Hewlett Packard Enterprise

HPE StoreEasy 1X60 Storage Administrator Guide

Abstract

This document describes how to install, configure, and maintain 16x0 and 18x0 models of HPE StoreEasy 1X60 Storage and is intended for system administrators. For the latest version of this guide, go to http://www.hpe.com/support/StoreEasy1000Manuals.

Part Number: B7D88-96608
Published: February 2018
Edition: 1

Notices

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

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

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard

website.

Acknowledgments

Intel®, Itanium®, Pentium®, Intel Inside®, and the Intel Inside logo are trademarks of Intel Corporation in the United States and other countries.

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

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Java® and Oracle® are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

Contents

About this guide

What you can find in this guide

The HPE StoreEasy Administration Guide describes the latest features and supported options available for the HPE StoreEasy 1X60 storage system. The topics include:

- Initial system setup
- User authentication
- Storage configuration
- File sharing options
- Network configuration
- System monitoring and troubleshooting

Audience

The HPE StoreEasy 1X60 administrator guide is intended as a quick reference for administrators and technicians managing storage solutions.

Terminology

Table 1: Table of commonly used terms

Terminology	Description
ACL	Access control list allows the ability to control access rights to computer objects.
ADS	Active Directory Service is a directory service that Microsoft developed for managing Windows domain networks.
array	A synonym of storage array, storage system, and virtual array. A group of disks in one or more disk enclosures combined with controller software that represents disk storage capacity as one or more virtual disks.
backups	A read-only copy of data copied to media, such as hard drives or magnetic tape, for data protection. A full backup involves copying of all the data to the media. An incremental backup copies only the data that has changed since the last full backup. Backups provide data protection if the system or hard drive fails as the data is copied and stored on a separate media.

Table Continued

Terminology	Description
CIFS	Common Internet File System protocol, initially implemented for the purpose of sharing files between computers. Service Message Block (SMB) protocol has replaced CIFS on Microsoft operating systems and various other various Operating Systems.
CLI	Command-line interface. An interface composed of various commands which are used to control operating system responses.
cluster	A group of logically integrated servers that enables high availability, increases capacity, or distributes processing.
CSR	Customer self-repair indicates that the system may be repaired by the customer. No OEM-trained technician intervention is required.
data protection	The process of protecting data from getting corrupted or lost as a result of hard drive failure. Methods used to provide data protection include RAID and backups.
DFS	Distributed File System is a client/server-based application that allows clients to access and process network-based files as if they were local to their computer.
DFSN	Distribute File System Namespace is an application that groups shared folders on several servers into one or more logically structured objects. Each namespace appears to an end user as a shared folder with a series of subdirectories.
DFSR	Distributed File System Replication is an application that enables organizations to use synchronized folders for servers on networks that have a limited bandwidth.
DHCP	Dynamic Host Configuration Protocol is a protocol used for assigning dynamic IP addresses to devices on a network.
DNS	Domain Name System is a method of converting or mapping Internet domain names into IP addresses.

Table Continued

Terminology	Description
fault tolerance	The capacity to cope with internal hardware problems without interrupting the data availability of the system, often by using backup systems brought online when a failure is detected. Many systems provide fault tolerance by using RAID architecture to give protect against loss of data when a single disk drive fails. Using RAID 1, 3, 5, 6, 10, or 50 techniques, the RAID controller can reconstruct data from a failed disk drive and write it to a spare or replacement disk drive.
FTP	File Transfer Protocol is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.
HBA	Host bus adapter is a storage controller that enables interconnections between a server and storage elements such as tape drives and disk enclosures. There are a variety of interface types available; the Fibre Channel (FC) and serial-attached (SAS) HBAs are the more commonly used.
HDD	Hard disk drive is a data storage device that uses magnetic storage to store and retrieve digital information using one or more rotating disks (platters) coated with magnetic material.
ICT	Initial Configuration Tasks provides a list of actions that must be performed during the initial setup and configuration of a StoreEasy system.
iLO	Integrated Lights-Out integrated into all HPE platforms to provide remote management of the system hardware.
iSCSI	Internet small computer system interface. Like an ordinary SCSI interface, iSCSI is standards-based and efficiently transmits block-level data between a host computer (such as a server that hosts Exchange or SQL Server) and a target device (such as the HPE All-in-One Storage System). By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances.
JBOD	Stands for "just a bunch of disks" which are in a storage enclosure that directly attaches to a storage server.

Table Continued

Terminology	Description
LAN	Local area network. A communications infrastructure designed to use dedicated wiring over a limited distance (typically a diameter of less than five kilometers) to connect to multiple intercommunicating nodes. Ethernet and token ring are the two most popular LAN technologies.
logical disk	A logical disk contains one or more volumes and spans multiple hard drives in an array. RAID configuration of storage is performed at the logical disk level. Also known as a LUN.
LUN	Logical unit number. An LUN results from mapping a logical unit number, port ID, and LDEV ID to a RAID group. The size of the LUN is determined by the emulation mode of the LDEV and the number of LDEVs associated with the LUN.
mount point	A host file system path or directory name where a host volume (device) is accessed.
NAS	Network attached storage.
NCT	Network Configuration Tool.
NFS	Network file system. The network protocol used in most Linux/UNIX environments to share folders through mount points.
NIC	Network interface card. A device that handles communication between a device and other devices on a network.
SAN	Storage area network. A network of storage devices available to one or more servers.
SAS	Serial Attached SCSI.
SATA	Serial Advanced Technology Attachment.
Volume	An accessible storage area on disk, either physical or virtual.
volume mapping	The process by which volume permissions (read only, read/write, or none) and LUNs are assigned to a host port.

Introduction to HPE StoreEasy 1X60 Storage

The HPE StoreEasy 1000 Storage system provides multi-protocol file sharing and application storage for a range of business environments. The 1660 and 1860 are Gen10 hardware platforms and can accommodate medium and large IT environments.

Models

This document covers the following HPE StoreEasy 1X60 Storage models:

- HPE StoreEasy 1660 Storage
- HPE StoreEasy 1860 Storage

Key message

HPE StoreEasy 1X60 storage systems are storage solutions that deliver multiprotocol file serving and application storage in a reliable and affordable form. Platforms with enhanced security features enable an organization to protect their intellectual property by taking advantage of the HPE hardware-enabled security and Windows Storage Server 2016 operating system security capabilities.

Getting started

The topic describes the installation requirements and step-by-step instructions for setting up an HPE StoreEasy 1X60 Storage system.

Installation

Follow the step-by-step instructions to install the HPE StoreEasy 1X60 Storage system:

- **Safety precautions**
- **Prerequisites**
- **Mounting the system in a rack**
- **Cabling instructions**
- **Power up**
- **Complete installation**
- **Launch the Initial Configuration Toolkit (ICT)**

Safety precautions while installing the rail kits and mounting the system in a rack

⚠ **CAUTION:**

Electrostatic Discharge (ESD) can damage the electronic components. Ensure that you are properly grounded (earthed) before beginning any installation procedure.

HPE recommends the following safety precautions:

- Only qualified individuals who know the procedures, precautions, and equipment hazards that contains hazardous electrical circuits must perform this installation.
- The rail kits, when installed, form only a shelf for the StoreEasy 1X60 to rest on. The StoreEasy 1X60 is not attached to the rail by any other means. Use extreme caution when pulling the StoreEasy 1X60 out from the rack. The storage system can slip and fall, which may cause damage or injury to the StoreEasy 1X60 Storage. HPE is not responsible for any damage or injury caused by mishandling of StoreEasy 1X60.
- Ensure that the rack is leveled and stable before working on the rack. The leveling jacks (feet) must extend to the floor and the full weight of the rack must rest firmly on the floor.
- Ensure that the rack has anti-tip measures, such as floor-bolting, anti-tip feet, ballast, or a combination of the measures as specified by the rack manufacturer and applicable codes.
- Ensure that sufficient personnel are available to support one or more products during the installation process. HPE recommends you use an appropriate lifting device as an installation aid.
- Ensure that the rack is loaded from bottom to top, with the heaviest appliances at the bottom to make the rack steady.
- Avoid overloading the branch circuit that provides power to the rack. The total rack load must not exceed 80 percent of the branch circuit rating.

Prerequisites

Verify contents of StoreEasy shipping container

Prerequisites
Ensure that you have the following items in the shipping box:

- **Hardware Components**
  - HPE StoreEasy 1X60 Storage system
  - Power cords
  - Rail kit for installing the system in a rack
  - Any other hardware options purchased
- **Documentation and Media**
  - *HPE StoreEasy 1X60 Read This First document*
  - *HPE StoreEasy 1X60 Storage Quick Start Guide*
  - Windows Storage Server 2016 Certificate of Authenticity (COA) label (affixed to the product)
  - An envelope containing HPE Integrated Lights-Out (iLO) Advanced Security license key and document
  - HPE StoreEasy 1X60 System Recovery DVD (if ordered)

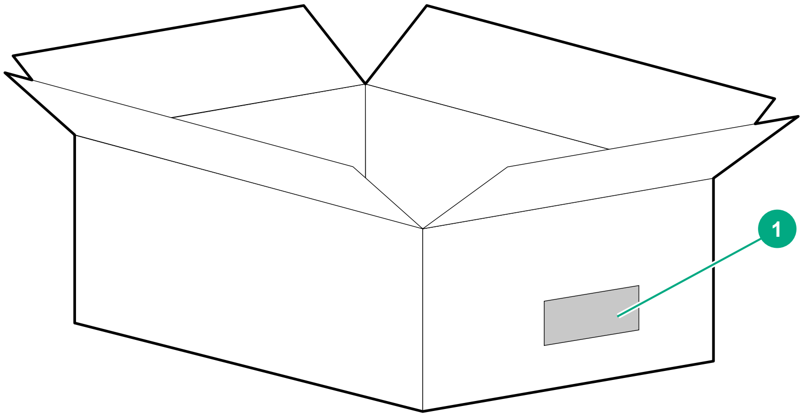
If any of the above-mentioned items are missing, contact Hewlett Packard Enterprise **https://www.hpe.com/us/en/contact-hpe.html** for assistance.

Locate serial number, COA

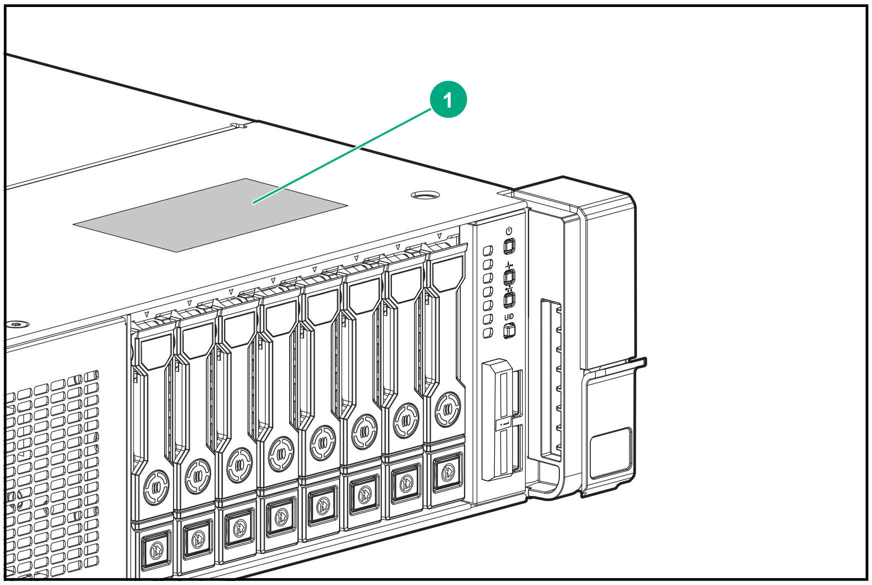
HPE personnel uses the system serial number to verify the StoreEasy model and warranty information. It is located in the following places on the system:

Procedure

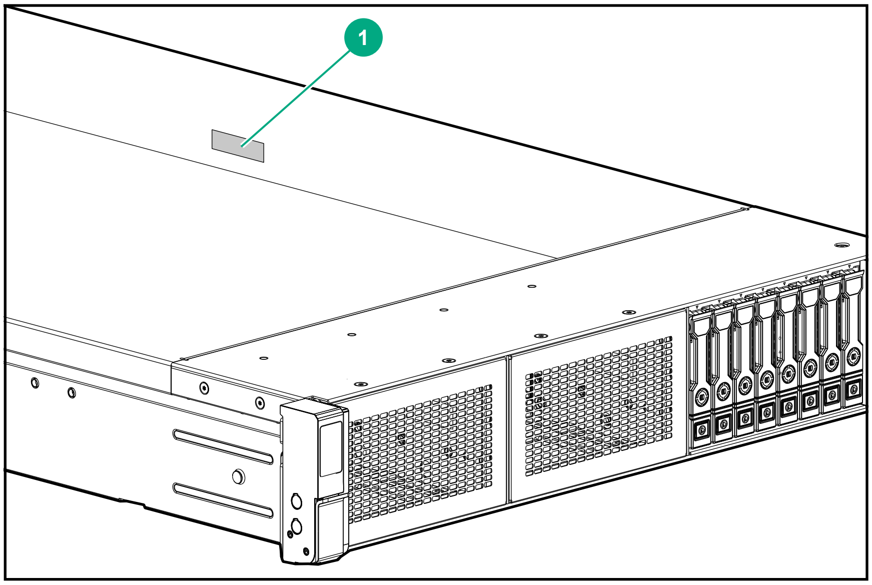
1. On a label (1) affixed outside the HPE StoreEasy 1X60 Storage shipping box.



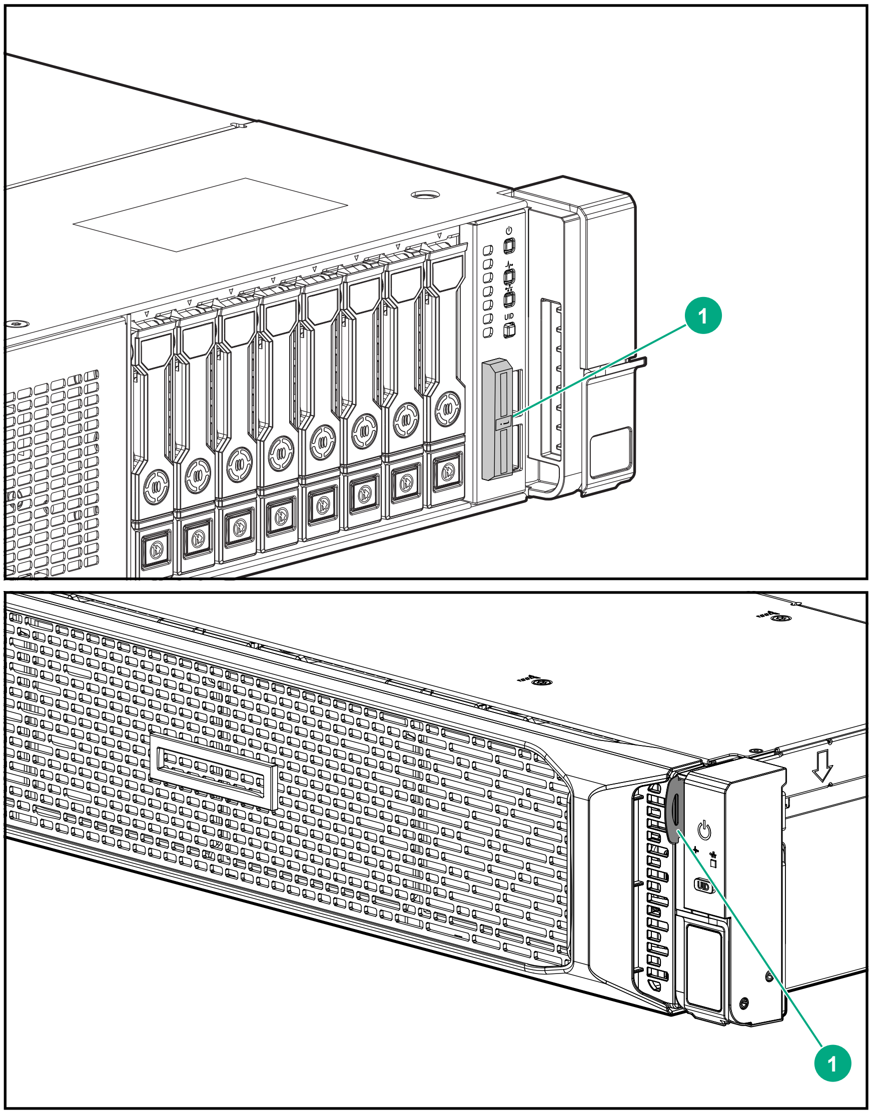
2. Top (1) of the HPE StoreEasy 1X60 Storage chassis (some models)



3. Inside (1) of the HPE StoreEasy 1X60 Storage chassis (some models)



4. Pull out serial number tab (1) on the product



Required tools for installation

The customer needs to provide the screws, cage nuts, and related tools for mounting the rails into the rack. While installing additional components in the system, HPE recommends to install the following tools:

- T-30 Torx screwdriver (processor or heatsink installation or removal)
- 1/4" flathead screwdriver (used to release the processor from a heatsink)
- T-10 Torx screwdriver (all other components that utilizes screws)

Mounting the system on a rack

⚠ **WARNING:**
Important safety information

Electrostatic Discharge (ESD) can damage the electronic components. Ensure that you are properly grounded (earthed) before beginning any installation procedure.

Qualified individuals who know the procedures, precautions, and equipment hazards that contains hazardous electrical circuits must perform this installation.

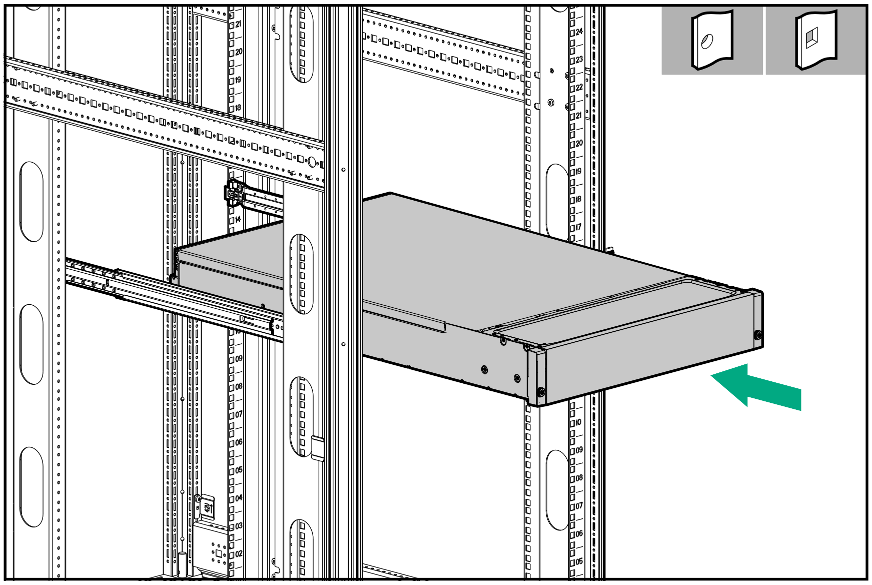
Procedure

1. The rail kits, when installed, form only a shelf for the StoreEasy 1X60 to rest on. The StoreEasy 1X60 is not attached to the rail by any other means. Use extreme caution when pulling the StoreEasy 1X60 out from the rack. The storage system can slip and fall, which may cause damage or injury to the StoreEasy 1X60 Storage. HPE is not responsible for any damage or injury caused by mishandling of StoreEasy 1X60.
2. Ensure that the rack is leveled and stable before working on the rack. The leveling jacks (feet) must extend to the floor and the full weight of the rack must rest firmly on the floor.
3. Ensure that the rack has anti-tip measures such as, floor-bolting, anti-tip feet, ballast, or a combination of the measures, specified by the rack manufacturer and applicable codes.
4. Ensure that sufficient personnel are available to support one or more products during the installation process. HPE recommends you use an appropriate lifting device as an installation aid.
5. Ensure that the rack is loaded from bottom to top, with the heaviest appliances at the bottom to make the rack steady.
6. Avoid overloading the branch circuit that provides power to the rack. The total rack load must not exceed 80 percent of the branch circuit rating.

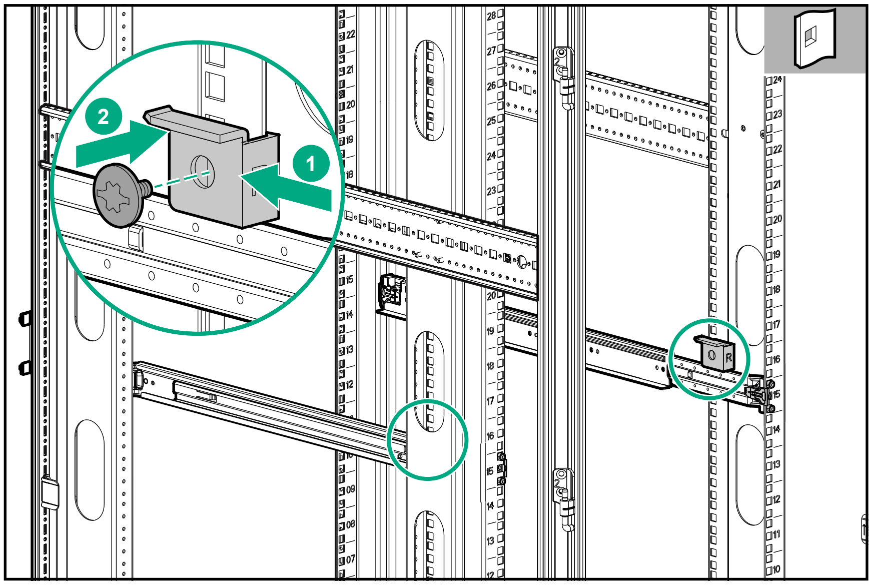
1U Rail instructions

Procedure

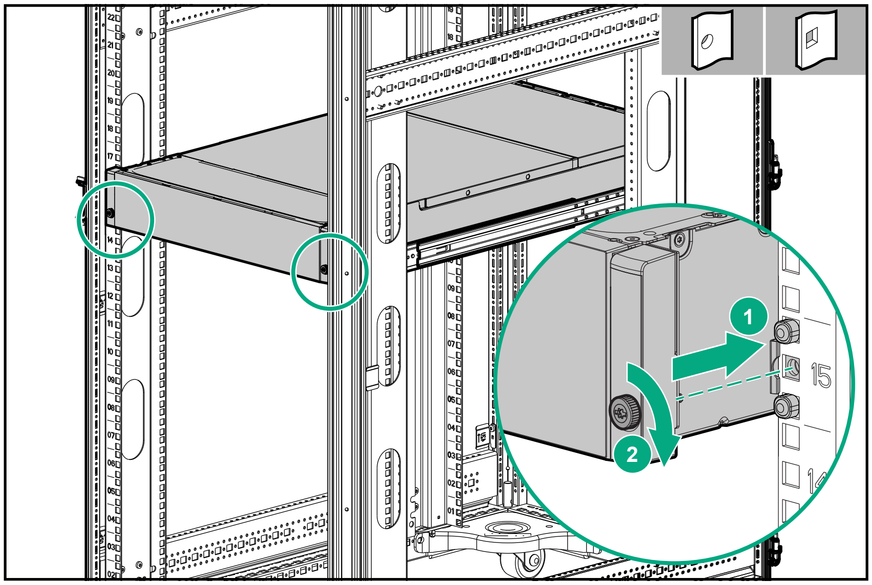
1. Slide the StoreEasy 1X60 into the position on the rails as shown in the following figure:



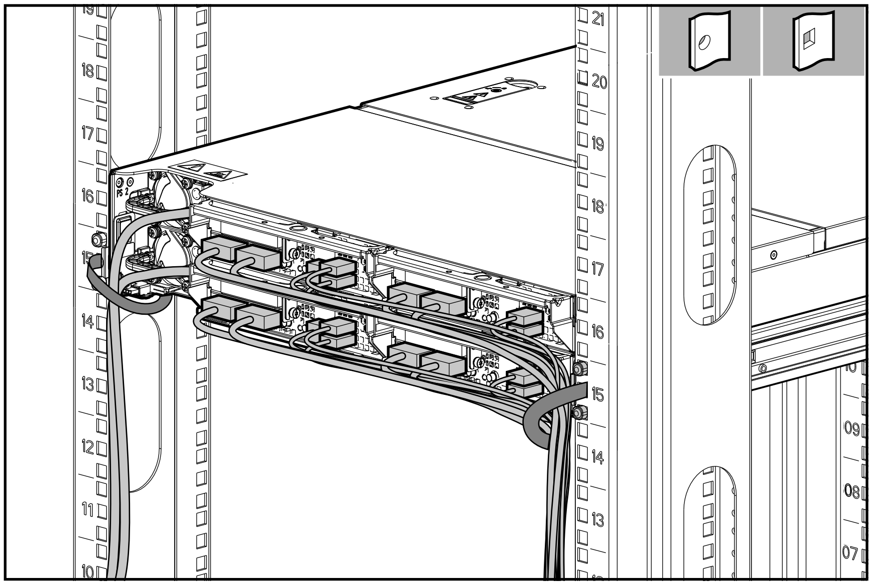
2. To secure the StoreEasy 1X60 to the rails, the Configure-to-Order (CTO) bracket at the rear ends of the rails must overlap the chassis tab as shown in the following figure:



3. Secure the StoreEasy 1X60 to the rack rails using thumbscrews on the front bezel as shown in the following figure:



4. Using the holes provided in the rear rack rails, install the tie wraps and route external cables, as required, as shown in following figure:



5. Connect all power cords to the facility power source.

2U Rail instructions

For detailed instructions on installing the HPE rack rails into square and round hole racks for HPE 2U Storage system, see *HPE Rack Rail Kit installation instructions document*, that is part of the shipped rail kit.

Cabling instructions

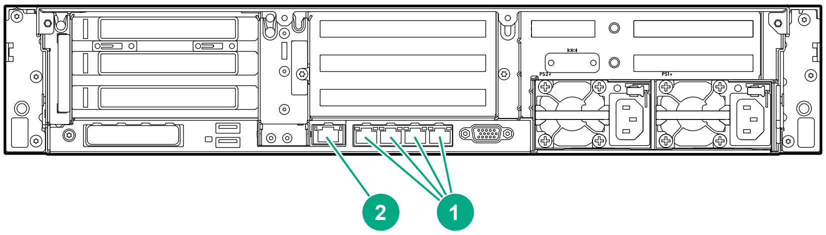
The iLO network port is used to remotely manage the StoreEasy 1X60 hardware and allows administrators to launch a remote console session to the system. HPE recommends that you connect the iLO port to your management network. The iLO port is preconfigured to obtain an IP address through DHCP. If your environment does not support DHCP, use a KVM and configure iLO to use a static IP address.

The 4 x 1GbE network ports are used for the storage network and to connect the system to infrastructure services, such as Active Directory, DNS, and NTP. The ports can be configured as segregated network ports or a network team. Ensure that your switch is prepared for either configuration.

Rear view of each model with legend and instructions

The rear view consists of:

1. Network Ports
2. iLO Port



If you have purchased additional interface cards for your StoreEasy 1X60, the following table guides you on where to install them. The numerical values indicate the order of installation.

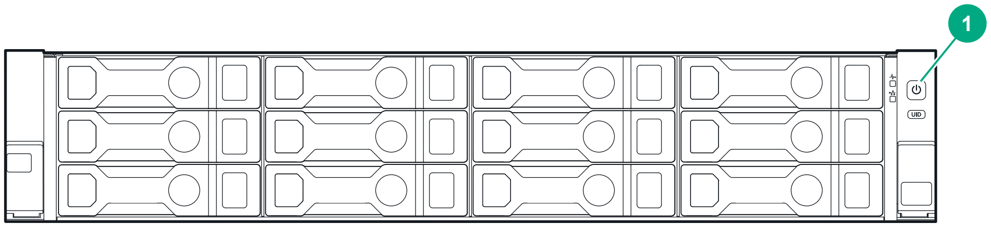
Description	PCIe Slot 1 (x8)	PCIe Slot 2 (x16)	PCIe Slot 3 (x8)	FlexLOM Slot	PCIe Slot 4 (x8)[1]	PCIe Slot 5 (x16)[1]	PCIe Slot 6 (x8)[1]
	Primary Riser				Secondary Riser [1]		
HPE M.2 Kit with 2 x M.2 SSDs	Slot Not Available	Slot Not Available	X	Slot Not Available	Slot Not Available	Slot Not Available	Slot Not Available
FlexLOM			Slot Not Available	1			
PCIe x16[2]		1		Slot Not Available		1	
PCIe x8 or less	1	2			1	2	3

[1] Slots for Secondary Riser require that the second processor is installed before they are available for use. PCIe Slot 4 and PCIe Slot 5 are not available when using the riser with the 2 x SFF cage.

[2] PCIe x16 on Primary Riser is only available on the StoreEasy 1660 system. The StoreEasy 1860 system uses this slot for the SAS expander card.

Power up

Power up the storage system using power button on the front panel as shown in the following figure:



1	Power button

NOTE:

If the StoreEasy 1X60 Storage system is attached to an external storage, including JBODs, power on the external storage system before you power on the StoreEasy 1X60 Storage system.

Complete installation

Using iLO / Console

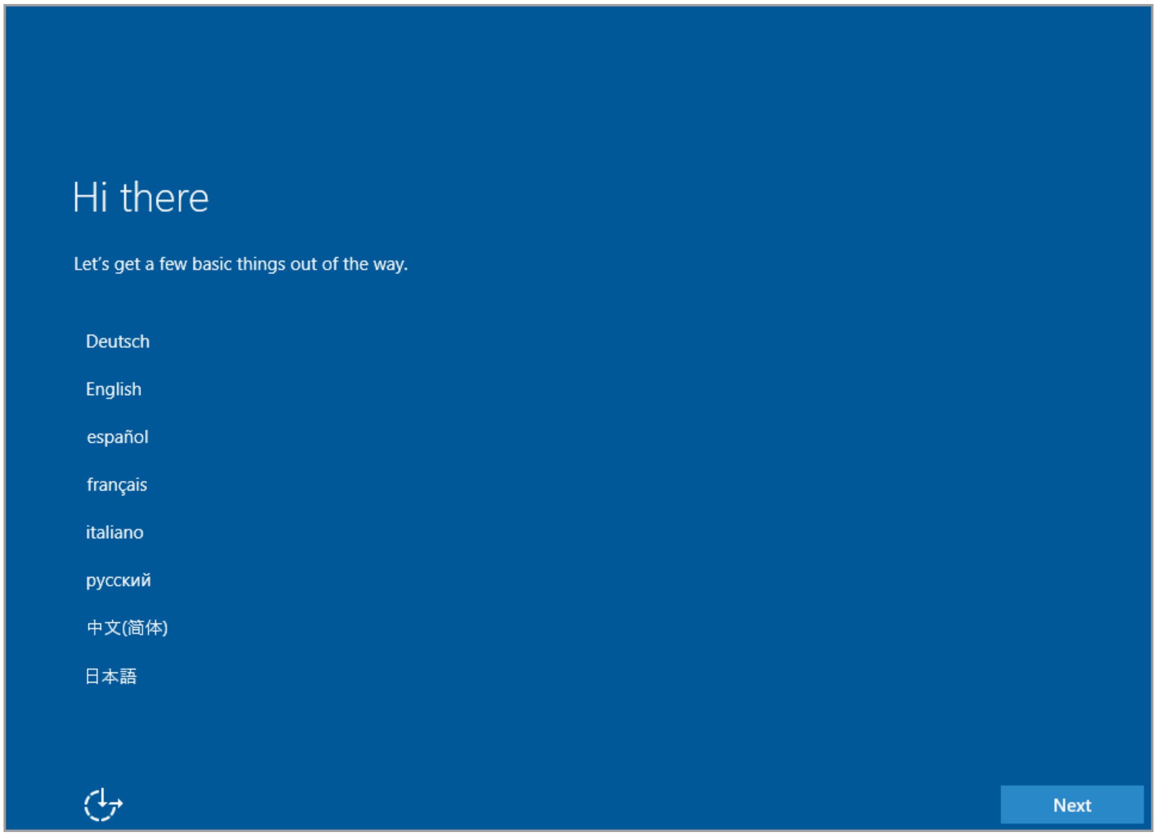
Before using the HPE StoreEasy management console as the primary management tool, complete the initial startup sequence. You can complete the initial startup sequence by connecting to the StoreEasy 1X60 using a KVM to configure a static IP or to gather the DHCP address from the boot screen.

Alternatively, you can complete the initial startup sequence by connecting to the StoreEasy 1X60 using the iLO Integrated Remote Console (IRC) remotely. If the iLO port is connected to a network segment with DHCP enabled and automatic DNS registration, use the DNS name. The DNS name, iLO initial login, and iLO initial password are available on the information tag attached to the front of the system on the right-hand side.

For more information on DHCP configuration and DNS registration, see HPE StoreEasy 1X60 Storage System Administrator Guide available at **Hewlett Packard Enterprise Support Center**.

Select language preference

Once StoreEasy 1X60 is booted, the language selection screen is displayed.



Hi there

Let’s get a few basic things out of the way.

NOTE:

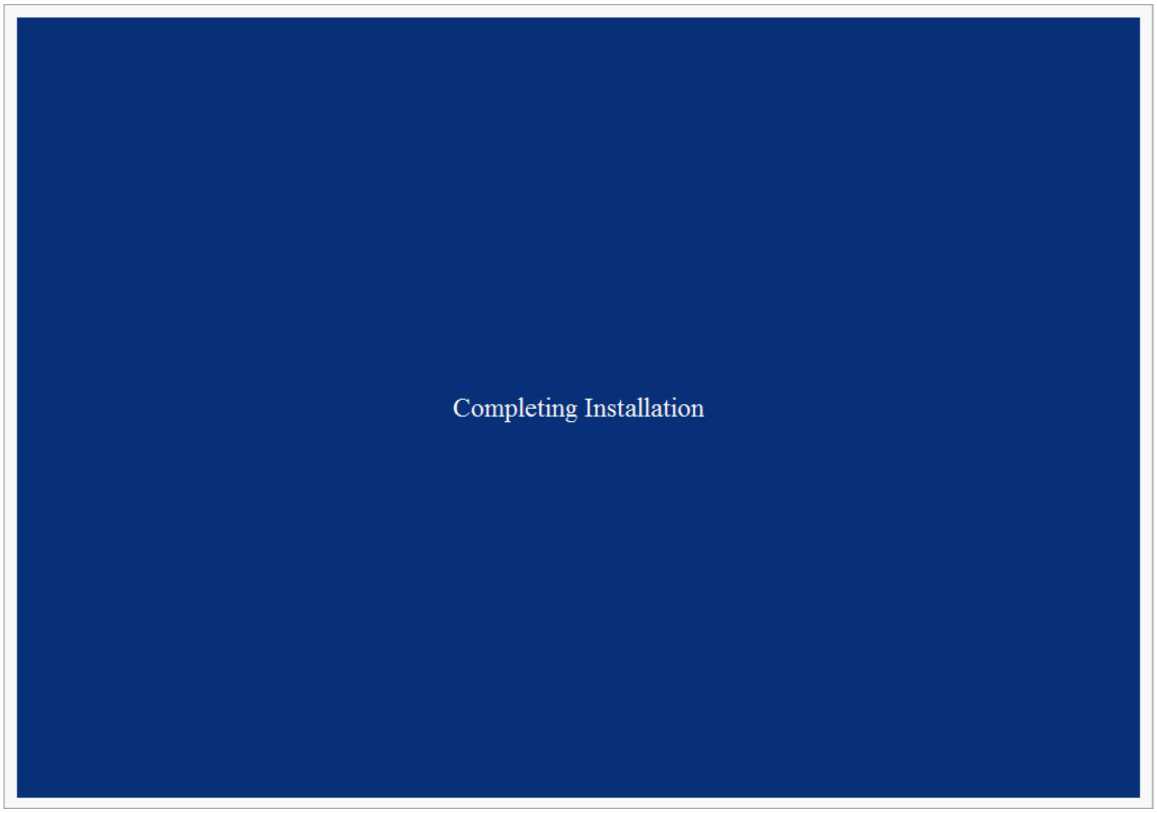
If the language selection screen does not display, contact Hewlett Packard Enterprise support, **Contact HPE**.

Accept End User Licence Agreement (EULA)

Read and accept the license terms.

Assign Administrator credentials

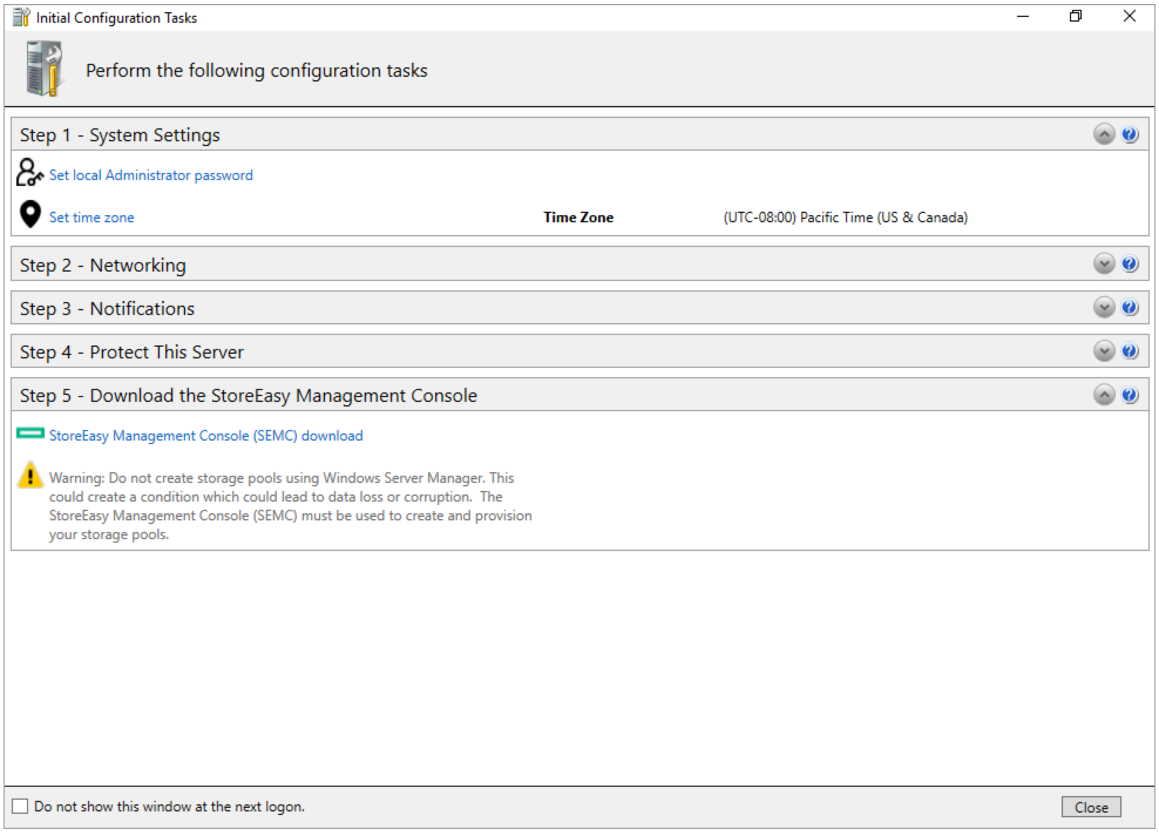
Once the preferred language choice, acceptance of licence terms and setup of the local admin password have been made, log in with the previously set administrator credentials. A post-installation process automatically starts and takes approximately 10-15 minutes. The system reboots at the end of the post installation.



Completing Installation

After the reboot, log in with the administrator account and password.

The system launches the Initial Configuration Tasks (ICT) application.



Initial Configuration Tasks

Perform the following configuration tasks

Step 1 - System Settings

Set local Administrator password

Set time zone — **Time Zone** (UTC-08:00) Pacific Time (US & Canada)

Step 2 - Networking

Step 3 - Notifications

Step 4 - Protect This Server

Step 5 - Download the StoreEasy Management Console

StoreEasy Management Console (SEMC) download

Warning: Do not create storage pools using Windows Server Manager. This could create a condition which could lead to data loss or corruption. The StoreEasy Management Console (SEMC) must be used to create and provision your storage pools.

☐ Do not show this window at the next logon.

Close

If ICT does not launch automatically, press **Windows + R** on your keyboard, type `OEMOOBE`, and click **OK**.

Launch the Initial Configuration Toolkit (ICT)

The Initial Configuration Task (ICT) window enables you to configure your system. After the initial configuration, the ICT window launches automatically for a user who is a member of the local administrator group. You can open only one instance of the ICT at a time.

Description of ICT and the steps it runs through

Once the HPE StoreEasy 1X60 Storage is connected to your network and to external storage enclosures (if present), power up the system and log on. Configure the system to complete the installation.

If you do not want to open the ICT window every time you log on, select the **Do not show this** check box.

You can also launch ICT by opening a command prompt and type **`C:\Windows\System32\OEMOOBE\OEMOOBE.EXE`**.

NOTE:

The ICT refreshes periodically. If you select an ICT task while a refresh is in progress, there is a delay before the application for that task is launched. You can also refresh ICT by pressing F5 button in your keypad.

ICT performs the following configuration tasks:

- ICT updates system settings, such as changing the local administrator password, time zone, and save reseller information.
- ICT launches the Network Configuration wizard to configure and validate the network configuration.
- ICT configures email alerts and registers the product.

- ICT creates storage pools and virtual disks.
- ICT enables software updates and enhancements directly from Windows updates.
- Set up optional data protection solutions on HPE StoreEasy 1X60 Storage with cloud-based data backup by replicating data using Vision Solutions Double-Take Availability. Both of these data protection solutions require separate licensing, but are available to use for a limited time through a free trial license.

Initial system configuration using ICT

Following are the Initial system configurations tasks included in ICT:

- **System Settings**
- **Networking**
- **Notifications**
- **Protection**
- **StoreEasy management console**

System Settings

This task group enables you to configure the system settings. The following aspects are included in this group:

- **Administrator password**
- **Time zone**

Administrator password

Set local administrator password: This enables you to change the administrator user password. The default password is the password that you entered during the initial setup of the server. To change the password, enter the new password in the **New password** and **Confirm password** fields and click **OK**.

