the DIMM configuration.
To determine the minimum configuration for DIMMs, see the Gen10 memory user guide in the [Hewlett Packard Enterprise Information Library](#).
Use care when handling DIMMs. For more information, see [DIMM handling guidelines](#).
2. Verify that the memory meets the server requirements and is installed according to the procedures found in the server user guide.
Some servers might require that memory channels be fully populated or that all memory within a memory channel is the same size, type, and speed. To determine if the memory is installed properly, see the server user guide in the [Hewlett Packard Enterprise Information Library](#).
3. Check any server LEDs that correspond to memory slots.
4. Test each channel of DIMMs, and test each DIMM.
 - a. To verify that the channel is working, place one DIMM in a channel and remove all other DIMMs. Use the same DIMM to test each channel.
 - b. To verify that the DIMM is working, place one DIMM in a known functioning channel. If the DIMM works, switch the DIMM with another DIMM.
Continue this process until you have identified the failed DIMM or until you have tested each DIMM.
5. Remove any third-party memory.
6. Update the system ROM.

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

7. Replace the DIMM.

For more information, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

DIMM configuration errors

Symptom

A POST error message displays indicating that there are issues with DIMM configuration.

Cause

- The memory channel was not populated in the correct order.
- An unsupported DIMM is installed in the server.

Action

Procedure

1. Verify that the DIMMs are supported on the server.

For a list of supported options, see the product QuickSpecs on the HPE ProLiant MicroServer Gen10 website:

<http://www.hpe.com/server/microserver>

2. Verify that the DIMMs are installed according to the DIMM population guidelines in the Gen10 memory user guide in the [Hewlett Packard Enterprise Information Library](#).
3. Update the system ROM.

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

Server is out of memory

Symptom

A POST error message is displayed indicating that the server is out of memory.

Cause

- The memory is not configured properly.
- An OS error is indicated.

Action

Procedure

1. Verify that the memory is configured properly.

To determine the memory configuration requirements, see the Gen10 memory user guide in the [Hewlett Packard Enterprise Information Library](#).

2. Verify that no operating system errors are indicated.

If operating system errors display, complete the steps necessary to resolve the errors.

3. Update the system ROM.

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

Server does not recognize new memory

Symptom

The server does not recognize a newly installed DIMM.

Cause

- The DIMM is not supported on the server.
- The DIMM is not properly installed.
- The memory limits are exceeded for the server.
- The DIMM is not properly seated.
- The DIMM is degraded.

Action

Procedure

1. Verify that the DIMM is supported on the server.

For a list of supported options, see the product QuickSpecs on the HPE ProLiant MicroServer Gen10 website:

<http://www.hpe.com/server/microserver>

2. Verify that the DIMM is installed according to the server requirements.

For more information, see the server user guide in the [Hewlett Packard Enterprise Information Library](#).

3. Verify that you have not exceeded the memory limits of the server or operating system.
4. Verify that the DIMM is seated properly.
5. Install the DIMM into a known working server to verify that the DIMM works.

Verify that the DIMM meets the requirements of the server on which you are testing.

6. Update the system ROM.

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

7. Replace the DIMM.

For more information, see the maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

Server does not recognize existing memory

Symptom

The server does not recognize existing memory.

Cause

- The memory is not configured properly.
- The DIMM is degraded.
- The DIMM is not installed or properly seated.

Action

Procedure

1. Verify that the memory is configured properly.

For guidelines about memory configuration, see the server user guide in the [Hewlett Packard Enterprise Information Library](#).

2. Reseat the DIMM.

Use care when handling DIMMs. For more information, see [DIMM handling guidelines](#).

3. Replace all degraded DIMMs.

For more information, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

4. Update the system ROM.

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

Correctable memory error threshold exceeded

Symptom

- Performance is degraded.
- ECC errors occur with no other symptoms.

Cause

- The DIMM is not installed or properly seated.
- The DIMM has failed.

Action

Procedure

1. Update the system ROM.

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

2. Replace the DIMM.

For more information, see the maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

Uncorrectable memory error

Symptom

- A POST error message displays
- Stop error or blue screen (Windows)
- Purple diagnostic screen (Linux)
- Linux kernel panic
- A system "hang"
- A system "freeze"
- Server restarts or powers down unexpectedly
- Parity errors occur

Cause

- The DIMM is not installed or properly seated.
- The DIMM has failed.

Action

Procedure

1. Reseat the DIMM.

Use care when handling DIMMs. For more information, see [DIMM handling guidelines](#).

2. Update the system ROM.

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

3. If issues continue to occur, replace the DIMM.

For more information, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

System board issues

Symptom

A POST error message is received indicating an issue exists with the system board.

Action

Procedure

1. Review all error messages for possible issues with other components. Then, troubleshoot the components identified.
2. Verify that no loose connections exist on the system board.

For more information, see [Loose connections](#).

3. Remove any components recently added.

For more information on removal and replacement procedures, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

4. Power down and remove all power from the server.

Remove the system battery for 10 minutes. Then, reinstall the battery and power on the server. To locate the system battery, see [System board components](#).

5. Reset the BIOS configuration settings to default.

For more information, see [Restoring and customizing configuration settings](#).

6. If issues continue to occur, contact the [Hewlett Packard Enterprise Support Center](#).

System battery is low or has lost power

Symptom

An error message is received indicating that the system battery is low or has lost power.

Cause

Real-time clock system battery is running low on power or has lost power.

Action

Procedure

- Replace the battery.

For more information, see the server maintenance and service guide in the [Hewlett Packard Enterprise Information Library](#).

Drive issues (hard drives and solid state drives)

Drives do not display

Symptom

The drives do not display on the server.

Cause

- The drive data cable is not functioning properly.
- The drive is not properly installed.
- The drives have failed.
- The drives are not recognized.

Action

Procedure

1. Verify that no loose connections exist.

For more information, see **Loose connections**.

2. Check the following components for updates:

- Embedded Marvell storage controller firmware
- Smart Array Controller firmware
- Host bus adapter firmware
- System ROM

3. Verify that the drive data cable is functioning properly by replacing it with a known functioning cable.

If the drive displays when the drive data cable is replaced, then issues exist with the original drive data cable. Replace the cable.