IMPORTANT:

HPE cannot assist with lost passwords.

Time zone

Set time zone: Enables you to change the date and time settings. You can change the time zone, date and time, and synchronize the date and time with an Internet time server.

Networking

This task group enables you to set the network IP and domain of HPE StoreEasy 1X60 Storage.

The following tasks are included in this group:

- **Configure networking**
- **Computer name and domain**

Configure networking

This enables you to configure the network interfaces using the Network Configuration Tool (NCT) wizard. For detailed information on NCT, see U*sing the Network Configuration Tool*.

Computer name and domain

Provide computer name and domain: Enables you to specify the computer name and domain. After specifying the computer name and the domain, the system asks for a reboot. Windows Storage Server 2016 is installed with a randomly generated computer name and domain. You may find the server easier to access remotely and easier to recognize in reports and logs if you assign it a name that is meaningful to you and that fits with the naming scheme for computers in your organization.

Consider the following when assigning a computer name:

- The recommended length for most languages is 15 characters or fewer. For languages that require more storage space per character, such as Chinese, Japanese, and Korean, the recommended length is 7 characters or fewer.
- HPE recommends that you use only Internet-standard characters in the computer name. Standard characters are the numbers from 0 through 9, uppercase and lowercase letters from A through Z, and the hyphen (-) character. Computer names cannot consist entirely of numbers.
- If you are using DNS on the network, you can use a wider variety of characters. These include Unicode characters and other non-standard characters, such as the ampersand (&). Using nonstandard characters may affect the ability of non-Microsoft software to operate on the network.
- The maximum length for a computer name is 63 bytes. If the name is longer than 15 bytes (15 characters in most languages, 7 characters in some), computers running Windows NT 4.0 and earlier versions will recognize this computer by the first 15 bytes of the name only. In addition, there are additional configuration steps for a name that is longer than 15 bytes.
- If a computer is a member of a domain, you must choose a computer name that differs from any other computer in the domain. To avoid name conflicts, the computer name should be unique on the domain, workgroup, or network.

In a Windows Active Directory Domain, passwords and permissions for computer objects and user accounts are easier to manage due to their storage in a centralized database that is replicated among the domain controllers.

To name the computer and join it to a domain, click **Provide computer name and domain** in the Initial Configuration Tasks window and then click **Change** on the Computer Name tab.

Notifications

This task group enables you to configure email alerts and register for proactive notifications.

The following tasks are included in this group:

- **Email alerts**
- **Register product**

Email alerts

Configure email alerts: It launches Online help for email alerts.

Register product

Register Product: Opens a web browser to the HPE product registration page.

ⓘ **IMPORTANT:**

HPE strongly recommends registering the system so that you can receive proactive notifications of system updates, critical issues, and announcements of feature updates. If your system is connected to a network that can access the Internet, you can perform the product registration from any other system. You can also access the Register Product link using any one of the following methods:

- Double-click the **Register Product** icon on the desktop, or
- Click **Register Product** on the Start screen, or
- Open **Server Manager** and select **Tools** > **StoreEasy** > **Register Product**.

Protection

This task group enables the HPE StoreEasy 1X60 Storage system to receive critical software updates and enhancements directly from Microsoft website. The following features are included in this group:

- **Enable automatic updating**
- **HPE Complete Vision Solutions Software**

Enable automatic updating

Enable automatic updating: Opens the **Windows Update Settings** dialog box that you can use to select the way Windows updates are downloaded and installed. The Windows Update feature simplifies the task of updating the operating system, and saves administrators time.

Features on the Windows Update dialog box are configurable by administrators group on the local computer.

HPE recommends, download updates using Windows Update (default option) only.

HPE Complete Vision Solutions Software

The HPE Complete Vision Solution Software offers Double-Take Availability and Double-Take Move to manage your system. The HPE Complete Vision Solutions Double-Take Availability continuously captures production server changes at the byte level and replicates them to a secondary server.

HPE StoreEasy management console

The HPE StoreEasy management console is a web-based management interface that is built to centralize key monitoring, provisioning, and configuration tasks to deliver a simpler, more efficient experience for administrators and their workflow.

It is designed to provide a responsive and direct experience to the administrators to view the system health and resources, through a desktop and mobile friendly user interface. Administrators can choose to use HPE StoreEasy management console as a complement to many traditional Windows Storage Server tools.

The HPE StoreEasy management console is accessible through your choice of supported browsers (Chrome, Firefox, Edge, and Internet Explorer) on desktop and mobile. At this time, HPE StoreEasy management console can only be used to manage a single HPE StoreEasy 1000 Storage system.

Authentication

You can authenticate users to access HPE StoreEasy management console using user name and password login. HPE StoreEasy management console uses a role-based security access (RBAC). The RBAC specifies the permissions an authenticated user is allowed to do on the StoreEasy Storage System.

Each user login account on the HPE StoreEasy management console must be assigned a role. An infrastructure administrator can perform the tasks of adding, removing, and editing a user account.

User Roles

Each resource in the HPE StoreEasy management console has a set of permissions associated with it. These permissions determine who can access the file and what they can do with the file.

Role	Description
Administrator	User with this permission can perform all operations in HPE StoreEasy management console. Only a Windows or domain user account that is also a member of the local Administrators group can be granted the Administrator role.
Operator	User with this permission can perform all operations in HPE StoreEasy management console except for user management.
Read only	This user has only read permission and is not allowed to create, edit, or delete operations.

HPE StoreEasy management console uses the Microsoft Windows-provided credential services. It adds role-based access control to the existing Microsoft account management to define the access privileges of users to HPE StoreEasy management console functions.

HPE StoreEasy management Console uses the following authentication sources to validate user credentials:

Local user: The local users are the Windows user accounts created on the HPE StoreEasy system. The default account administrator is given privilege to access StoreEasy management console by default.

Domain user: While using Microsoft Active Directory domain authentication, the server has to be joined to a domain which the Active Directory user accounts have access to. If the Active Directory needs administrator and operator roles, then select the domain account which is a member of the local administrator group. Specify the following login credentials:

Username: `domain\username`

Password: HPE StoreEasy system password is used to access the HPE StoreEasy management Console.

Prerequisites to log into the HPE StoreEasy management console

- The latest version of the following browsers is supported for running HPE StoreEasy management console web interface:
  - Google Chrome
  - Mozilla Firefox
  - Microsoft Edge
  - Internet Explorer

  NOTE:

  For Internet Explorer browser, when the HPE StoreEasy management console is run remotely, add `https:\\IP` to trusted sites.

- The following settings must be enabled in the browser:

- **Javascript**: Client-side JavaScript is used by this application.
- **Cookies**: Cookies must be enabled for certain features to function correctly.
- **Pop-up windows**: Pop-up windows must be enabled for certain features to function correctly. Verify that pop-up blockers are disabled.
- **TLS**: To access the web interface, you must enable TLS in your browser.

User mapping: NFS (network file system) is a network file sharing protocol that allows remote access to files over a network. It is used in networks with computers running UNIX, Linux, or Mac OS operating systems. NFS is supported on all HPE StoreEasy 1X60 Storage systems.

The following NFS account mappings are supported by HPE StoreEasy:

- Active Directory® Domain Services (AD DS) mapped user access
- Unmapped anonymous user access
- Unmapped UNIX user access

For more information about NFS, see **The Storage Team at Microsoft – File Cabinet Blog**.

Installation and Port configuration

HPE StoreEasy management console uses 8443 as default port. The port is configurable and the user can provide any port during installation. If the user agrees to use the default port, the application will use port 8443.

Firewall Settings

Name of the Application	Local port	Remote port	Enable
NetBIOS TCP Port 49258	49258	Any	yes
Network Storage System-HTTPS-3202	3202	Any	Yes
Network Storage System-HTTP-3201	3201	Any	Yes
Microsoft iSCSI Software Target Service-UDP-138	138	Any	Yes
Microsoft iSCSI Software Target Service-TCP-135	135	Any	Yes
Microsoft iSCSI Software Target Service-TCP-3260	3260	Any	Yes
OEM OOBE Discovery Service (WSD-IN)	3702	Any	Yes
OEM OOBE Discovery Service (WSD-OUT)	Any	3702	Yes

Table Continued

Name of the Application	Local port	Remote port	Enable
LPD Service	515	Any	Yes
Windows Standards-Based Storage Management CIM-XML indications inbound	5990	Any	Yes
Windows Standards-Based Storage Management SLP outbound	427	Any	Yes
Failover Clusters	135	Any	Yes
SNMP Service (UDP Out)			
DFS Management (SMB-In)	445	Any	Yes
DFS Management (DCOM-In)	135	Any	Yes
File Server Remote Management (SMB-In)	445	Any	Yes
File Server Remote Management (DCOM-In)	135	Any	Yes
Server for NFS (NFS-UDP-In)	2049	Any	Yes
Portmap for UNIX-based Software (TCP-In)	111	Any	Yes
World Wide Web Services (HTTP Traffic-In)	443	Any	Yes
Messaging System-HTTP-3202	3202	Any	Yes
Messaging System-HTTP-3201	3201	Any	Yes
Remote Desktop - User Mode (TCP-In)	3389	Any	Yes
Remote Desktop - User Mode (UDP-In)	3389	Any	Yes

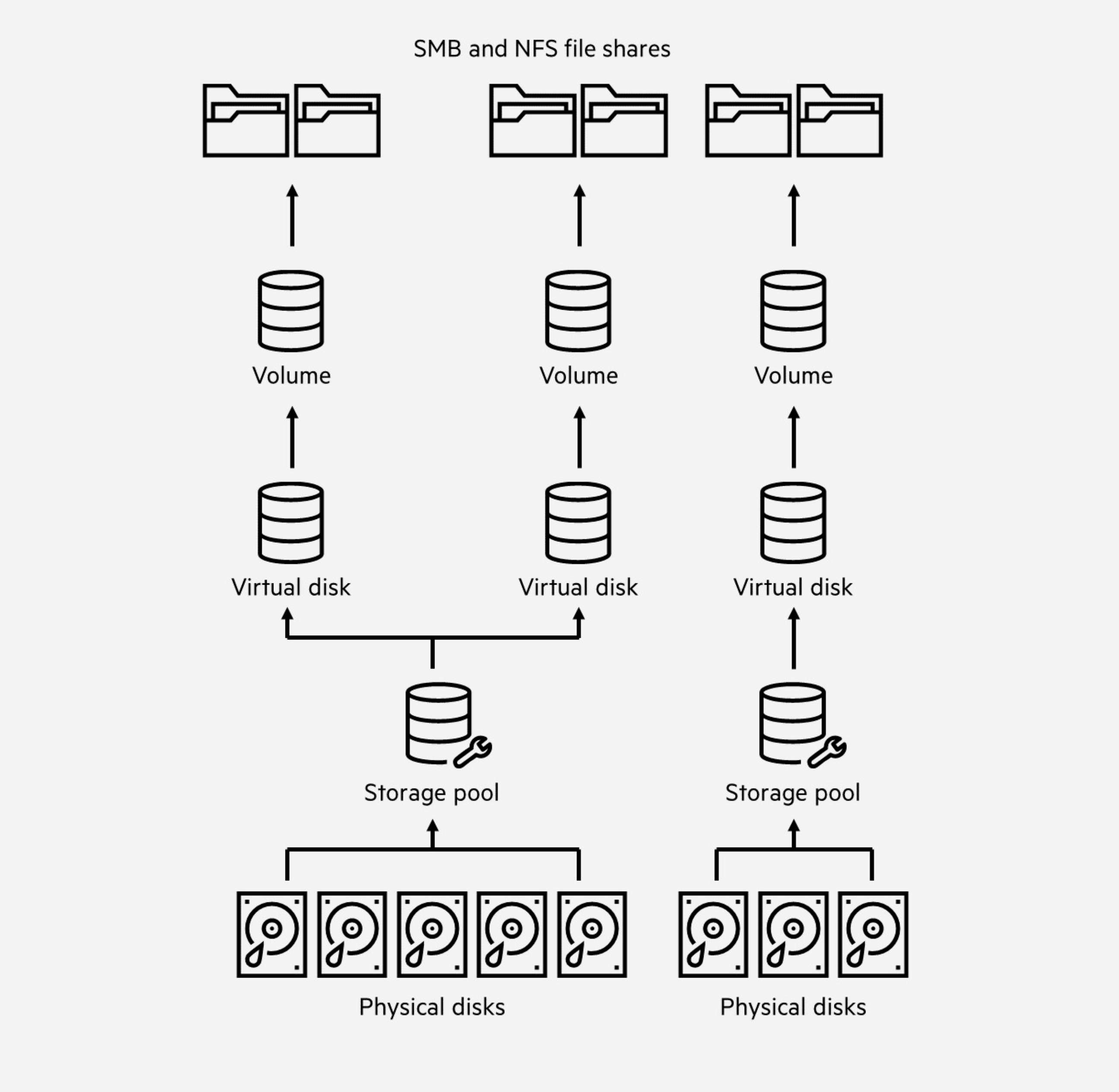
Table Continued

Name of the Application	Local port	Remote port	Enable
Core Networking - Dynamic Host Configuration Protocol for IPv6(DHCPV6-Out)	546	547	Yes
Remote Desktop - User Mode (UDP-In)			
File and Printer Sharing (LLMNR-UDP-Out)	Any	5355	Yes
Windows Remote Management (HTTP-In)	5985	Any	Yes

System Architecture

Each StoreEasy 1X60 system comes pre-configured with the Windows Storage Server 2016 installed from the factory. Applicable Windows Server roles and features have been enabled for managing a file storage system. For more information on complete list of the Roles and Features installed, see **Appendix**.

Figure provides a high-level overview of a generic StoreEasy 1X60 system, depicting the physical and logical components that are needed to enable reliable, flexible and performant file data storage services for application and user workloads.



HPE StoreEasy data storage resources to client systems and application

Each component in the different layers of the system architecture serves a distinct function that higher-level components rely on. These properties are discussed in more detail in the following sections, starting from low level components.

Physical disks: Physical disks are the most granular physical components in the data path of the StoreEasy system architecture. Their main purpose is to provide persistence of data across power cycles. StoreEasy supports both hard drives (HDD) and solid-state drives (SSD) in both large form factor (LFF) and small form factor (SFF) as standard storage options.

Types of Drives: The supported drives in the StoreEasy 1X60 systems for the internal storage is determined by the specific StoreEasy platform being deployed. When adding external storage, the types and number of drives supported is dependent upon the enclosure purchased. For specifics, see **Hardware components** and **External Storage Enclosures** with the supported specific hard disk drives and solid state drives details.

Drive interfaces have two distinct popular interfaces available in the HPE StoreEasy 1X60 systems.

- **Serial ATA (SATA)**: Used when performance is not the top consideration and your business requires a cost-effective, high-capacity storage for file serving
- **Serial-attached SCSI (SAS)**: Have greater performance than SATA disks, SAS disk drives deliver the speed, reliability, and high availability that file services and storage require

Hard disk drives (HDD) are classified by the three different classes and types of workloads:

- **Entry**: Low workload (I/O) and generally used for boot and backup solutions. This type of hard disk drive is only available on certain HPE systems. Interface type is SATA 6 Gb.
- **Midline**: Medium workload (I/O) and generally used for high capacity and high availability storage: Backup, archive, and file services. Interface types are SAS 12 Gb and SATA 6 Gb in both SFF and LFF formats.
- **Enterprise**: Mission critical and high workload (I/O) and generally used by Email, Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and databases. Interface type is SAS 12 Gb for both SFF and LFF formats.

Solid State Drives (SSD) are classified by three different workload types:

- **Read Intensive (RI)**: Selected for Boot or swap, Read caching, Web Servers, Bulk storage, Active archiving, or Analytics.
- **Mixed-Use (MU)**: Selected when a balance is needed for both Business intelligence and Business transaction processing.
- **Write Intensive (WI)**: Select for OLTP or Financial, Business intelligence, Big data analytics, Virtualization, Scientific, Collaboration infrastructure, and Enterprise business.

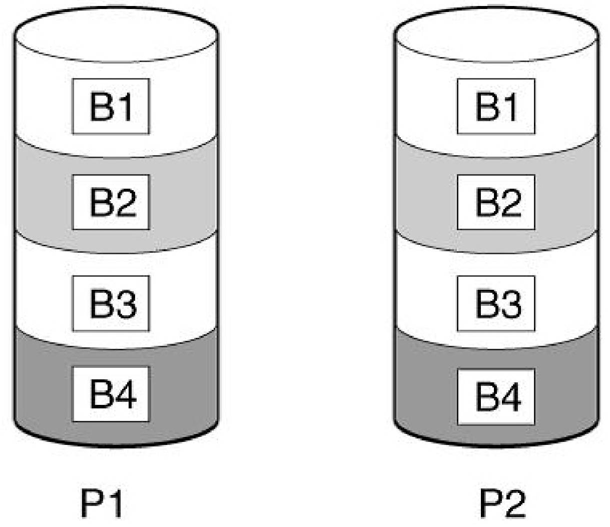
Solid State Drives come in the following drive interface types: 12 Gb SAS (SFF), 6 Gb SATA (SFF, M.2, and enablement kits) or PCIe/NVMe (SFF, Add-in and Mezz cards). Currently HPE StoreEasy 1X60 systems only support the 12 Gb SAS or 6 Gb SATA options.

RAID Arrays: The StoreEasy 1X60 systems use the P-Class HPE Smart Array controllers to combine multiple drives connected to the controller into a hardware-based redundant array of inexpensive drives (RAID). The advantage of using a RAID configured array is that you increase capacity, performance, security and reliability based on the type of controller and level of RAID deployed.

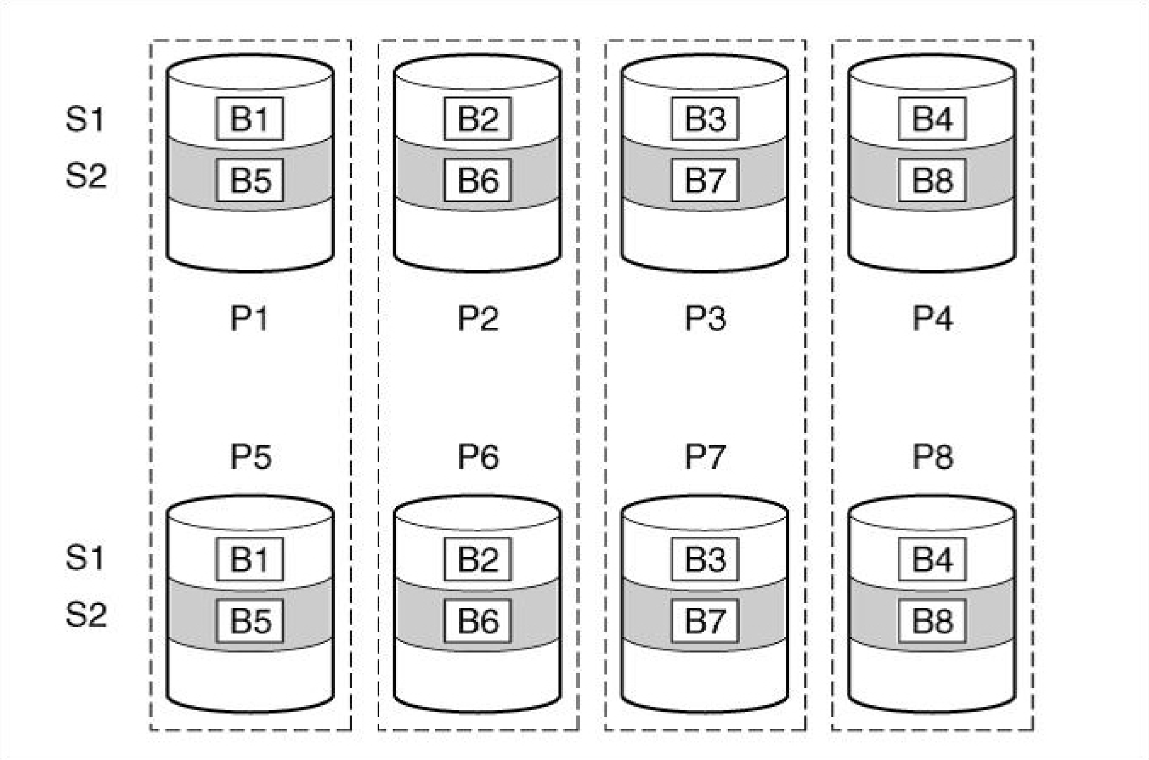
We are going to focus on the recommend RAID configurations that are considered a *best practice* when configuring your physical disks into RAID arrays. For more information, see *HPE Smart Array SR Gen10 User Guide*.

Mirroring

RAID 1 and 1+0 (RAID 10): In RAID 1 and RAID 1+0 (RAID 10) configurations, data is duplicated to a second drive. The usable capacity is C x (n/2) where C is the drive capacity with n drives in the array. When the array contains only two physical drives, the fault-tolerance is known as RAID 1.



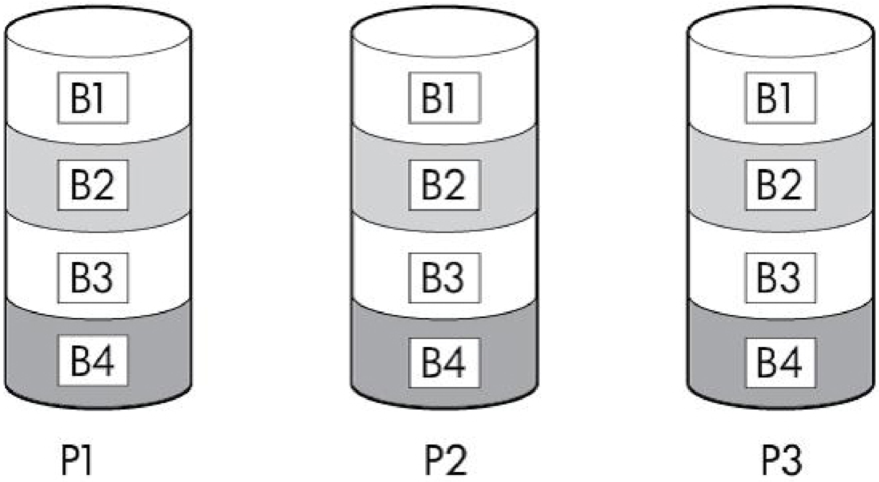
When the array has more than two physical drives than it is known as RAID 1+0 or RAID 10. If a physical drive fails, the remaining drive in the mirrored pair can still provide all the necessary data. Several drives in the array can fail without incurring data loss, as long as no two failed drives belong to the same mirrored pair. The total drive count must increment by 2 drives when adding additional capacity to an existing mirrored configuration.



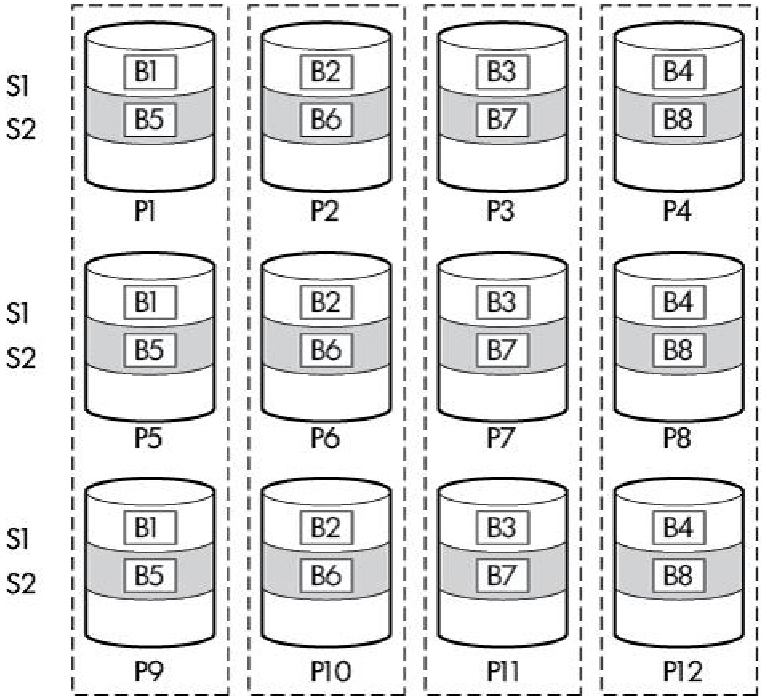
This method has the following benefits:

- It is useful when high performance and data protection are more important than usable capacity.
- This method has the highest write performance of any fault-tolerant configuration.
- No data is lost when a drive fails, as long as no failed drive is mirrored to another failed drive.
- Up to half of the physical drives in the array can fail.

RAID 1 (ADM) and RAID 10 (ADM): In RAID 1 (ADM) and RAID 10 (ADM) configurations, data is duplicated to two additional drives. The usable capacity is C x (n / 3) where C is the drive capacity with n drives in the array. A minimum of 3 drives is required. When the array contains only three physical drives, the fault-tolerance method is known as RAID 1 (ADM).



When the array has more than three physical drives, drives are mirrored in trios, and the fault-tolerance method is known as RAID 10 (ADM). If a physical drive fails, the remaining two drives in the mirrored trio can still provide all the necessary data. Several drives in the array can fail without incurring data loss, as long as no three failed drives belong to the same mirrored trio. The total drive count must increment by 3 drives.

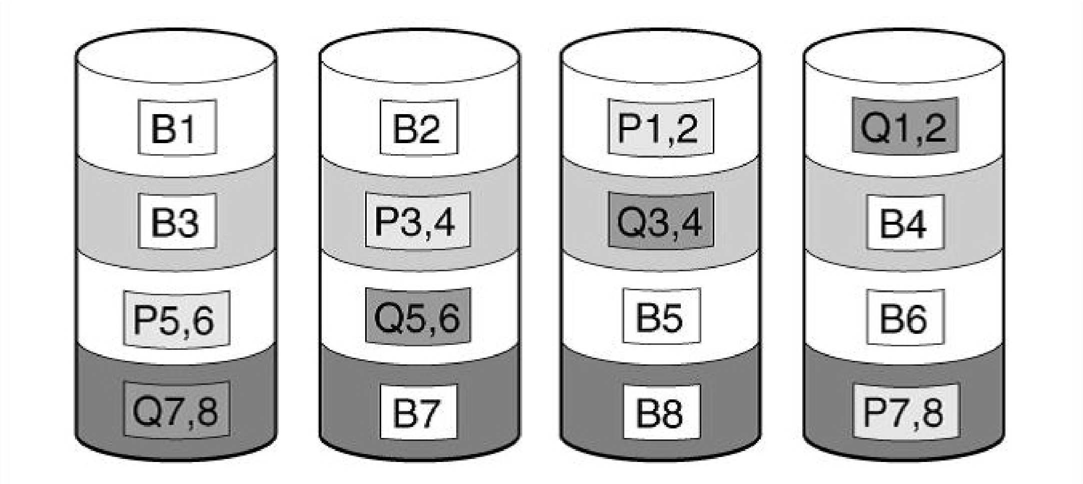


This method has the following benefits:

- It is useful when high performance and data protection are more important than usable capacity.
- This method has the highest read performance of any configuration due to load balancing.
- This method has the highest data protection of any configuration.
- No data is lost when two drives fail, as long as no two failed drives are mirrored to another failed drive.
- Up to two-thirds of the physical drives in the array can fail.

Double Parity

RAID 6: RAID 6 protects data using double parity. With RAID 6, two different sets of parity data are used (denoted by Px,y and Qx,y in the figure), allowing data to still be preserved if two drives fail. Each set of parity data uses a capacity equivalent to that of one of the constituent drives. The usable capacity is C x (n - 2) where C is the drive capacity with n drives in the array. A minimum of 4 drives is required.



This method is most useful when data loss is unacceptable but cost is also an important factor. The probability that data loss will occur when an array is configured with RAID 6 (ADG) is less than it would be if it were configured with RAID 5.

This method has the following benefits:

- It is useful when data protection and usable capacity are more important than write performance.
- It allows any two drives to fail without loss of data.

RAID 60: RAID 60 is a nested RAID method in which the constituent hard drives are organized into several identical RAID 6 logical drive sets (parity groups). The smallest possible RAID 60 configuration has eight drives organized into two parity groups of four drives each.

For any given number of hard drives, data loss is least likely to occur when the drives are arranged into the configuration that has the largest possible number of parity groups. For example, five parity groups of four drives are more secure than four parity groups of five drives. However, less data can be stored on the array with the larger number of parity groups.

The number of physical drives must be exactly divisible by the number of parity groups. Therefore, the number of parity groups that you can specify is restricted by the number of physical drives. The maximum number of parity groups possible for a particular number of physical drives is the total number of drives divided by the minimum number of drives necessary for that RAID level (three for RAID 50, four for RAID 60).

All data is lost if a third drive in a parity group fails before one of the other failed drives in the parity group has finished rebuilding. A greater percentage of array capacity is used to store redundant or parity data than with non-nested RAID methods.

This method has the following benefits:

- Higher performance than for RAID 6, especially during writes.
- Better fault tolerance than either RAID 0 or RAID 6.
- Up to 2n physical drives can fail (where n is the number of parity groups) without loss of data, as long as no more than two failed drives are in the same parity group.

Storage Pool: A storage pool is the aggregation of physical drives into a RAID group. When a HPE StoreEasy 1X60 system physical disks have been configured into one or more hardware-based RAID array configurations, the Windows operating system will see these RAID array logical drives as one or more storage pools. The tools that will be used for creating and managing the storage pools are:

- **HPE StoreEasy management console**
- HPE Smart Storage Administrator

⚠ **WARNING:**

Do not use the Windows Server Manager to create storage pools on a HPE StoreEasy 1X60 system. This would create a storage spaces RAID configuration which is not a supported configuration on the HPE StoreEasy systems.

Instructions for creating the storage pools using these tools are in this administrator guide under the topic of **Creating Storage pool**. After the storage pool(s) are created than the next step would be to create the logical elements starting with establishing logical partitions.

Logical Elements

Virtual Disks: After establishing the storage arrays then a virtual disk configuration can be created which will establish the logical partition configuration for the designated storage pool.

The virtual disk creates the logical partition using the storage pool selected. Instructions for creating the virtual disk are in this administrator guide under the topic of **Creating virtual disks**. Once the virtual disk is created then a volume can be established.

Volume: When a volume is created it establishes the file system layout to be used for storing file information on the volume. There are two file system types that can be used with the Windows operating system - NTFS or ReFS. When selecting the file system to use there are some feature sets that are only available on a specific file system type. Take the time to evaluate what best meets your use case before implementing. You can have different file systems on different volumes

The key features of ReFS are as follows:

- Metadata integrity with checksums.
- Integrity streams providing optional user data integrity.
- Allocate on write transactional model for robust disk updates (also known as copy on write).
- Large volume, file and directory sizes.
- Storage pooling and virtualization makes file system creation and management easy.
- Data striping for performance (bandwidth can be managed) and redundancy for fault tolerance.
- Disk scrubbing for protection against latent disk errors.
- Resiliency to corruptions with "salvage" for maximum volume availability in all cases.
- Shared storage pools across machines for additional failure tolerance and load balancing (applies only to storage spaces).

However, ReFS does not have all of the feature sets that may be of importance in your environment. NTFS may still be a more appropriate option. In the following table is a list of what is available based on whether you select NTFS or ReFS.

File System Feature	NTFS	ReFS
Supports Case-sensitive filenames	Yes	Yes
Preserves Case of filenames	Yes	Yes

Table Continued

File System Feature	NTFS	ReFS
Supports Unicode in filenames	Yes	Yes
Preserves & Enforces ACL's	Yes	Yes
Supports Sparse files	Yes	Yes
Supports Reparse Points	Yes	Yes
Supports Open By FileID	Yes	Yes
Supports USN Journal	Yes	Yes
Supports Hard Links	Yes	No
Supports file-based Compression	Yes	No
Supports Disk Quotas	Yes	No
Supports Deduplication	Yes	No
Supports Object Identifiers	Yes	No
Supports Encrypted File System	Yes	No
Supports Named Streams	Yes	No
Supports Transactions	Yes	No
Supports Extended Attributes	Yes	No

Follow the instructions for **Creating volume**, once the file system is selected. Once the volume is created then you will have the foundation in place to be able to establish your directory structures and establish file sharing.

File Shares – SMB and NFS: There are several file sharing protocols available that can be used on the HPE StoreEasy 1X60 systems. These file sharing protocols include Network File Systems (NFS), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), and Microsoft Server Message Block (SMB). Of these protocols the two more popular protocols to be deployed are: SMB and NFS. File shares can be established at the volume level or on specific directory folders. Different file sharing protocols can be enabled using specific network names for access across a network to a variety of clients. Permissions can then be granted to those shares based on users or groups of users in each of the file sharing protocols.

After determined which file shares need to be established, then follow instructions for **Creating file shares**.

Authentication

Active Directory

IMPORTANT:

Before adding the StoreEasy system nodes to Active Directory domain, ensure that there is a network connectivity between each node and domain controller.

The HPE StoreEasy 1X60 Storage requires minimum 2 IP addresses. These addresses can be statically assigned or can be assigned by a DHCP server. If you are using static addressing, ensure that both forward and reverse DNS information (A and PTR records) is pre-staged in the DNS server.

Use the following table to document the network information before preceeding with system setup.

Table 2: Network information

Network device	Fully qualified DNS Network device name (FQDN)	IP address
System		
iLO		

Restrictive Active Directory environments

If the StoreEasy system is placed in a restrictive Active Directory environment, it might require pre-staging Active Directory objects or certain administrative permissions. For more information, see the following Microsoft articles:

How to Create a Cluster in a Restrictive Active Directory environment
Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory

Local users and groups

The local users are the Windows user accounts created on StoreEasy system. The default account administrator is given privilege to access StoreEasy management Console by default.

User and group information and permissions determine whether a user can access files. If HPE StoreEasy Storage system deployed into a work group environment, the user and group information is stored locally on the device. By contrast, if HPE StoreEasy 1X60 Storage is deployed into a domain environment, user and group information is stored on the domain.

Storage Pools

A storage Pool is an aggregation of physical storage resources (disks) in a **storage system**. Storage systems contain information about the storage ports through which they can be accessed. You can provision logical storage spaces, known as **volumes**, from storage pools.

You can choose one or more storage pools when adding a storage system to the appliance. Storage Pools are created on a storage system using the management software for that system. You cannot create or delete storage pools from the appliance-you can only add or remove them from management. After you add Storage Pools, you can provision volumes on them.

Storage Pools Overview

Use HPE StoreEasy management console to create, edit, grow, and delete storage pools. A storage pool contains a set of physical disk drives that are grouped together and from which one or more Virtual Disks are created.

Pool set may offer two 11-drive pools with drive designated as a spare, which is available to either pool.

Creating Storage Pool

The Storage Pool can be created by:

Creating storage pool using HPE StoreEasy management console

Creating Storage Pool using HPE StoreEasy management console

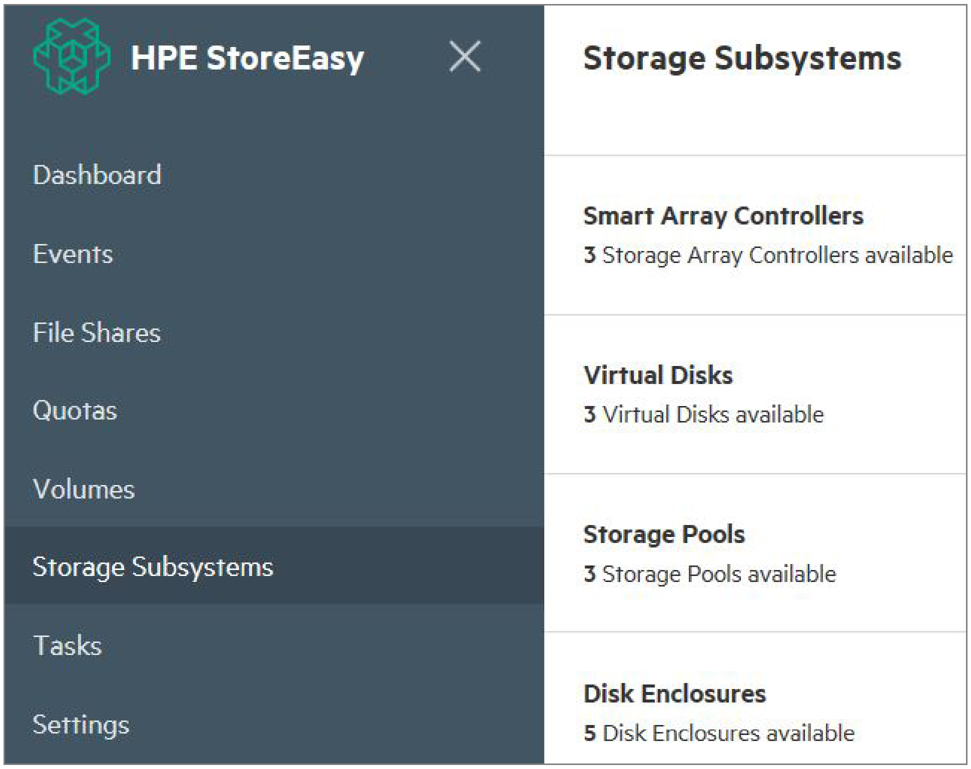
The HPE StoreEasy management console is used to create storage pools and assign spare drives.

The following table describes the fields that are available on Storage Pool page:

Field	Description
Name	Storage Pool name
Total Size	Total size of the Storage Pool
Used Size	Storage space used by the Storage Pool
Utilization	Horizontal graph representing the utilized storage space
Resiliency Setting	RAID type used by the Storage Pool

Follow the steps to create Storage Pool in HPE StoreEasy management console:

1. Open **HPE StoreEasy**.
2. Click **Storage Subsystems** in the left pane.



Storage Subsystems

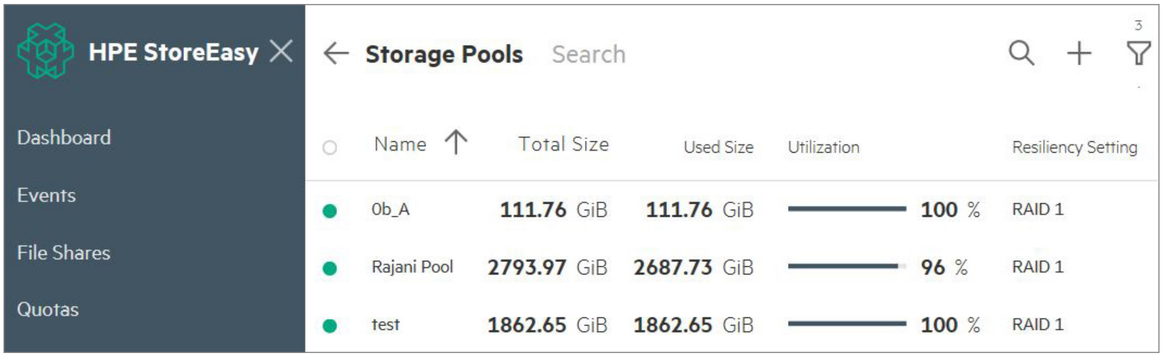
Smart Array Controllers
3 Storage Array Controllers available

Virtual Disks
3 Virtual Disks available

Storage Pools
3 Storage Pools available

Disk Enclosures
5 Disk Enclosures available

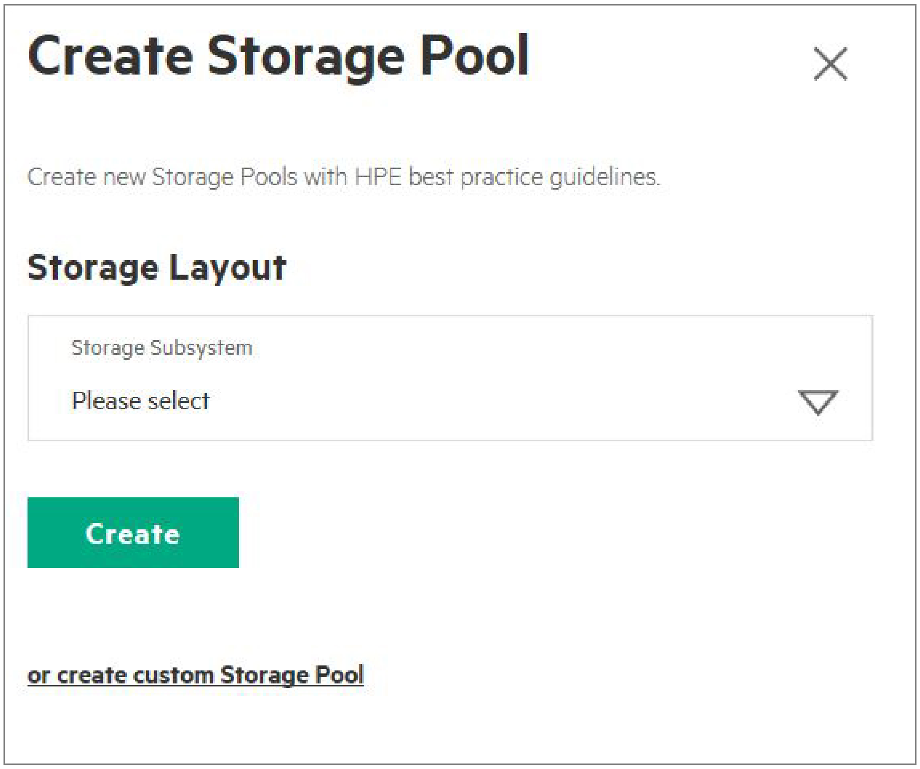
3. Click **Storage Pools**.



○	Name	Total Size	Used Size	Utilization	Resiliency Setting
●	0b_A	111.76 GiB	111.76 GiB	100 %	RAID 1
●	Rajani Pool	2793.97 GiB	2687.73 GiB	96 %	RAID 1
●	test	1862.65 GiB	1862.65 GiB	100 %	RAID 1

4. Click + icon on the top left corner.

5. From the **Create Storage Pool** page, select the storage subsystem.



Create Storage Pool

Create new Storage Pools with HPE best practice guidelines.