4. Verify that the drives are properly installed when the server is operating.

If the drives are not properly installed, the drives might overheat, which could cause slow response or drive failure.

5. Verify that the selected boot mode supports the drive partition format.

For more information, see **Boot option**.

6. Verify that the drive bay is working properly by installing the hard drive in a different drive bay.

7. Use one of the following to check the status of the drives:

- If the drives are connected to the LFF/SFF drive SATA port, use the **Marvell Storage Utility** or the **Marvell BIOS Utility**.
- If the drives are connected to an HPE Smart HBA or Smart Array controller option, use the **HPE Smart Storage Administrator**.

8. Verify that the replacement drives within an array are the same size or larger and are the same drive type, such as SAS, SATA, or SSD.

9. Reboot the server.

If the drive displays, check the drive firmware for updates.

If the drive does not display, replace the drive.

Data is inaccessible

Symptom

The data on the drives cannot be accessed.

Cause

- The files are corrupt.
- Viruses exist on the server.
- A TPM is installed, but not properly enabled on the server.

Action

Procedure

1. Run the repair utility for the operating system to verify that the files are not corrupt.
2. Run the current version of a virus scan utility to verify that no viruses exist on the server.
3. If a TPM is installed and being used with BitLocker, verify that the TPM is enabled in the Aptio Setup Utility.

For more information, see **Enabling the Trusted Platform Module**. Additionally, see the TPM replacement recovery procedure in the operating system documentation.

4. Migrate encrypted data to a new server.

When migrating encrypted data to a new server, follow the recovery procedures in the operating system documentation.

Server response time is slow

Symptom

The server response time is slow.

Cause

- The drive is full.
- The operating system encryption technology is causing a decrease in performance.
- A recovery operation is pending on the logical drive.

Action

Procedure

1. Verify that the drive is not full.

Hewlett Packard Enterprise recommends that drives have a minimum of 15 percent free space.

2. Review information about the operating system encryption technology, which could cause a decrease in server performance.

For more information, see the operating system documentation.

3. If you are using an HPE Smart HBA or Smart Array controller, use HPE SSA to verify that a recovery operation is not pending on the logical drive.

For more information, see **HPE Smart Storage Administrator**.

USB drive key issues

System does not boot from the USB drive key

Symptom

The system does not boot from the USB drive key.

Cause

- The drive boot order is not set to boot from the USB drive key.
- The USB drive key is not properly seated.

Action

Procedure

1. Verify that the drive boot order in the Aptio Setup Utility is set to allow the server to boot from the USB drive key.
2. Verify that the selected boot mode supports the USB drive key partition format.
For more information, see **Boot option**.
3. Reseat the USB drive key.
4. Move the USB drive key to a different USB port, if available.

CD-ROM and DVD drive issues

System does not boot from the CD-ROM or DVD drive

Symptom

The system does not boot from the CD-ROM or DVD drive.

Cause

- The drive boot order is not set to boot from the CD-ROM or DVD drive.
- The CD-ROM or DVD drive is damaged.
- The CD-ROM or DVD drive is not connected or cabled properly.

Action

Procedure

1. Verify that the drive boot order in the Aptio Setup Utility is set so that the server boots from the CD-ROM or DVD drive first.
2. Verify that all cords and cables are securely and properly connected.
For more information, see **Loose connections**.
3. Verify that the media from which you are attempting to boot is not damaged and is a bootable CD-ROM or DVD drive.
4. If you are attempting to boot from an external USB CD-ROM or DVD drive, see the operating system and server documentation to verify that booting from an external USB CD-ROM or DVD drive is supported.

Data from the CD-ROM or DVD is inconsistent, or CD-ROM or DVD cannot read data

Symptom

The data from the CD-ROM or DVD drive is inconsistent or cannot be read.

Cause

- The CD or DVD has material or residue on the surface.
- The CD or DVD is not valid for the drive.

Action

Procedure

1. Clean the drive and media.
2. If a paper or plastic label has been applied to the surface of the CD-ROM or DVD in use, remove the label and any adhesive residue.
3. Verify that the inserted CD or DVD format is valid for the drive. For example, make sure that you are not inserting a DVD into a drive that only supports CDs.

Drive is not detected

Symptom

The CD-ROM or DVD drive is not detected.

Cause

- The CD-ROM or DVD drive is not cabled properly.
- The CD-ROM or DVD drive cables are not connected properly.
- The CD-ROM or DVD drive cable is not working.
- The driver is not correct or up-to-date.

Action

Procedure

1. Verify that no loose connections exist.

For more information, see **Loose connections**.

2. Verify that the power-SATA Y-cable is properly connected to the optical drive.

Verify that one end of the power-SATA Y-cable is connected to the optical drive, and verify that the split ends of the Y-cable are connected to the system board and the power supply.

3. Verify that the cables are connected according to the instructions found in the documentation for the CD-ROM or DVD drive and the server.

For more information, see the CD-ROM or DVD drive documentation, or see the server documentation in the **Hewlett Packard Enterprise Information Library**.

4. Verify that the cables are working properly.

To verify, replace the cable with a known functioning cable. If the drive displays, then replace the original cable.

5. Verify that the correct driver is installed and current.

Tape drive issues

This section includes the most common tape drive issues. Actions are listed in the order that they should be attempted. If the issue is resolved, it is not necessary to complete the remaining actions. All actions might not apply to all tape drives.

For more information, see the Storage section of the **Hewlett Packard Enterprise Information Library**. To download the HPE Library and Tape Tools (L&TT), see the **Hewlett Packard Enterprise website**.

Tape drive does not eject

Symptom

The tape drive is stuck and will not eject.

Cause

- The SAS/HBA/driver configuration of the drive is incorrect.
- The tape drive is damaged.
- One or more tape drive cables are damaged.

Action

Procedure

1. Manually press the Eject button.
Wait for up to 10 minutes for the tape to rewind and eject.
2. Perform a forced eject.
 - a. Press and hold the Eject button for at least 10 seconds.
 - b. Wait for up to 10 minutes for the tape to rewind and eject.
The green Ready LED should flash.
3. Power cycle the drive.
Wait for up to 10 minutes for the drive to become ready again.
4. Check for conflicts in backup software services.
5. Check the SAS/HBA/driver configuration of the drive.
6. Check media and cables. Discard any media or cables that are damaged.
7. If issues continue to occur, contact the [**Hewlett Packard Enterprise Support Center**](#).

Read/write issues are occurring

Symptom

The tape drive is experiencing read or write issues.

Action

Procedure

1. Run the Drive Assessment Test found in HPE Library and Tape Tools.
Running the Drive Assessment Test overwrites the tape. If it is not possible to overwrite the tape, run the logs-based Device Analysis Test instead.
2. Run the Media Assessment Test in HPE Library and Tape Tools.
This test is read-only.

Tape drive backup fails

Symptom

The tape drive backup fails to complete without issues.

Action

Procedure

1. Run the Drive Assessment Test in HPE Library and Tape Tools.
Running the Drive Assessment Test overwrites the tape. If it is not possible to overwrite the tape, run the logs-based Device Analysis Test instead.
2. Check the backup logs.
3. Verify that a supported configuration is being used.

4. Check for media damage, such as:
 - Incorrect label placement
 - Broken, missing, or loose leader pin
 - Damaged cartridge seam
 - Usage in incorrect environment
5. Check for software issues.
 - a. Check the backup software.
 - b. Verify that the virus scanning software is not scheduled to run at the same time as the backup.
6. Verify that a tape can be formatted.

Media issues

Action

Procedure

1. Verify that the correct media part number is being used.
2. Pull a support ticket using HPE Library and Tape Tools.
 - Look for issues in the cartridge health section.
 - Look for issues in the drive health section.
3. Run the Media Assessment Test in HPE Library and Tape Tools.
4. Check for media damage, such as:
 - Incorrect label placement
 - Broken, missing, or loose leader pin
 - Damaged cartridge seam
 - Usage in incorrect environment
5. Check the Tape Error LED. If the LED is flashing, do the following:
 - a. Reload the suspect tape.

If the Tape Error LED stops flashing, the issue has cleared.

If the LED continues to flash, discard the suspect media.
 - b. Load a new or known good tape.
6. Discard any media that has been used at temperatures greater than 45°C (113°F) or less than 5°C (41°F).

External device issues

Video issues

Screen is blank for more than 60 seconds after powering up the server

Symptom

The screen is blank for more than 60 seconds after the server is powered up.

Cause

- The monitor is not receiving power.
- The monitor is not cabled properly.
- The monitor cables are not connected properly.
- The power is not sufficient for a PCIe device or graphics controller installed on the server.
- A video expansion board is installed, but is not powered or configured properly.

- A video expansion board installed on the server is not supported.
- The video drive is not current.

Action

Procedure

1. Verify that the monitor power cord is plugged into a working grounded (earthed) AC outlet.
2. Power up the monitor and be sure that the monitor light is on, indicating that the monitor is receiving power.
3. Verify that the monitor is cabled to the intended server or KVM connection.
4. Check the cable connection from the monitor to the server, and then from the server to the power outlet.
5. Press any key, or enter the password, and wait for the screen to activate to be sure the energy-saver feature is not in effect.
6. Verify that a PCIe device or graphics controller does not need additional power to operate. For more information, see the device documentation.
7. Verify that a video expansion board has not been added to replace onboard video, which would make it seem as if the video is not working.

Disconnect the video cable from the onboard video. Then, reconnect it to the video jack on the expansion board. All servers automatically bypass onboard video when a video expansion board is present.

8. Press any key, or enter the password, and wait for the screen to activate to verify that the power-on password feature is not in effect.

You can also tell if the power-on password is enabled if a key symbol is displayed on the screen when POST completes.

If you do not have access to the password, disable the power-on password using the Security menu of the Aptio Setup Utility.

Monitor does not function properly with energy saver features

Symptom

The monitor does not function properly with energy saver features.

Cause

The monitor does not support energy saver features.

Action

Procedure

- Verify that the monitor supports energy saver features. If the monitor does not support energy saver features, disable the features.

Video colors do not display correctly

Symptom

The video colors do not correctly display on the monitor.

Cause

- The video cable is not securely connected to the correct port.
- The monitor and KVM switch are not compatible with the video output of the server.
- The video cable is damaged.

Action

Procedure

1. Verify that no loose connections exist.
For more information, see **Loose connections**.
2. Verify that the VGA or Display port cable is securely connected to the correct connector on the server and the monitor.
3. Verify that the monitor and KVM switch are compatible with the video output of the server.
4. If using a KVM switching device, verify that all cables and connectors are the proper length and are supported by the switch.
For more information, see the switch documentation.
5. Verify that the VGA or Display port cable is not damaged by replacing the cable with a known functioning cable.

Slow-moving horizontal lines are displayed

Symptom

Slow-moving horizontal lines are displayed on the monitor.

Cause

Magnetic field interference is occurring.

Action

Procedure

- Move the monitor away from other monitors or power transformers.

Mouse and keyboard issues

Procedure

1. If you are using a KVM switching device, verify that the server is properly connected to the switch.
2. If you are using a KVM switching device, verify that all cables and connectors are the proper length and are supported by the switch.
3. Verify that the current drivers for the operating system are installed.
4. Verify that the device driver is not corrupted by replacing it with a known functioning driver.
5. Restart the system. Check to see if the input device functions correctly after the server restarts.
6. Verify that the keyboard or mouse is connected to the correct port.
Observe whether the keyboard lights flash at POST or the Num Lock LED illuminates. If not, change the port connections.
7. Clean the keyboard or mouse.
8. Replace the device with a known working equivalent device (a similar mouse or keyboard). Verify that the device is connected to the same USB connector on the front/rear panel as the original device.
 - If the issue still occurs with the new mouse or keyboard, then the port on the system board is defective. Replace the system board. For more information, see the server maintenance and service guide in the **Hewlett Packard Enterprise Information Library**.
 - If the issue no longer occurs, then the original input device is defective. Replace the device.