Storage Layout

6. Click **Create**.

Deleting Storage Pools

The Storage Pools can be deleted using:

Deleting Storage Pools using Smart Storage Administrator

Deleting Storage Pools using Smart Storage Administrator

Follow the steps to delete Storage Pools using Smart Storage Administrator:

1. Click **Start** menu on your desktop.
2. Select **Windows System** > **Smart Storage Administrator**.
3. Select **Smart Array Controller**.
4. Select **Actions** from the right pane, and click **Configure**.
5. Select **Logical Devices** under **Controller Devices**.
6. Select the array which you want to delete. Click **Delete array**.
7. Click **Yes** in the confirmation message.

Adding disks to Storage Pools

The disks can be added to Storage Pools using:

Adding disks to Storage Pools using Smart Storage Administrator

Adding disks to Storage Pools using Smart Storage Administrator

Follow the steps to add disks to Storage Pools using Smart Storage Administrator:

1. Click **Start** menu on your desktop.
2. Select **Windows System** > **Smart Storage Administrator**
3. Under **Available Devices** > **Smart Array Controllers**, Select the controller with the array (pool) to which you need to add the disks.

   ⓘ **IMPORTANT:**

   The SSA arrays are referred as pools.

4. Select **Actions** from the right pane, and click **Configure**.
5. Click **Logical Devices**.
6. Select the array where the disks to be added. After array selection, multiple actions associated to the array are displayed.
7. Click **Manage data drives**. This action opens a separate window.
8. Select **Available Array Action(s)**.
9. Select **Add Drive(s)** .

   NOTE:

   Selecting Physical Drives: Clicking on the drives would allow the user to select specific drives (disks) to be added. The user can select **Select all** option to select all the available disks for expansion.

   The process of expansion might take some time, during which cache of the controller disabled. User is not allowed to add any disks to any available arrays. Progress of the process can be seen by hovering on the warning sign.

10. Click **Ok**.

Replacing failed disks

Follow the steps to replace failed disks:

1. Identify the server and power off.
2. Pull out the failed drives.
3. Insert the healthy drives.
4. Power on the server
5. Check the health status of the server and the physical disks.

Volumes

A volume is a detectable unit of HPE StoreEasy management console data storage.

You can create a volume on a physical disk or a virtual disk. A virtual disk is a collection of one or more physical disks from a previously created storage pool. The layout of data across the physical disks can increase the reliability and performance of the volume.

Volumes overview

The Volumes page provides the details of volumes created on the connected enclosures and arrays. All volumes available in the system, including operating system volumes are displayed.

The following operational and informational icons are available in the **Volumes** page:

Icon	Function	Description
🔍	Search	Allows the user to locate the specified volume. Searches for the text you enter in the **Search** box. Enter the search string in the **Search** bar to filter the individual element from the existing list of resources.
+	Add	Enables the user to add a volume.

Table Continued

Icon	Function	Description
⛛	Filter	Filter tool is used to limit the information displayed to the specified criteria by entering the data you want to filter on. You can filter the volumes based on the following status: • ALL: This displays all the available volumes. The total number of available volumes are shown above the filter icon. • ◆ Critical: This option filters the volumes that are in critical state which needs immediate user attention. • ⚠ Warning: This indicates the abnormal state of a volume that requires interaction before further execution. In most cases warning represents the degraded, stressed, aborted, dormant, relocating, detached, and incomplete state of the volumes. • ● OK: Indicates the healthy status of the volume. • ○ Unknown: This indicates the unknown state of the volume. The unknown error occurs if there is a loss of communication or if the state of the volume is unknown.
↑	Sort	Determines whether items are displayed in ascending or descending order.

Creating Volumes

The Volumes can be created by:

- **Creating Volumes using HPE StoreEasy management console**
- **Creating Volumes using Server Manager**

Creating Volumes Using HPE StoreEasy management console

Create Volume page enables you to create a simple volume or advanced volume.

To create a simple volume, perform the following steps:

1. Click **Volumes** in the left navigation menu.
2. Click + add icon in the **Volumes** page.
3. Enter the name for a volume in the **Create Volume** page.

   Use a backslash as required as part of volume names. For example, `DataVolume`. They are not case-sensitive. Do not use the reserved characters like, **<** (less than), **>** (greater than), **"** (double quote), **/** (forward slash), **|** (vertical bar),**?** (question mark) and ***** (asterisk).

4. Select the Virtual Disk from the **Virtual Disk** drop-down menu on which the volume will be created.

   To add new virtual disk, click **Create new Virtual Disk**. For the detailed procedure, refer to **Create a virtual disk**.

5. Click **Create**.

To create a volume with advanced configurations, perform the following steps:

1. Click **Volumes** in the left navigation menu.
2. Click + add icon in the **Volumes** page.
3. Select **Show Advanced configuration options** in the **Create Volume** page.
4. Enter the name for a volume in the **Name** section.

   Use a backslash as required as part of volume names. For example, `DataVolume`. They are not case-sensitive. Do not use the reserved characters like, **<** (less than), **>** (greater than), **"** (double quote), **/** (forward slash), **|** (vertical bar),**?** (question mark) and ***** (asterisk).

5. Select the Virtual Disk from the **Virtual Disk** drop-down menu on which the volume will be created.

   To add new virtual disk, click **Create new Virtual Disk**. For the detailed procedure, refer to **Create a virtual disk**.

6. Click ✎ edit icon in the **Deduplication** section to configure deduplication.

   Data deduplication optimizes free space on a volume. It looks for duplicated portions on the volume and compress it for additional savings.

7. Select any of the following modes of deduplication from the **Mode** drop-down menu and click **OK**:

   - Disabled: Data deduplication is disabled.
   - General Purpose File Server: Reduces the storage capacity utilization by half (2:1).
   - VDI Server: Hosts a desktop operating system on a centralized server. Reduces the storage utilization by 20:1 ratio.
   - Virtualized backup server

   NOTE:

   The files will be deduplicated and optimized in the background only. To configure additional throughput optimization schedules, use Server Manager or PowerShell. Deduplication is not supported on the ReFS system.

8. Click ✎ edit icon in the **Snapshot Size Limit** section and select either of the following options to configure the snapshot size limit:

   - No Limit
   - Use Limit

   Snapshot is a backup copy created at a particular point in time. Snapshot size limits the amount of volume capacity used to store backup copies. Size limit is capacity on volume that can be used to store these backups. To create a snapshot, you need a minimum of 300 MiB space.

9. Click **OK**.
10. Select either of the following file systems from the **File System** section:

    - NTFS (default): Provides continuously available volumes that can be accessed simultaneously from multiple nodes of a failover cluster. It continuously monitors and updates the issues in the background without taking the volume offline. For more information, see **https://technet.microsoft.com/en-us/library/dn466522(v=ws.11).aspx**.
    - ReFS: Resilient File System (ReFS) has additional file system features. For more information, see **https://technet.microsoft.com/en-us/library/hh831724(v=ws.11).aspx**.

11. Select the drive letter from the **Drive Letter** drop-down menu.
12. Select the allocation unit from the **Allocation Unit** drop-down menu and click **Create**.

Creating Volumes using Server Manager

The following table describes the fields that are available on Create Volume page through Server Manager:

Field	Description
Volume	Name of the Volume
Status	Represents the state of the volume
File System Label	Label assigned to a specific volume
Provisioning	Type of provisioning. For example, Thin or Fixed
Capacity	Total capacity of the volume
Free Space	Available free space
Deduplication rate	
Deduplication Savings	
Percent Used	Horizontal graph representing the utilized storage space

You can create new volume using Server Manager:

1. Go to **Windows Server Manager** > **File and Storage Services** > **Volumes**.
2. Click **Tasks**, located at the right corner.
3. Select **New Volume...**.

4. Select the desired server and disk.
5. click **Create**.

Deleting Volumes

The volumes can be deleted by:

Deleting Volumes using HPE StoreEasy management console

Deleting Volumes using HPE StoreEasy management console

- Click **Delete** in the **Edit Volume** window.
- Select **Are you sure** and click **Yes, Delete** to confirm deletion.

IMPORTANT:

All the data on the volume will be lost. HPE recommends the users to back up the data before deleting.

NOTE:

File shares must be removed before deleting a volume.

Managing file and folder permissions

Managing folder permissions

File system elements are composed of the folders and subfolders that are created under each logical storage element (partitions, logical disks, and volumes). Folders are used to further subdivide the available file system, providing another level of granularity for management of the information space. Each of these folders can contain separate permissions and share names that can be used for network access. Folders can be created for individual users, groups, projects, and so on.

The folders can be managed using Server Manager. The folder management includes:

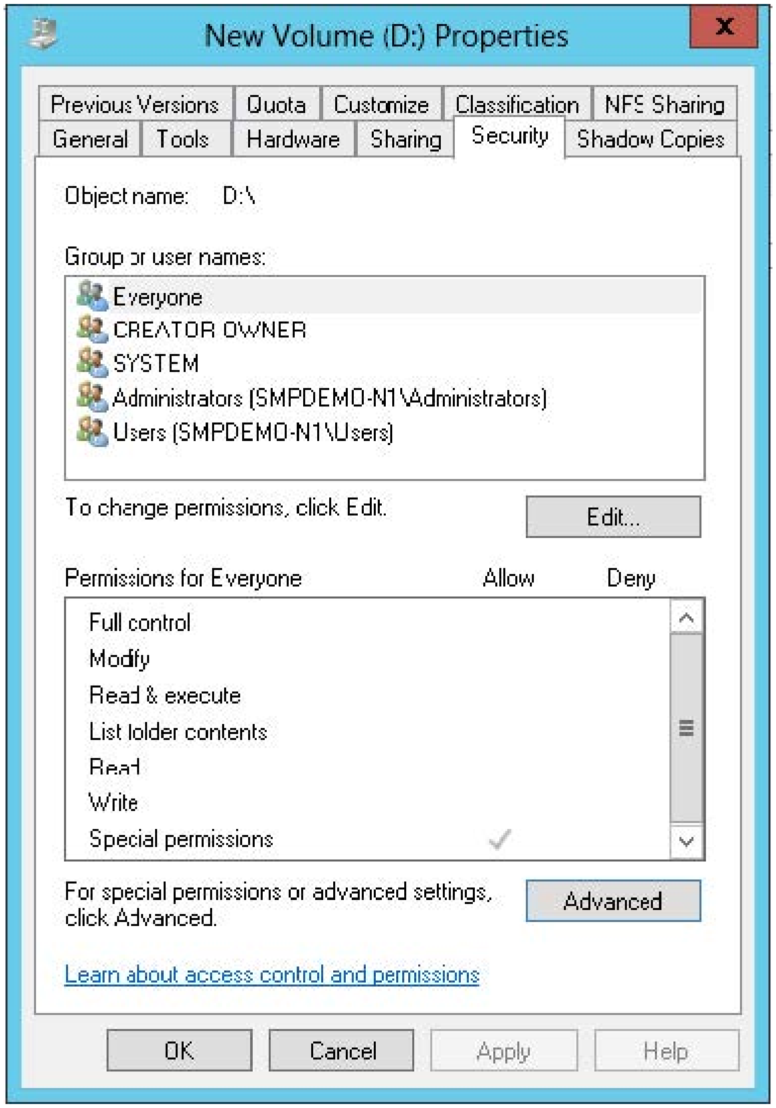
- Accessing a specific volume or folder
- Creating a new folder
- Deleting a folder
- Modifying folder properties
- Creating a new share for a volume or folder
- Managing shares for a volume or folder

Managing file permissions

Security at the file level is managed using Windows Explorer. File level security includes settings for permissions, ownership, and auditing for individual files.

Follow the steps to manage file permissions:

1. Using Windows Explorer, access the folder or file that needs to be changed, and then right-click the folder.
2. Click **Properties**
3. Click **Security** tab.



Object name: D:\

Group or user names:

- Everyone
- CREATOR OWNER
- SYSTEM
- Administrators (SMPDEMO-N1\Administrators)
- Users (SMPDEMO-N1\Users)

To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Write		
Special permissions	✓	

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

4. Several options are available on the Security tab:

- To add users and groups to the permissions list, click **Add**. Follow the dialog box instructions.
- To remove users and groups from the permissions list, highlight the desired user or group, and then click **Remove**.
- The center section of the Security tab lists permission levels. When new users or groups are added to the permissions list, select the appropriate boxes to configure the common file-access levels.

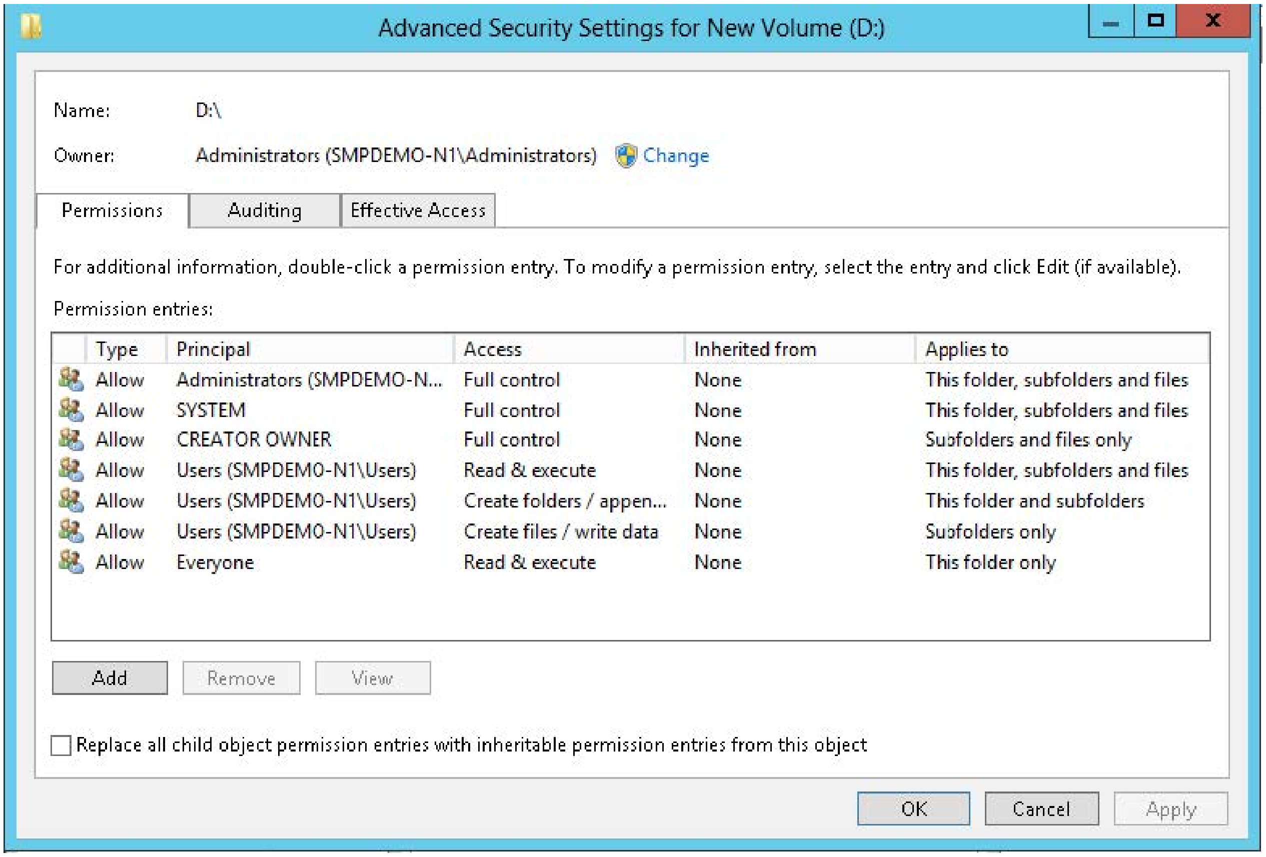
Advanced tab:

In Advanced Security Settings for New Volume, there are three subsections:

- Permissions
- Auditing

  Effective Access

Permissions: To modify ownership of files, or to modify individual file access level permissions, click **Advanced** > **Permissions**.



Advanced Security Settings for New Volume (D:)

Name: D:\

Owner: Administrators (SMPDEMO-N1\Administrators) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

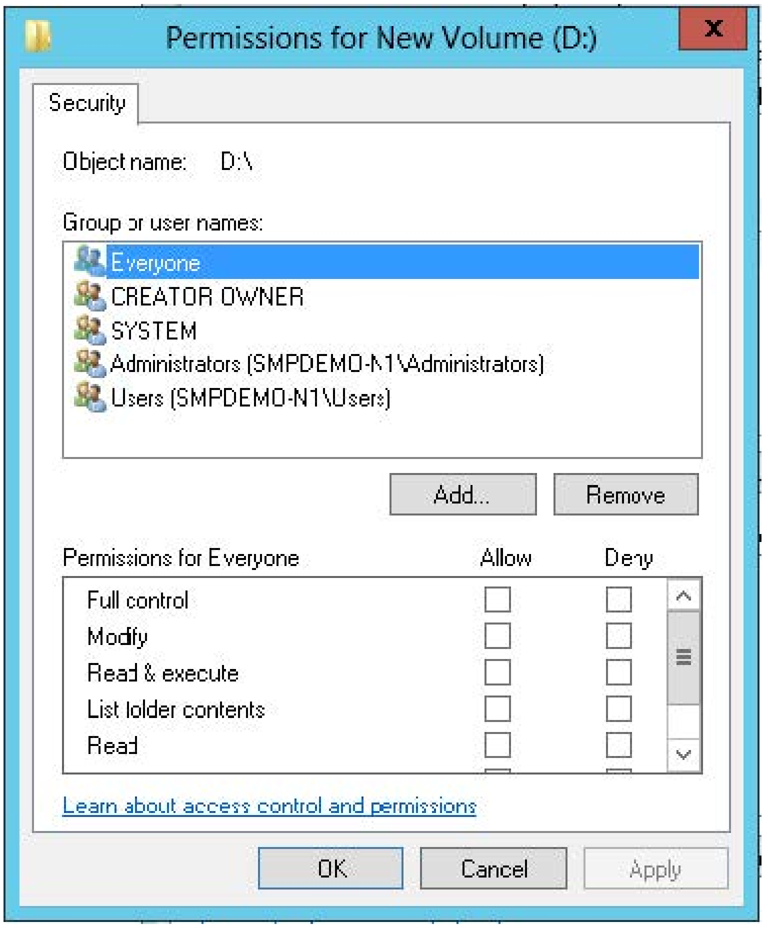
Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (SMPDEMO-N...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	Users (SMPDEMO-N1\Users)	Read & execute	None	This folder, subfolders and files
Allow	Users (SMPDEMO-N1\Users)	Create folders / appen...	None	This folder and subfolders
Allow	Users (SMPDEMO-N1\Users)	Create files / write data	None	Subfolders only
Allow	Everyone	Read & execute	None	This folder only

□ Replace all child object permission entries with inheritable permission entries from this object

The following functionalities are available in Advanced Security Settings:

- Add a new user or group, click **Add**, and then follow the dialog box instructions.
- Remove a user or group, click **Remove**.
- Replace permission entries on all child objects. This allows all child folders and files to inherit the current folder permissions by default.
- Modify specific permissions assigned to a particular user or group — Select the desired user or group, and then click **Edit**.

Enable or disable permissions by selecting the **Allow** box to enable permission or the **Deny** box to disable permission. If neither box is selected, permission is automatically disabled.


Permissions for New Volume (D:)
Security
Add...
Remove
Learn about access control and permissions
OK
Cancel
Apply

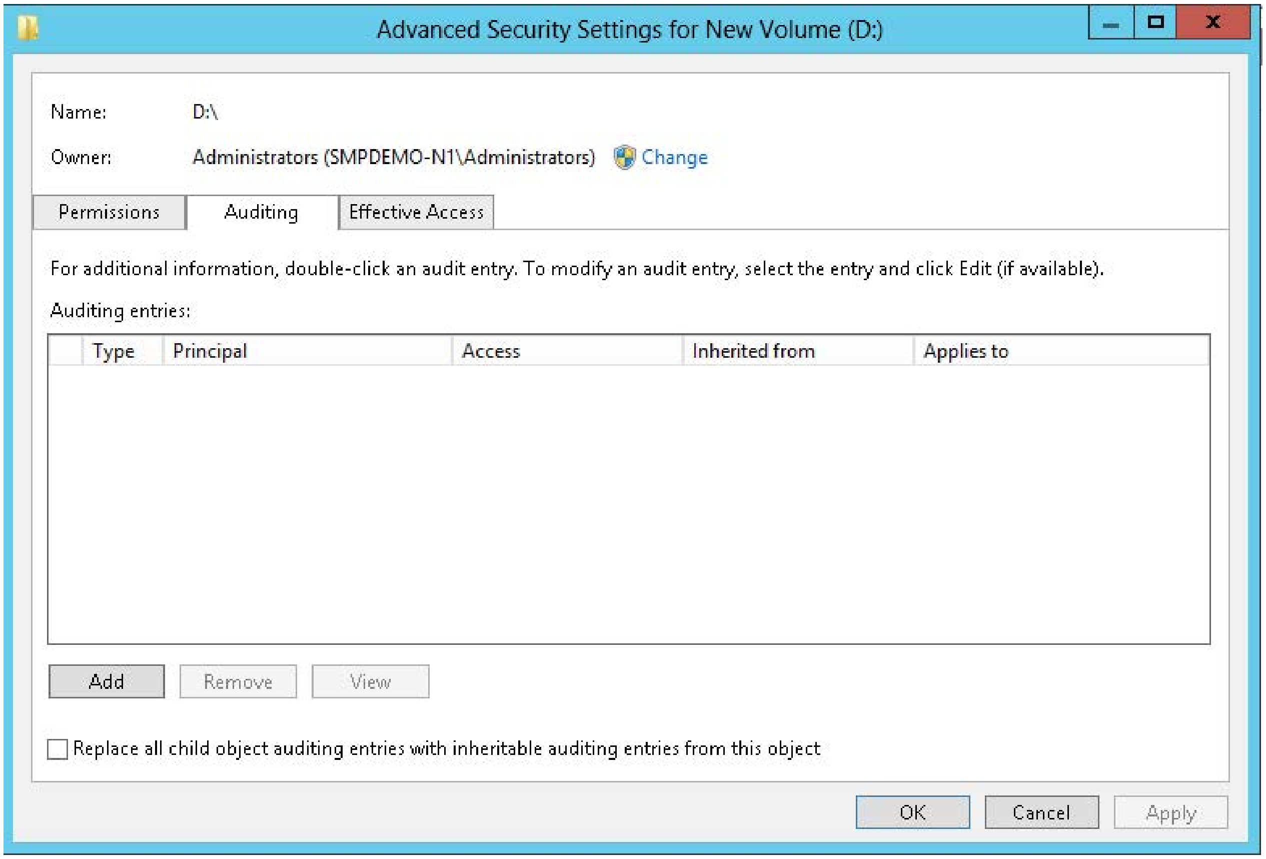
Object name: D:\

Group or user names:

- Everyone
- CREATOR OWNER
- SYSTEM
- Administrators (SMPDEMO-N1\Administrators)
- Users (SMPDEMO-N1\Users)

Permissions for Everyone	Allow	Deny
Full control	□	□
Modify	□	□
Read & execute	□	□
List folder contents	□	□
Read	□	□

Auditing: Another area of the Advanced Security Settings is the **Auditing** tab. Auditing allows you to set rules for the auditing of access, or attempted access, to files or folders. Users or groups can be added, deleted, viewed, or modified through the **Auditing** tab.



Advanced Security Settings for New Volume (D:)

Name: D:\

Owner: Administrators (SMPDEMO-N1\Administrators) Change

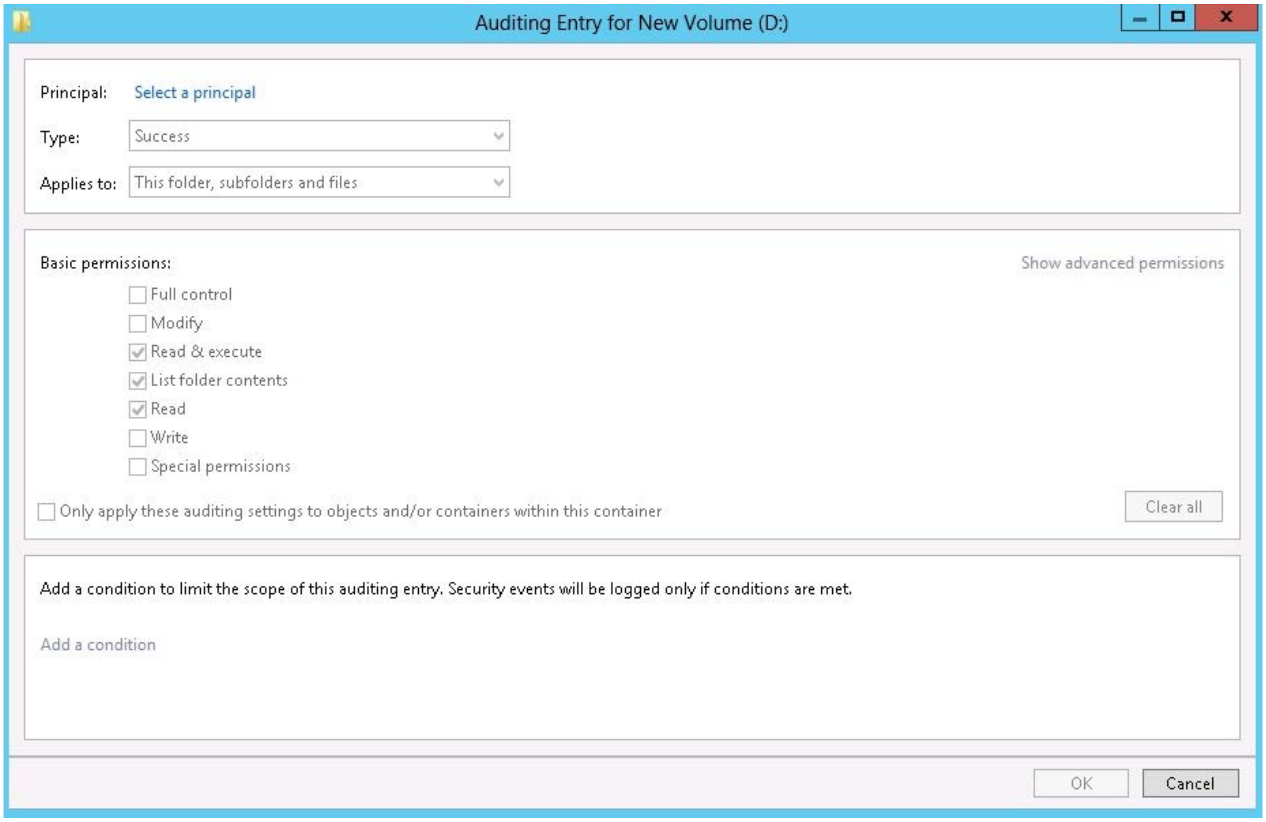
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to

□ Replace all child object auditing entries with inheritable auditing entries from this object

Click **Add** to display the Auditing Entry screen.



Auditing Entry for New Volume (D:)

Principal: Select a principal

Type: Success

Applies to: This folder, subfolders and files

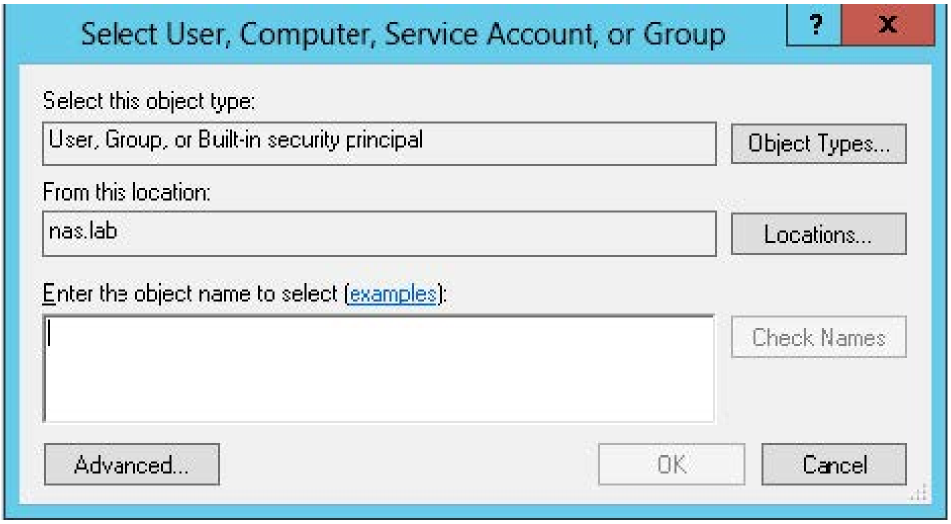
Basic permissions:

□ Full control
□ Modify
☑ Read & execute
☑ List folder contents
☑ Read
□ Write
□ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Click **Select a principal** to display the Select User or Group screen.



Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
nas.lab

Enter the object name to select (examples):

NOTE:

Click **Advanced** to search for users or groups.

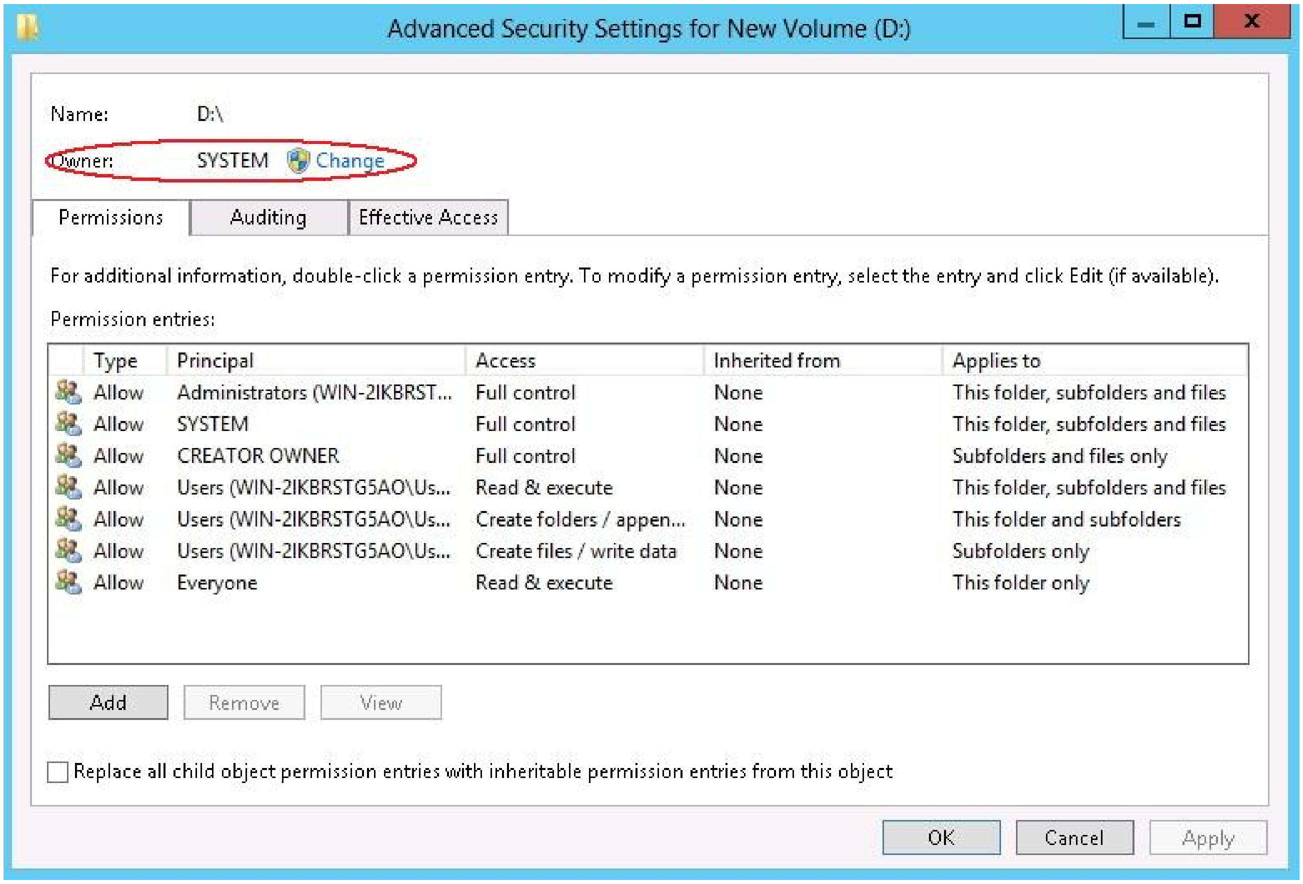
Follow the steps for auditing reports:

1. Select the user or group.
2. Click **OK**.
3. Select the desired Successful and Failed audits for the user or group.
4. Click **OK**.

NOTE:

Enable to audit to configure auditing information. Use the local Computer Policy Editor to configure the audit policy on HPE StoreEasy 1X60 Storage.

The Owner tab allows taking ownership of files. Typically, administrators use this area to take ownership of files when the file ACL is incomplete or corrupt. By taking ownership, you gain access to the files, and then manually apply the appropriate security configurations.



Name: D:\

Owner: SYSTEM Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Administrators (WIN-2IKBRST...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	CREATOR OWNER	Full control	None	Subfolders and files only
Allow	Users (WIN-2IKBRSTG5AO\Us...	Read & execute	None	This folder, subfolders and files
Allow	Users (WIN-2IKBRSTG5AO\Us...	Create folders / appen...	None	This folder and subfolders
Allow	Users (WIN-2IKBRSTG5AO\Us...	Create files / write data	None	Subfolders only
Allow	Everyone	Read & execute	None	This folder only

□ Replace all child object permission entries with inheritable permission entries from this object

File Shares

File Shares are shared folders on a HPE StoreEasy Storage systems that hold files which users and groups can access over a network. The same set of files and folders can be simultaneously accessed using both the Network File Systems (NFS) and Server Message Block (SMB) protocols. The HPE StoreEasy Storage product family provides SMB, NFS, and iSCSI target server capability that enables storage provisioning over TCP/IP networks. This solution allows customers to connect SMB clients, NFS clients, and iSCSI initiators to HPE StoreEasy Storage and deploy an end-to-end NAS solution.

To interact with a file share, a user must have the appropriate share permissions to be able to map or mount the File Share (from an SMB or NFS client). In HPE StoreEasy management console, such permissions are referred to as share permissions. These share permissions are used to allow discretionary access, including access to the shared folder. Once the user has set the share-level permissions, the user has to set the folder permission at the root of the share to be able to access the shared folder. These permissions are referred as the folder permissions.

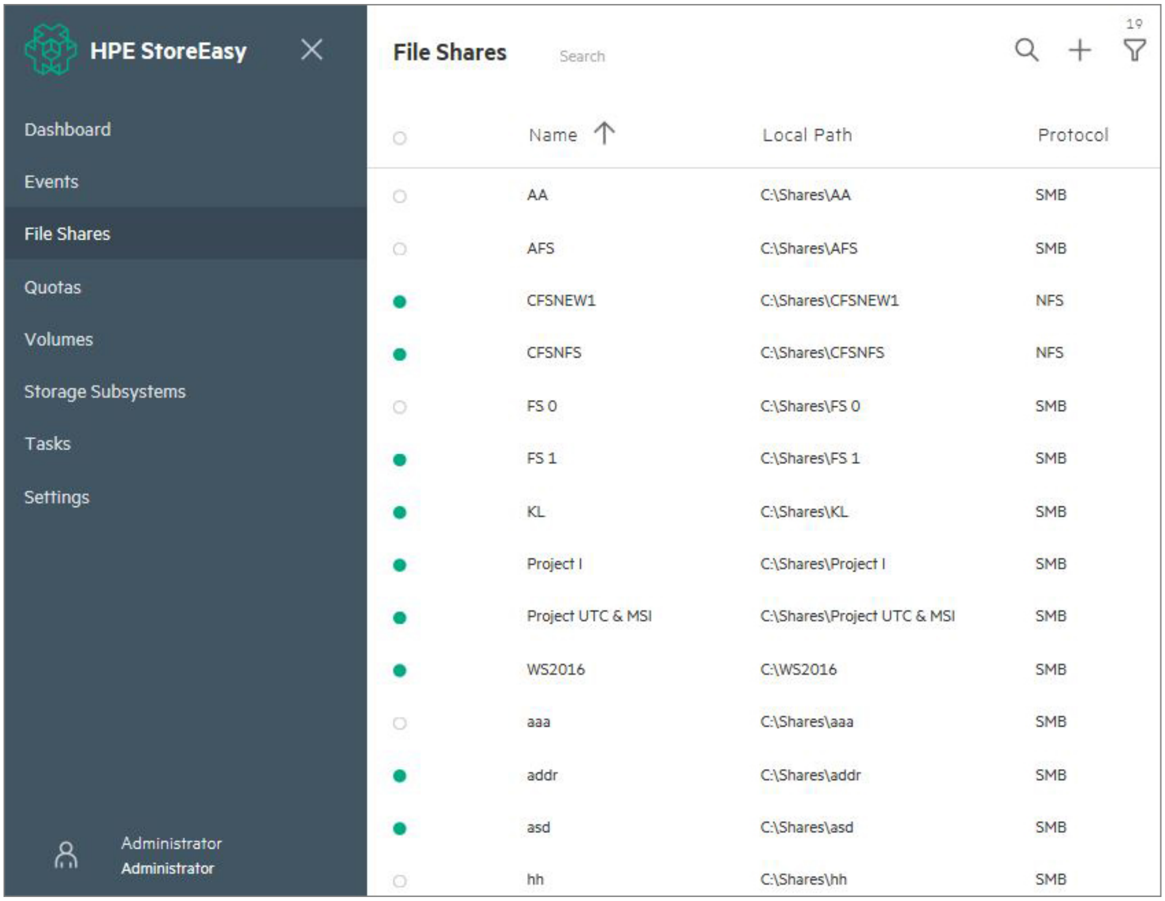
HPE StoreEasy management console allows administrators with Administrator and Operator roles to provision SMB and NFS protocol file shares. Each one accessed using an appropriate network protocol. Each network protocol enables the client to access the files or directories stored in File Shares for that protocol typeover the network. File Shares properties include share type (which defines the access protocol), share path, client filters list, and share-level permissions. File sharing protocols (except NFS) supply a user and group context for all connections over the network. NFS supplies a machine-based context.

File Shares Overview

File Shares page in HPE StoreEasy management console provides the list of all available File Shares, local path where the File Shares are created and the File Share protocols.

To view File Shares, select **File Shares** from the HPE StoreEasy management console left navigation pane.

File Shares screen components



○	Name ↑	Local Path	Protocol
○	AA	C:\Shares\AA	SMB
○	AFS	C:\Shares\AFS	SMB
●	CFSNEW1	C:\Shares\CFSNEW1	NFS
●	CFSNFS	C:\Shares\CFSNFS	NFS
○	FS 0	C:\Shares\FS 0	SMB
●	FS 1	C:\Shares\FS 1	SMB
●	KL	C:\Shares\KL	SMB
●	Project I	C:\Shares\Project I	SMB
●	Project UTC & MSI	C:\Shares\Project UTC & MSI	SMB
●	WS2016	C:\WS2016	SMB
○	aaa	C:\Shares\aaa	SMB
●	addr	C:\Shares\addr	SMB
●	asd	C:\Shares\asd	SMB
○	hh	C:\Shares\hh	SMB

You can perform the following operations in the **File Shares** screen:

Icon	Function	Description
🔍	Search	Allows the user to locate the specific File Share based on the File Share name. Searches for the text you enter in the **Search** box. Enter the search string in the **Search** bar to filter the individual File Share from the existing list of resources.
+	Add	Allows you to create new SMB or NFS File Shares on a local path along with selecting the authentication method and file system permission settings for multi-protocol access of the shared folder. SMB is a network file sharing protocol using which you can access files or other resources at a remote server. SMB functions as an application-layer network protocol. This allows you to read, create, and update files on the remote server. NFS is a network file sharing protocol used to access files from any location on the network, transparently. An NFS server makes a directory available to other hosts on the network, by sharing the directory. It allows the user to designate all or a portion of a file system on a server which can be accessed by the clients with appropriate permissions assigned to them. You can store and update files on a remote system.

Table Continued

Icon	Function	Description
⛛	Filter	Filter tool is used to limit the information displayed to the specified criteria by entering the data you want to filter on. You can filter the File Shares based on the following status: • **ALL:** This displays all the available File Shares. The total number of available File Shares are shown above the filter icon. • ◆ **Critical:** This option filters the File Shares that are in critical state which needs immediate user attention. • ▲ **Warning:** This indicates the abnormal state of a quota that requires interaction before further execution. In most cases warning represents the degraded, stressed, aborted, dormant, relocating, detached, and incomplete state of the quota. • ● **OK:** Indicates the healthy status of the quota. • ○ **Unknown:** This indicates the unknown state of the quota. The unknown error occurs if there is a loss of communication or if the state of the quota is unknown.
↑	Sort	Determines whether items are displayed in ascending or descending order.

SMB File Shares

SMB File Shares Overview

Access-based enumeration

Displays only the files and folders that a user has permissions to access.

SMB encryption

SMB encryption provides end-to-end encryption of SMB data and protects data from eavesdropping occurrences and untrusted networks.

Caching

Allows the user to have access to shared files even when they are working offline without access to the network.

Permissions

This action allows the user to set the appropriate permissions to access the file share.

HPE StoreEasy management console provides following permissions:

- Shared Permissions
- Folder Permissions

Creating SMB File Shares

The SMB files can be created from:

Creating SMB file Shares using HPE StoreEasy management console

Creating SMB File Shares Using HPE StoreEasy management console

Procedure

1. Select **File Shares** from the left navigation pane and click add icon (+) in the **File Shares** page.
2. Select **SMB** in the **Protocol** section of the **Create File Share** page.

   SMB File Sharing allows you to read, create, and update files on the remote server. SMB functions as an application-layer network protocol.
3. Enter a name for the File Share in the **Name** field of the **General** section.