Network controller issues

Network controller has stopped working

Symptom

The network controller is no longer working.

Action

Procedure

1. Check the network controller LEDs to see if any statuses indicate the source of the issue.
For more information about LEDs, see the network controller or server documentation.
2. Verify that the correct network driver is installed for the controller and that the driver file is not corrupted. Reinstall the driver.
3. Verify that no loose connections exist.
For more information, see **Loose connections**.
4. Verify that the network cable is working by replacing it with a known functional cable.
5. Verify that the network controller is not damaged.
6. Verify that a software issue did not cause the failure.
For more information, see the operating system documentation.
7. Verify that the server and operating system both support the controller.
For more information, see the operating system or server documentation.
8. Verify that the controller is enabled in the **Aptio Setup Utility**.
9. Verify that the system ROM and controller drivers are current.
For more information, see **Keeping the system current**.
10. Verify that a valid IP address is assigned to the controller and that the configuration settings are correct.

Network controller is installed but not working

Symptom

The network controller is not working.

Action

Procedure

1. Check the network controller LEDs for statuses that indicate the source of the issue.
For more information about LEDs, see the network controller or server documentation.
2. Verify that no loose connections exist.
For more information, see **Loose connections**.
3. Verify that the correct cable type is used for the network speed or that the correct SFP or DAC cable is used.
For dual-port 10GB network devices, both SFP ports should have the same media (for example, DAC cable or equivalent SFP+ module). Mixing different types of SFP (SR/LR) on a single device is not supported.
4. Verify that the network cable is working by replacing it with a known functional cable.
5. Verify that a software issue did not cause the failure.
For more information, see the operating system or server documentation.

6. Verify that the controller is enabled in the **Aptio Setup Utility**.
7. Verify that the system ROM and controller drivers are current.
For more information, see **Keeping the system current**.
8. Verify that a valid IP address is assigned to the controller and that the configuration settings are correct.
9. Verify that the network controller is fully seated into the applicable (or supported) PCIe slot.

Network controller stopped working when an expansion board was added

Symptom

The network controller stopped working when an expansion board was added to the server.

Cause

- The network controller is not seated or properly connected.
- The OS or server does not support the network controller.
- The server configuration changed when the expansion board was installed.
- The network controller drivers have not been updated.
- The driver parameters do not match the configuration of the network controller.

Action

Procedure

1. Verify that no loose connections exist.
For more information, see **Loose connections**.
2. Verify that the server and operating system both support the controller.
For more information, see the operating system documentation.
3. Verify that the new expansion board has not changed the server configuration, requiring reinstallation of the network driver.
 - a. Uninstall the network controller driver for the malfunctioning controller in the operating system.
 - b. Restart the server and run the appropriate option in the **Aptio Setup Utility**.
Verify that the server recognizes the controller and that resources are available for the controller.
 - c. Restart the server, and then reinstall the network driver.
4. Verify that the correct drivers are installed.
For more information, see the operating system documentation.
5. Verify that the driver parameters match the configuration of the network controller.
For more information, see the operating system documentation.
6. Verify that the PCIe slots are populated according to the population guidelines.
For more information, see the server user guide in the **Hewlett Packard Enterprise Information Library**.
7. Verify that the network controller is fully seated into the applicable, or supported, PCIe slot.

Expansion board issues

System requests recovery method during expansion board replacement

Symptom

The system request a recovery method while the expansion board is being replaced on a BitLocker-encrypted server.

Action

Procedure

- Verify that BitLocker was disabled before replacing the expansion board.

When replacing an expansion board on a BitLocker-encrypted server, always disable BitLocker before replacing the expansion board. If BitLocker is not disabled, the system requests the recovery method selected when BitLocker was configured. Failure to provide the correct recovery password(s) will result in the loss of access to all encrypted data. Once the expansion board is replaced, enable BitLocker.

For more information on BitLocker, see BitLocker for Servers on the [Microsoft website](#).

Error messages during system bootup

When an error or unexpected shutdown event occurs, an error message displays during the system bootup. The following table lists the error messages that might occur.

Error message	Description
Error: Fan failure detected, the system will shut down shortly.	The fan does not work when the system is powered on. The system will automatically shut down because there is no working fan in the system. See Fan and thermal issues .
Error: Required fan not installed, the system will shut down shortly.	The fan is not installed when the system is powered on. The system will automatically shut down because there is no fan in the system. See Fan and thermal issues .
Warning: Fan failure detected at last boot.	The fan was not working when the system was last powered on. See Fan and thermal issues .
Warning: Required fan not installed at last boot.	The fan was missing when the system was last powered on. See Fan and thermal issues .
Error: Thermal temperature condition has been degraded, the system may or may not shut down depending on thermal shutdown setting.	Either the environmental temperature or the internal system temperature has triggered a warning condition. If the Thermal Shutdown option is enabled in the Aptio Setup Utility, the system will automatically initiate a graceful shutdown to protect the system. To check, access the Aptio Setup Utility. Then, select Advanced > Hardware Health Configuration . See Fan and thermal issues .

Table Continued

Error message	Description
Warning: System was probably shut down due to the thermal temperature condition being set to degraded at last boot.	<p>Either the environmental temperature or the internal system temperature triggered a warning condition when the system was last powered on.</p> <p>If the Thermal Shutdown option was enabled and the OS power button is set to shut down the system, a graceful shutdown occurred to protect the system.</p> <p>See <u>Fan and thermal issues</u>.</p>
Warning: System was shut down due to thermal temperature condition being set to failed at last boot.	<p>Either the environmental temperature or the internal system temperature triggered a failed condition when the system was last powered on. The system shuts down immediately for protection.</p> <p>See <u>Fan and thermal issues</u>.</p>
Warning: Power fault detected at last boot.	<p>A power fault event was detected during the last boot.</p> <p>See <u>Power issues</u>.</p>

Software issues

Operating system issues and resolutions

Operating system issues

Operating system locks up

Symptom

The operating system locks up.

Action

Procedure

- Scan for viruses with an updated virus scan utility.

Errors are displayed in the error log

Symptom

Error messages are displayed in the error log.

Action

Procedure

- Follow the information provided in the error log. For more information, see the operating system documentation.

Updating the operating system

Prerequisites

Before updating the operating system, read the release notes for each update.

Use care when applying operating system updates (service packs, hotfixes, and patches). Some updates overwrite files specific to Hewlett Packard Enterprise. If you do not require specific fixes from the update, Hewlett Packard Enterprise recommends that you do not apply the updates.

Procedure

1. Perform a full system backup.
2. Apply the operating system update using the instructions provided.
3. Install the current drivers.

If you apply the update and have issues, locate the files to correct the issues on the [**Hewlett Packard Enterprise website**](#).

Restoring a backup version

If you recently upgraded the operating system or software and cannot resolve the issue, try restoring a previously saved version of the system. Before restoring the backup, make a backup of the current system. If restoring the previous system does not correct the issue, you can restore the current set to be sure you do not lose additional functionality.

For more information, see the documentation provided with the backup software.

Prerequisites for reconfiguring or reloading software

About this task

If all other options have not resolved the problem, consider reconfiguring the system. Before you take this step, do the following:

Procedure

1. Weigh the projected downtime of a software reload against the time spent troubleshooting intermittent problems. You might consider starting over by removing and reinstalling the software containing issues.
2. Be sure the server has adequate resources (processor speed, drive space, and memory) for the software.
3. Be sure the server ROM is current.
4. Be sure you have printed records of all troubleshooting information you have collected to this point.
5. Be sure you have two good backups before you start. Test the backups using a backup utility.
6. Check the operating system and application software resources to be sure you have the latest information.
7. If the last-known functioning configuration does not work, try to recover the system with operating system recovery software. For more information, see the operating system documentation.

Linux resources

For troubleshooting information specific to Linux operating systems, see the [Linux for ProLiant website](#).

To assist in possible LINUX installation issues on HPE ProLiant servers, capture either the sosreport or supportconfig before contacting [Hewlett Packard Enterprise technical support](#). For more information, see [Linux tools \(sosreport and supportconfig\)](#).

Linux tools (sosreport and supportconfig)

To assist in possible Linux installation issues on HPE ProLiant servers, Hewlett Packard Enterprise will request operating system configuration information. To assist Hewlett Packard Enterprise with any investigation please gather the system configuration information before contacting [Hewlett Packard Enterprise technical support](#). After contacting Hewlett Packard Enterprise technical support you will be provided details of how to make the collected information available to Hewlett Packard Enterprise.

For each of the following Linux distributions, use the tool indicated:

- Red Hat Enterprise Linux (and distributions based on RHEL) — sosreport
- SLES — supportconfig
- Ubuntu — sosreport

Other distributions are likely to use either the sosreport or supportconfig. If your distribution does not provide either, use the distribution provided method of collecting information equivalent to sosreport and/or supportconfig. If you need to install supportconfig or sosreport, use the standard software management tools provided by your distribution.

Please note that this may not be the only information you are asked to collect. Hewlett Packard Enterprise technical support will provide details on how to collect any additional data required. The collection of any extra data may require you to install additional Hewlett Packard Enterprise or distribution provided software.

Application software issues

Software locks up

Symptom

The software locks up.

Cause

- The software might be incompatible with other software on the server.
- Known issues might exist with the software.
- The server configuration might have changed.
- The server might be infected by a virus.

Action

Procedure

1. Check the application log and operating system log for entries indicating why the software locked up.
2. Check for incompatibility with other software on the server.
3. Check the support website of the software vendor for known issues.
4. Review log files for changes made to the server that might have caused the issue.
5. Scan the server for viruses with an updated virus scan utility.

Errors occur after a software setting is changed

Symptom

The system locks up after settings were changed.

Cause

The new system settings are not supported.

Action

Procedure

- Check the system logs to determine what changes were made. Then, change the settings back to the original configuration.

Errors occur after the system software is changed

Symptom

Errors occur after the system software is changed.

Action

Procedure

- Change the settings back to the original configuration. If more than one setting was changed, change the settings back one at a time to isolate the cause of the issue.

Errors occur after an application is installed

Symptom

Errors occur after an application is installed on a server.

Action

Procedure

- Check the application log and operating system log for entries indicating why the software failed.
- Check system settings to determine if they are the cause of the error. You might need to obtain settings from the server setup utility and manually set the software switches. For more information, see the application documentation, the vendor website, or both.
- Check for overwritten files. To determine which files are added by the application, see the application documentation.
- Reinstall the application.
- Verify that you have the most current drivers.

ROM issues

System requests recovery method during a firmware update

Symptom

The system requests a recovery method during a firmware update.

Action

Procedure

1. When updating the firmware on a BitLocker-encrypted server, do the following:

- a. Always disable BitLocker before updating the firmware.

If BitLocker is not disabled, the system requests the recovery method selected when BitLocker was configured. Failure to provide the correct recovery password(s) results in loss of access to all encrypted data.

- b. Update the firmware.

If BitLocker is configured to measure option ROMs, follow the firmware upgrade steps in **Keeping the system current**.

BitLocker can be configured to measure the following option ROMs:

- NIC
- Smart Array storage
- Standup HBAs

- c. After the firmware updates are complete, enable BitLocker.

For more information on BitLocker, see BitLocker for servers on the [Microsoft website](#).

Updating firmware

Procedure

1. Check the firmware version on the device.
2. Determine the latest firmware version available.
3. If a Trusted Platform Module (TPM) is installed and enabled on the server, disable BitLocker before updating the firmware.

For more information, see the operating system documentation.

4. Download and update the firmware to the current version supported for the hardware configuration.
5. Verify the firmware update by checking the firmware version.
6. If a TPM is installed and enabled on the server, enable BitLocker after the firmware update is complete.

For more information, see the operating system documentation.