   A File Share name can contain only letters, numbers, and the dash (-) character. It should not be more than 80 characters in length. Do not use illegal characters like, `\ / [ ] : &#124; < > + = ; , * ? "`.
4. Select the available Volume in which the file share will be created from the **Volume** drop-down menu or enter the Volume name in the Search (🔍) string to locate a specific Volume.

   You can also create a Volume by clicking **Create new Volume** from the **Volume** drop-down menu. To create a Volume, see **Create a volume** section.
5. The local path in which the file share will be created is populated by default.

   Click **Customize Path** toggle button, if a custom directory must be shared. This allows you to create a share on any folder or subfolder on the volume, otherwise the share will be created on the selected volume with the default share path.

   A pathname must include directory or file name, separated by the backward-slash (\) character. For example, `C:\Shares\Test`.
6. Click add icon (+) in the **Share Permissions** section to set security permissions on files.

   Share permissions are the permissions set for a file while sharing. The share permissions determine the type of access others have to the shared files across the network.

a. Enter the account name of the user if you want to provide the access. The account name can be User, Service account, Computer, and Groups.

b. Select either **Allow** or **Deny** access type. These options allows grant or deny access to the files.

c. Select either of the three types of share permissions from the **Access Permissions** drop-down menu and click **OK**:

   - Full Control: The user can perform read, write, edit, and delete Files Shares.
   - Change: Allows the user to read and write.
   - Read: Allows the user to view or access the File Share.

   Click **Remove** in the **Configure Share Permission** action pane to remove Share permission

7. Click add icon (+) in the **Folder Permissions** section to configure new Folder permissions.

   To change or remove folder permissions from an existing user, click the edit icon (✏) next to the existing user name under **Folder Permissions** section.

   a. Enter the account name of the user if you want to provide the access. The account name can be User, Service account, Computer, and Groups.

   b. Select either **Allow** or **Deny** access type. These options allows grant or deny access to the folders.

   c. Select any of the following options from the **Applies To** drop-down menu for which you want to allow or deny access permissions:

      - The folder, subfolders, and files
      - Only Folder
      - The folder and subfolders
      - The folder and files
      - The subfolder and files
      - Only files
      - Only subfolders

8. Select either of the following permissions from the **Access Permissions** drop-down menu and click **OK**:

Access Permissions	**Meaning**
Full Control	The user can perform read, write, edit, and delete folders.
Modify	The user can read, write, and edit the folder contents.
Read and Execute	Permits viewing and accessing of the folder contents as well as executing of the file Share.

Table Continued

Access Permissions	Meaning
List folder contents	Allows viewing and listing of files and subfolders as well as executing of files; inherited by folders only.
Read	Allows the user to view or access the File Share.
Write	Allows writing to a file.

a. Click **Advanced Permissions** toggle button for granting or denying the following advanced permissions and click **OK**.

Advanced Permissions	Meaning
Full Control	The user can perform read, write, edit, and delete folders.
Traverse folder/execute file	The user writes to a file.
List folder/read data	Allows viewing and listing of files and subfolders as well as executing of files; inherited by folders only.
Read attributes	
Read extended attributes	
Create files/write data	Allows user to read and write.
Create folders/append data	
Write extended attributes	
Write attributes	
Delete subfolders and files	
Delete	
Read permission	
Change permission	
Take ownership	

9. Enter the description for creating a File Share in the **Description** field of the **Additional Configuration Options**.

10. Select either or all the following Share properties from the **Share Properties** section:

    - **Enable SMB encryption:** Allows you to automatically encrypt the data before it is stored.
    - **Access-based enumeration:** Displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, the storage system hides the folder from the user's view. This feature is active only when viewing files and folders in a shared folder.
    - **Enable cache:** Storage system caches hold the data that comes in from external systems such as a host server, decoupling the storage from the compute engine. This allows you to optimize the speed of the storage system and improves efficiency.

If you select Enable Cache, you have option to select **Enable Branch Cache**. Branch Cache fetches content from the host server and caches the content at the local system.

11. Select the available Quota from the **Quota** field or click **Add new Quota Template** to create a Quota Template. To create a Quota Template, see **Creating a Quota Template** section.
12. Click **Create**.

Deleting SMB File Shares

SMB File Shares can be deleted from:

Deleting SMB File Shares using HPE StoreEasy management console

Deleting SMB File Shares Using HPE StoreEasy management console

Procedure

1. Select **File Shares** from the left navigation pane and click any of the available SMB File Share.
2. Click edit icon (✎) in the **File Share** page.
3. Click **Delete** in the **Edit File Share** page.
4. Choose **Delete the quota on the folder** and **Are you sure?**.
5. Click **Yes, Delete** to confirm deletion.

   Sharing for particular File Share will be stopped, but the folder remains intact.

   NOTE:

   Before deleting a share, warn all users to save the data and exit that share. Ensure that no one is using that share.

Changing SMB File Share properties

The SMB File Share properties can be changes using:

Changing SMB File Share properties using HPE StoreEasy management console

Changing SMB File Share properties using HPE StoreEasy management console

Procedure

1. Select **File Shares** from the HPE StoreEasy management console left navigation pane and click any of the available SMB File Shares.
2. Click edit icon (✎) in the **File Share** page to edit security permissions for shares and folders. You can also modify the share properties and the Quota applied.
3. Click add icon (+) in the **Share Permissions** section to set security permissions on files.

Share permissions are the permissions set for a file while sharing. The share permissions determine the type of access others have to the shared files across the network.

a. Enter the account name of the user if you want to provide the access. The account name can be User, Service account, Computer, and Groups.

b. Select either **Allow** or **Deny** access type. These options allows grant or deny access to the files.

c. Select either of the three types of share permissions from the **Access Permissions** drop-down menu and click **OK**:

   - Full Control: The user can perform read, write, edit, and delete Files Shares.
   - Change: Allows the user to read and write.
   - Read: Allows the user to view or access the File Share.

   Click **Remove** in the **Configure Share Permission** action pane to remove Share permission

4. Click add icon (+) in the **Folder Permissions** section to configure new Folder permissions.

   To change or remove folder permissions from an existing user, click the edit icon (✎) next to the existing user name under **Folder Permissions** section.

   a. Enter the account name of the user if you want to provide the access. The account name can be User, Service account, Computer, and Groups.

   b. Select either **Allow** or **Deny** access type. These options allows grant or deny access to the folders.

   c. Select any of the following options from the **Applies To** drop-down menu for which you want to allow or deny access permissions:

      - The folder, subfolders, and files
      - Only Folder
      - The folder and subfolders
      - The folder and files
      - The subfolder and files
      - Only files
      - Only subfolders

5. Select either of the following permissions from the **Access Permissions** drop-down menu and click **OK**:

Access Permissions	Meaning
Full Control	The user can perform read, write, edit, and delete folders.
Modify	The user can read, write, and edit the folder contents.

Table Continued

Access Permissions	Meaning
Read and Execute	Permits viewing and accessing of the folder contents as well as executing of the file Share.
List folder contents	Allows viewing and listing of files and subfolders as well as executing of files; inherited by folders only.
Read	Allows the user to view or access the File Share.
Write	Allows writing to a file.

a. Click **Advanced Permissions** toggle button for granting or denying the following advanced permissions and click **OK**.

Advanced Permissions	Meaning
Full Control	The user can perform read, write, edit, and delete folders.
Traverse folder/execute file	The user writes to a file.
List folder/read data	Allows viewing and listing of files and subfolders as well as executing of files; inherited by folders only.
Read attributes	
Read extended attributes	
Create files/write data	Allows user to read and write.
Create folders/append data	
Write extended attributes	
Write attributes	
Delete subfolders and files	
Delete	
Read permission	
Change permission	
Take ownership	

6. Enter the description for creating a File Share in the **Description** field of the **Additional Configuration Options**.
7. Select either or all the following Share properties from the **Share Properties** section:

- **Enable SMB encryption:** Allows you to automatically encrypt the data before it is stored.
- **Access-based enumeration:** Displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, the storage system hides the folder from the user's view. This feature is active only when viewing files and folders in a shared folder.
- **Enable cache:** Storage system caches hold the data that comes in from external systems such as a host server, decoupling the storage from the compute engine. This allows you to optimize the speed of the storage system and improves efficiency.

If you select Enable Cache, you have option to select **Enable Branch Cache**. Branch Cache fetches content from the host server and caches the content at the local system.

8. Select the available Quota from the **Quota** field or click **Add new Quota Template** to create a Quota Template. To create a Quota Template, see **Creating a Quota Template** section.
9. Click **Apply** to save the changes.

NFS File Shares

The Network File System (NFS) is a client/server application that lets a computer user view and optionally store and update files on a remote computer as though they were on the users own computer. The **NFS** protocol is one of the several distributed file system standards for network-attached storage (NAS). The NFS protocol is the default protocol used by UNIX/Linux clients.

Creating NFS File Shares

The NFS File Shares can be created using:

Creating NFS File Shares using HPE StoreServ management console

Creating NFS File Shares Using HPE StoreEasy management console

Procedure

1. Select **File Shares** from the left navigation pane and click add icon (+) in the **File Shares** page.
2. Select **NFS** in the **Protocol** section of the **Create File Share** page.

   NFS File Share allows
3. Enter a name for the File Share in the **Name** field of the **General** section.

   A File Share name can contain only letters, numbers, and the dash (-) character. It should not be more than 80 characters in length. Do not use illegal characters like, `\ / [ ] : &#124; < > + = ; , * ? "`.
4. Select the available Volume in which the file share will be created from the **Volume** drop-down menu or enter the Volume name in the Search (🔍) string to locate a specific Volume.

   You can also create a Volume by clicking **Create new Volume** from the **Volume** drop-down menu. To create a Volume, see **Create a volume** section.
5. The local path in which the file share will be created is populated by default.

   Click **Customize Path** toggle button, if a custom directory must be shared. This allows you to create a share on any folder or subfolder on the volume, otherwise the share will be created on the selected volume with the default share path.

   A pathname must include directory or file name, separated by the backward-slash (\) character. For example, `C:\Shares\Test`.
6. Click add icon (+) in the **Share Permissions** section to set security permissions on files.

   Share permissions are the permissions set for a file while sharing. The share permissions determine the type of access others have to the shared files across the network.

   a. Select any of the following type from the **Type** drop-down menu:

      - Host
      - Netgroup
      - Client group
      - All Machines

   b. Select either of the three types of share permissions from the **Access Permissions** drop-down menu and click **OK**:

      - Read only: The user can only view the Files Shares.
      - Read and write: Allows the user to read and write.
      - No Access: User do not have access to the File Share.

      Choose **Allow Root Access**.

7. Click **OK**.

8. Click add icon (+) in the **Folder Permissions** section to configure new Folder permissions.

   To change or remove folder permissions from an existing user, click the edit icon (✎) next to the existing user name under **Folder Permissions** section.

   a. Enter the account name of the user if you want to provide the access. The account name can be User, Service account, Computer, and Groups.
   b. Select either **Allow** or **Deny** access type. These options allows grant or deny access to the folders.
   c. Select any of the following options from the **Applies To** drop-down menu for which you want to allow or deny access permissions:

      - The folder, subfolders, and files
      - Only Folder
      - The folder and subfolders
      - The folder and files
      - The subfolder and files
      - Only files
      - Only subfolders

9. Select either of the following permissions from the **Access Permissions** drop-down menu and click **OK**:

Access Permissions	Meaning
Full Control	The user can perform read, write, edit, and delete folders.
Modify	The user can read, write, and edit the folder contents.
Read and Execute	Permits viewing and accessing of the folder contents as well as executing of the file Share.
List folder contents	Allows viewing and listing of files and subfolders as well as executing of files; inherited by folders only.
Read	Allows the user to view or access the File Share.
Write	Allows writing to a file.

a. Click **Advanced Permissions** toggle button for granting or denying the following advanced permissions and click **OK**.

Advanced Permissions	Meaning
Full Control	The user can perform read, write, edit, and delete folders.
Traverse folder/execute file	The user writes to a file.
List folder/read data	Allows viewing and listing of files and subfolders as well as executing of files; inherited by folders only.
Read attributes	
Read extended attributes	
Create files/write data	Allows user to read and write.
Create folders/append data	
Write extended attributes	
Write attributes	
Delete subfolders and files	
Delete	
Read permission	
Change permission	
Take ownership	

10. Click edit icon (✎) in the **Authentication** section to specify an array of authentication types that a user can use to access NFS shares.

    a. The acceptable values for this parameter are, Sys (AUTH_SYS authentication):

- Kerberos v5 Authentication (krb5)
- Kerberos v5 Authentication and integrity (krb5i)
- Kerberos v5 Authentication and privacy (krb5p)

For more information on the authentication types, see **Authentication**.

b. Select **AUTH_SYS** in the **No Server Authentication** section.

c. Select **Unmapped user access** to select any of the following options and click **OK**:

- Allowed unmapped user access by UID/GID
- Allow anonymous access

11. Enter the description for creating a File Share in the **Description** field of the **Additional Configuration Options**.
12. Select the available Quota from the **Quota** field or click **Add new Quota Template** to create a Quota Template.
13. Click **Create**.

Deleting NFS File Shares

The NFS File Shares can be deleted using:

Deleting NFS File Shares using HPE StoreEasy management console

Deleting NFS File Shares Using HPE StoreServ management console

- In the **Edit File Share** action pane, click **Delete**.
- Select **Delete the quota on the folder** and **Are you sure?** Click **Yes, Delete** to confirm deletion.

NOTE:

If Quota is not selected to be deleted then only file share will be deleted and Quota on the folder will remain. All the clients connected to the file share will be disconnected.

IMPORTANT:

HPE recommends you to save the data before deleting the file share.

Directory Quotas

Quotas allow you to limit the space that is allowed for a volume or folder. Multiple thresholds can be defined. Quota can be configured using the available quota templates. Multiple quotas cannot be set on a single path. You can override existing quota settings, which means, if you set another quota the current one will be deleted and new quota will be set. Quotas cannot be nested.

Notifications are generated when the quota limit is reached or exceeded. The following message appears on top of the resource page in UI:

- **Warning:** Quota usage has exceeded threshold value of <threshold %>.
- **Critical:** Quota usage is at or above 100%.

Directory Quotas Overview

The **Quota** page displays the list of available quotas in the system, quota path, quota template applied, quota usage and quota type.

You can access quotas by clicking **Quotas** in the HPE StoreEasy management console left navigation menu.

You can perform the following operations in the **Quotas** page:

Icon	Function	Description
🔍	Search	Allows the user to locate the specified data. Searches for the text you enter in the **Search** box. Enter the search string in the **Search** bar to filter the individual element from the existing list of resources.
+	Add	Create quota to limit the space allowed for a volume or folder and generate notifications when the quota limits are approached or exceeded.
⏷	Filter	Filter tool is used to limit the information displayed to the specified criteria by entering the data you want to filter on. You can filter the quotas based on the following status: • ALL: This displays all the available quotas. The total number of available quotas are shown above the filter icon. • ◆ Critical: This option filters the quotas that are in critical state which needs immediate user attention. • ⚠ Warning: This indicates the abnormal state of a quota that requires interaction before further execution. In most cases warning represents the degraded, stressed, aborted, dormant, relocating, detached, and incomplete state of the quota. • ● OK: Indicates the healthy status of the quota. • ○ Unknown: This indicates the unknown state of the quota. The unknown error occurs if there is a loss of communication or if the state of the quota is unknown.

Viewing Quota State and Status

Quota status is calculated as following:

To calculate usage percentage: Usage percentage = (usage in bytes*100)/size in bytes.

Check	Status Mapping
Usage % less than lowest threshold %	● OK

Table Continued

Usage % more than lowest threshold % but less than 100%	▲ Warning
Actual % equal to or more than 100%	◆ Critical
Thresholds not set on Quota	○ Unknown

Quota Templates

Quota templates are templates that users can create. You can specify different options for creating a Quota template. When you are applying quota on a path, you can choose one of these templates.

A quota template defines a space limit, type of quota (hard or soft), set of notifications generated automatically when quota usage reaches the defined threshold levels.

NOTE:

The Quotas can be edited independent of the Quota template.

Creating Quota Templates

Quota Templates can be created by using:

Creating Quota Templates using HPE StoreEasy management console

Creating Quota Templates Using HPE StoreEasy management console

To create a Quota template, perform the following:

1. Select **Settings** > **Quota Templates** from the left navigation menu.
2. Click + icon on top right-side of the **Quota Templates** page.
3. Select either of the following Quota type of from the **Quota Type** section:
   - Limit capacity: Reusable hard Quota Template.
   - Monitor capacity: Soft Quota Template
4. Click + or - icon in the **Limit (MiB)** section to increase or decrease the quota limit for the folder or a share.
5. Select the appropriate units in the **Units** drop-down menu. The available units are MiB, GiB, TiB, PiB.
6. Click + icon in the **Thresholds** section to add threshold (warning and alert limits for the system utilization and performance).
7. Click + or - icon to set the threshold limit.

   NOTE:

   The maximum threshold is 250 percent.
8. Select any of the following options from the **Trigger Actions** section to notify the user when the maximum threshold limit is reached:

- **Send Email**: An email message will be sent to the user when the folder/Quota/Share reaches the maximum limit. You can use the email template provided in the **Send email** section.
- **Log Event**: An event is logged when the maximum threshold limit is reached.
- **Run Command**: You can provide a command script which will run when the threshold limit is reached.
- **Create Report**: Specified reports are created and saved on the system when the threshold limit is reached.

9. Enter the name for the Template in the **Name** field of the **Template** section.
10. Enter the description (optional) for the Template in the **Description** section and click **Create**
11. Choose **Send email to user** check box under the **Recipient** field of the **Send Email** section and enter the following details:
    - Additional email address
    - Subject for sending the email notification. For example, `[Quota Threshold]% capacity threshold exceeded`.
    - Message. For example: `User [Source Io Owner] has exceeded the [Quota Threshold] % quota threshold for the quota on [Quota Path] on server [Server]. The quota limit is [Quota Limit MB] MB, and [Quota Used MB] MB currently is in use ([Quota Used Percent]% of limit).`
12. Enter the name for a template in the **Name** field in the **Template** section.
13. Provide the description (optional) in the **Description** field and click **Create**.

Delete Quota Templates

The Quota Templates can be deleted using:

Delete Quota Templates using HPE StoreEasy management console

Deleting Quota Templates Using HPE StoreEasy management console

To delete a quota template, perform the following:

1. Select **Settings** > **Quota Templates** from the left navigation menu.
2. Click any of the existing quota templates that you choose to delete from the **Quota Templates** page.
3. Click edit icon (✎) on the top right-side of the page.
4. Click **Remove**.

Modifying Quota Templates

The Quota Templates can be modified using:

Modifying Quota Templates using HPE StoreEasy management console

Modifying Quota Templates Using HPE StoreEasy management console

The user can modify the existing template as per their requirements. This option allows you to modify the quota type, increase or decrease the quota limit, modify the threshold alert limits and notifications.

To edit a quota template, perform the following:

1. Select **Settings** > **Quota Templates** from the left navigation menu.
2. Click any of the existing quota templates that you choose to modify from the **Quota Templates** page and click edit icon (✎) on the top right-side of the page.
3. Select either **Limit capacity** or **Monitor capacity** quota type.

   Limit Capacity creates the hard quota and **Monitor Capacity** creates the soft quota.

4. Click + or - icon in the **Limit** section to increase or decrease the quota limit for the folder or a share.
5. Select the appropriate units in the **Unit** section drop-down menu. The available units are MiB, GiB, TiB, PiB.
6. Click + icon in the **Thresholds** field to modify the warning and alert limits that is set for the system utilization and performance and to modify the type of notifications generated when the maximum threshold is reached.

   NOTE:

   The maximum threshold is 250 percent.

7. Select any of the following options from the **Trigger Actions** section to notify the user when the maximum threshold limit is reached:

   - Send Email: An email message will be sent to the user when the folder/Quota/Share reaches the maximum limit. You can use the email template provided in the **Send email** section.
   - Log Event: An event is logged when the maximum threshold limit is reached.
   - Run Command:
   - Create Report

8. Select any of the following options in the **Template** section:

   - Do not update derived Quotas
   - Only update Quotas that match the template
   - Update all derived Quotas

9. Click **OK** to update the quota template.

Snapshots

Snapshot is a backup copy created at a particular point in time. Size limit is capacity on volume that can be used to store these backups. Snapshot is a set of pointers used to denote the data stored on a storage device like disk drive, a tape or a Storage Area Network (SAN).

Snapshots helps to easily access the stored data and speeds up the data recovery process.

Creating a Snapshot

A minimum of 300 MiB of free space is required to create a Snapshot.

Click the add (+) icon in the **Volumes** detailed view page to create a snapshot.

You can configure the snapshot size by selecting one of the following in the **Create Volume** page:

- No Limit
- Use Limit

Deleting snapshots

Deleting snapshots Using HPE StoreEasy management console

The older snapshots can be deleted without losing the data and the new snapshots can be used for restoring. Windows clears the old backups once the snapshot limit is set.

- Click edit icon in the snapshot field.
- Select **Are you sure** and click **Yes, Delete** to confirm deletion.

NOTE:

A Volume is still secure but you will not be able to restore from this snapshot.

Networking

Networking allows communication between application on different systems on a network and allows access to shared resources. The networking depends on transport protocols, like TCP/IP.

To view Networking:

1. Click **Settings** from the left navigation menu.
2. Click **Networking**.

Networking Overview

The following tasks are available in the **Networking** page:

- **Network Interfaces**
- **Network Teams**
- **Network Team Interfaces**

Network Interfaces

Network Interfaces enables you to configure the physical network interfaces. Network interface is generally a network interface card and IP addresses are assigned to the network interfaces.

View Network Interfaces

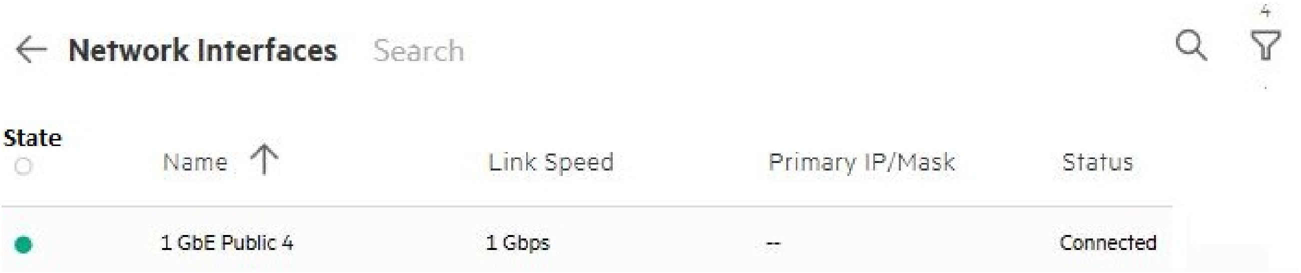
The **Network Interfaces** pages displays the list of all the available Network Interfaces of the HPE StoreEasy Storage system which can be managed by the management console of the HPE StoreEasy.

To access Network Interfaces, click **Settings** > **Networking** > **Network Interfaces** from the left navigation menu in the management console of the HPE StoreEasy.

The following user icons are available in the **Network Interfaces** page:

<table>
<tr><th>Icon</th><th>Function</th><th>Description</th></tr>
<tr><td>🔍</td><td>Search</td><td>Allows you to search the available Network Interfaces by the user-friendly name assigned by the user.</td></tr>
<tr><td>⏷</td><td>Filter</td><td>The Filter icon allows you to limit the information displayed to the specified criteria. The total number of Network Interfaces appears at the top of the filter icon. You can view the filters in a vertical filters sidebar by clicking the Filter icon on the top right-side of the <b>Network Interfaces</b> page. You can change the filter parameter to change the items that are displayed in the list. You can also select multiple filters.
You can filter the events based on their Health Status:
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>ALL</td><td>This displays all the available network interfaces. The total number of available network interfaces are shown above the filter icon.</td></tr>
<tr><td>Critical (◆)</td><td>This option filters the network interfaces that are in critical state which needs immediate user attention.</td></tr>
<tr><td>Warning (▲)</td><td>This indicates the abnormal state of an network interface that requires interaction before further execution. In most cases warning represents the degraded, stressed, aborted, dormant, relocating, detached, and incomplete state of the network interfaces.</td></tr>
<tr><td>OK (●)</td><td>Indicates the healthy status of the network interface.</td></tr>
<tr><td>Unknown (○)</td><td>This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.</td></tr>
</table></td></tr>
<tr><td>↑</td><td>Sort</td><td>Determines whether network interfaces are displayed in ascending or descending order.</td></tr>
</table>

The following image shows the key components of the **Network Interfaces** page.



State	Name	Link Speed	Primary IP/Mask	Status
●	1 GbE Public 4	1 Gbps	--	Connected

View Network Interface Details

To view the Network Interface details:

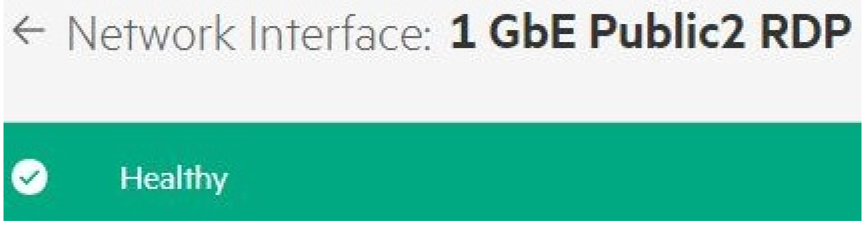
1. Click **Settings** > **Networking** > **Network Interfaces** from the left navigation menu in the management console for HPE StoreEasy.
2. Click on any of the available network interfaces to view the following details:

Property	Description
Name	Displays the name of the network interface using which the user identifies the network interface.
Interface Name	Displays the unique device name of the network interface.
Full Duplex	Represent the mode of transmission. Full duplex enabled represents that the to and fro transmissions are enabled. If the Full Duplex is disabled, only to or from transmissions are allowed at a time.
Link Speed	Displays the speed of the network interface.
Network Team	Displays the link to the associated network team. Click on this link to view more information on **Network Teams**.
IP Configuration	
Mode	Represents the Static IP routing or DHCP based routing that is used to configure a network interfaces. You can select **DHCP** (the default) so that the IP address will be assigned by a DHCP server on the network or, select **Static IP** to statically configure an address, subnet mask, and default gateway.
IPv4 Address	Specifies the address of the IPv4 used by the operating system that is being deployed.
Subnet Mask	It is a mask which determines to what subnet an IP address belongs. It is a 32-bit number which masks an IP address. The subnet mask divides the IP address into network address and host address.
Gateway	A gateway can translate the protocol of one network to a different protocol used by another network. The networks that use different types of hardware and different protocols, such as TCP/IP and OSI, can communicate with each other through a gateway.
DNS Configuration	
Mode	Static or DHCP.
Primary	Represents the default DNS server. These DNS servers has IPv4 address and apply across all port sets and subnets defined within the configuration.
Secondary	Represents the Secondary DNS server if primary DNS server is unavailable.
Tertiary	Tertiary server is used if the primary and secondary DNS servers are unavailable.

The following user icon is available in the network interface details page:

Icon	Function	Description
✎	Edit	Enables the user to change the name of the existing network interfaces.
←	Back button	Allows the user to return to the network interfaces home page.

The state of the network interface is displayed at the top of the network interface details page as shown in the following image. For details on the network interface states, see **View Network Interface State and Status**.



View Network Interface State and Status

The health status of Network Interface is mapped from any of the status or state information of each of the Network Interface. The parameters considered for status mapping are first individually mapped to one of the values of OK, Critical, Warning, Disabled or Unknown.

Once the individual mapping is completed, the overall status is arrived as per the following rules:

- If one of the values is Unknown, the overall status will be Unknown.
- If one of the values is Critical and the rest of the value is Warning, Disabled or OK, the overall status will be Critical.
- If one of the values is Warning and the rest of the value is OK or Disabled, the overall status will be Warning.
- If one of the values is Disabled and the rest of the value is OK, the overall status will be Disabled.
- If all values are OK, the overall status is OK.

The following table details the various parameters considered to view Network Interfaces state and status:

State/Status	Overall Status	Status Mapping
Health Status	Unknown (○)	**Unknown:** This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.
	OK (●)	**Present/Started:** Indicates the healthy status of the network interface.
	Disabled	**Disabled:** Indicates that the network interface is disconnected or disabled.
Operational Status	OK (●)	**OK:** Indicates the healthy status of the network interface.
		Starting: Indicates that the network interface is either starting or running.

Table Continued

		Service: Indicates that the interface is available for HPE StoreEasy management console operations. Once the request is received to start a network interface, the resource tries to bring the interface online.
		Stopping: Indicates that the interface is in the process of moving to an OK, warning, critical or unknown state. Interface being brought to an orderly stop.
	Warning (▲)	**Degraded:** Indicates that one of the tasks is failed or the element is responding to commands, but is not running in an optimal operating state.
		Stressed: The element is functioning, but needs attention.
	Critical (◆)	**Predictive Failure:** Element is functioning nominally but predicting a failure shortly.
		Error: Indicates that the task is in an unhealthy state that prevents further execution.
		Non recoverable error: Element is in non-recoverable error.
	Unknown (○)	**Lost Communication:** Element is known to exist and has been contacted successfully in the past, but is unreachable.
		Unknown: This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.
		No Contact: The monitoring system has knowledge of this element, but has never been able to establish communications with it.
Connection Status	Unknown (○)	**Unknown:** This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.
	OK (●)	**Connected:** Indicates that the network interface is connected.
	Disabled	**Disconnected:** Indicates that the network interface is disconnected.

Editing a Network Interface

The **Edit Network Interface** page allows you to change the name and the IP settings of the existing Network Interface.

To edit the Network Interface, perform the following

1. Click **Settings** > **Networking** > **Network Interfaces** from the left navigation menu in the management console of the HPE StoreEasy.
2. Click on the available network interfaces that you choose to modify.
3. Click edit (✎) icon on top right-side of the **Network Interface** page.

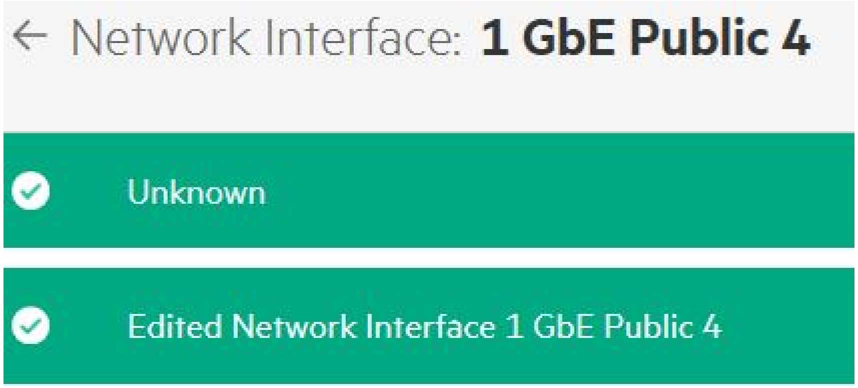
4. Enter the user-friendly name for the Network Interface in the **Name** field in the **Edit Network Interfaces** page.

5. Click edit (✎) in the **IP Settings** section and choose any of the following modes:

   - **Use DHCP**
   - **Manually assign IP and DNS address**

6. Click **OK** and click **Apply** to save the changes.

   The state of the edit task performed will appear on the top of the **Network Interface** page as shown in the following image.



← Network Interface: **1 GbE Public 4**

✓ Unknown

✓ Edited Network Interface 1 GbE Public 4

Network Teams

Network teaming is used to increase available bandwidth, load balancing, and improve fault tolerance. The maximum number of teams that you can create is equal to the number of physical network interfaces on the system.

Viewing Network Teams

The **Network Teams** page displays the list of available network teams in the system, their mode of teaming, load balancing, and number of available team members.

You can access the Network Team by clicking **Settings** > **Networking** > **Network Teams** from the left navigation menu in the management console of the HPE StoreEasy.

The following user icons are available in the **Network Teams** page:

Icon	Function	Description
🔍	Search	Allows the user to search specific Network Team by their name.
+	Add	Click on this icon to create a new Network Team where you can specify the mode of teaming, load balancing and you can add team members.

Table Continued

<table>
<tr><th>Icon</th><th>Function</th><th>Description</th></tr>
<tr><td>⛛</td><td>Filter</td><td>The Filter icon allows you to limit the information displayed to the specified criteria. The total number of Network Teams appears at the top of the filter icon. You can view the filters in a vertical filters sidebar by clicking the Filter icon on the top right-side of the <b>Network Teams</b> page. You can change the filter parameter to change the items that are displayed in the list. You can also select multiple filters.
You can filter the events based on their Health Status:
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>ALL</td><td>This displays all the available Network Teams. The total number of available Network Teams are shown above the filter icon.</td></tr>
<tr><td>Critical (◆)</td><td>This option filters the Network Teams that are in critical state which needs immediate user attention.</td></tr>
<tr><td>Warning (▲)</td><td>This indicates the abnormal state of a Network Team that requires interaction before further execution. In most cases warning represents the degraded, stressed, aborted, dormant, relocating, detached, and incomplete state of the Network Teams.</td></tr>
<tr><td>OK (●)</td><td>Indicates the healthy status of the Network Teams.</td></tr>
<tr><td>Unknown (○)</td><td>This indicates the unknown state of the Network Team. The unknown error occurs if there is a loss of communication or if the state of the Network Teams is unknown.</td></tr>
</table></td></tr>
<tr><td>↑</td><td>Sort</td><td>Determines whether Network Teams are displayed in ascending or descending order.</td></tr>
</table>

Viewing Network Team Details

The network teams details pages provides the detailed information about the available network teams in the system, their mode of teaming, load balancing, and number of team members in each of the network teams.

To view the network team details, click **Settings** > **Networking** > **Network Teams** from the left navigation menu in the management console for HPE StoreEasy, and then click on any of the available network teams to view the following details:

Property	Description
General	
Name	Name of the network team using which the user identifies the network team.

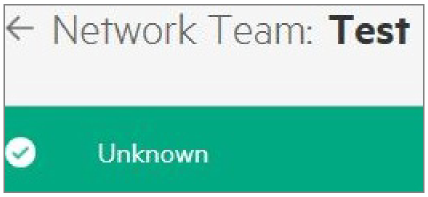
Table Continued

Property	Description
Teaming Mode	The following are the modes of network teaming: • Switch Independent: In this mode, the switches are not aware that different interfaces on the server comprise a team. All the teaming is done exclusively on the server. • LACP: Link Aggregation Control Protocol (LACP) dynamically identify links that are connected between the host and a given switch which enables the creation of the Network Team. • Static: This is a Switch Dependent mode which requires the switch to participate in teaming.
Load Balancing	Load balancing allows you to manage two or more servers as single cluster. This action distributes traffic across several servers by using the TCP\IP networking protocol. The following are the Load Balancing options available: • Transport Ports • IP Addresses • MAC Addresses • Hyper-V Port • Dynamic
Team Members	
Name	Name of the network team member using which the user identifies the network team member.
State	State of the network team member.
Link Speed	The speed of the interface.
Administrative Mode	The active network traffic uses the network interface, if the administrative mode is active. If the administrative is Standby, the network interface will be used if there is any interface failure.
Network Team Interfaces	
Name	Name of the network team.
State	State of the network team.
Link Speed	The speed of the interface.

The following operational and informational icons are available in the **Network Teams** page:

Icon	Function	Description
✎	Edit	Allows the user to change the teaming mode, load balancing and the team members.
←	Back button	Allows the user to go to the network teams home page.

The network teams details page also displays the state of the network team running from unknown, present, started to disabled as shown in the following image.



← Network Team: **Test**

✓ Unknown

View Network Interface State and Status

The health status of Network Interface is mapped from any of the status or state information of each of the Network Interface. The parameters considered for status mapping are first individually mapped to one of the values of OK, Critical, Warning, Disabled or Unknown.

Once the individual mapping is completed, the overall status is arrived as per the following rules:

- If one of the values is Unknown, the overall status will be Unknown.
- If one of the values is Critical and the rest of the value is Warning, Disabled or OK, the overall status will be Critical.
- If one of the values is Warning and the rest of the value is OK or Disabled, the overall status will be Warning.
- If one of the values is Disabled and the rest of the value is OK, the overall status will be Disabled.
- If all values are OK, the overall status is OK.

The following table details the various parameters considered to view Network Interfaces state and status:

State/Status	Overall Status	Status Mapping
Health Status	Unknown (○)	**Unknown:** This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.
	OK (●)	**Present/Started:** Indicates the healthy status of the network interface.
	Disabled	**Disabled:** Indicates that the network interface is disconnected or disabled.
Operational Status	OK (●)	**OK:** Indicates the healthy status of the network interface.
		Starting: Indicates that the network interface is either starting or running.
		Service: Indicates that the interface is available for HPE StoreEasy management console operations. Once the request is received to start a network interface, the resource tries to bring the interface online.
		Stopping: Indicates that the interface is in the process of moving to an OK, warning, critical or unknown state. Interface being brought to an orderly stop.

Table Continued

	Warning (▲)	**Degraded:** Indicates that one of the tasks is failed or the element is responding to commands, but is not running in an optimal operating state.
		Stressed: The element is functioning, but needs attention.
	Critical (◆)	**Predictive Failure:** Element is functioning nominally but predicting a failure shortly.
		Error: Indicates that the task is in an unhealthy state that prevents further execution.
		Non recoverable error: Element is in non-recoverable error.
	Unknown (○)	**Lost Communication:** Element is known to exist and has been contacted successfully in the past, but is unreachable.
		Unknown: This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.
		No Contact: The monitoring system has knowledge of this element, but has never been able to establish communications with it.
Connection Status	Unknown (○)	**Unknown:** This indicates the unknown state of the network interface. The unknown error occurs if there is a loss of communication or if the state of the network interface is unknown.
	OK (●)	**Connected:** Indicates that the network interface is connected.
	Disabled	**Disconnected:** Indicates that the network interface is disconnected.

Creating a Network Team

HPE StoreEasy management console allows you to create a network team.

NOTE:

Default Network Team interface is created along with the network team.

To create a network team, perform the following:

1. Click **Settings** from the left navigation menu.
2. Click **Networking** > **Networking Teams**
3. Click + add icon in the **Network Teams** page.
4. Enter the name for the network team.
5. Select any of the following teaming mode from the **Teaming Mode** drop-down menu:

    - Switch Independent: In this mode, the switches are not aware that different interfaces on the server comprise a team. All the teaming is done exclusively on the server.
    - LACP: Link Aggregation Control Protocol (LACP) mode is also commonly referred to as IEEE 802.3ad as it was developed in the IEEE 802.3ad committee before being published as IEEE 802.1ax. IEEE

802.1ax works by using the Link Aggregation Control Protocol (LACP) to dynamically identify links that are connected between the host and a given switch. This enables the automatic creation of a team and, in theory but rarely in practice, the expansion and reduction of a team simply by the transmission or receipt of LACP packets from the peer entity. Typical server-class switches support IEEE 802.1ax but most require the network operator to administratively enable LACP on the port.

- Static: This is a Switch Dependent mode which requires the switch to participate in teaming. This mode requires configuration on both the switch and the host to identify which links form the team. Since this is a statically configured solution there is no additional protocol to assist the switch and the host to identify incorrectly plugged cables or other errors that could cause the team to fail to perform. This mode is typically supported by server-class switches.

6. Click + add icon in the **Team Members** section to add one or more network interface to form a network team either for load balancing or failover.

7. Click 🔍 search icon to select the required network interface.

   Upon selecting the network interface, the name, speed and status of the network interface will be displayed.

8. Click **OK** to go to **Create Network Team** page.
9. Click **Create** to save the changes.

To delete a team member:

1. Click ✏ edit icon in the **Team Members** section.
2. Click **Remove**.

Editing a Network Team

Network interfaces that are part of the network team can be changed.

NOTE:

Editing Network Team configurations might lead to temporary disconnection.

- Click edit icon in the **Network Team** properties window.
- Select the teaming mode from **Teaming Mode** drop-down menu.
- Select the load balancing from **Load Balancing** drop-down menu.
- Click edit icon and click **Remove** to remove the team members.

Deleting a Network Team

To delete a network team:

1. Click **Settings** from the left navigation menu.
2. Click **Networking** > **Networking Teams**.
3. Click on any of the available Network Team and click edit icon in the **Network Team** properties page.

- Click **Delete** in the **Edit Network Team** window.
- Choose **Are you sure?** and click **Yes, Delete** to confirm deletion.

Network Team Interfaces

Network team interface enables you to configure the physical network interfaces to suit your environment.

View Network Team Interface

The **Network Team Interfaces** page displays the list of available network team interfaces in the system, the associated network team name, VLAN ID, Primary IP address and their connection status.

You can access Network Team Interfaces by clicking **Settings** > **Networking** > **Network Team Interfaces** from the left navigation menu in the management console of the HPE StoreEasy.

The following user icons are available in the **Network Team Interfaces** page:

Icon	Function	Description
🔍	Search	Allows the user to search specific Network Team Interfaces by their name that is assigned by the user with the specific user permissions.
+	Add	Click on this icon to create a new Network Team Interfaces where you can specify the mode of teaming, load balancing and you can add team members.