Software tools and solutions

Server mode

Software or configuration utility	Server mode
<u>Aptio Setup Utility</u>	Offline
<u>HPE Smart Storage Administrator</u>	Online and offline
<u>Marvell Storage Utility</u>	Online
<u>Marvell BIOS Utility</u>	Offline

Product QuickSpecs

For more information about product features, specifications, options, configurations, and compatibility, see the product QuickSpecs on the HPE ProLiant MicroServer Gen10 website:

<http://www.hpe.com/server/microserver>

Aptio Setup Utility

The Aptio Setup Utility is embedded in the system ROM. This utility enables you to perform a wide range of configuration activities, including the following:

- Configuring system devices and installed options
- Enabling and disabling system features
- Displaying system information
- Selecting the primary boot controller
- Configuring memory options

Using the Aptio Setup Utility

To use the Aptio Setup Utility, use the following keys:

Key	Action
F2 or Del (during POST)	Access the Aptio Setup Utility.
Left and right arrows	Navigate the menus.
Up and down arrows	Navigate menu items.
Enter	Select menu items.
F4	Save selections and exit the utility.
F1	Access help for the highlighted configuration option.
Esc	Exit the utility.

Default configuration settings are applied to the server in either of the following scenarios:

- When the system powers up for the first time
- When the system is restored to the default settings

Default configuration settings are sufficient for typical server operations. However, you can modify the configuration settings as needed. The system prompts you to access the Aptio Setup Utility every time the system is powered up.

Boot option control

This feature enables you:

- To choose the boot mode, select **Advanced > Boot Option**.
- To set the boot option priority, select **Boot > Boot Option Priorities**.
- To select the one time boot option, select **Save & Exit > Boot Override**.

This menu allows you to select the boot device for a specific boot and does not modify the boot order configuration settings.

To select the one time boot option directly during POST, press the **F11** key when prompted during system boot, and then select the preferred boot device.

Boot option

Use this option to set the boot mode for the system. The following boot modes are supported:

- UEFI boot mode — The UEFI boot mode is the default boot mode. It configures the server to boot UEFI-compatible operating systems, and is required to use certain Aptio Setup Utility options.
- Legacy boot mode — This boot mode configures the server to boot traditional operating systems in legacy BIOS-compatibility mode. Certain situations might require that you operate in legacy boot mode, such as booting custom OS images that were installed using legacy boot mode or created using a legacy BIOS system.

Selecting the boot mode

Procedure

1. Reboot the server.
2. To access the Aptio Setup Utility, press the **Del** or **F2** key.
3. Select **Advanced > Boot Option > Boot Mode**.
4. Select a boot mode setting, and then press the **Enter** key.
5. To confirm the change and exit the utility, press the **F4** key.

Restoring and customizing configuration settings

The following options are available for restoring or customizing the configuration settings:

- Reset all configuration settings to the factory default settings.
- Restore and use the system default configuration settings.
- Configure default settings as necessary, and then save the configuration as the user default configuration.
- Restore the user default configuration.

To restore the user default configuration, select **Save & Exit > Default Option > Restore User Default**.

Clearing the BIOS configuration settings

The server BIOS configuration settings such as the system date and time, boot sequence, and hardware settings are stored in the CMOS. These settings are configured in the Aptio Setup Utility.

You might need to clear the CMOS if any of the following conditions occur:

- POST errors or boot issues
- Corrupted BIOS settings
- Incorrect settings made in the Aptio Setup Utility have caused error messages to be unreadable.

- If there is a hardware compatibility issue of a known compatible component.
- If the power-on password is forgotten.

⚠ CAUTION:

Be careful when clearing or altering the BIOS settings. Changing some settings might prevent the server from booting up correctly or might result in data loss.

Clearing the CMOS resets the BIOS settings to their factory default state. To clear the CMOS:

- If the Aptio Setup Utility is accessible, **use the Restore Defaults option under the Save & Exit menu.**
- If the Aptio Setup Utility is not accessible, **use the CMOS header.**

After clearing the CMOS, use the Aptio Setup Utility to reconfigure the BIOS settings.

Clearing the BIOS settings by using the Aptio Setup Utility

Procedure

1. Reboot the server.
2. To access the Aptio Setup Utility, on the enter setup prompt, press the **F2** or **Del** key.
3. Select the **Save & Exit** menu.
4. Under **Default Options**, select **Restore Defaults**, and then press the **Enter** key.
5. Select **Yes**.
6. To confirm the change and exit the utility, press the **F4** key.

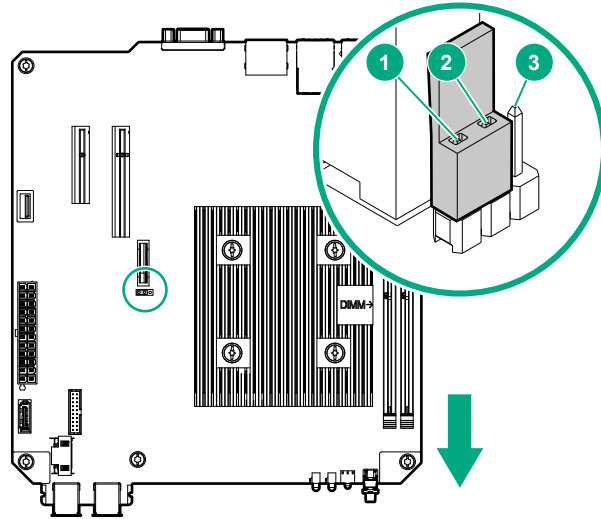
Clearing the BIOS settings by using the CMOS header

About this task

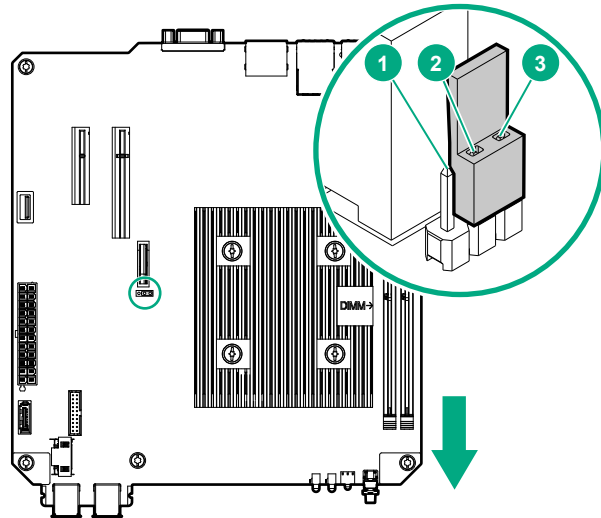
The arrow shown in the steps 6 and 7 illustrations points to the front of the server.