<table>
<tr><th>Icon</th><th>Function</th><th>Description</th></tr>
<tr><td>⏷</td><td>Filter</td><td>The Filter icon allows you to limit the information displayed to the specified criteria. The total number of Network Team Interfaces appears at the top of the filter icon. You can view the filters in a vertical filters sidebar by clicking the Filter icon on the top right-side of the <b>Network Team Interfaces</b> page. You can change the filter parameter to change the items that are displayed in the list. You can also select multiple filters.
You can filter the events based on their Health Status:
<table>
<tr><th>Status</th><th>Description</th></tr>
<tr><td>ALL</td><td>This displays all the available Network Team Interfaces. The total number of available Network Teams are shown above the filter icon.</td></tr>
<tr><td>Critical (◆)</td><td>This option filters the Network Team Interfaces that are in critical state which needs immediate user attention.</td></tr>
<tr><td>Warning (▲)</td><td>This indicates the abnormal state of an Network Team Interface that requires interaction before further execution. In most cases warning represents the degraded, stressed, aborted, dormant, relocating, detached, and incomplete state of the Network Team Interface.</td></tr>
<tr><td>OK (●)</td><td>Indicates the healthy status of the Network Team Interface.</td></tr>
<tr><td>Unknown (○)</td><td>This indicates the unknown state of the Network Team Interface. The unknown error occurs if there is a loss of communication or if the state of the Network Team Interface is unknown.</td></tr>
</table></td></tr>
<tr><td>↑</td><td>Sort</td><td>Determines whether Network Teams are displayed in ascending or descending order.</td></tr>
</table>

View Network Team Interface Details

To view the Network Team Interface details:

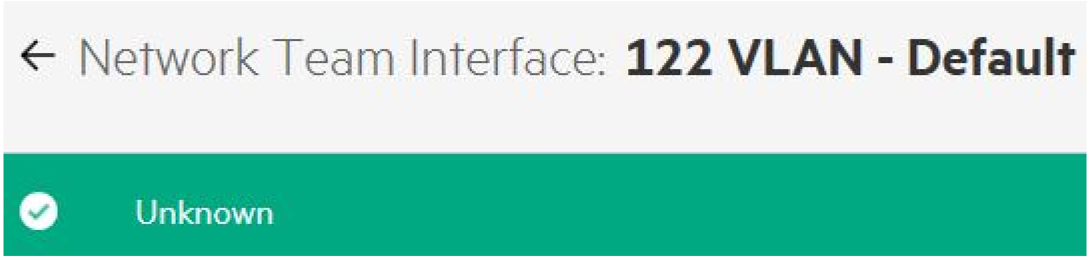
1. **Settings** > **Networking** > **Network Team Interfaces** from the left navigation menu in the management console of the HPE StoreEasy.
2. Click on any of the available network team interfaces to view the following details:

Property	Description
General	
Name	Displays the name of the network team interface using which the user identifies the Network Team Interfaces.
VLAN ID	Displays the Virtual LAN ID number which is the combination of one or more physical network interface or adapter. 0 VLAN ID is the default VLAN. Primary VLAN is determined by Windows which cannot be deleted. The primary VLAN ID cannot be modified any VLAN ID other than 0.
Primary	Displays the Primary IP Address of the network team interface.
Network Team	Displays the link to the network Team associated. Click on this link to view more details about the network team.
IP Configuration	
Mode	Represents the Static IP routing or DHCP based routing that is used to configure a Network Team Interfaces. You can select **DHCP** (the default) so that the IP address will be assigned by a DHCP server on the network or, select **Static IP** to statically configure an address, subnet mask, and default gateway.
IPv4 Address	Specifies the address of the IPv4 used by the operating system that is being deployed.
Subnet Mask	It is a mask which determines to what subnet an IP address belongs. It is a 32-bit number which masks an IP address. The subnet mask divides the IP address into network address and host address.
Gateway	A gateway can translate the protocol of one network to a different protocol used by another network. The networks that use different types of hardware and different protocols, such as TCP/IP and OSI, can communicate with each other through a gateway.
DNS Configuration	
Mode	Static or DHCP.
Primary	Represents the default DNS server. These DNS servers has IPv4 address and apply across all port sets and subnets defined within the configuration.
Secondary	Represents the Secondary DNS server if primary DNS server is unavailable.
Tertiary	Tertiary server is used if the primary and secondary DNS servers are unavailable.

The following user icons are available in the **Network Team Interface** page.

Icon	Function	Description
✎	Edit	Allows the user to modify the existing network interfaces where you change the VLAN ID and the IP Settings.
←	Back button	Allows the user to go to the network team interfaces home page.

The Network Team Interface details page displays the state of the network team interface running from unknown, present, started to disabled as shown in the following image.



← Network Team Interface: **122 VLAN - Default**

✓ Unknown

Viewing Network Team Interface State and Status

The health status of Network Team Interface is mapped from any of the status or state information of each of the Network Team Interface. The parameters considered for status mapping are first individually mapped to one of the values of OK, Critical, Warning, Disabled or Unknown.

Once the individual mapping is completed, the overall status is arrived as per the following rules:

- If one of the values is Unknown, the overall status will be Unknown.
- If one of the values is Critical and the rest of the value is Warning, Disabled or OK, the overall status will be Critical.
- If one of the values is Warning and the rest of the value is OK or Disabled, the overall status will be Warning.
- If one of the values is Disabled and the rest of the value is OK, the overall status will be Disabled.
- If all values are OK, the overall status is OK.

The following table details the various parameters considered to view Network Team Interface interfaces state and status:

State	Overall Status	Status Mapping
Health	OK (●)	**Unknown:** This indicates the unknown state of the Network Team Interface . The unknown error occurs if there is a loss of communication or if the state of the Network Team Interface is unknown.
	Warning (▲)	**Present/Started:** Indicates the healthy status of the Network Team Interface.
	Critical (◆)	**Disabled:** Indicates that the Network Team Interface is disconnected or disabled.
Operational	OK (●)	**OK:** Indicates the healthy status of the Network Team Interface.
		Starting: Indicates that the Network Team Interface is either starting or running.

Table Continued

		Service: Indicates that the resource is available to use. Once the request is received to start a Network Team Interface, the resource makes an attempt to bring the interface online.
		Stopping: Indicates that the interface is in the process of moving to a OK, warning, critical or unknown state. Interface being brought to an orderly stop.
	Warning (▲)	**Degraded:** Indicates that one of the task is failed or the element is responding to commands, but is not running in an optimal operating state.
		Stressed: The element is functioning, but needs attention.
	Critical (◆)	**Predictive Failure:** Element is functioning nominally but predicting a failure in the near future.
		Error: Indicates that the task is in an unhealthy state that prevents further execution.
		Non recoverable error: Element is in non-recoverable error.
	Unknown (○)	**Lost Communication:** Element is known to exist and has been contacted successfully in the past, but is currently unreachable.
		Unknown: This indicates the unknown state of the Network Team Interface. The unknown error occurs if there is a loss of communication or if the state of the Network Team Interface is unknown.
		No Contact: The monitoring system has knowledge of this element, but has never been able to establish communications with it.
Connection	Unknown (○)	**Unknown:** This indicates the unknown state of the Network Team Interface. The unknown error occurs if there is a loss of communication or if the state of the Network Team Interface is unknown.

Table Continued

	OK (●)	**Connected:** Indicates that the Network Team Interface is connected.
	Disabled	**Disconnected:** Indicates that the Network Team Interface is disconnected.

Creating a Network Team Interface

1. Click **Settings** > **Networking** > **Network Team Interfaces** from the left navigation menu in the management console of the HPE StoreEasy.
2. Click add (+) icon on the top right-side of the **Network Team Interfaces** page.
3. Select the network team from the **Network Team** drop-down menu in the **Create Network Team Interface** page.

   You can also create a new network team by clicking **Create new Network Team** from the drop-down menu. For creating a new network team, see **Creating a new network team**.
4. Click + or - icon in the **VLAN ID** section to specify the VLAN ID number.
5. Click edit (✎) icon in the **IP Settings** field to configure the IP and click on any of the following modes:
   - **Use DHCP**
   - **Manually assign IP and DNS addresses**
6. Click **OK** and click **Create** in the **Create Network Team Interface** page.

Editing a Network Team Interface

NOTE:

The primary Network Team Interface cannot be deleted, you can only configure the Network Team Interface using the default VLAN ID.

1. Click **Settings** > **Networking** > **Network Team Interfaces** from the left navigation menu in the management console of the HPE StoreEasy.
2. Click on the Network Team Interfaces that you choose to modify.
3. Click edit icon (✎) in the **Network Team Interface** page.
4. Click + or - icon in the **VLAN ID** section to set the VLAN ID.
5. Click edit icon (✎) in the **IP Settings** section to configure the IP and click on any of the following modes:
   - **Use DHCP**
   - **Manually assign IP and DNS addresses**
6. Click **OK**.
7. Click **Apply** in the **Edit Network Team Interface** page to save the changes.

The status of this task is displayed on top of the Network Team Interface details page.

Deleting a Network Team Interface

1. Select **Settings** from the left navigation menu.
2. Click **Networking** > **Network Team Interfaces**.
3. Click on any of the available network team interfaces that you choose to modify.
4. Click edit icon in the **Network Team Interface** page.
5. Click **Delete** in the **Edit Network Team Interface** page.
6. Select **Are you sure** and click **Yes, Delete** to confirm deletion.

NOTE:

Once the network team interface is deleted, network connectivity on the network team interface will be lost.

Troubleshooting, servicing, and maintenance

Certificate of Authenticity

For technical support purposes, record the Certificate of Authenticity (COA) product key and make a print copy of the End User License Agreement (EULA) as needed.

The COA label is used to:

- Replace the main board/motherboard.
- Upgrade the factory-installed operating system using the Microsoft Upgrade program for license validation.
- Reinstall the operating system because of a failure that has permanently disabled it.

NOTE:

Maintain the COA or a copy of the COA license information. During system board replacement, the COA is necessary to re-establish the license of the operating system.

Adding storage

Storage growth may occur in three forms:

- Extend unallocated space from the original logical disks or LUNs.
- Alter LUNs to include additional storage.
- Add new LUNs to the system.

Expanding storage: Expansion is the process of adding physical disks to an array which is already configured. The logical drives (or volumes) in the array before the expansions are unchanged. Only the amount of free space in the array changes. The expansion process is entirely independent of the Operating System.

For more information on expanding storage on the array, see *Storage Array Hardware User Documentation*.

Extending storage: The storage extension can be performed using:

- Windows Storage Utilities
- Disk Management

Windows Storage Utilities: Volume extension grows the storage space of a logical drive. During this process, the administrator adds new storage space to an existing logical drive on the same array, usually after the array has been expanded. This new storage space is either by expansion or by deleting another logical drive on the same array. Unlike drive expansion, the operating system must be aware of the changes to the logical drive size.

Following are the reasons for storage extension:

- Increase raw data storage.
- Improve performance by increasing the number of spindles in a logical drive volume.
- To change fault-tolerance (RAID) configurations.

For more information about RAID levels, see **Smart Array Controller User Guide**.

Disk Management

The Disk Management snap-in provides management of hard disks, volumes, or partitions. It can be used to extend a dynamic volume only.

NOTE:

Disk Management cannot be used to extend basic disk partitions.

Following are the guidelines for extending a dynamic volume:

- Use the Disk Management utility.
- Extend a volume only if it does not have a file system or if it is formatted NTFS.
- You cannot extend volumes formatted using FAT or FAT32.
- You cannot extend striped volumes, mirrored volumes, or RAID 5 volumes.

For more information on Disk Management, see *Disk Management Online Help*.

System Recovery

Recovering HPE StoreEasy 1X60 Storage

The HPE StoreEasy 1X60 Storage is recovered using System Recovery DVD (if ordered). If you have not ordered the System Recovery DVD, download the free System Recovery image from HPE Software Depot. Save the downloaded image file in a USB flash drive or DVD to perform system recovery. For information on creating a system recovery USB flash drive or DVD, see *Creating a USB flash drive with an image file* and *Creating a DVD with an image file* from HPE Software Depot.

NOTE:

Disconnect any external storage prior to booting the server to recover the image. Otherwise, the system might hang as it is trying to enumerate the volumes in the external storage.

System Recovery DVD

The System Recovery DVD can be ordered optionally with HPE StoreEasy 1X60 Storage system.

Using the System Recovery DVD, you can install an image or recover from a catastrophic failure.

At any time, you may boot from the DVD and restore the server to the factory condition. This enables you to recover the system if all other means to boot the server fail.

While the recovery process makes every attempt to preserve the existing data volumes, you must have a backup of your data before recovering the system.

IMPORTANT:

All data on the original OS logical drive is erased during the recovery process.

During system recovery, you can replace the existing drives with drives of the same size or larger, but have to be the same type of drive. HPE recommends that the replacement drives be the same size and type as the original drives.

If you replace any disk drives and then perform a system recovery, you must ensure that the replacement drives do not contain a logical drive partition. Reboot the server and select <F10> for intelligent provisioning and then select the Smart Storage Administrator to review the current provisioning on the drives. Remove any old logical partitions from the replacement drives for the operating system. See the online help in the Smart Storage Administrator on how to remove array logical partitions.

⚠ **WARNING:**

If restoring to a system that shares data and OS partition on the same drives then do not remove any partitions since this would put your data at risk of loss or corruption.

Using the System Recovery DVD to save system data

Boot the System Recovery DVD and when prompted, select Windows Recovery Environment. Perform the following steps:

1. Select the keyboard layout.
2. Select **Troubleshoot** > **Advanced Options** > **Command Prompt**.
3. Enter **WPEINIT** and wait for approximately ten seconds before proceeding.
4. Enter **IPCONFIG** at the command prompt to confirm that the network interface has an IP address.

   NOTE:

   - If your network is not using DHCP, manually assign the IP address and DNS information. The following are some examples of the commands for manually assigning an IP address:

     - netsh interface ip set address "connection name" static 192.168.0.101 255.255.255.0 192.168.0.1
     - netsh interface ip add dns "connection name" 208.67.222.222
     - netsh interface ip add dns "connection name" 208.67.220.220 index=2

     For more information on using the netsh command, go to https://technet.microsoft.com/enus/library/bb490943.aspx.

   - Starting the network might take some time. Continue to the next step only after a valid IP address is assigned to the network interface.

5. Enter NET USE Z: \\servername\sharename at the command prompt, where \\servername\sharename is the UNC path to a network share where the data will be copied.
6. If prompted, enter the username and password for the share that you are accessing.

When the share is mapped to *Z: drive*, use Robocopy to copy files from the system to the network share. For more information, see **Robocopy**.

Drive letters are not assigned after a restore to Data Volumes

When a system that has existing data volumes (non-operating system volumes) is restored using the System Recovery DVD, the data volumes will not have drive letters assigned to them. This is by design. The volume labels are retained and can be used to identify the data volumes.

You can assign drive letters to volumes using diskpart.exe or Disk Management. Follow the steps for using disk management:

1. Click **Start** > **Windows PowerShell**.
2. Enter **diskmgmt.msc** and press **Enter**.
3. Right-click the **disk and partition** the one for which you want to assign a drive letter and select **Change Drive Letter and Paths**.

Creating a system recovery USB flash drive using the System Recovery DVD

If you create a backup copy of the System Recovery DVD using a USB flash drive, it is also possible to restore the system.

To create a system recovery USB flash drive using the System Recovery DVD:

1. Obtain a blank 8 GB or larger USB flash drive.
2. Insert the USB flash device into your workstation or laptop.
3. Open an elevated command prompt with Administrator privileges.
4. Enter **diskpart** in command prompt window.
5. Enter **list disk**, at the diskpart prompt.
6. Identify the disk number that corresponds to the flash drive. This is typically the last disk listed.
7. Enter **sel disk <USB drive number>**. For example, sel disk 4.
8. Enter **clean**. The clean command delete everything from the USB flash device. Ensure that you have the proper disk selected.
9. Enter **create par primary**.
10. Enter **sel par 1**.
11. Enter `format fs=fat32 quick`.
12. Enter **active**, to mark partition as active.
13. Enter **assign letter=<drive letter>** to assign a drive letter to the USB drive. For example, assign letter=U.
14. Enter **exit**.
15. Insert the System Recovery DVD into the computer.
16. Using Windows Explorer or a comparable utility, open the DVD to view all the contents, including hidden and system files.
17. Select all files (including `bootmgr`) on the DVD.
18. Copy all of the selected files to the root of the USB flash drive.

Creating a USB flash drive with an image file from HPE Software Depot

Follow the procedure to create a system recovery USB flash drive with an image file from HPE Software Depot:

1. After downloading the image file, mount the ISO locally to access the files. Insert a USB flash drive into the system.
2. Open an elevated command prompt with Administrator privileges.

3. Type **diskpart**, and then press **Enter**.
4. Type **list disk** to determine the USB flash drive number or drive letter, and press **Enter**.
5. Note the drive number or drive letter of the USB flash drive.
6. Type **select disk <x>**, where <x> is the drive number or drive letter of the USB flash drive, and press **Enter**.
7. Type **clean** to delete the data from the USB flash drive, and press **Enter**.
8. Type **create part pri** to create a new primary partition in the USB flash drive, and press **Enter**.
9. Type **select part 1** to select the partition that you just created , and press **Enter**.
10. To format the partition as FAT32, type format fs=fat32 quick, and press **Enter**.

    IMPORTANT:

    Since the server platforms are configured with Unified Extensible Firmware Interface (UEFI), you must format the USB flash drive as FAT32 instead of NTFS. To format the partition as FAT32, type: format fs=fat32 quick and press **Enter**.

11. Type **active** to mark the partition as active and press **Enter**.
12. Type **Exit** to quit diskpart context commands and press **Enter**.
13. Copy the installation files included in the disc image file (ISO) to the root of the USB flash drive.

Creating a DVD with an image file from HPE Software Depot

Follow the steps to create a system recovery DVD with an image file from HPE Software Depot:

1. Insert a blank **dual layer** DVD in the drive.
2. Locate the ISO image file on your system and then double-click it.
3. The Windows Disk Image Burner window appears.
4. Select the disk burner that you want to use. This is applicable only if you have more than one disk burners.
5. Select **Verify disc** after burning to verify that the ISO image has burned correctly. It is recommended to verify the disc to ensure that the ISO burns correctly to the DVD.
6. Click **Burn**.
7. On completion, the appropriate status is displayed on the screen.

Restoring the factory image with a DVD or USB flash device

Prerequisite: Disconnect any external storage from the system prior to restoring the HPE StoreEasy system.

1. For direct access, insert the System Recovery DVD or a bootable USB flash device (prepared with a System Recovery image).
2. For remote management access, connect to the server using iLO from a client PC. Insert the System Recovery DVD in the client PC or attach a bootable USB flash device that is prepared with a System Recovery image.
3. Reboot the server and select F11 during the boot. Manually select the device which has the recovery media.
4. Click **HPE StoreEasy System Recovery**.

ⓘ **IMPORTANT:**

Do not interrupt the recovery process.

5. Remove the directly connected DVD or flash device (or remotely connected iLO virtual DVD or flash device) from the server. Ensure to reconnect any external storage that was detached and reboot the server before proceeding.

Backing up and restoring HPE StoreEasy 1X60 Storage with Windows Recovery Environment

To use Windows Recovery Environment, you must have created a system backup with the Windows Server Backup utility. You can either perform a single back up or schedule a regular back up.

Perform the following steps to create a one-time system backup using Server Manager:

1. Open **Server Manager**.
2. Select **Tools** > **Windows Server Backup**.
3. In the Local Backup window, create one-time backup of the data by performing one of the following steps:

    a. Select **Action** > **Backup Once**.

    b. In the left pane, right-click on Local Backup.

    c. Select **Backup Once**.

4. The Backup Once Wizard is launched.
5. During one-time backup, the **different options** option is selected by default. The Schedule backup options is unavailable. Click **Next** to continue.
6. Select Full Server (recommended) to backup all server data, applications, and system state and click **Next** to continue.
7. Select **Remote Shared Folder** as the destination type and click Next to continue.
8. Enter the path to the remote folder in Location and select the desired option in the Access control group. Click **Next** to continue.
9. Review the items selected for the backup and click **Backup**.
10. A backup of the items is created and saved at the specified destination. The backup activity is also displayed on the Local Backup window.

Perform the following steps to restore the system with Windows Recovery Environment:

1. For direct access, connect the cable and insert the System Recovery DVD in the HPE StoreEasy system or attach a bootable USB flash drive that is prepared with a System Recovery image.
2. For remote management access, connect to the server using iLO from the client PC. Insert the System Recovery DVD in the HPE StoreEasy system or attach a bootable USB flash device that is prepared with a System Recovery image.
3. Reboot the server to either the USB flash device or USB DVD drive.
4. Reboot the server and select **<F11>** during the boot and manually select the device which has the recovery media is mounted.

5. During the booting the USB or DVD you need to watch for the prompt to select any key to boot to finish booting to the DVD.
6. Select **Windows Recovery Environment**.
7. The recovery environment is loaded and the System Recovery Options wizard opens.
8. Select the language and keyboard layout.
9. Select Troubleshoot to access the repair tools that allow you to recover or troubleshoot Windows.
10. Select **Advanced** options to access the advanced repair options.
11. Select System Image Recovery to restore the system using a previously created system recovery image.
12. Select the target operating system to be restored.
13. The Re-image your computer wizard is launched, which scans the computer for a system image. If it is unable to locate a system image, the following message is displayed:
14. Attach an external drive or insert a DVD that contains the backup files and click Retry. If you want to recover from the network, click Cancel.
15. Select one of the following options and click Next:

    - Use the latest available image, Select to use the backup image that was recently created. If you are restoring from the network, this option is unavailable.
    - Select a system image, Select to restore from the network.

16. If you are restoring from the network, click Advanced, and then select Search for a system image on the network.
17. Click **Yes** on the confirmation message to proceed with the network connectivity.
18. Enter the share path where the backup image is stored and click **OK**.
19. Enter the network login credentials for authentication and click **OK**.
20. Select the system image from the list and click **Next**.
21. Select the date and time of the system image that you want to restore and click **Next**.
22. Select Format and repartition disks to delete existing partitions and reformat all disks during the restore process and click Next. If you do not want to restore certain disks, click Exclude Disks.

    NOTE:

    If the Format and repartition disks option is unavailable, click Install Drivers to install the drivers for the disks that you want to restore.

23. Verify the system image details and click Finish to start the recovery process.
24. Click **Yes** on the confirmation message to proceed with Windows recovery.

    IMPORTANT:

    Do not interrupt the recovery process.

    When the system recovery completes, the system reboot. If you had external storage that was detached as recommended than reattach the storage and reboot the server.

Proceed with reconfiguring the server, following the steps in this administrator guide for configuring the system.

Troubleshooting

The HPE StoreEasy 1X60 Storage provides several monitoring and troubleshooting options. You can access the following troubleshooting alerts and solutions to maintain the system health:

- Notification alerts
- Customer advisories
- HPE Active Health system viewer (**http://www.hpe.com/support/ahsv-ug-en**)
- Hardware component LEDs
- HPE and Microsoft support websites
- HPE Insight Remote Support software
- Microsoft Systems Center Operations Manager (SCOM)
- HPE SIM 7.6 or later, which is required for proper HPE StoreEasy 1X60 Storage or HPE SIM integration
- HPE StoreEasy management console health information

NOTE:

For the latest version of HPE SIM, see **HPE SPOCK**.

Generic Windows event based troubleshooting

Event Viewer can be used for event analysis. When Event Viewer is opened, the left-hand pane displays a folder view, where you can find all of the different event logs, as well as the views that can be customized with events from many logs at once. For instance, the Administrative Events view in recent versions of Windows displays all of the Error, Warning, and Critical events whether they originated from the Application log or the System log. The middle pane displays a list of events, and clicking on it will display the details of the event in the preview pane - or you can double-click on any of them to pull it up in a separate window, which can be handy when you are looking through a big set of events and want to find all the important things before beginning an internet search. The right-hand pane gives you quick access to actions like creating custom views, filtering, or even creating a scheduled task based on a particular event.

Maintaining HPE StoreEasy 1X60 Storage

HPE recommends the following maintenance guidelines for upgrading your system components (operating system, software, firmware, and drivers), depending on your environment:

IMPORTANT:

- It is recommended that HPE StoreEasy Service Releases be installed as released. These service releases contain important Windows Updates and Hot Fixes.
- It is recommended by Microsoft that you allow the Microsoft Windows updating service to update your system automatically to ensure that you have the latest security and malware prevention updates installed.

Determining the current HPE StoreEasy 1X60 Storage image version

You can find the current version using the registry or through the StoreEasy management console.

Here are the instructions for extracting the information through the registry.

- Log in to the server blade.
- Open an administrative command window.
- Enter the reg query command as shown in the following example, `C:\> reg query HKLM\Software \Wow6432Node\Hewlett-Packard Enterprise\StorageWorks /s`

  The following information appears:

  ```
  HKEY_LOCAL_MACHINE\Software\Wow6432Node\Hewlett-Packard Enterprise\StorageWorks\QuickRestore
  BASE REG_SZ 5.00.0.x
  QRVersion REG_SZ 5.0x.0x.xxx
  ```

The QRVersion field lists the version.

Applying service releases using the Update tool

The Update Tool is used to install hotfixes and updated HPE components on the HPE Storage system. The utility "Update Tool" is designed to provide an integrated, enhanced and seamless end user experience exploiting the cluster aware update (CAU) feature. It presents a uniform graphical user interface to upgrade standalone and cluster nodes from local and remote processors. In addition to that, this interface allows performing the complete operations with minimal number of clicks while keeping a provision for advanced parameter selection exploiting the underlying framework.

Installing updates using the Update Tool procedure:

1. Double-click **Update Tool**.
2. Select any mode from the list (Standalone, Co-ordinate, or Cluster mode). If you select:
   - Standalone mode, the system navigates to the Update Tool Summary page.
   - Cluster mode or Co-ordinator mode, the system navigates to the Update Tool Input page.
3. Click **Next**.
4. On the **Update Tool Input** page, enter the required settings and click **Next**. The Update Tool Summary page appears.
5. Click **Install**. The installation starts and the tool navigates to the **Update Tool Result** page, which provides the status of the installation.

   NOTE:

   For Standalone mode, you cannot cancel the installation once the installation begins.
6. Click **Open Log** to view the log files that the system generates during the update installation.

   NOTE:

   For a cluster system, you must select individual nodes and then click **Open Log** to view the logs for that particular node.
7. The update will complete installation after you reboot the system.
8. Click **Ok**.

NOTE:

If the components in the SR package doesn't requires reboot, the application closes.

Hewlett Packard Enterprise Support websites

To troubleshoot problems with HPE StoreEasy 1X60 Storage, select HPE Server, Storage and Networking at the **HPE Support & Drivers**. Search for *HPE StoreEasy 1X60 Storage* or use the product ID or component information. For example, SAS I/O module. After entering the details, use the following links for troubleshooting information:

- Drivers, software, and firmware: Provides drivers and software for your operating system.
- Top issues and solutions: Provides a listing of customer notices, advisories, and bulletins applicable for the product or component.
- Manuals: Provides the latest user documentation applicable to the product or component. User guides can be a useful source for troubleshooting information. The **Hewlett Packard Enterprise Information Library** is an excellent source for finding all the manuals published.

For HPE StoreEasy 1X60 Storage, the following ProLiant server manuals are useful for troubleshooting assistance. For the HPE StoreEasy 1660 or 1860 models, see *ProLiant DL380 Gen10 Server User Guide* or *ProLiant DL380 Gen10 Server Maintenance and Service Guide*.

For more information on troubleshooting servers, see *Troubleshooting Guide for HPE ProLiant Gen10 servers* and *Error Message Guide for HPE ProLiant Gen10 Servers and HPE Synergy* at **Hewlett Packard Enterprise Information Library**.

IMPORTANT:

Some troubleshooting procedures found in ProLiant server guides may not apply to HPE StoreEasy 1X60 Storage models. If necessary, check with HPE Support representative for further assistance.

Product Feedback

The Product Feedback feature enables you to send your suggestions, ideas on product improvement, or feedback on HPE StoreEasy 1000 Storage to storeeasyproductfeedback@hpe.com. You can access the Product Feedback dialog box using the following methods:

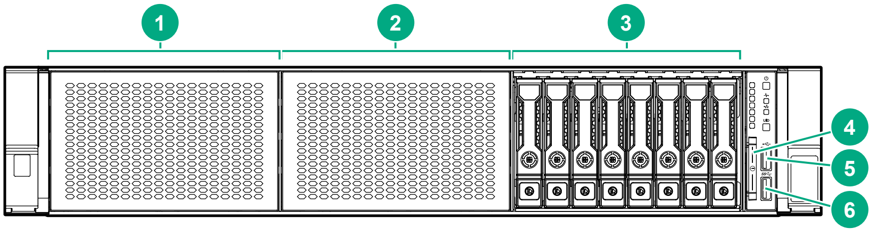
- Double-click the **Product Feedback** icon on the desktop.
- Click **Product Feedback** on the **Start** screen.

Hardware Components of HPE StoreEasy 1X60 Storage system

Component identification

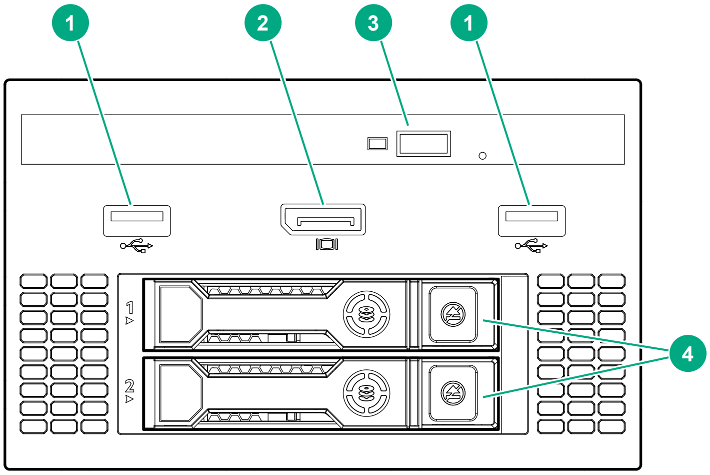
Front panel components

SFF front panel components



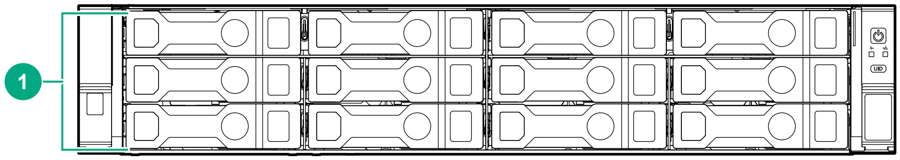
Item	Description
1	Box 1 (optional drives or **universal media bay**)
2	Box 2 (optional drives)
3	Box 3 Drives 1-8
4	Serial label pull tab or optional **Systems Insight Display**
5	iLO service port
6	USB 3.0 port

Universal media bay components



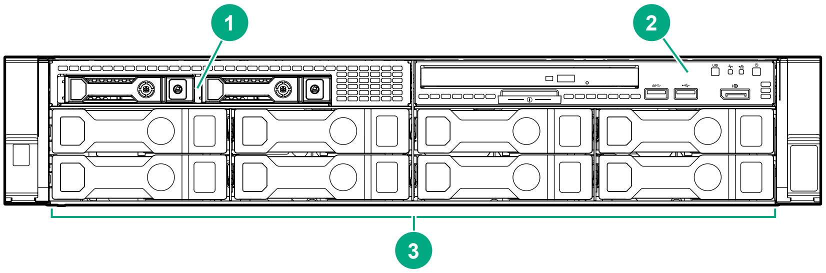
Item	Description
1	USB 2.0 port
2	Video display port
3	Optical disk drive (optional)
4	Drives (optional)

12-drive LFF front panel components



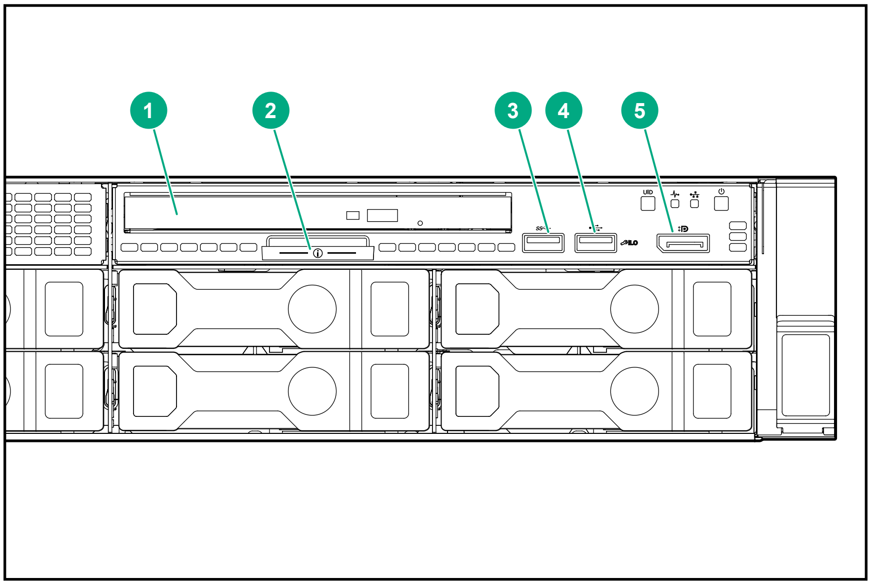
Item	Description
1	Drive bays

8-drive LFF model front panel components



Item	Description
1	Drives (optional)
2	**LFF power switch module**
3	Drive bays

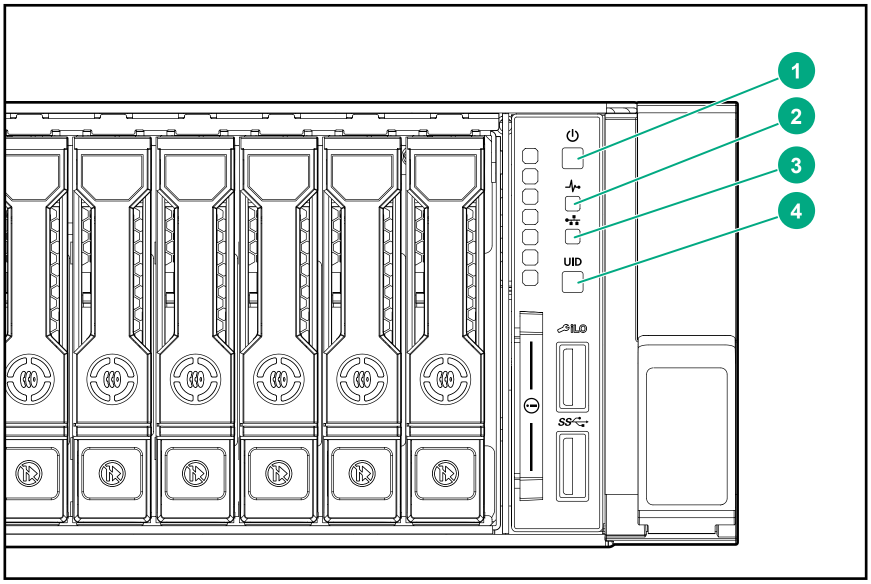
LFF power switch module components



Item	Description
1	Optical disk drive
2	Serial label pull tab
3	USB 3.0 port
4	iLO service port
5	Video display port

Front panel LEDs and buttons

SFF front panel LEDs and button



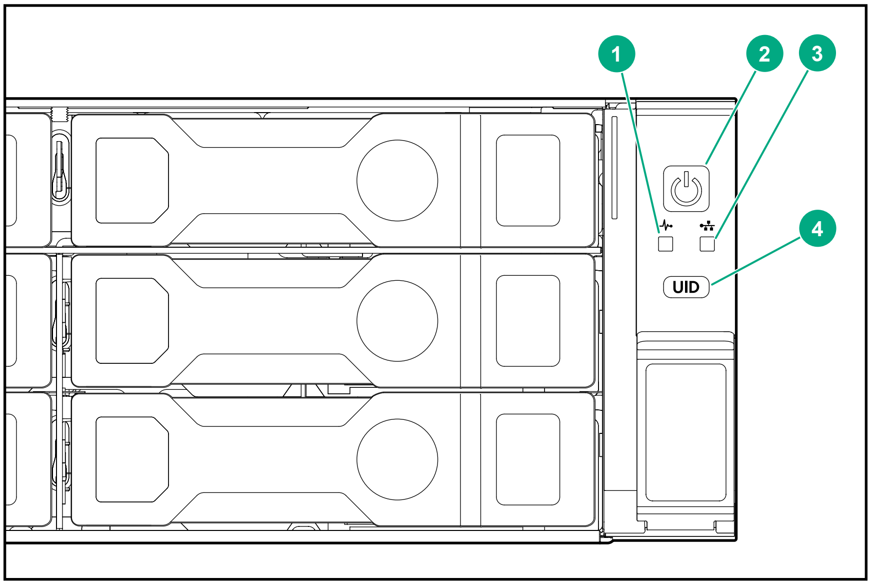
Item	Description	Status
1	Power On/Standby button and system power LED*	Solid green = System on Flashing green (1 Hz/cycle per sec) = Performing power on sequence Solid amber = System in standby Off = No power present†
2	Health LED*	Solid green = Normal Flashing green (1 Hz/cycle per sec) = iLO is rebooting Flashing amber = System degraded Flashing red (1 Hz/cycle per sec) = System critical**
3	NIC status LED*	Solid green = Link to network Flashing green (1 Hz/cycle per sec) = Network active Off = No network activity
4	UID button/LED*	Solid blue = Activated Flashing blue: • 1 Hz/cycle per sec = Remote management or firmware upgrade in progress • 4 Hz/cycle per sec = iLO manual reboot sequence initiated • 8 Hz/cycle per sec = iLO manual reboot sequence in progress Off = Deactivated

*When all four LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see "**Power fault LEDs**."

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

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

LFF 12-drive model front panel LEDs and button



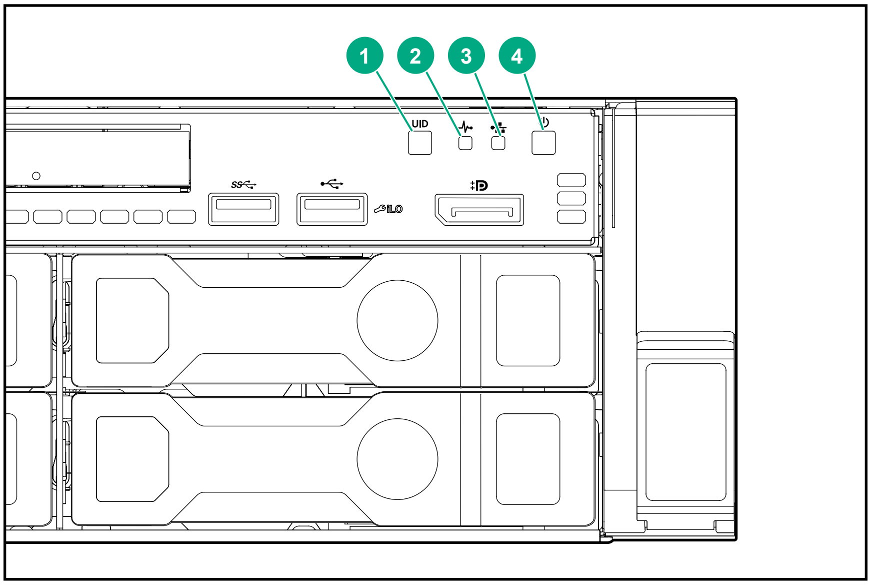
Item	Description	Status
1	Health LED*	Solid green = Normal Flashing green (1 Hz/cycle per sec) = iLO is rebooting Flashing amber = System degraded Flashing red (1 Hz/cycle per sec) = System critical**
2	Power On/Standby button and system power LED*	Solid green = System on Flashing green (1 Hz/cycle per sec) = Performing power on sequence Solid amber = System in standby Off = No power present†
3	NIC status LED*	Solid green = Link to network Flashing green (1 Hz/cycle per sec) = Network active Off = No network activity
4	UID button/LED*	Solid blue = Activated Flashing blue: • 1 Hz/cycle per sec = Remote management or firmware upgrade in progress • 4 Hz/cycle per sec = iLO manual reboot sequence initiated • 8 Hz/cycle per sec = iLO manual reboot sequence in progress Off = Deactivated

*When all four LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see "**Power fault LEDs**."

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

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

LFF power switch module LEDs and button



Item	Description	Status
1	UID button/LED*	Solid blue = Activated Flashing blue: • 1 Hz/cycle per sec = Remote management or firmware upgrade in progress • 4 Hz/cycle per sec = iLO manual reboot sequence initiated • 8 Hz/cycle per sec = iLO manual reboot sequence in progress Off = Deactivated
2	Health LED*	Solid green = Normal Flashing green (1 Hz/cycle per sec) = iLO is rebooting Flashing amber = System degraded Flashing red (1 Hz/cycle per sec) = System critical**

Table Continued

Item	Description	Status
3	NIC status LED*	Solid green = Link to network Flashing green (1 Hz/cycle per sec) = Network active Off = No network activity
4	Power On/Standby button and system power LED*	Solid green = System on Flashing green (1 Hz/cycle per sec) = Performing power on sequence Solid amber = System in standby Off = No power present†

*When all four LEDs described in this table flash simultaneously, a power fault has occurred. For more information, see "**Power fault LEDs**."

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

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

UID button functionality

The UID button can be used to display the Server Health Summary when the server will not power on. For more information, see the latest *HPE iLO User Guide* on the **Hewlett Packard Enterprise website**.

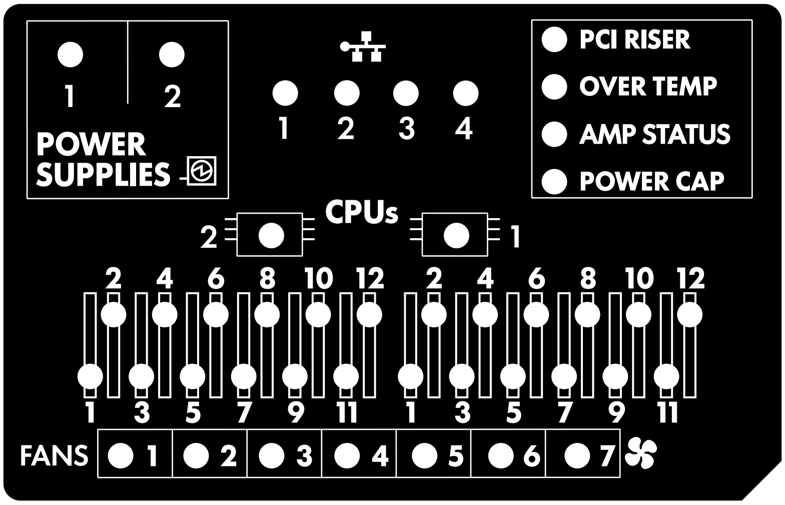
Front panel LED power fault codes

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

Subsystem	LED behavior
System board	1 flash
Processor	2 flashes
Memory	3 flashes
Riser board PCIe slots	4 flashes
FlexibleLOM	5 flashes
Removable HPE Smart Array SR Gen10 controller	6 flashes
System board PCIe slots	7 flashes
Power backplane or storage backplane	8 flashes
Power supply	9 flashes

Systems Insight Display LEDs

The Systems Insight Display LEDs represent the system board layout. The display enables diagnosis with the access panel installed.