Procedure

1. **Power down the server** on page 17.
2. Disconnect the power cord from the AC source, and then from the server.
3. Disconnect all peripheral cables from the server.
4. **Remove the chassis cover** on page 20.
5. **Remove the system board assembly** on page 23.
6. Remove the jumper from its default position on pins 2 and 3, and place them on pins 1 and 2.



7. After five seconds, remove the jumper from pins 1 and 2, and move it back to the default position on pins 2 and 3.



8. **Install the system board assembly** on page 21.
9. **Install the chassis cover** on page 21.
10. Connect all peripheral cables to the server.
11. Connect the power cord to the server power jack, and then to the AC source.
12. **Power up the server** on page 17.

Embedded UEFI Shell

The system BIOS in this server 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 Aptio Setup Utility.

For more information, see the UEFI Shell Specification on the UEFI website:

<http://www.uefi.org/specifications>

Secure Boot configuration

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 Secure Boot is enabled, only firmware components and operating systems with boot loaders that have an appropriate digital signature can be executed during the boot process. Only operating systems that support Secure Boot and have a UEFI boot loader signed with one of the authorized keys can boot.

User can customize the certificates embedded in the UEFI BIOS by adding or removing their own certificates.

Enabling the Trusted Platform Module

Procedure

1. To access the Aptio Setup Utility, on the enter setup prompt, press the **F2** or **Del** key.
2. Select **Advanced > Trusted Computing**, and then press the **Enter** key.
3. Verify that the TPM device name is displayed.
4. To exit the utility, press the **Esc** key.

The server reboots without user input. During this system reboot, the TPM is enabled.

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

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.

For more information on adjusting TPM usage in BitLocker, see the Microsoft website:

<http://technet.microsoft.com/en-us/library/cc732774.aspx>

Utilities and features

HPE Smart Storage Administrator

The HPE SSA is a configuration and management tool for HPE Smart HBA and Smart Array controller options. The HPE SSA exists in the following interface formats:

- HPE SSA GUI
- HPE SSA CLI
- HPE SSA Scripting

Although all formats support configuration tasks, some of the advanced tasks are available in only one format.

In this server, HPE SSA can be accessed in both online and offline modes. In online mode, SSA is only accessible from the local server.

To access, install, and launch HPE SSA in an online environment, download the HPE SSA executables from the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>). Under **Select your HPE product**, enter the product name or number, and then click **Go**.

To access, install, and launch HPE SSA in an offline environment, download the HPE SSA ISO image from the HPE Smart Storage Administrator website:

<http://www.hpe.com/servers/ssa>

For more information, see the *HPE Smart Storage Administrator User Guide*:

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

Marvell Storage Utility

The Marvell Storage Utility is a browser-based configuration and management utility for the embedded Marvell storage controller. Use this utility to create and manage RAID virtual disks and arrays using the drives connected to the embedded storage controller.

For more information, see the *Marvell Storage Utility User Manual for 88SE9230 and 88SE9220* included in the SATA management tool package for the server. To download this package, go to the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>). Under **Select your HPE product**, enter the product name or number, and then click **Go**.

Marvell BIOS Utility

The Marvell BIOS Utility is built into the embedded Marvell storage controller ROM. Use this utility to create and manage RAID virtual disks and arrays using the drives connected to the embedded storage controller.

Accessing the Marvell BIOS Utility under legacy boot mode

Procedure

1. Reboot the server.
2. On the POST drive information screen, press **Ctrl+M**.

Accessing the Marvell BIOS Utility under UEFI boot mode

Procedure

1. Download the Marvell BIOS Utility package from the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>) and save the package in a USB key.
2. Attach the USB media to the server.
3. Reboot the server.
4. To access the **One-Time Boot Menu**, when prompted, press the **F11** key.
5. Select **UEFI: Built-in EFI Shell**.
6. To obtain the assigned file system volume for the USB key, enter the `map -r` command at the UEFI Shell prompt.
7. Change to the file system that contains the Marvell BIOS Utility package, and then press the **Enter** key.

If no other storage devices are mounted on the system, the USB drive is `fs0:` on the UEFI shell.

8. Enter the following command:

```
fs0:\> ui64.efi
```

where 0 is the server directory for the USB device containing the Marvell BIOS Utility package.

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 loads for USB 1.0, USB 2.0, and USB 3.0 speeds.
- In legacy boot mode, Hewlett Packard Enterprise provides legacy USB support in the preboot environment before the operating system loads for USB 1.0 and USB 2.0 speeds. USB 3.0 ports can be used with all devices in legacy boot mode but are not available at USB 3.0 speeds in the preboot environment. Standard USB support (USB support from within the operating system) is provided by the OS through the appropriate USB device drivers. Support for USB 3.0 varies by operating system.

The pre-OS behavior of the USB ports is configurable in the **Aptio Setup Utility**.

Keeping the system current

Firmware

Firmware is a software program that is stored in the system ROM chip on the system board or to an optional controller. Firmware controls the system when it is first powered on and then passes control to the operating system.

The firmware on the system board of the server is called the system ROM or the BIOS. The firmware on another piece of hardware configured in the server is called the option ROM.

Firmware update

Update the firmware (also called "flashing the ROM") as part of regular server maintenance. In addition, check for specific firmware updates in between regular updates to help keep the server performing optimally.

Firmware updates are created for, but are not limited to, the following reasons:

- To provide critical problem fixes that ensure system stability, such as upgrades that might prevent server unresponsiveness and other issues that could put the system at risk.
- To correct product issues, such as ROM or processor functionality.
- To improve system performance or make the system more serviceable.