Description	Status

Processor LEDs	Off = Normal
	Amber = Failed processor

DIMM LEDs	Off = Normal
	Amber = Failed DIMM or configuration issue

Fan LEDs	Off = Normal Amber = Failed fan or missing fan
NIC LEDs	Off = No link to network Solid green = Network link Flashing green = Network link with activity If power is off, the front panel LED is not active. For status, see **Rear panel LEDs** on page 113.
Power supply LEDs	Off = Normal Solid amber = Power subsystem degraded, power supply failure, or input power lost.

PCI riser LED	Off = Normal
	Amber = Incorrectly installed PCI riser cage

Over temp LED	Off = Normal Amber = High system temperature detected

Table Continued

Description	Status
Amp Status LED	Off = AMP modes disabled Solid green = AMP mode enabled Solid amber = Failover Flashing amber = Invalid configuration
Power cap LED	Off = System is in standby, or no cap is set. Solid green = Power cap applied

When the health LED on the front panel illuminates either amber or red, the server is experiencing a health event. For more information on the combination of these LEDs, see **Systems Insight Display combined LED descriptions** on page 111).

Systems Insight Display combined LED descriptions

The combined illumination of the following LEDs indicates a system condition:

- Systems Insight Display LEDs
- System power LED
- Health LED

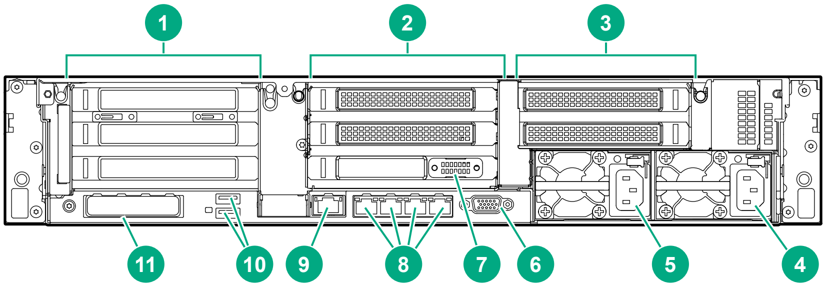
Systems Insight Display LED and color	Health LED	System power LED	Status
Processor (amber)	Red	Amber	One or more of the following conditions may exist: • Processor in socket X has failed. • Processor X is not installed in the socket. • Processor X is unsupported. • ROM detects a failed processor during POST.
Processor (amber)	Amber	Green	Processor in socket X is in a pre-failure condition.
DIMM (amber)	Red	Green	One or more DIMMs have failed.
DIMM (amber)	Amber	Green	DIMM in slot X is in a pre-failure condition.
Over temp (amber)	Amber	Green	The Health Driver has detected a cautionary temperature level.
Over temp (amber)	Red	Amber	The server has detected a hardware critical temperature level.

Table Continued

Systems Insight Display LED and color	Health LED	System power LED	Status
PCI riser (amber)	Red	Green	The PCI riser cage is not seated properly.
Fan (amber)	Amber	Green	One fan has failed or has been removed.
Fan (amber)	Red	Green	Two or more fans have failed or been removed.
Power supply (amber)	Red	Amber	One or more of the following conditions may exist: • Only one power supply is installed and that power supply is in standby. • Power supply fault • System board fault
Power supply (amber)	Amber	Green	One or more of the following conditions may exist: • Redundant power supply is installed and only one power supply is functional. • AC power cord is not plugged into redundant power supply. • Redundant power supply fault • Power supply mismatch at POST or power supply mismatch through hot-plug addition
Power cap (off)	—	Amber	Standby
Power cap (green)	—	Flashing green	Waiting for power
Power cap (green)	—	Green	Power is available.
Power cap (flashing amber)	—	Amber	Power is not available.

IMPORTANT:
If more than one DIMM slot LED is illuminated, further troubleshooting is required. Test each bank of DIMMs by removing all other DIMMs. Isolate the failed DIMM by replacing each DIMM in a bank with a known working DIMM.

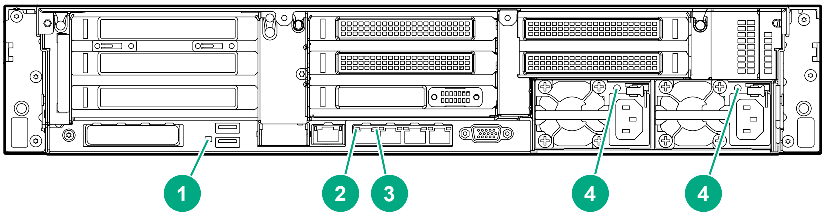
Rear panel components



Item	Description
1	Primary riser slots 1-3 (Optional drive cage)
2	Optional riser slots 4-6 (Optional drive cage)
3	Optional riser slots 7-8 (Optional drive cage)
4	Power supply 1
5	Power supply 2
6	Video port
7	Serial port (optional)*
8	1Gb RJ-45 ports 1–4
9	iLO management port
10	USB 3.0 ports
11	FlexibleLOM slot

*When a tertiary riser cage is installed as shown, the serial port can installed in riser slot 6.

Rear panel LEDs

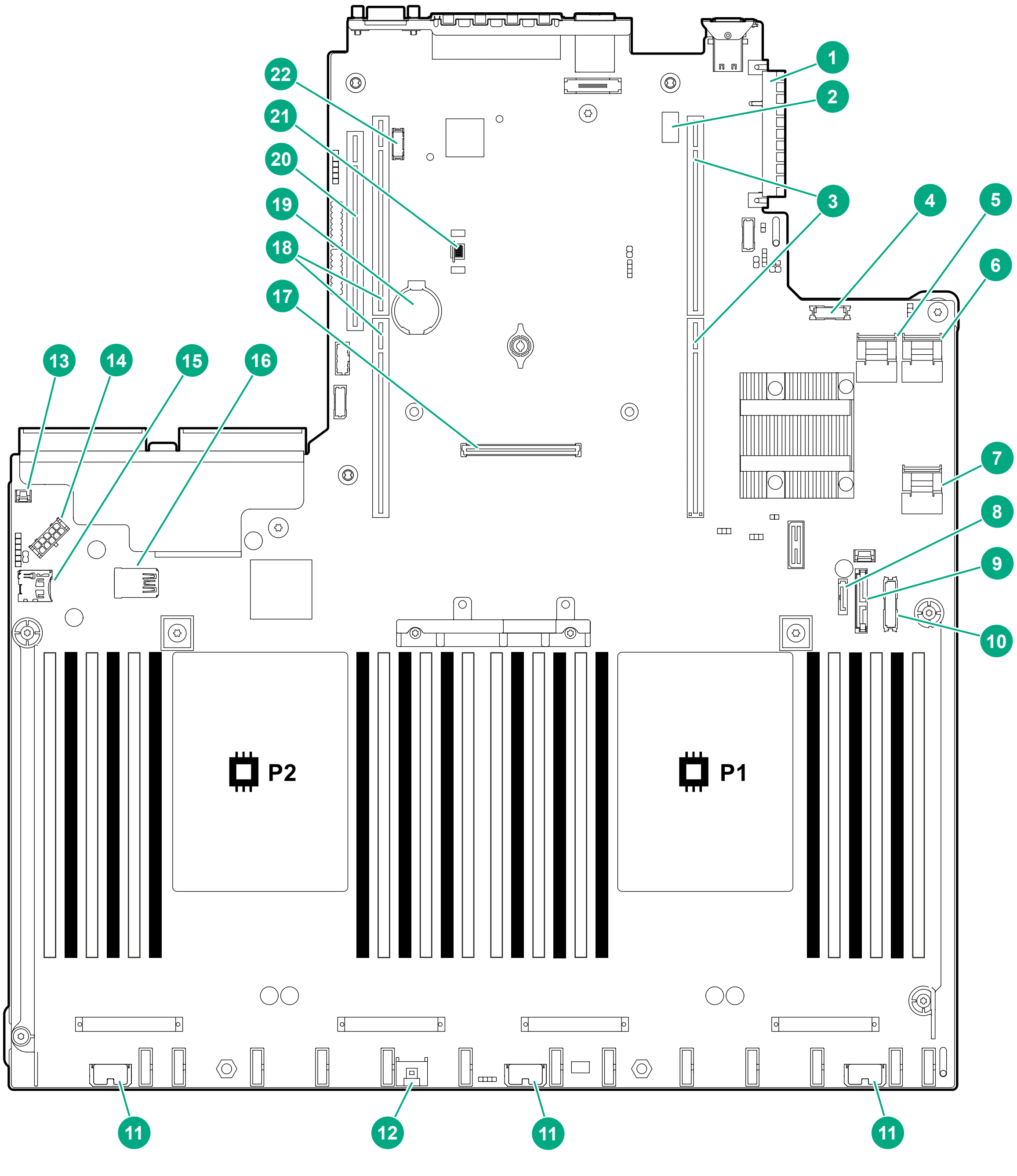


Item	Description	Status
1	UID LED	Off = Deactivated Solid blue = Activated Flashing blue = System being managed remotely

2	Link LED	Off = No network link
		Green = Network link

3	Activity LED	Off = No network activity Solid green = Link to network Flashing green = Network activity
4	Power supply LEDs	Off = System is off or power supply has failed. Solid green = Normal

System board components



Item	Description
1	FlexibleLOM connector
2	System maintenance switch
3	Primary PCIe riser connector
4	Front display port/USB 2.0 connector

Table Continued

Item	Description
5	x4 SATA port 1
6	x4 SATA port 2
7	x2 SATA port 3
8	x1 SATA port 4
9	Optical disk drive/SATA port 5
10	Front power/USB 3.0 connector
11	Drive backplane power connectors
12	Smart Storage Battery connector
13	Chassis intrusion detection connector
14	Drive backplane power connector
15	Micro SD card slot
16	Dual internal USB 3.0 ports
17	Type-a Smart Array connector
18	Secondary PCIe riser connector*
19	System battery
20	Tertiary PCIe riser connector*
21	TPM connector
22	Serial port connector (optional)

* Requires a second processor

System maintenance switch descriptions

Position	Default	Function

S1[1]	Off	Off = security is enabled.
		On = security is disabled.

S2	Off	Off = System configuration can be changed. On = System configuration is locked.
S3	Off	Reserved
S4	Off	Reserved
S5[1]	Off	Off = Power-on password is enabled. On = Power-on password is disabled.
S6[1], [2], [3]	Off	Off = No function On = Restore default manufacturing settings
S7	Off	Reserved (Internal use only)

Table Continued

Position	Default	Function
S8	—	Reserved
S9	—	Reserved
S10	—	Reserved
S11	—	Reserved
S12	—	Reserved

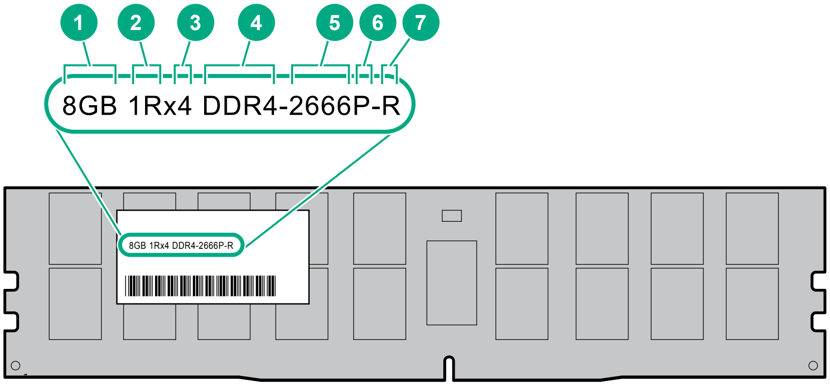
[1] To access the redundant ROM, set S1, S5, and S6 to On.

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

[3] When the system maintenance switch position 6 is set to the On position and Secure Boot is enabled, some configurations cannot be restored. For more information, see **#unique_159**.

DIMM label identification

To determine DIMM characteristics, see the label attached to the DIMM. The information in this section helps you to use the label to locate specific information about the DIMM.



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

Table Continued

Item	Description	Example

3	Data width on DRAM	x4 = 4-bit
		x8 = 8-bit
		x16 = 16-bit

4	Memory generation	PC4 = DDR4
5	Maximum memory speed	2133 MT/s 2400 MT/s 2666 MT/s

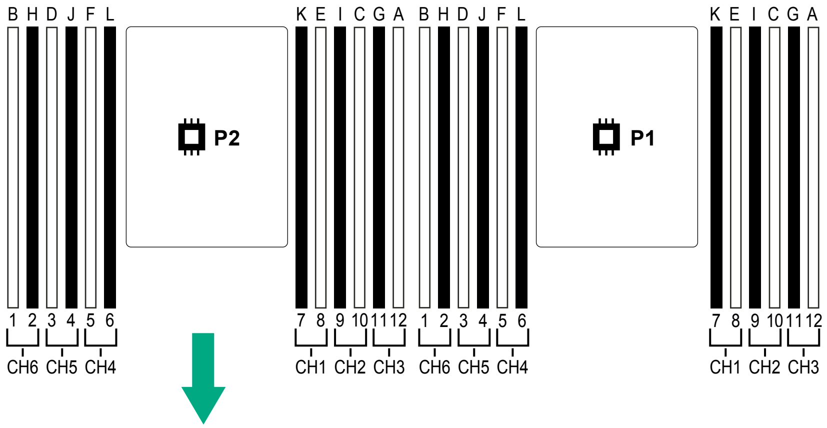
6	CAS latency	P = CAS 15-15-15
		T = CAS 17-17-17
		U = CAS 20-18-18
		V = CAS 19-19-19 (for RDIMM, LRDIMM)
		V = CAS 22-19-19 (for 3DS TSV LRDIMM)

7	DIMM type	R = RDIMM (registered)
		L = LRDIMM (load reduced)
		E = Unbuffered ECC (UDIMM)

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

DIMM slot locations

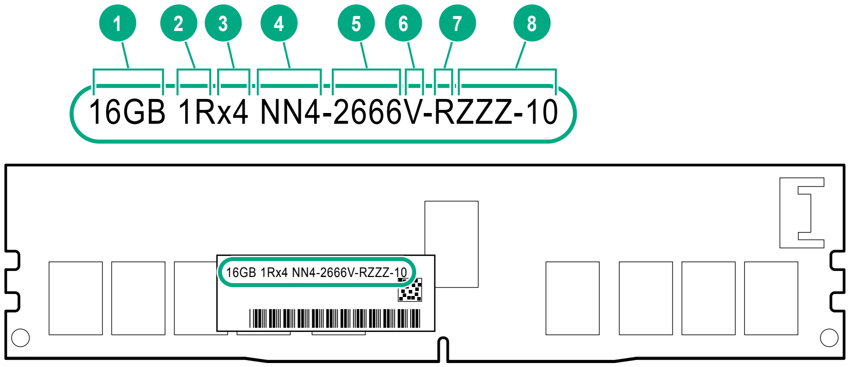
DIMM slots are numbered sequentially (1 through 12) for each processor. The supported AMP modes use the letter assignments for population guidelines.



NVDIMM identification

NVDIMM boards are blue instead of green. This change to the color makes it easier to distinguish NVDIMMs from DIMMs.

To determine NVDIMM characteristics, see the full product description as shown in the following example:

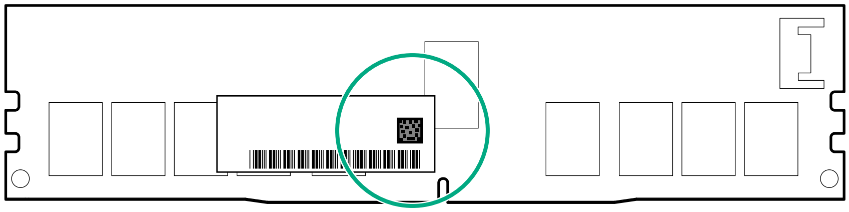


Item	Description	Definition
1	Capacity	16 GiB
2	Rank	1R (Single rank)
3	Data width per DRAM chip	x4 (4 bit)
4	Memory type	NN4=DDR4 NVDIMM-N
5	Maximum memory speed	2667 MT/s
6	Speed grade	V (latency 19-19-19)
7	DIMM type	RDIMM (registered)
8	Other	—

For more information about NVDIMMs, see the product QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**).

NVDIMM 2D Data Matrix barcode

The 2D Data Matrix barcode is on the right side of the NVDIMM label and can be scanned by a cell phone or other device.

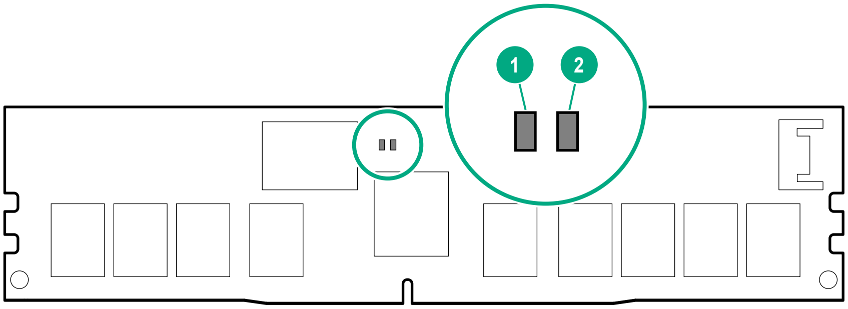


When scanned, the following information from the label can be copied to your cell phone or device:

- (P) is the module part number.
- (L) is the technical details shown on the label.
- (S) is the module serial number.

Example: (P)HMN82GR7AFR4N-VK (L)16GB 1Rx4 NN4-2666V-RZZZ-10(S)80AD-01-1742-11AED5C2

NVDIMM LED identification



Item	LED description	LED color
1	Power LED	Green
2	Function LED	Blue

NVDIMM-N LED combinations

State	Definition	NVDIMM-N Power LED (green)	NVDIMM-N Function LED (blue)
0	AC power is on (12 V rail) but the NVM controller is not working or not ready.	On	Off
1	AC power is on (12 V rail) and the NVM controller is ready.	On	On
2	AC power is off or the battery is off (12 V rail off).	Off	Off
3	AC power is on (12 V rail) or the battery is on (12 V rail) and the NVDIMM-N is active (backup and restore).	On	Flashing

NVDIMM Function LED patterns

For the purpose of this table, the NVDIMM-N LED operates as follows:

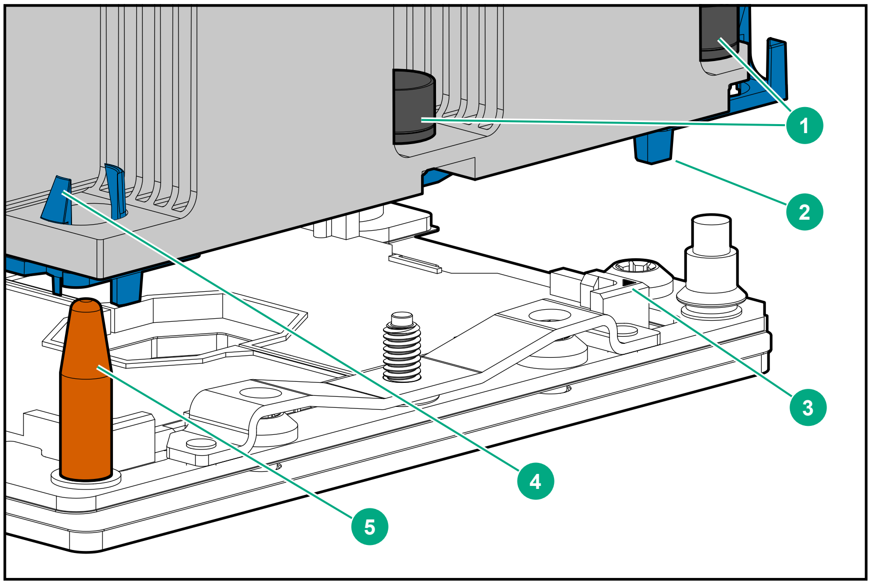
- Solid indicates that the LED remains in the on state.
- Flashing indicates that the LED is on for 2 seconds and off for 1 second.
- Fast-flashing indicates that the LED is on for 300 ms and off for 300 ms.

State	Definition	NVDIMM-N Function LED
0	The restore operation is in progress.	Flashing
1	The restore operation is successful.	Solid or On
2	Erase is in progress.	Flashing
3	The erase operation is successful.	Solid or On
4	The NVDIMM-N is armed, and the NVDIMM-N is in normal operation.	Solid or On

Table Continued

State	Definition	NVDIMM-N Function LED
5	The save operation is in progress.	Flashing
6	The NVDIMM-N finished saving and battery is still turned on (12 V still powered).	Solid or On
7	The NVDIMM-N has an internal error or a firmware update is in progress. For more information about an NVDIMM-N internal error, see the IML.	Fast-flashing

Processor, heatsink, and socket components

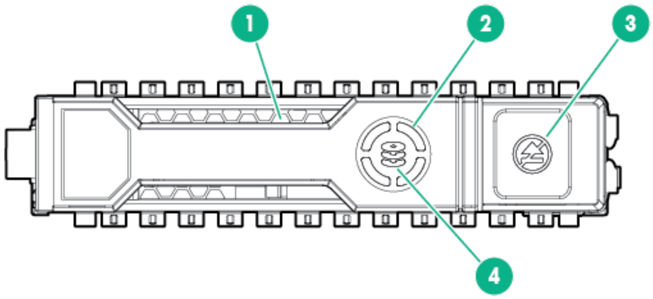


Item	Description
1	Heatsink nuts
2	Processor carrier
3	Pin 1 indicator[1]
4	Heatsink latch
5	Alignment post

[1] Symbol also on the processor and frame.

Drives

SAS/SATA drive components and LEDs

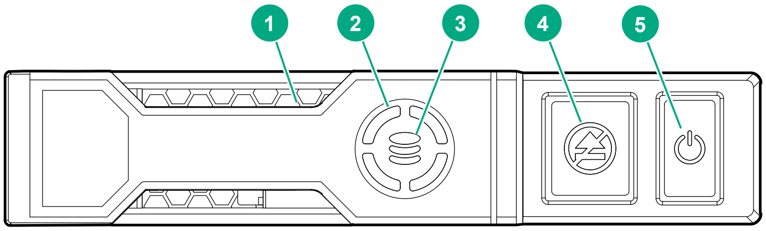


Item	Description	Status
1	Locate	- Solid blue = The drive is being identified by a host application. - Flashing blue = The drive carrier firmware is being updated or requires an update.
2	Activity ring LED	- Rotating green = Drive activity. - Off = No drive activity.
3	Do not remove LED	- Solid white = Do not remove the drive. Removing the drive causes one or more of the logical drives to fail. - Off = Removing the drive does not cause a logical drive to fail.
4	Drive status LED	- Solid green = The drive is a member of one or more logical drives. - Flashing green = The drive is rebuilding or performing a RAID migration, strip size migration, capacity expansion, or logical drive extension, or is erasing. - Flashing amber/green = The drive is a member of one or more logical drives and predicts the drive will fail. - Flashing amber = The drive is not configured and predicts the drive will fail. - Solid amber = The drive has failed. - Off = The drive is not configured by a RAID controller.

NVMe SSD LEDs

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

CAUTION:
Do not remove an NVMe SSD from the drive bay while the Do not remove LED is flashing. The Do not remove LED flashes to indicate that the device is still in use. Removing the NVMe SSD before the device has completed and ceased signal/traffic flow can cause loss of data.

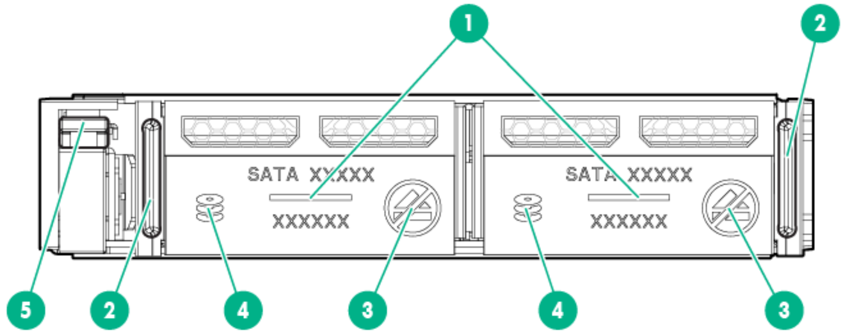


Item	LED	Status	Definition
1	Locate	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity ring	Rotating green	Drive activity
		Off	No drive activity
3	Drive status	Solid green	The drive is a member of one or more logical drives.
		Flashing green	The drive is doing one of the following: • Rebuilding • Performing a RAID migration • Performing a strip size migration • Performing a capacity expansion • Performing a logical drive extension • Erasing
		Flashing amber/ green	The drive is a member of one or more logical drives and predicts the drive will fail.
		Flashing amber	The drive is not configured and predicts the drive will fail.
		Solid amber	The drive has failed.
		Off	The drive is not configured by a RAID controller.
4	Do not remove	Solid white	Do not remove the drive. Drive must be ejected from the PCIe bus prior to removal.

Table Continued

Item	LED	Status	Definition
		Flashing white	The drive ejection request is pending.
		Off	The drive has been ejected.
5	Power	Solid green	Do not remove the drive. Drive must be ejected from the PCIe bus prior to removal.
		Flashing green	The drive ejection request is pending.
		Off	The drive has been ejected.

uFF drive components and LEDs

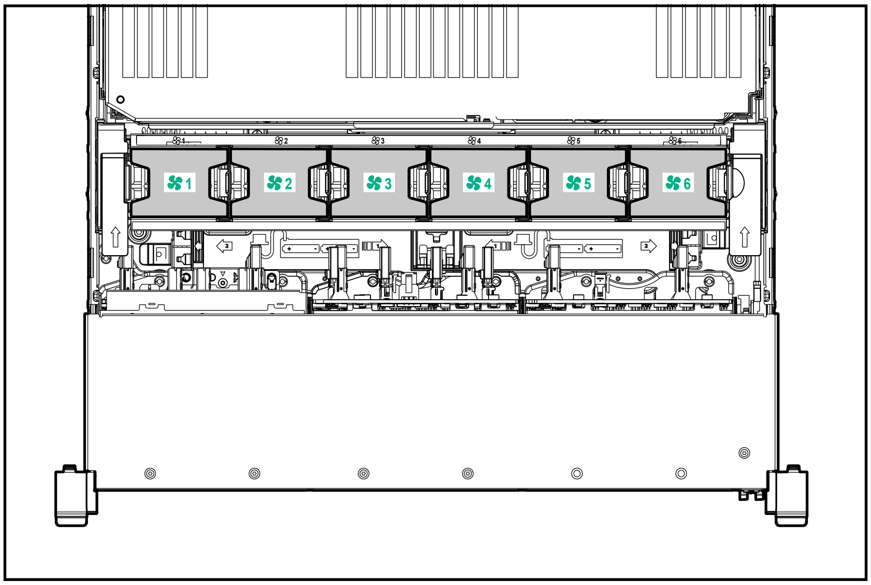


Item	Description	Status
1	Locate	• Off—Normal • Solid blue—The drive is being identified by a host application • Flashing blue—The drive firmware is being updated or requires an update
2	uFF drive ejection latch	Removes the uFF drive when released
3	Do not remove LED	• Off—OK to remove the drive. Removing the drive does not cause a logical drive to fail. • Solid white—Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.

Table Continued

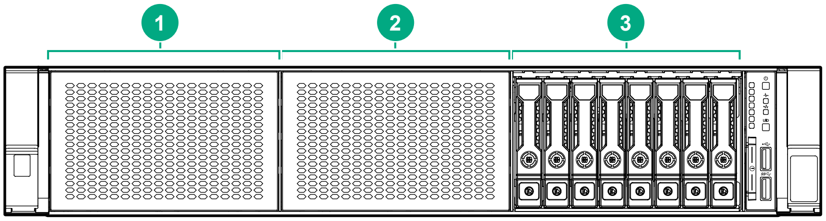
Item	Description	Status
4	Drive status LED	• Off—The drive is not configured by a RAID controller • Solid green—The drive is a member of one or more logical drives • Flashing green (4 Hz)—The drive is operating normally and has activity • Flashing green (1 Hz)—The drive is rebuilding or performing a RAID migration, stripe size migration, capacity expansion, logical drive extension, or is erasing • Flashing amber/green (1 Hz)—The drive is a member of one or more logical drives that predicts the drive will fail • Solid amber—The drive has failed • Flashing amber (1 Hz)—The drive is not configured and predicts the drive will fail
5	Adapter ejection release latch and handle	Removes the SFF flash adapter when released

Fan bay numbering

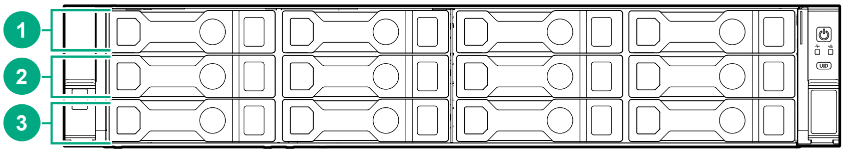


Drive box identification

Front boxes

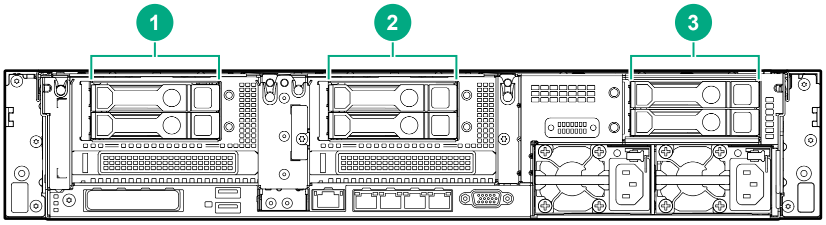


Item	Description
1	Box 1
2	Box 2
3	Box 3

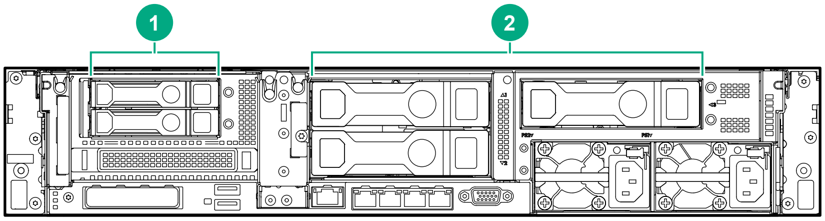


Item	Description
1	Box 1
2	Box 2
3	Box 3

Rear boxes

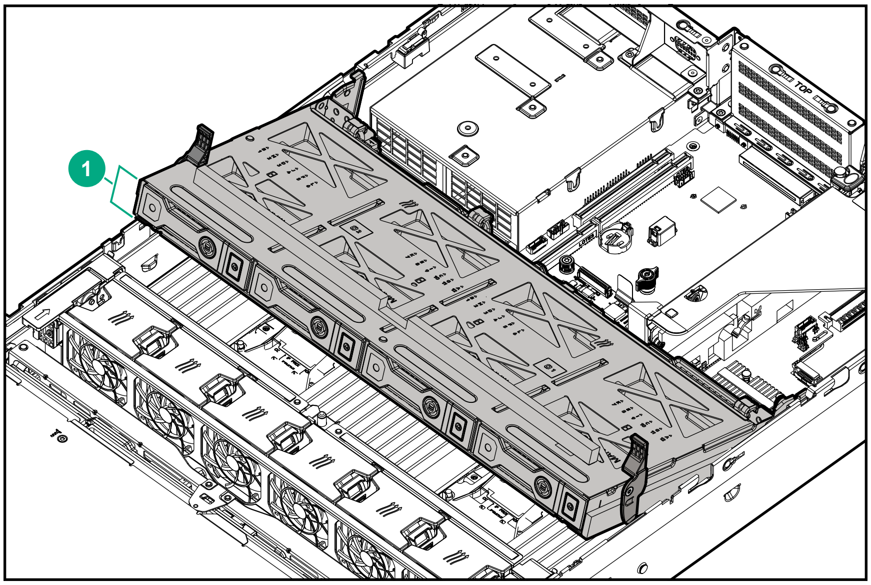


Item	Description
1	Box 4
2	Box 5
3	Box 6



Item	Description
1	Box 4
2	Box 6

Midplane box (LFF only)



Item	Description
1	Box 7

Drive bay numbering

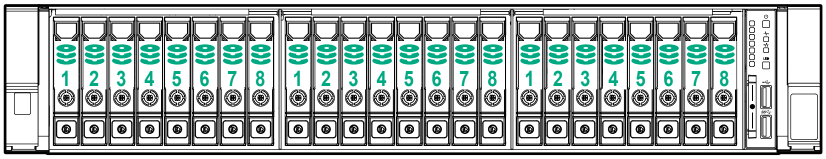
Drive bay numbering depends on how the drive backplanes are connected:

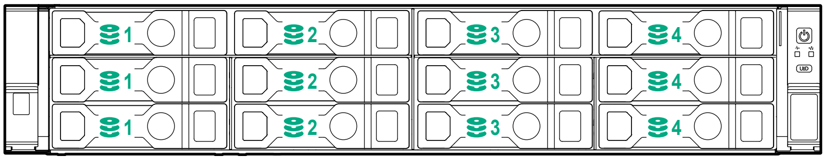
- To a controller
    - Embedded controllers use the onboard SATA ports.
    - Type-a controllers install to the type-a smart array connector.
    - Type-p controllers install to a PCIe riser.
- To a SAS expander

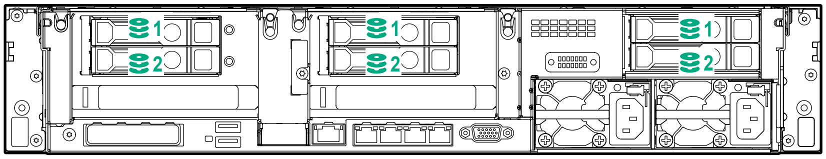
  Installs in the primary or secondary PCIe riser

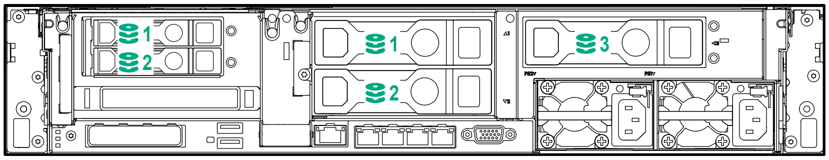
Drive bay numbering: Smart Array controller

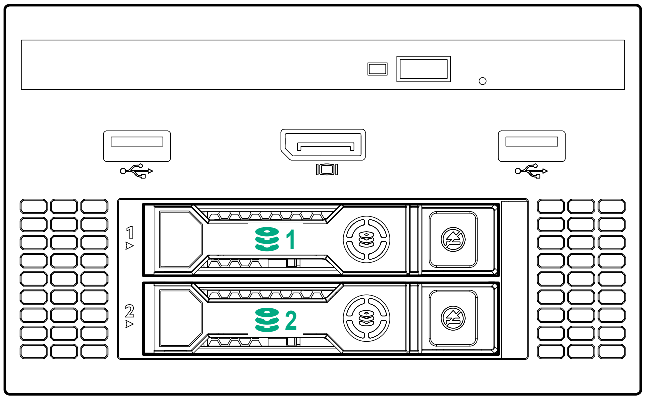
When the drive backplane is connected directly to a storage controller, then each drive box starts at 1. The following images are examples of common configurations.

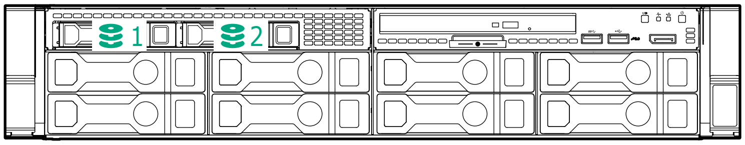


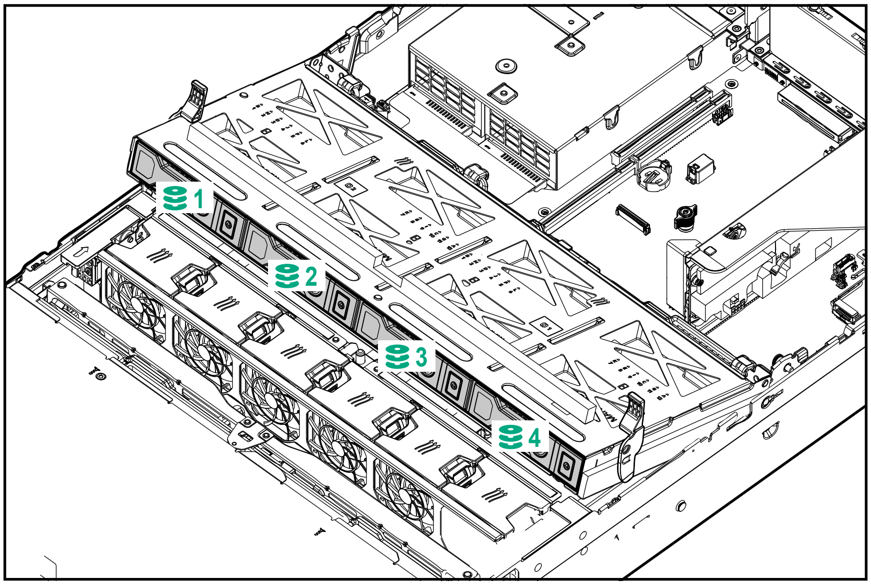












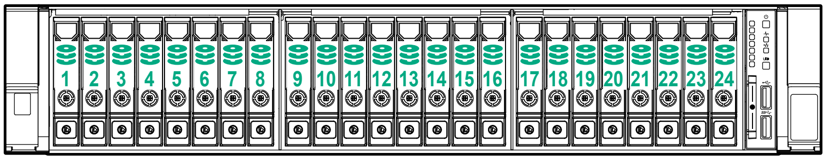
Drive bay numbering: SAS expander

Drive numbering through a SAS Expander is continuous.

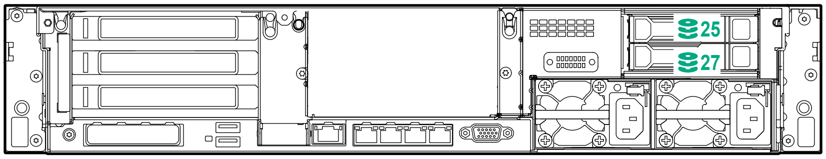
- SAS expander port 1 always connects to port 1 of the controller.
- SAS expander port 2 always connects to port 2 of the controller.
- SAS expander port 3 = drive numbers 1-4.
- SAS expander port 4 = drive numbers 5-8.
- SAS expander port 5 = drive numbers 9-12.
- SAS expander port 6 = drive numbers 13-16.

- SAS expander port 7 = drive numbers 17-20.
- SAS expander port 8 = drive numbers 21-24.
- SAS expander port 9 = drive numbers 25-28.

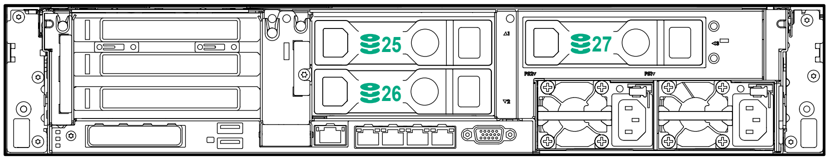
Common configuration examples:



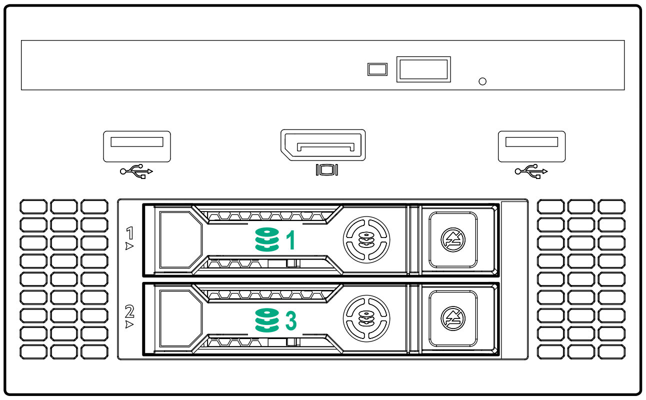
When any stacked 2SFF drive cage is connected to the SAS expander, the drive numbering skips the second number to allow **uFF drive bay numbering** on page 132. For example, when a rear 2SFF drive cage is connected to SAS expander port 9, then the drive numbers are 25 and 27.

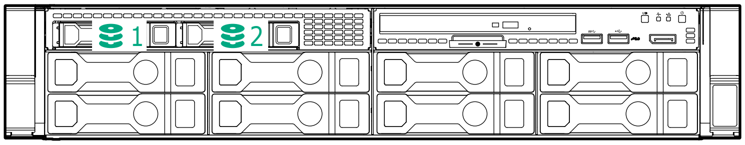


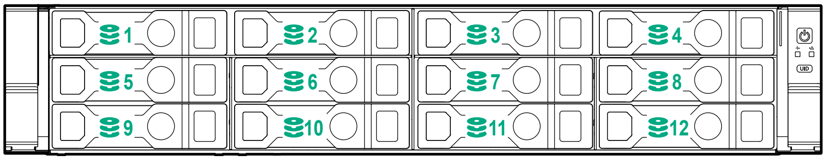
When the front 24SFF bays are populated, any installed rear 2SFF drives are always 25 and 27.

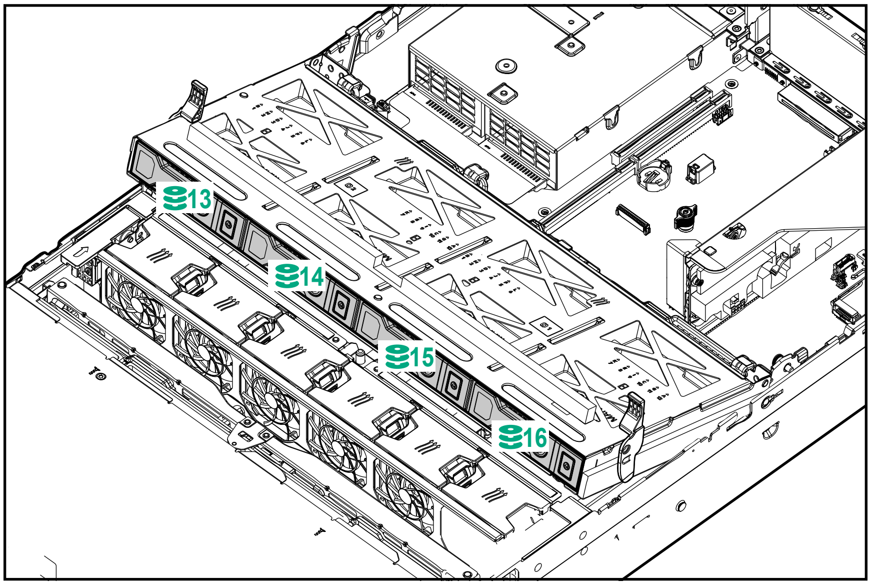


If a 2SFF drive cage is connected to SAS expander port 3, then the drive numbers are 1 and 3.

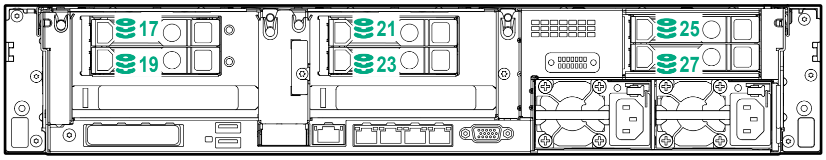






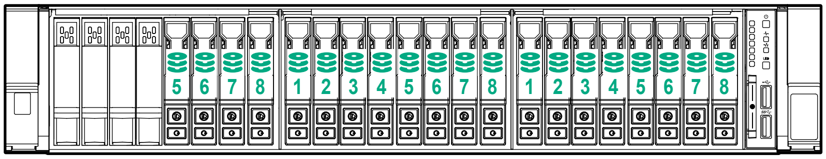


Front 12LFF + Midplane 4LFF + All rear 2SFF:



Drive bay numbering: NVMe drives

If the server is populated with NVMe drives and NVMe risers:

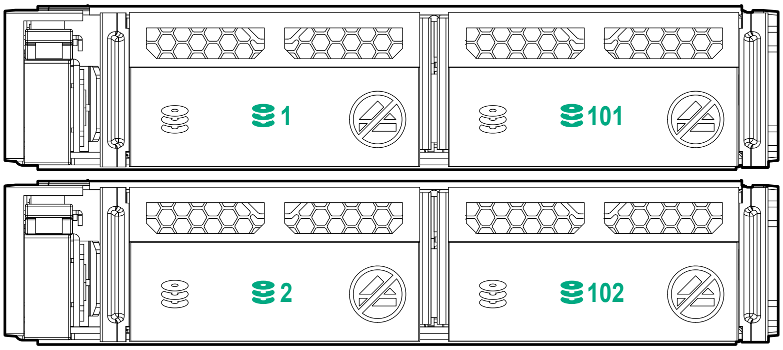


uFF drive bay numbering

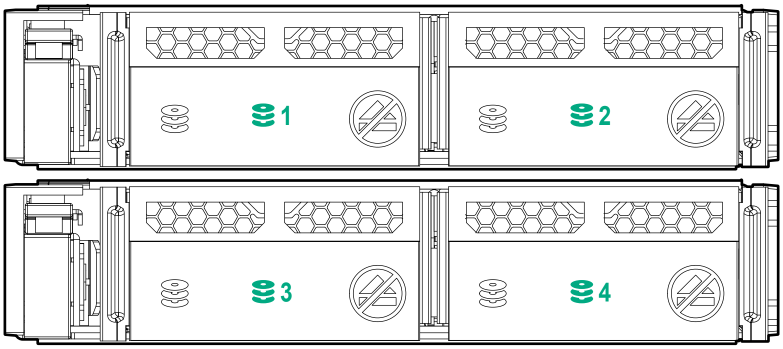
There are two uFF drives in each drive carrier.

If the drives are connected to a controller:

- The left bay = The default bay number of the server
- The right bay = The default bay number of the server + 100



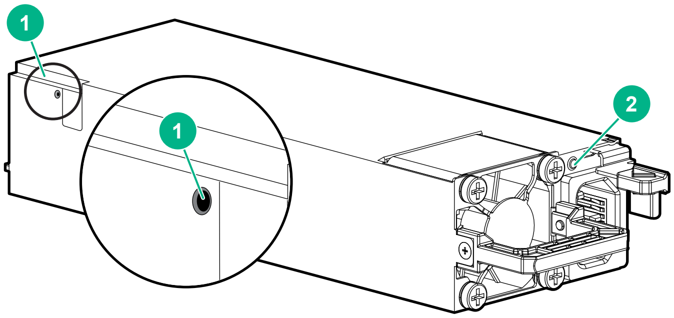
If the drives are connected to a SAS expander:



For example:

- If the drives are connected to port 3 of the SAS expander, then the uFF drives are 1-4.
- If the drives are connected to port 9 of the SAS expander, then the uFF drives are 25-28.

HPE Flex Slot Power Supply with Integrated Battery Backup Unit components and LED



1. Battery check button
2. Power LED

For more information about the HPE Flex Slot Power Supply with Integrated Battery Backup Unit, see the document that ships with the component.

The label on the component indicates that the flex slot power supply has an integrated battery back up module.

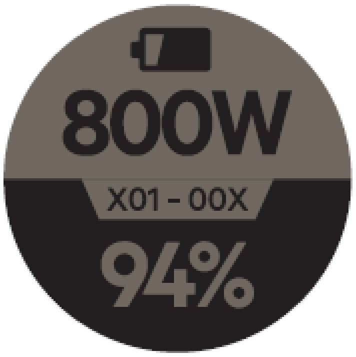


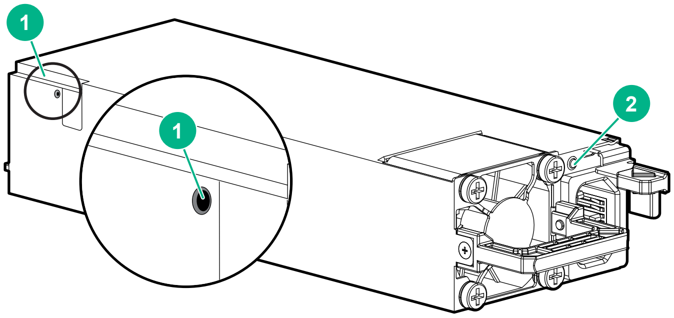
Figure 1: HPE Flex Slot Power Supply with Integrated Battery Backup Unit label

Checking the battery backup charge level

Procedure

1. Using a ball tip pen, press and release the battery check button.

   After releasing the button, you may have to wait up to seven seconds before the LED starts flashing.

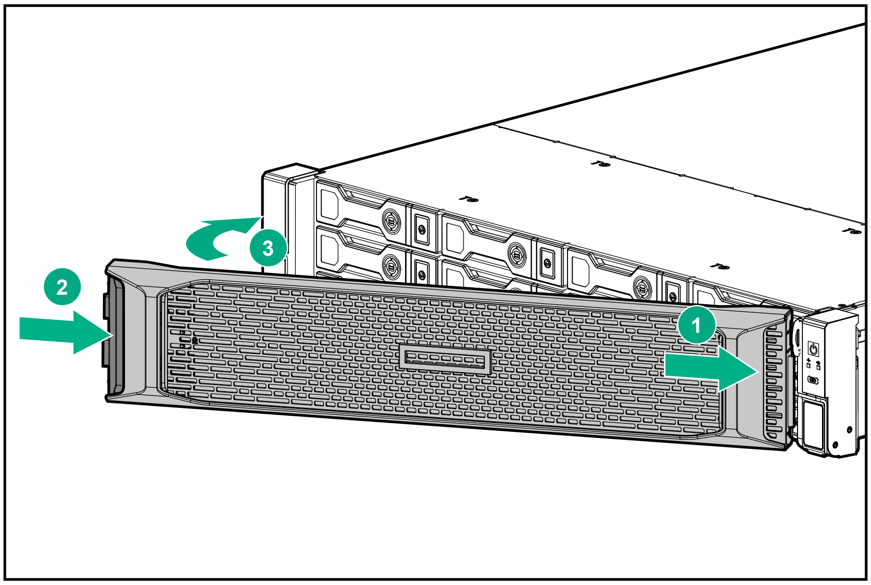
2. Note the number of LED flashes and reference the following table.

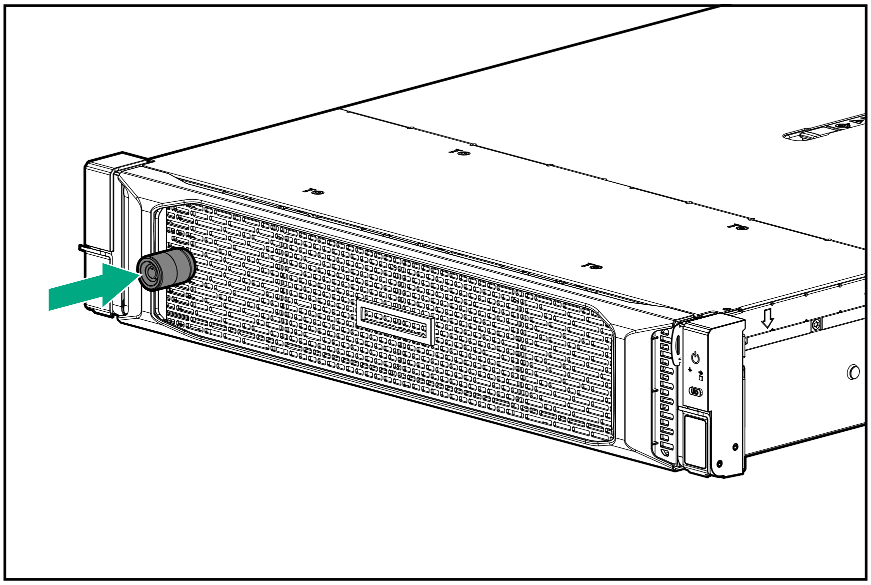
Flashes	Battery State RSOC[1]
0	Battery bad/failed
1	RSOC <= 29%
2	30% <= RSOC <= 62%
3	63% <= RSOC <= 94%
4	95% <= RSOC

[1] Relative State of Charge

The battery will fully charge within one hour of being installed into the server.

Installing the bezel and bezel lock





Power supply options

Hot-plug power supply calculations

For hot-plug power supply specifications and calculators to determine electrical and heat loading for the server, see the Hewlett Packard Enterprise Power Advisor website (**http://www.hpe.com/info/poweradvisor/online**).

Installing a redundant hot-plug power supply

CAUTION:

All power supplies installed in the server must have the same output power capacity. Verify that all power supplies have the same part number and label color. The system becomes unstable and might shut down if it detects different power supplies.

CAUTION:

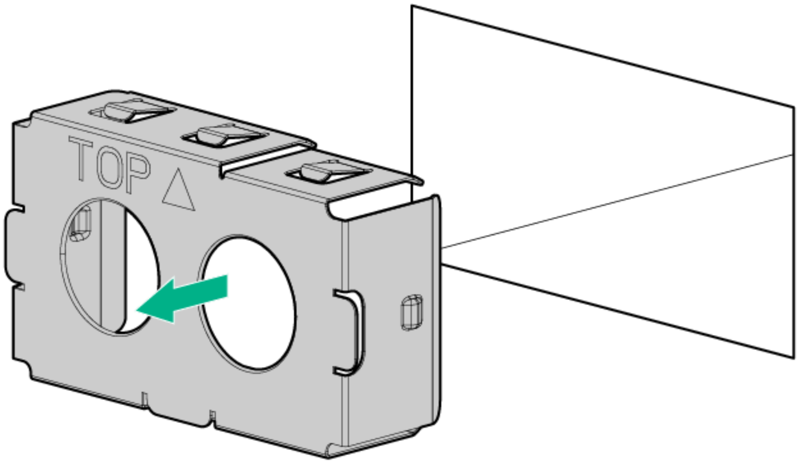
To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

Procedure

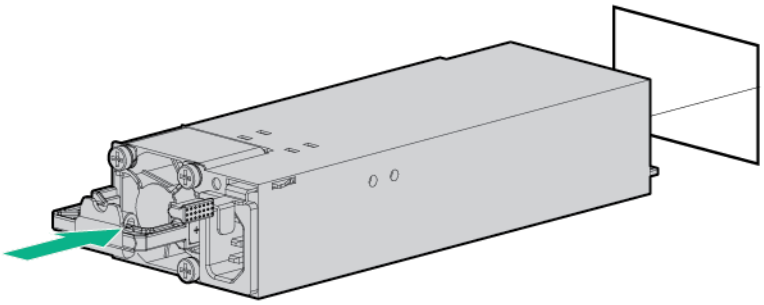
1. **Release the cable management arm to access the rear panel**.
2. Remove the blank.

   WARNING:

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



3. Insert the power supply into the power supply bay until it clicks into place.



4. Connect the power cord to the power supply.
5. Route the power cord.

   Use the cable management arm and best practices when routing cords and cables.
6. Connect the power cord to the power source.
7. Observe the power supply LED.

Fan options

△ **CAUTION:**
To avoid damage to server components, fan blanks must be installed in fan bays 1 and 2 in a single-processor configuration.

△ **CAUTION:**
To avoid damage to the equipment, do not operate the server for extended periods of time if the server does not have the optimal number of fans installed. Although the server might boot, Hewlett Packard Enterprise does not recommend operating the server without the required fans installed and operating.

Valid fan configurations are listed in the following table.

Configuration	Fan bay 1	Fan bay 2	Fan bay 3	Fan bay 4	Fan bay 5	Fan bay 6
1 processor	Fan blank	Fan blank	Fan	Fan	Fan	Fan
1 processor 24-SFF or 12-LFF configuration with high-performance fans	Fan	Fan	Fan	Fan	Fan	Fan
2 processors	Fan	Fan	Fan	Fan	Fan	Fan

For a single-processor configuration, excluding 24-SFF and 12-LFF configurations, four fans and two blanks are required in specific fan bays for redundancy. A fan failure or missing fan causes a loss of redundancy. A second fan failure or missing fan causes an orderly shutdown of the server.

For a dual-processor configuration or single-processor 24-SFF or 12-LFF configurations, six fans are required for redundancy. A fan failure or missing fan causes a loss of redundancy. A second fan failure or missing fan causes an orderly shutdown of the server.

High-performance fans might be necessary in 24-SFF and 12-LFF configurations for the following installations:

- Optional GPU riser installations
- ASHRAE compliant configurations

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

The server supports variable fan speeds. The fans operate at minimum speed until a temperature change requires a fan speed increase to cool the server. The server shuts down during the following temperature-related scenarios:

- At POST and in the OS, iLO performs an orderly shutdown if a cautionary temperature level is detected. If the server hardware detects a critical temperature level before an orderly shutdown occurs, the server performs an immediate shutdown.
- When the Thermal Shutdown feature is disabled in the BIOS/Platform Configuration (RBSU), iLO does not perform an orderly shutdown when a cautionary temperature level is detected. Disabling this feature does not disable the server hardware from performing an immediate shutdown when a critical temperature level is detected.

CAUTION:
A thermal event can damage server components when the Thermal Shutdown feature is disabled in the BIOS/Platform Configuration (RBSU).

Installing high-performance fans

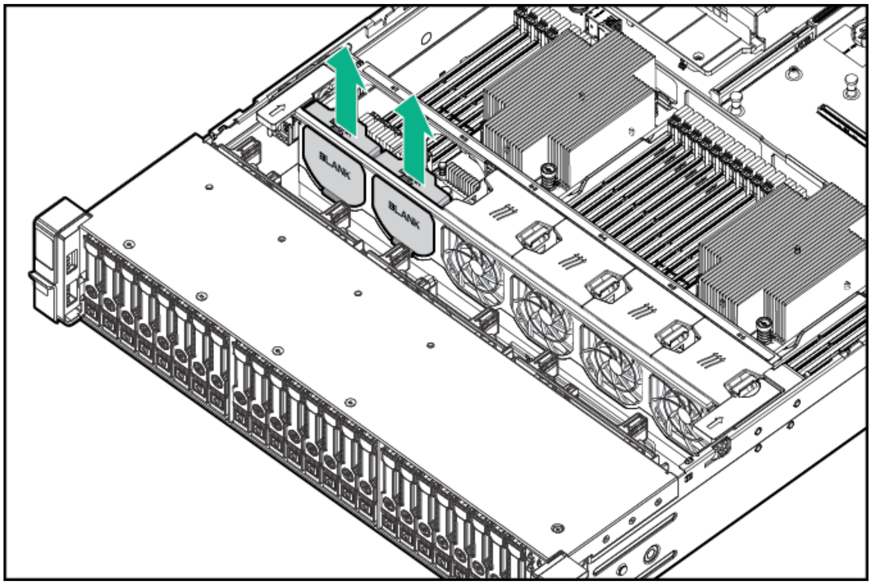
CAUTION:
Caution: To prevent damage server, ensure that all DIMM latches are closed and locked before installing the fans.

CAUTION:

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

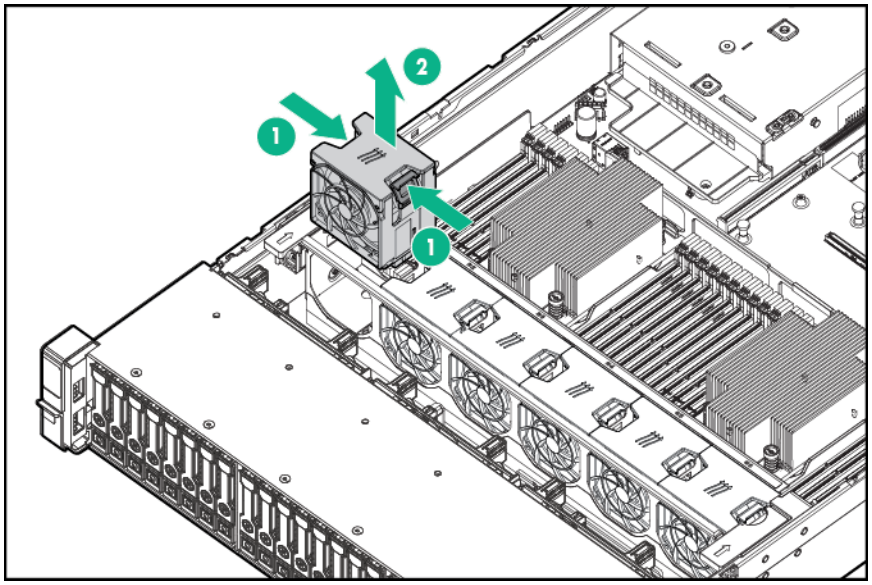
Procedure

1. **Extend the server from the rack**.
2. **Remove the access panel**.
3. If installed, remove all fan blanks.

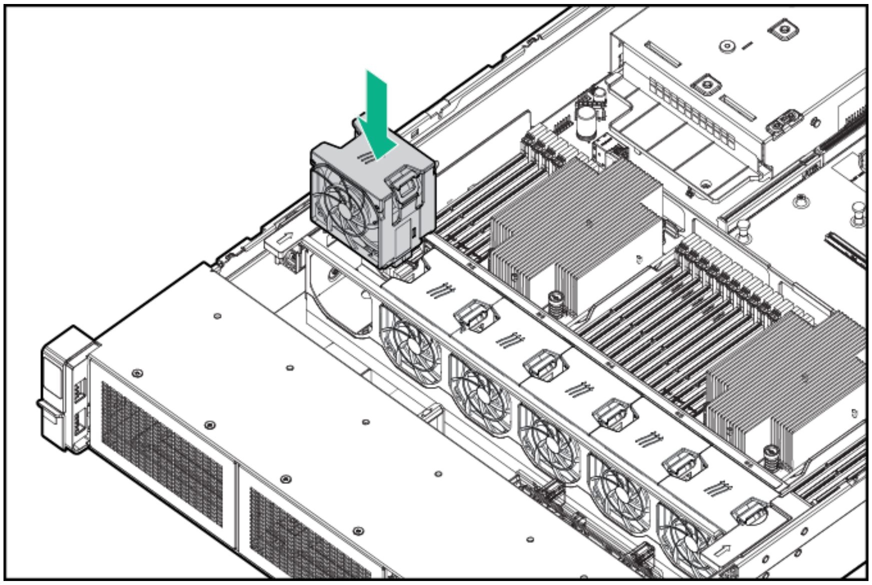


4. **Remove the air baffle**.
5. Remove all standard fans.

IMPORTANT:
Do not mix standard fans and high-performance fans in the same server.



6. Install high-performance fans in all fan bays.



7. **Install the air baffle**.
8. **Install the access panel**.
9. **Install the server into the rack**.

Memory options

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

DIMM and NVDIMM population information

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

HPE SmartMemory speed information

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

Installing a DIMM

The server supports up to 32 DIMMs.

Prerequisites

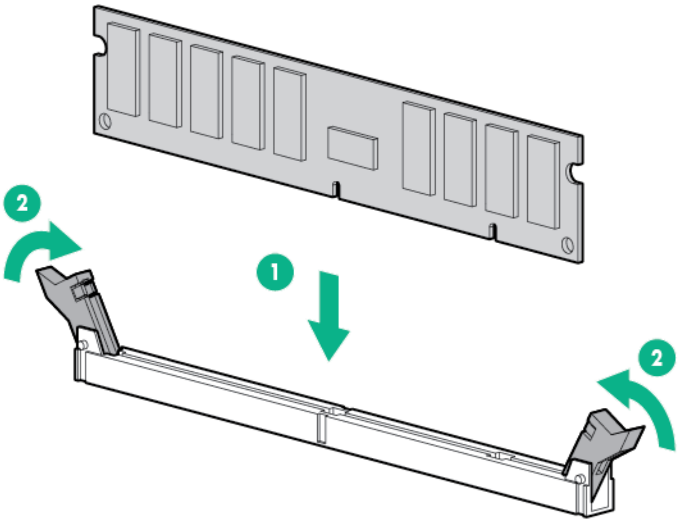
Before installing this option, be sure you have the following:

The components included with the hardware option kit

For more information on specific options, see the server QuickSpecs on the **Hewlett Packard Enterprise website**.

Procedure

1. **Power down the server**.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Do one of the following:
   a. **Extend the server from the rack**.
   b. **Remove the server from the rack**.
4. **Remove the access panel**.
5. Open the DIMM slot latches.
6. Install the DIMM.



7. **Install the access panel**.
8. Install the server in the rack.
9. Connect each power cord to the server.
10. Connect each power cord to the power source.
11. **Power up the server**.

Use the BIOS/Platform Configuration (RBSU) in the UEFI System Utilities to configure the memory mode.

For more information about LEDs and troubleshooting failed DIMMs, see "**Systems Insight Display combined LED descriptions**."

HPE 16GB NVDIMM option

HPE NVDIMMs are flash-backed NVDIMMs used as fast storage and are designed to eliminate smaller storage bottlenecks. The HPE 16GB NVDIMM for HPE ProLiant Gen10 servers is ideal for smaller database storage bottlenecks, write caching tiers, and any workload constrained by storage bottlenecks.

The HPE 16GB NVDIMM is supported on select ProLiant Gen10 servers and can support up to 12 NVDIMMs in 2 socket servers (up to 192GB) and up to 24 NVDIMMs in 4 socket servers (up to 384GB). The HPE Smart Storage Battery provides backup power to the memory slots allowing data to be moved from the DRAM portion of the NVDIMM to the Flash portion for persistence during a power down event.

For more information on HPE NVDIMMs, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/persistentmemory**).

Server requirements for NVDIMM support

Before installing an HPE 16GB NVDIMM in a server, make sure that the following components and software are available:

- A supported HPE server using Intel Xeon Scalable Processors: For more information, see the NVDIMM QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**).
- An HPE Smart Storage Battery
- A minimum of one regular DIMM: The system cannot have only NVDIMM-Ns installed.

- A supported operating system with persistent memory/NVDIMM drivers. For the latest software information, see the Hewlett Packard Enterprise website (**http://persistentmemory.hpe.com**).
- For minimum firmware versions, see the HPE 16GB NVDIMM User Guide on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/nvdimm-docs**).

To determine NVDIMM support for your server, see the server QuickSpecs on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/qs**).

Installing an NVDIMM

⚠ **CAUTION:**

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

⚠ **CAUTION:**

To avoid damage to the hard drives, memory, and other system components, be sure to install the correct DIMM baffles for your server model.

⚠ **CAUTION:**

DIMMs are keyed for proper alignment. Align notches in the DIMM with the corresponding notches in the DIMM slot before inserting the DIMM. Do not force the DIMM into the slot. When installed properly, not all DIMMs will face in the same direction.

⚠ **CAUTION:**

Electrostatic discharge can damage electronic components. Be sure you are properly grounded before beginning this procedure.

⚠ **CAUTION:**

Failure to properly handle DIMMs can damage the DIMM components and the system board connector. For more information, see the DIMM handling guidelines in the troubleshooting guide for your product on the Hewlett Packard Enterprise website:

- HPE ProLiant Gen10 (**http://www.hpe.com/info/gen10-troubleshooting**)
- HPE Synergy (**http://www.hpe.com/info/synergy-troubleshooting**)

⚠ **CAUTION:**

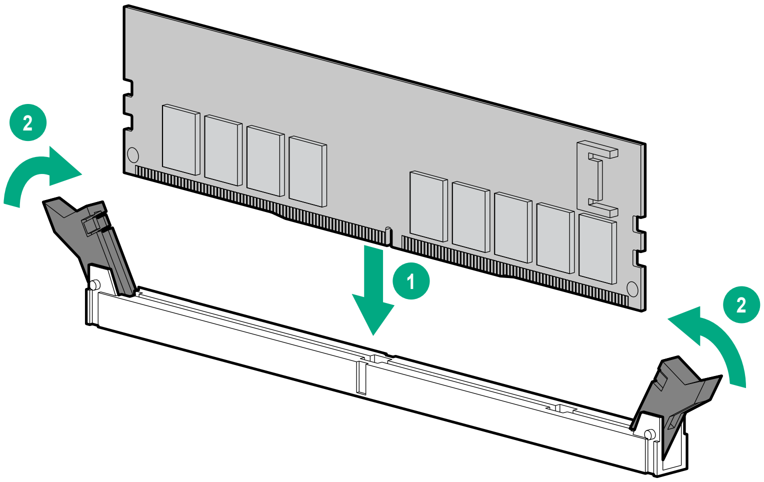
Unlike traditional storage devices, NVDIMMs are fully integrated in with the ProLiant server. Data loss can occur when system components, such as the processor or HPE Smart Storage Battery, fails. HPE Smart Storage battery is a critical component required to perform the backup functionality of NVDIMMs. It is important to act when HPE Smart Storage Battery related failures occur. Always follow best practices for ensuring data protection.

Prerequisites

Before installing an NVDIMM, be sure the server meets the **Server requirements for NVDIMM support** on page 141.

Procedure

1. **Power down the server**.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Do one of the following:
   a. **Extend the server from the rack**.
   b. **Remove the server from the rack**.
4. **Remove the access panel**.
5. If the Smart Storage battery is not installed, do one of the following:
   - **Remove the air baffle**.
   - **If installed on LFF models, remove the midplane drive cage.**
6. Locate any NVDIMMs already installed in the server.
7. Verify that all LEDs on any installed NVDIMMs are off.
8. Install the NVDIMM.



9. If it is not already installed, **install the Smart Storage battery**.
10. **Install the access panel**.
11. Slide or install the server into the rack.
12. Connect each power cord to the server.
13. **Power up the server**.
14. If required, sanitize the NVDIMM-Ns. For more information, see **NVDIMM sanitization** on page 144.

Configuring the server for NVDIMMs

After installing NVDIMMs, configure the server for NVDIMMs. For information on configuring settings for NVDIMMs, see the *HPE 16GB NVDIMM User Guide* on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/nvdimm-docs**).

The server can be configured for NVDIMMs using either of the following:

- UEFI System Utilities—Use System Utilities through the Remote Console to configure the server for NVDIMM memory options by pressing the **F9** key during POST. For more information about UEFI System Utilities, see the Hewlett Packard Enterprise website (**http://www.hpe.com/info/uefi/docs**).
- iLO RESTful API for HPE iLO 5—For more information about configuring the system for NVDIMMs, see **https://hewlettpackard.github.io/ilo-rest-api-docs/ilo5/**.

NVDIMM sanitization

Media sanitization is defined by NIST SP800-88 Guidelines for Media Sanitization (Rev 1, Dec 2014) as "a general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means."

The specification defines the following levels:

- Clear: Overwrite user-addressable storage space using standard write commands; might not sanitize data in areas not currently user-addressable (such as bad blocks and overprovisioned areas)
- Purge: Overwrite or erase all storage space that might have been used to store data using dedicated device sanitize commands, such that data retrieval is "infeasible using state-of-the-art laboratory techniques"
- Destroy: Ensure that data retrieval is "infeasible using state-of-the-art laboratory techniques" and render the media unable to store data (such as disintegrate, pulverize, melt, incinerate, or shred)

The NVDIMM-N Sanitize options are intended to meet the Purge level.

For more information on sanitization for NVDIMMs, see the following sections in the *HPE 16GB NVDIMM User Guide* on the Hewlett Packard Enterprise website (**http://www.hpe.com/info/nvdimm-docs**):

- NVDIMM sanitization policies
- NVDIMM sanitization guidelines
- Setting the NVDIMM-N Sanitize/Erase on the Next Reboot Policy

NIST SP800-88 *Guidelines for Media Sanitization* (Rev 1, Dec 2014) is available for download from the NIST website (**http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf**).

NVDIMM relocation guidelines

Requirements for relocating NVDIMMs or a set of NVDIMMs when the data must be preserved

- The destination server hardware must match the original server hardware configuration.
- All System Utilities settings in the destination server must match the original System Utilities settings in the original server.
- If NVDIMM-Ns are used with NVDIMM Interleaving ON mode in the original server, do the following:

- ◦ Install the NVDIMMs in the same DIMM slots in the destination server.
- ◦ Install the entire NVDIMM set (all the NVDIMM-Ns on the processor) on the destination server.

This guideline would apply when replacing a system board due to system failure.

If any of the requirements cannot be met during NVDIMM relocation, do the following:

- ◦ Manually back up the NVDIMM-N data before relocating NVDIMM-Ns to another server.
- ◦ Relocate the NVDIMM-Ns to another server.
- ◦ Sanitize all NVDIMM-Ns on the new server before using them.

Requirements for relocating NVDIMMs or a set of NVDIMMs when the data does not have to be preserved

If data on the NVDIMM-N or set of NVDIMM-Ns does not have to be preserved, then

- Move the NVDIMM-Ns to the new location and sanitize all NVDIMM-Ns after installing them to the new location. For more information, see **NVDIMM sanitization** on page 144.
- Observe all DIMM and NVDIMM population guidelines. For more information, see **DIMM and NVDIMM population information** on page 140.
- Observe the process for removing an NVDIMM.
- Observe the process for installing an NVDIMM.
- Review and configure the system settings for NVDIMMs. For more information, see **Configuring the server for NVDIMMs** on page 144.

HPE Scalable Persistent Memory (CTO only)

HPE Scalable Persistent Memory is an integrated storage solution that runs at memory speeds with terabyte capacity unlocking new levels of performance for your business workloads. It provides a complete hardware and software solution utilizing the following components:

- DRAM for application performance
- A tier of flash for persistence
- A backup power source to move data from DRAM to flash

HPE Scalable Persistent Memory is ideal for enabling in-memory compute with persistence and any workload that could benefit from low-latency DRAM-level performance. This option is available as HPE Factory Configure To Order (CTO) SKUs only.

For configuration details for HPE Scalable Persistent Memory, see the *HPE Scalable Persistent Memory User Guide* at **http://www.hpe.com/info/nvdimm-docs**.

For more information about HPE Scalable Persistent Memory, see **http://www.hpe.com/info/persistentmemory**.

Controller options

The server supports the following storage controllers:

- Embedded controllers

  Enabled through System Utilities and configured through HPE Smart Storage Administrator (Intelligent Provisioning)

- Type-a controllers

  Type-a controllers install in the type-a smart array connector.

- Type-p controllers

  Type-p controllers install in a PCIe expansion slot

Installing a storage controller

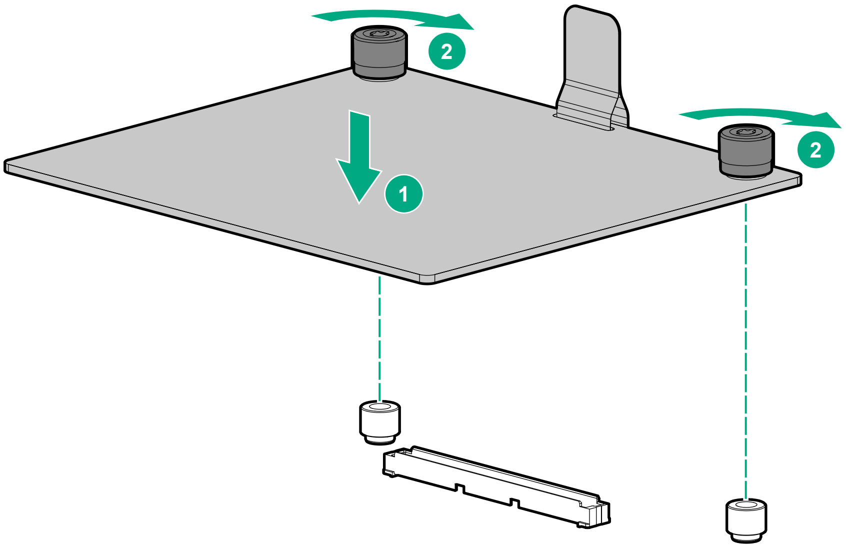
Prerequisites

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

The components included with the hardware option kit

Procedure

1. **Power down the server**.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Do one of the following:
   - **Extend the server from the rack**.
   - **Remove the server from the rack**.
4. **Remove the access panel**.
5. Do one of the following:
   - **Remove the air baffle**.
   - **If installed, remove the 4LFF midplane drive cage**.
6. Do one of the following:
   - For Type-a Smart Array controllers, install the controller into the Smart Array connector.



- For Type-p Smart Array controllers, **install the controller into an expansion slot**.

7. **Cable the controller**.

The installation is complete.

Installing a midplane 4LFF SAS/SATA drive cage

Observe the following:

- A 1U heatsink is required for each processor when installing this option.
- If you have a TPM, install it prior to this option.
- If you have a type-a controller, install it prior to this option.

Prerequisites

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

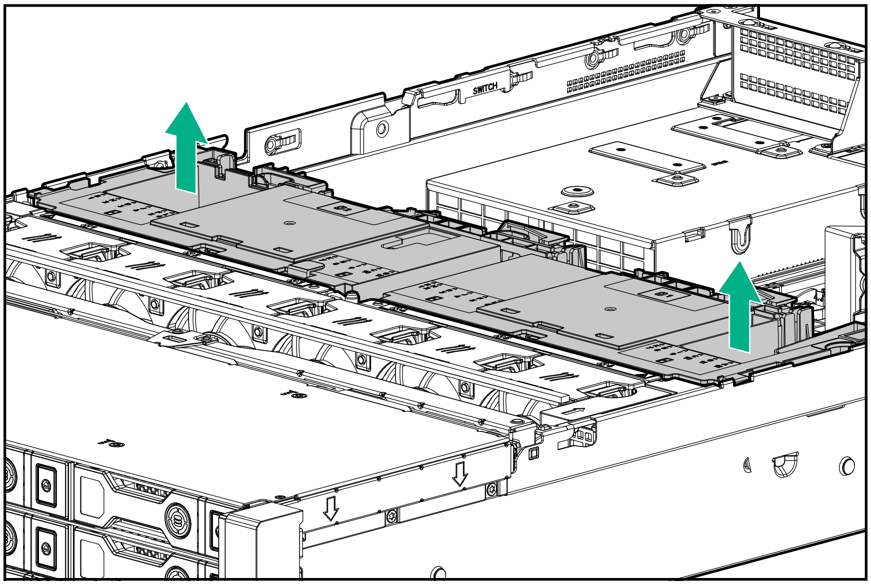
The components included with the hardware option kit

Procedure

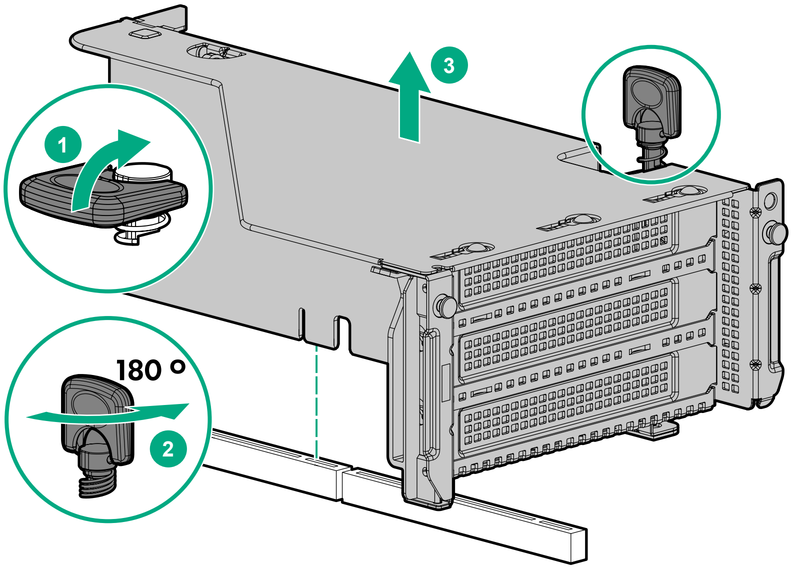
1. **Power down the server**.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Do one of the following:

- **Extend the server from the rack**.
- **Remove the server from the rack**.

4. **Remove the access panel**.
5. **Remove the air baffle**.
   The air baffle is no longer needed. The drive cage acts as an air baffle for the server.



6. Remove all riser cages.



7. Connect the power cable to the drive backplane power connector on the system board.
8. If connecting the data cable to the system board or a controller, connect the data cable.
9. Prepare the drive cage for installation by lifting the latches on the drive cage.
10. Install the drive cage:

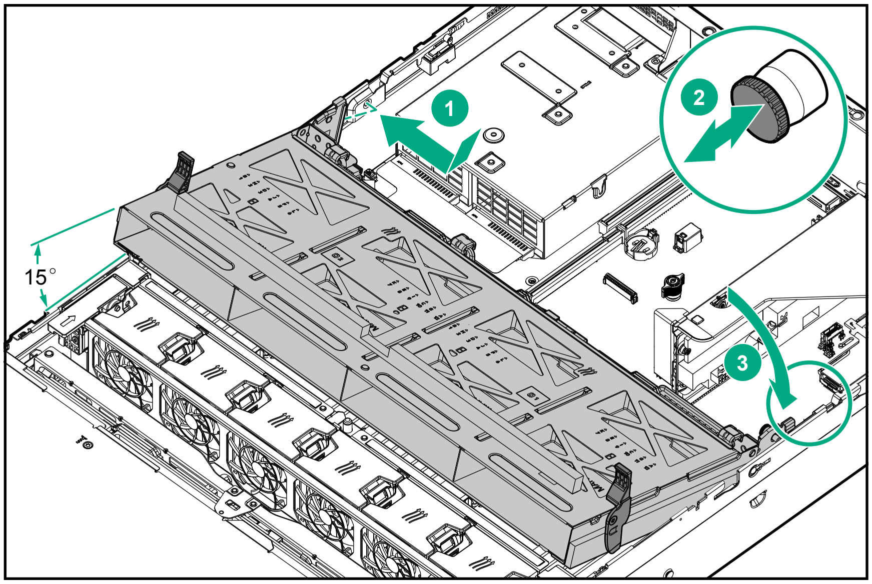
CAUTION:
Do not drop the drive cage on the system board. Dropping the drive cage on the system board might damage the system or components. Remove all drives and use two hands when installing or removing the drive cage.

a. Locate the alignment pins on the rear of the drive cage.

b. Align the pin on the rear left of the drive cage to the server and then insert the pin.

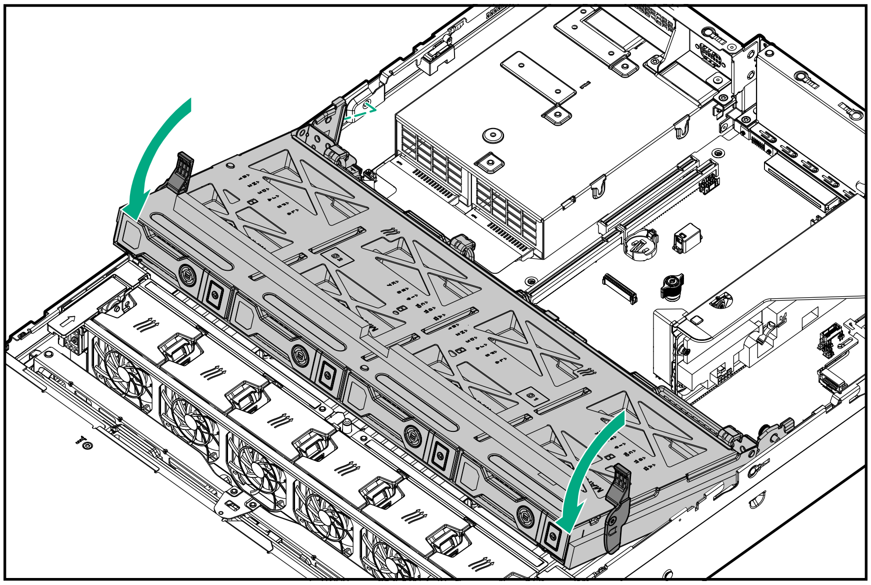
c. Gently lower the opposite side of the drive cage.

d. Pull the plunger pin on the rear right of the drive cage and then lower the drive cage until the plunger pin engages.



11. Install drives or drive blanks.

12. Push down on the latches to lower the drive cage into place.



13. Connect the power and data cables to the drive backplane.

The installation is complete.