Server downtime and time spent removing, returning, and ultimately replacing hardware might be avoided by first updating the firmware during the troubleshooting process. Many product issues that result in hardware replacement are preventable or correctable with a firmware update. Hewlett Packard Enterprise recommends checking for a firmware update before sending a part back to Hewlett Packard Enterprise for replacement.

On servers that have add-on options, Hewlett Packard Enterprise recommends checking for firmware upgrades for each installed option whenever an update to the system ROM or to another option is performed. This ensures that the entire system is running the latest updates for each component.

Multiple methods exist to update the system ROM:

- EFI tool under Embedded UEFI Shell
- Online Flash components

Product entitlement is required to perform updates.

CAUTION:

Any kind of system interruption during the firmware update results in errors that might corrupt the BIOS settings. These errors prevent the server from booting up. To prevent these update errors, observe the following cautions:

- Attach a UPS to the server to provide backup power to the system when updating the firmware.
 - Do not perform a forced shutdown of the server.
 - Do not perform a forced closure of the firmware update tool.
-

Updating the system ROM using the EFI tool from within the Embedded UEFI Shell

About this task

For systems configured in UEFI boot mode, use the following procedure to update the firmware.

Procedure

1. Access the System ROM Flash component for your server from the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>) and save the package in a USB key.
2. Copy the file to a USB device.
3. Attach the USB device to the server.
4. To access the **One-Time Boot Menu** option, when prompted, press the **F11** key.
5. Select **UEFI: Built-in EFI Shell**.
6. To obtain the assigned file system volume for the USB key, enter the `map -r` command at the UEFI Shell prompt.
7. Change to the file system that contains the System ROM Flash Binary file that you downloaded for your server. Enter one of the `fsx` file systems available, such as `fs0` or `fs1`, and then press the **Enter** key.

If no other storage devices are mounted on the system, the USB drive is `fs0`: on the UEFI shell.

8. To change from the current directory to the directory that contains the binary file, enter the `cd` command.
9. To flash the system ROM from the downloaded binary file, enter the `flashbios.nsh` command.
10. Reboot the server.

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

Online Flash components

Online Flash components provide updated system firmware that can be installed directly on supported operating systems. To download this component, go to the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>). Under **Select your HPE product**, enter the product name or number, and then click **Go**. To update the firmware, follow the instructions inside the firmware update package. The firmware update takes effect after rebooting the server.

Drivers, firmware, and software updates

IMPORTANT:

Always perform a backup before installing or updating device drivers.

- For the latest option ROM and driver updates for Hewlett Packard Enterprise hardware options, download the individual drivers, firmware, and components from the Hewlett Packard Enterprise Support Center website (<http://www.hpe.com/support/hpesc>). Under **Select your HPE product**, enter the product name or number, and then click **Go**.
- For the latest system ROM and other systems software components, download the individual drivers, firmware, and components from the server download page on the Hewlett Packard Enterprise website:

<http://www.hpe.com/downloads/microservergen10>

Operating System Version Support

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

HPE Pointnext Portfolio

HPE Pointnext 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.

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

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

Utilize our Advisory and Transformation Services in the following areas:

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

For more information, see the Hewlett Packard Enterprise website:

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

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:

<http://www.hpe.com/info/pcn>

Resources for troubleshooting

Online resources

Hewlett Packard Enterprise Information Library

HPE ProLiant Server documentation is available in the [Hewlett Packard Enterprise Information Library](#).

Service notifications, advisories, and notices

To search for service notifications, see the [Hewlett Packard Enterprise Support Center](#). Enter the product name or number, and then click **Go**. Select **Top Issues and Solutions**, and then **Advisories Bulletins and Notices**. The complete list of documents is displayed.

Subscription services

Receive support alerts, product support communications, driver updates, software releases, firmware updates, and customer replaceable component information in your email by signing up on the [Hewlett Packard Enterprise website](#).

To change options for support alerts you already receive, click the link to sign in on the right.

White papers

White papers are electronic documentation on complex technical topics. Some white papers contain in-depth details and procedures. Topics include Hewlett Packard Enterprise products, Hewlett Packard Enterprise technology, OS, networking products, and performance. See one of the following websites:

- [Hewlett Packard Enterprise Support Center](#)
- [Hewlett Packard Enterprise Information Library](#)

Product installation resources

Registering the server

To experience quicker service and more efficient support, register the server at the My License Portal website:

<https://myenterpriselicense.hpe.com/>

Power capacity

See the HPE Power Advisor on the [Hewlett Packard Enterprise website](#).

Spare part numbers

Hewlett Packard Enterprise continually improves and changes product parts. For complete and current supported spare parts information, see the Hewlett Packard Enterprise PartSurfer website:

- Desktop: <http://www.hpe.com/info/partssurfer>
- Mobile: <http://partsurfermobile.ext.hpe.com>

Teardown or removal and replacement procedure videos

For more information about removal and replacement procedures for HPE ProLiant servers, see the [Hewlett Packard Enterprise website](#).

DDR4 memory configuration

Locate the DDR4 Smart Memory Configurator on the [Hewlett Packard Enterprise website](#).

Device driver information

See the device driver information on the [Hewlett Packard Enterprise website](#).

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>

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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

Acronyms and abbreviations

API

application program interface

CSR

Customer Self Repair

DAC

direct attach cable

DDR4

double data rate-4

ESD

electrostatic discharge

HBA

host bus adapter

HPE SSA

HPE Smart Storage Administrator

ISO

International Organization for Standardization

KVM

kernel-based virtual machine

LFF

large form factor

LR

long reach

PCIe

Peripheral Component Interconnect Express

POST

Power-On Self-Test

REACH

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

RoHS

Restriction of Hazardous Substances

SATA

serial ATA

SD

Secure Digital

SFP

small form-factor pluggable

SR

short range

SSD

solid state drive

TPM

Trusted Platform Module

UEFI

Unified Extensible Firmware Interface

UPS

uninterruptible power supply