Installing a rear 2SFF SAS/SATA drive cage in the primary or secondary riser

Prerequisites

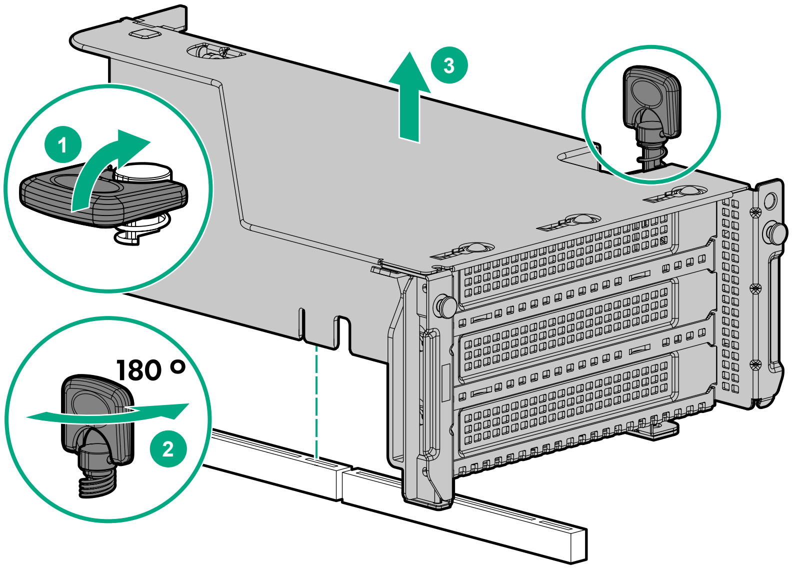
Before installing this option, be sure that you have the following:

- T-10 Torx screwdriver
- The components included with the hardware option kit
- The front drive bays are fully populated with 12 LFF or 24 SFF drives.
- High performance fans are installed in all fan bays.

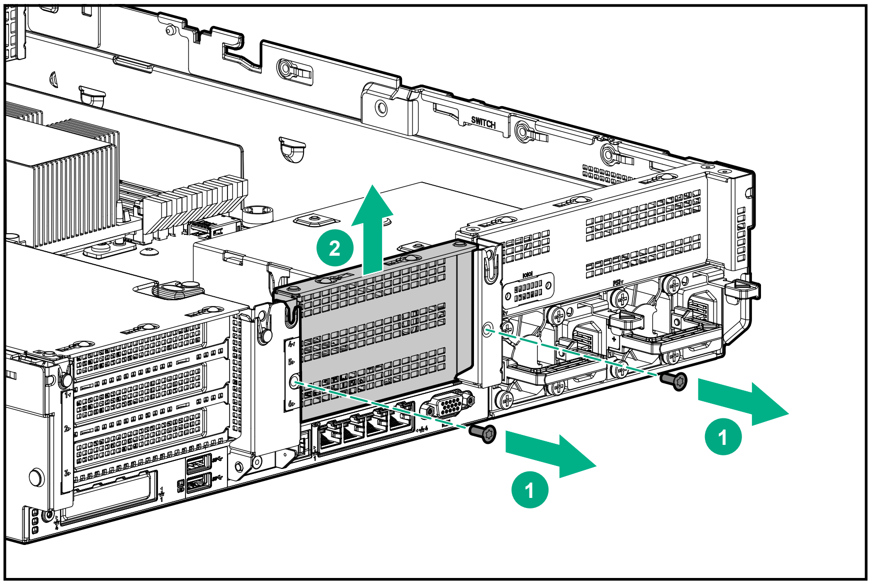
Procedure

1. **Power down the server**.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Do one of the following:
   - **Extend the server from the rack**.
   - **Remove the server from the rack** .
4. **Remove the access panel**.
5. Do one of the following:

For primary bays, remove the riser cage.

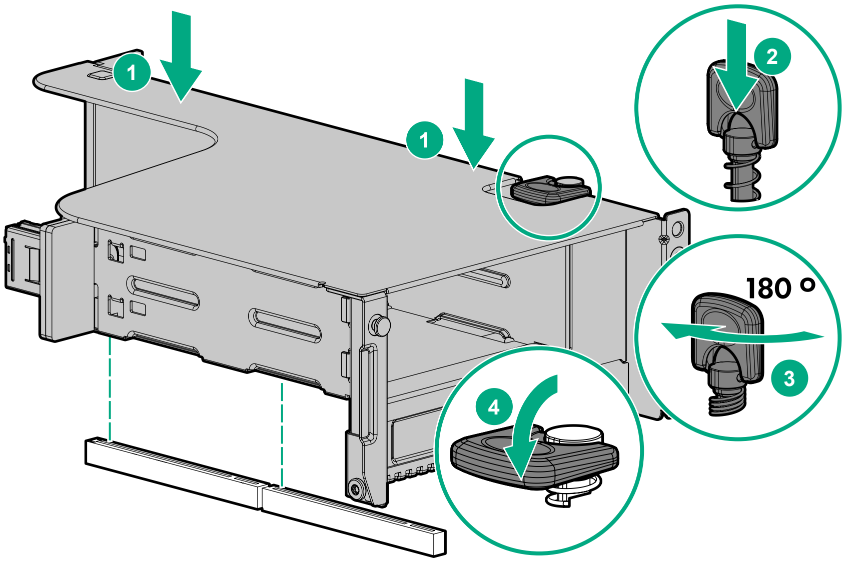


For secondary bays, remove the rear wall blank.



6. **Install a SAS expander or other expansion card, if needed**.

7. Install the drive cage.



8. **Cable the drive backplane**.
9. **Install drives or drive blanks**.
10. **Install the access panel**.
11. Slide the server into the rack.
12. Connect each power cord to the server.
13. Connect each power cord to the power source.
14. **Power up the server**.

The installation is complete.

Installing a rear 2SFF SAS/SATA drive cage over the power supplies

Prerequisites

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

- T-10 Torx screwdriver
- The components included with the hardware option kit
- The front bays are fully populated with 12 LFF or 24 SFF drives
- High performance fans are installed in all fan bays

Procedure

1. **Power down the server**.
2. Remove all power:

a. Disconnect each power cord from the power source.

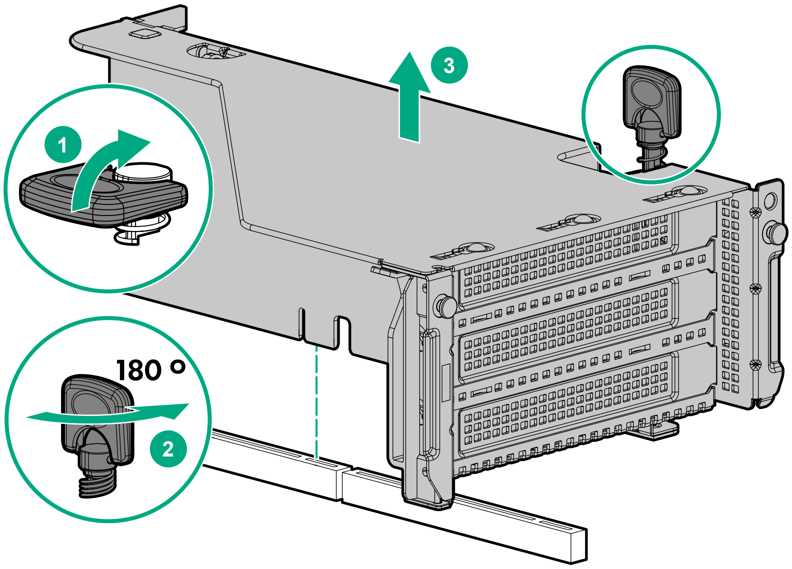
b. Disconnect each power cord from the server.

3. Do one of the following:

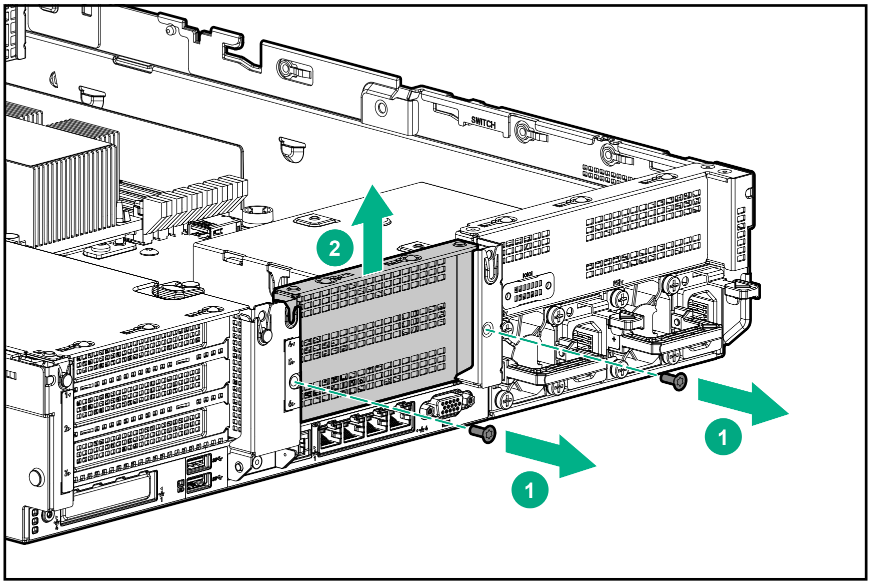
   - **Extend the server from the rack**.
   - **Remove the server from the rack** .

4. **Remove the access panel**.

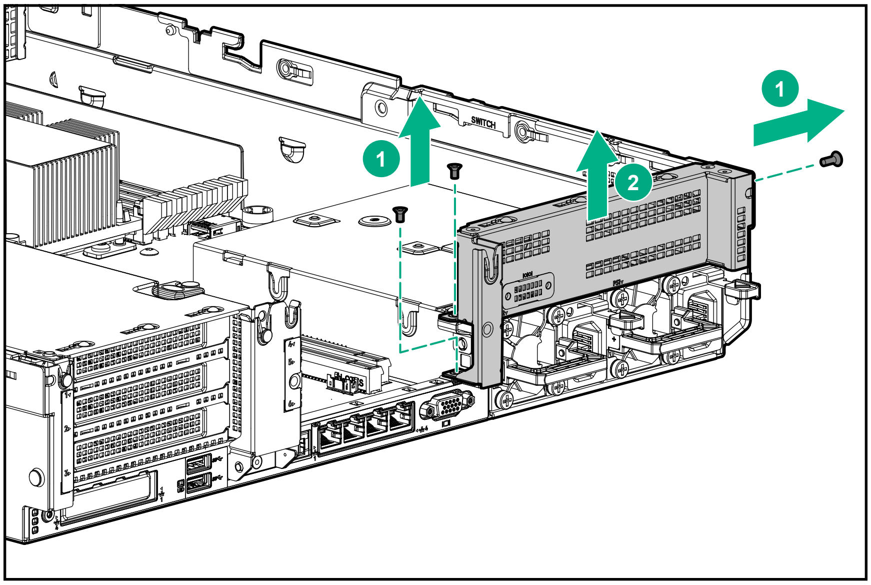
5. Do one of the following:
   If installed, remove the secondary riser cage.



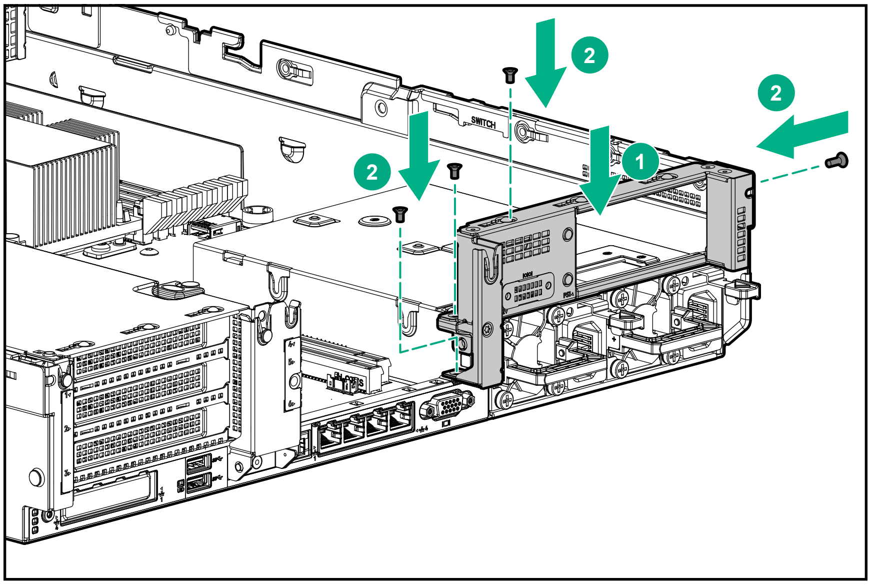
Remove the secondary wall blank.



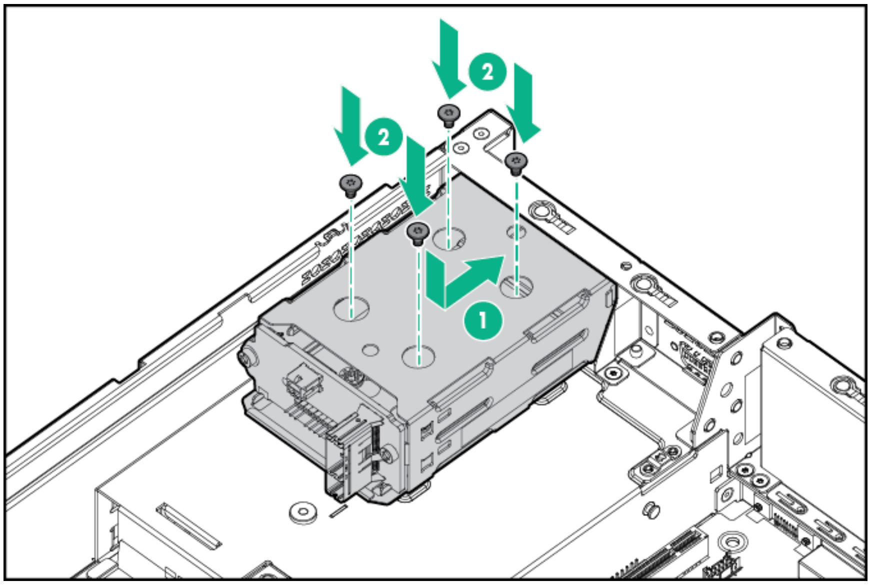
6. Remove the tertiary wall blank.



7. Install the drive cage compatible rear wall.



8. Install the drive cage.



9. Install drives or drive blanks.
10. Install the secondary rear wall or a riser cage.
11. **Cable the drive backplane**.
12. **Install the access panel**.
13. Slide the server into the rack.
14. Connect each power cord to the server.
15. Connect each power cord to the power source.
16. **Power up the server**.

The installation is complete.

Installing a secondary riser cage

Prerequisites

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

- The components included with the hardware option kit
- T-10 Torx screwdriver

Procedure

1. Observe the following alert:

> **CAUTION:**
> To prevent damage to the server or expansion boards, power down the server and remove all AC power cords before removing or installing the PCI riser cage.

2. **Power down the server**.
3. Remove all power:

a. Disconnect each power cord from the power source.

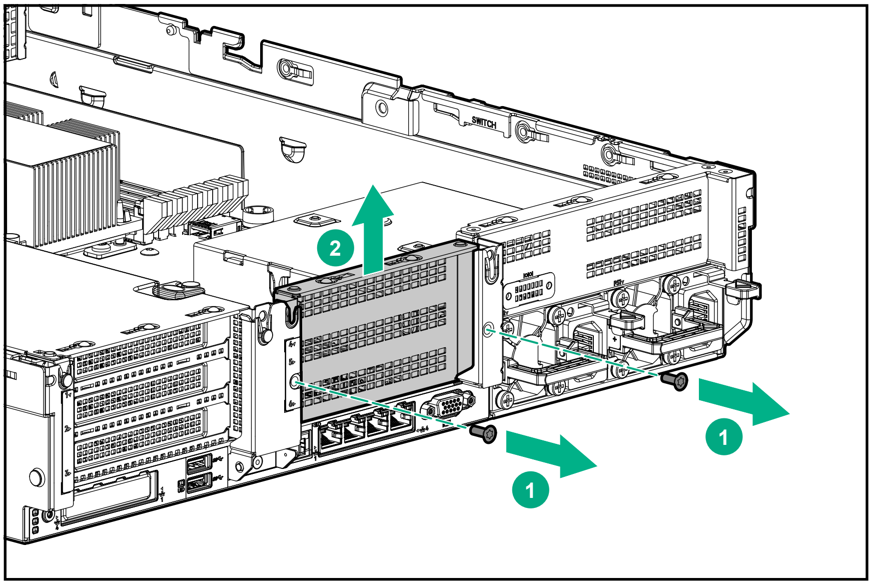
b. Disconnect each power cord from the server.

4. Do one of the following:

   - **Extend the server from the rack**.
   - **Remove the server from the rack**.

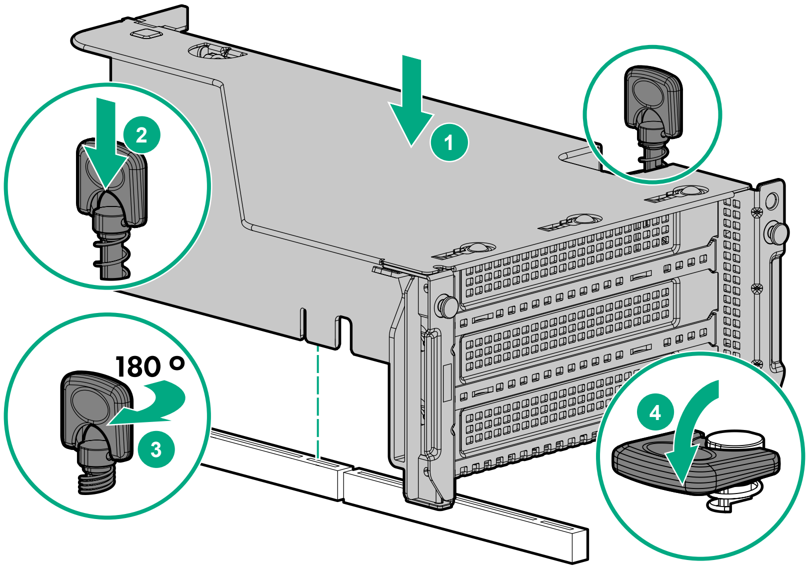
5. **Remove the access panel**.

6. Remove the rear wall blank.



7. **Install any expansion boards, if needed**.

8. Install the riser cage:



The installation is complete.

Installing a 12G SAS Expander Card

- For 24SFF configurations, install 8SFF front drive cages in boxes 1 and 2.
- For configurations including a 2SFF rear drive cage, install the drive cage over the power supplies.
- HPE recommends installing the SAS expander card into slot 3 of the primary PCIe riser expansion card.
- To ensure that cables are connected correctly, observe the labels on the cable and port.
- Be sure that you have the latest firmware for the controllers and the expander card. To download the latest firmware, see the **Hewlett Packard Enterprise website**.

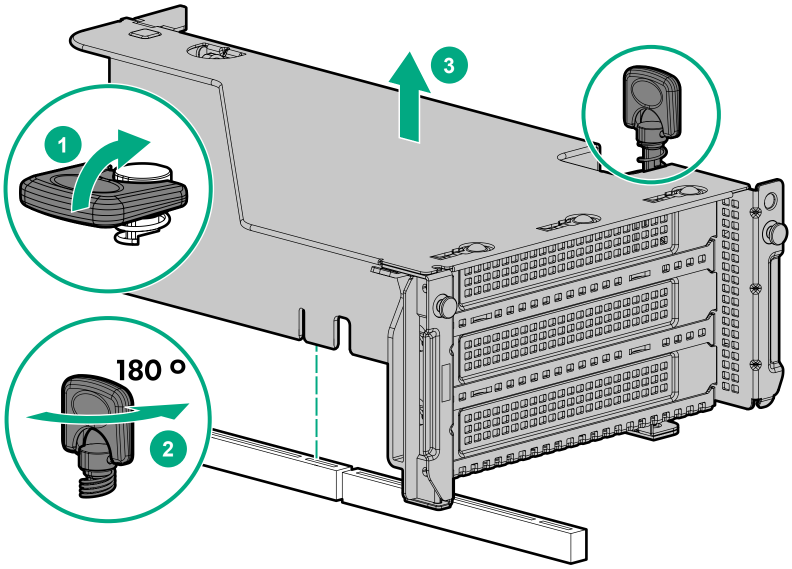
Prerequisites

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

- The components included with the hardware option kit
- Storage cables for each drive box
- A storage controller

Procedure

1. **Power down the server**.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Do one of the following:
   - **Extend the server from the rack**.
   - **Remove the server from the rack** .
4. **Remove the access panel**.
5. **Remove the air baffle**.
6. **Remove the fan cage**.
7. Remove the riser cage.



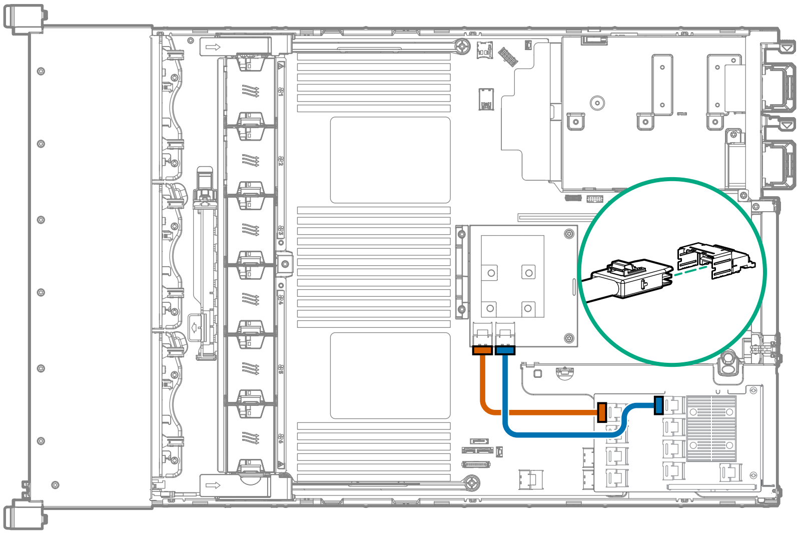
8. Locate slot 3, and then **remove the expansion slot blank**.
9. **Install the 12G SAS expander card**.

    IMPORTANT:
    The 12G SAS expander card requires a controller. The server supports embedded, type-a, and type-p Smart Array controllers. If using a type-p Smart Array controller, then install the controller in slot 1.

10. Using the labels on each cable, connect the cables to the SAS expander.

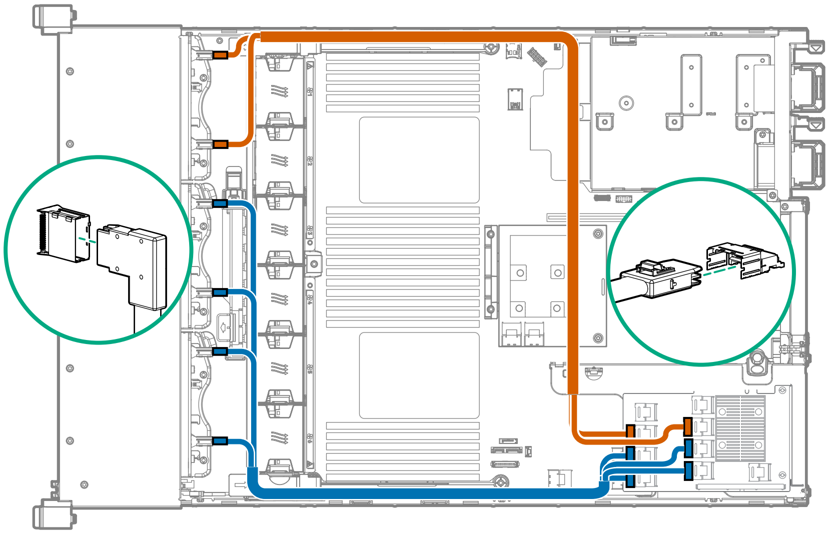
    For drive numbering, see "**Drive bay numbering: SAS expander** on page 129".

11. **Install the riser cage**.
12. **Connect cables from the 12G SAS expander to the controller**.



13. **Connect cables from the 12G SAS expander to the drive backplanes**.

    A standard configuration is shown. For additional cabling diagrams, see "**#unique_226**".



14. **Install the fan cage**.

15. **Install the air baffle**.

16. **Install the access panel**.

17. **Install the server into the rack**.

18. Connect each power cord to the server.

19. Connect each power cord to the power source.

20. **Power up the server** .

The installation is complete.

Installing a Smart Storage Battery

Prerequisites

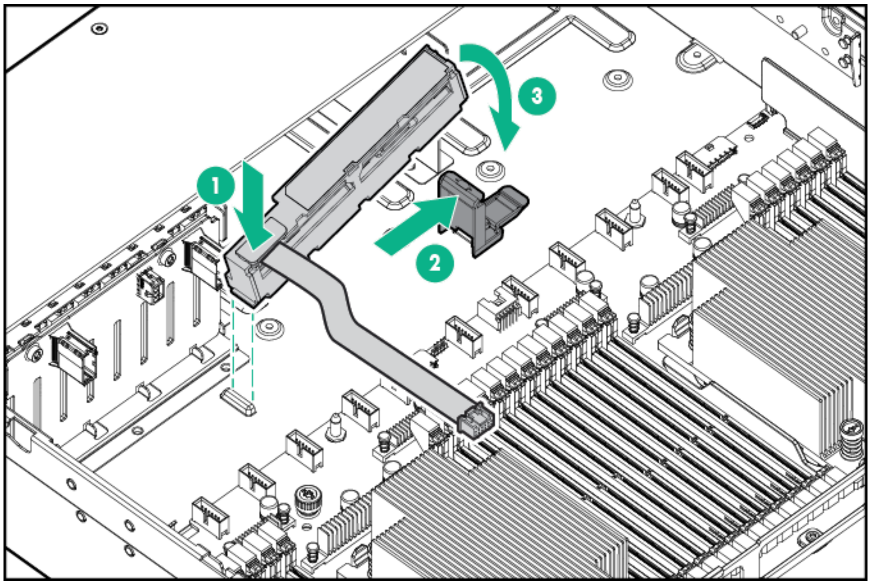
Before installing this option, be sure that you have the following:

The components included with the hardware option kit

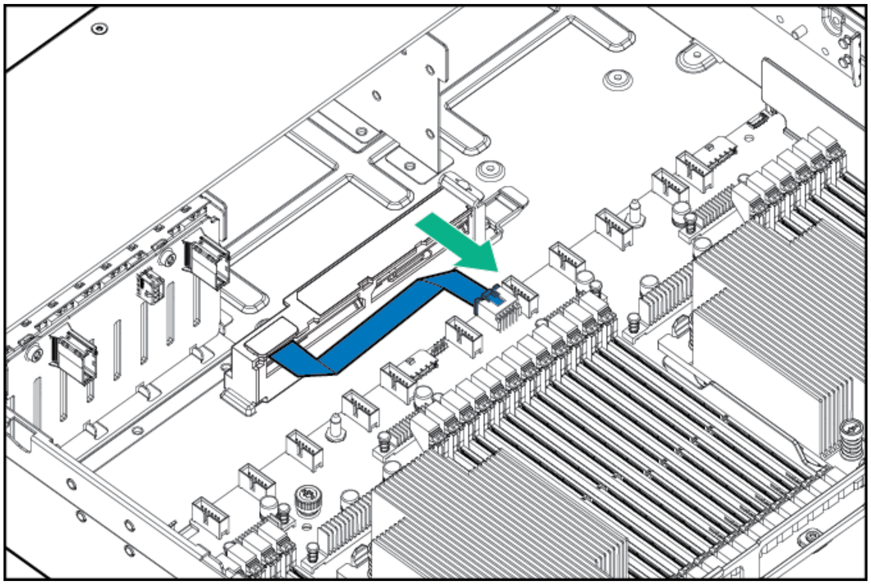
Procedure

1. **Power down the server** .
2. Do one of the following:
   - Disconnect each power cord from the power source.
   - Disconnect each power cord from the server.
3. Do one of the following:
   - **Extend the server from the rack**.
   - **Remove the server from the rack**.

4. **Remove the access panel**.
5. Do one of the following:
   - **Remove the air baffle**.
   - **If installed on LFF models, remove the midplane drive cage.**
6. Install the Smart Storage battery.



7. Install the cable.



8. Install the fan cage.
9. **Install the air baffle**.
10. **Install the access panel**.
11. Slide the server into the rack.
12. Connect each power cord to the server.

13. Connect each power cord to the power source.

14. **Power up the server** .

The installation is complete.

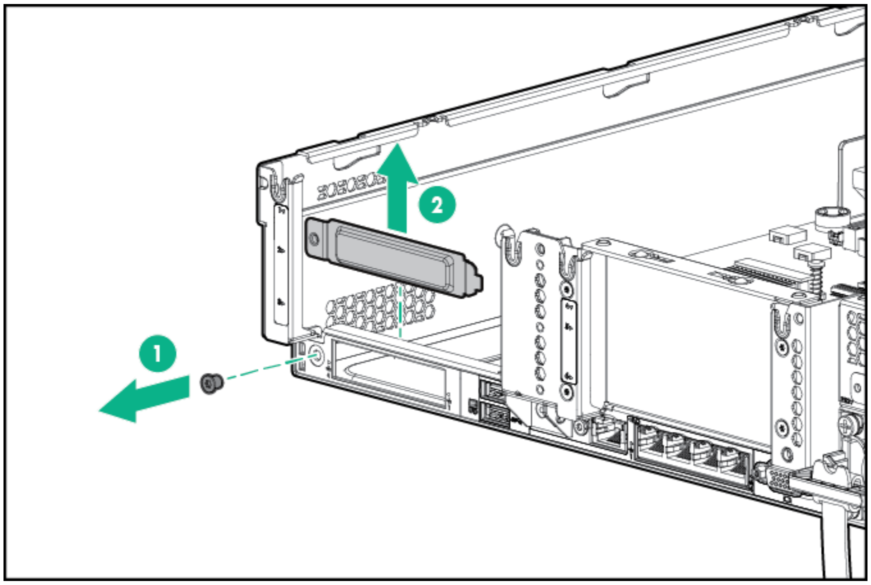
Installing a FlexibleLOM adapter

Prerequisites

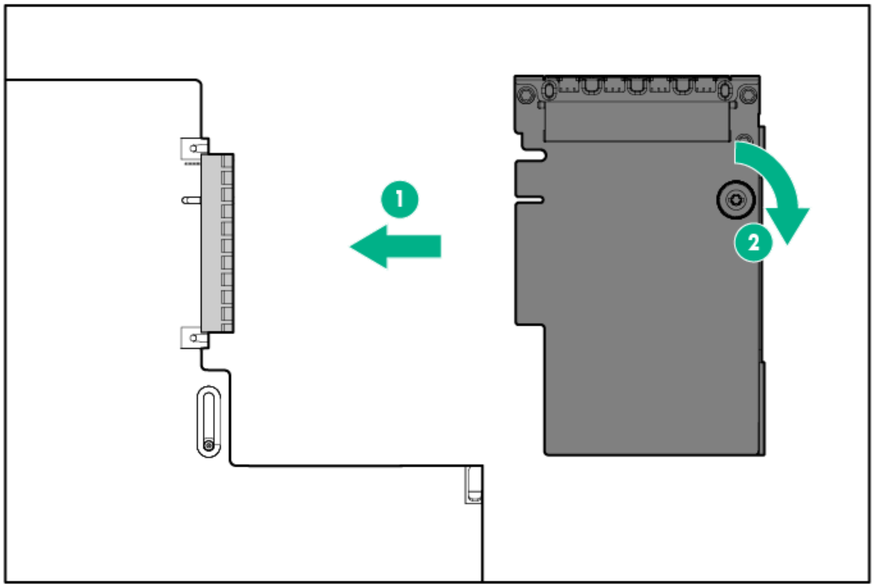
- The components included with the hardware option kit
- A T-10 Torx screwdriver might be needed to unlock the access panel.

Procedure

1. **Power down the server** .
2. Do one of the following:
   - Disconnect each power cord from the power source.
   - Disconnect each power cord from the server.
3. Do one of the following:
   - **Extend the server from the rack**.
   - **Remove the server from the rack**.
4. **Remove the access panel**.
5. **Remove the primary riser cage**.
6. Remove the FlexibleLOM blank.



7. Install the FlexibleLOM adapter:



8. Install the riser cage.
9. **Install the access panel**.
10. Slide the server into the rack.
11. Connect the LAN segment cables.
12. Connect each power cord to the server.
13. Connect each power cord to the power source.
14. **Power up the server** .

The installation is complete.

Installing a processor

Observe the following:

- Before performing this procedure, HPE recommends **identifying the processor-heatsink module components**.
- Intelligent System Tuning supports specific processors and configurations. For more information, see the product QuickSpecs on the HPE website.

Prerequisites

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

- The components included with the hardware option kit
- T-30 Torx screwdriver

Procedure

1. Observe the following alerts.

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

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

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

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

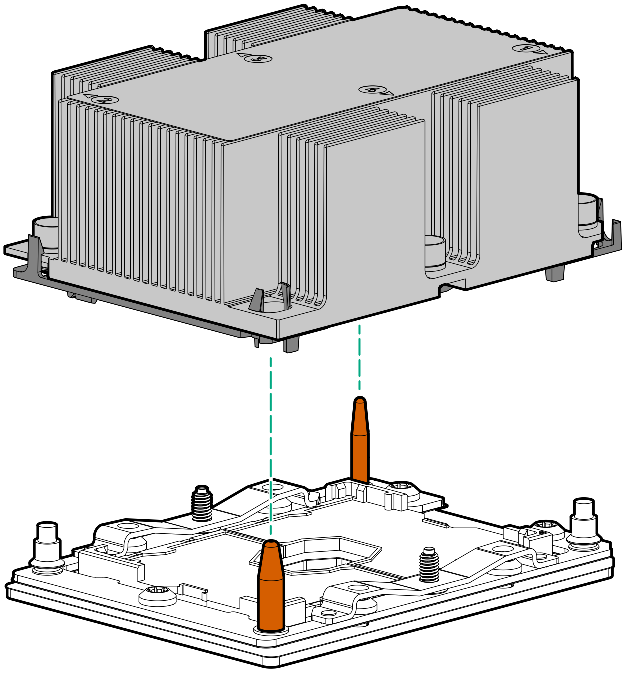
   To download firmware and view installation instructions, see the **Hewlett Packard Enterprise Support Center website**.

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

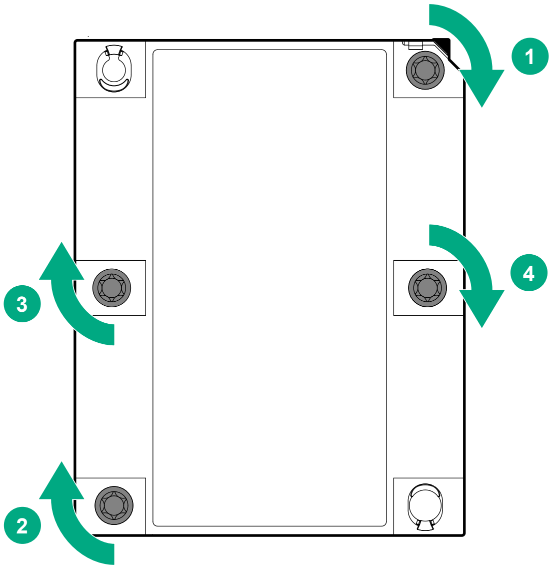
2. **Power down the server**.
3. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
4. Do one of the following:
   - **Extend the server from the rack**.
   - **Remove the server from the rack**.
5. **Remove the access panel**.
6. Do one of the following:
   - **Remove the air baffle**.
   - **If installed, remove the 4LFF midplane drive cage**.
7. Install the processor heatsink assembly:
   a. Remove the dust cover.
   b. Locate the Pin 1 indicator on the processor frame and the socket.
   c. Align the processor heatsink assembly with the alignment posts and gently lower it down until it sits evenly on the socket.

The heatsink alignment posts are keyed. The processor will only install one way.

A standard heatsink is shown. Your heatsink might look different.



d. Using a T-30 Torx screwdriver, tighten the nuts until they stop.



The installation is complete.

HPE Trusted Platform Module 2.0 Gen10 option

Overview

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

This procedure includes three sections:

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

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

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

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

HPE Trusted Platform Module 2.0 Guidelines

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

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

- Do not remove an installed TPM. Once installed, the TPM is bound to the system board. If an OS is configured to use the TPM and it is removed, the OS may go into recovery mode, data loss can occur, or both.
- When installing or replacing hardware, Hewlett Packard Enterprise service providers cannot enable the TPM or the encryption technology. For security reasons, only the customer can enable these features.
- When returning a system board for service replacement, do not remove the TPM from the system board. When requested, Hewlett Packard Enterprise Service provides a TPM with the spare system board.
- Any attempt to remove the cover of an installed TPM from the system board can damage the TPM cover, the TPM, and the system board.
- If the TPM is removed from the original and powered up on a different , data stored in the TPM including keys will be erased.

- When using BitLocker, always retain the recovery key/password. The recovery key/password is required to complete Recovery Mode after BitLocker detects a possible compromise of system integrity or system configuration.
- Hewlett Packard Enterprise is not liable for blocked data access caused by improper TPM use. For operating instructions, see the TPM documentation or the encryption technology feature documentation provided by the operating system.

Installing and enabling the HPE TPM 2.0 Gen10 Kit

Installing the Trusted Platform Module board

Preparing the server for installation

Procedure

1. Observe the following warnings:

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

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

2. Update the system ROM.

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

3. Power down the server (**#unique_198**).
4. Remove all power:

   a. Disconnect each power cord from the power source.

   b. Disconnect each power cord from the server.

5. Do one of the following:

   - Extend the server from the rack.
   - Remove the server from the rack.

6. Place the server on a flat, level work surface.
7. **Remove the access panel**.
8. Do one of the following:

- **Remove the air baffle**.
- **If installed, remove the 4LFF midplane drive cage**.

9. Remove any components or cables that may prevent access to the TPM connector.
10. Proceed to **Installing the TPM board and cover** on page 167.

Installing the TPM board and cover

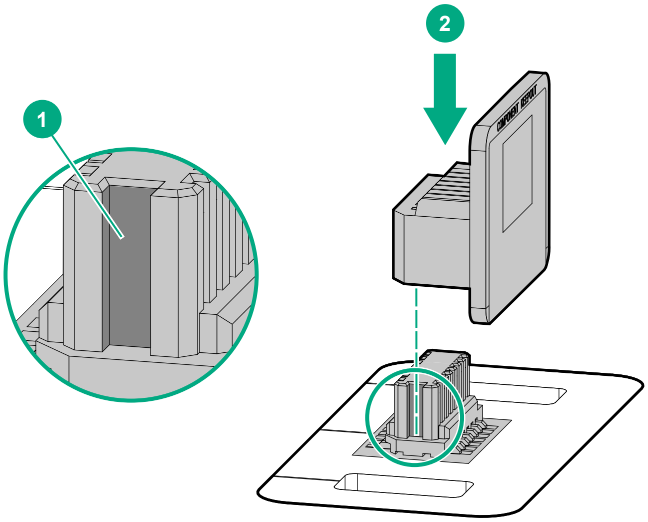
Procedure

1. Observe the following alerts:

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

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

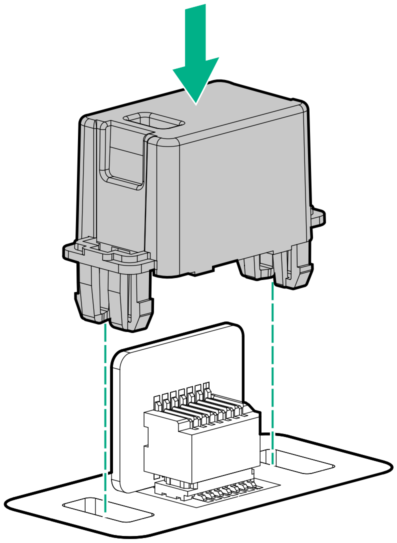
2. Align the TPM board with the key on the connector, and then install the TPM board. To seat the board, press the TPM board firmly into the connector. To locate the TPM connector on the system board, see the server label on the access panel.



3. Install the TPM cover:

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

   b. To snap the cover into place, firmly press straight down on the middle of the cover.



4. Proceed to **#unique_238**.

Preparing the server for operation

Procedure

1. Install any options or cables previously removed to access the TPM connector.
2. Do one of the following:
    - **Install the air baffle**.
    - **Install the 4LFF midplane drive cage**.
3. **Install the access panel**.
4. Install the server in the rack.
5. Connect power cords to the server.
6. Press the Power On/Standby button.

Enabling the Trusted Platform Module

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

- By default, the Trusted Platform Module is enabled as TPM 2.0 when the is powered on after installing it.
- In UEFI Boot Mode, the Trusted Platform Module can be configured to operate as TPM 2.0 or TPM 1.2.
- In Legacy Boot Mode, the Trusted Platform Module configuration can be changed between TPM 1.2 and TPM 2.0, but only TPM 1.2 operation is supported.

Enabling the Trusted Platform Module as TPM 2.0

Procedure

1. During the startup sequence, press the **F9** key to access **System Utilities**.
2. From the System Utilities screen, select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module options**.
3. Verify the following:
   - "Current TPM Type" is set to **TPM 2.0**.
   - "Current TPM State" is set to **Present and Enabled**.
   - "TPM Visibility" is set to **Visible**.
4. If changes were made in the previous step, press the **F10** key to save your selection.
5. If F10 was pressed in the previous step, do one of the following:
   - If in graphical mode, click **Yes**.
   - If in text mode, press the **Y** key.
6. Press the **ESC** key to exit System Utilities.
7. If changes were made and saved, the prompts for reboot request. Press the **Enter** key to confirm reboot.

   If the following actions were performed, the reboots a second time without user input. During this reboot, the TPM setting becomes effective.
   - Changing from TPM 1.2 and TPM 2.0
   - Changing TPM bus from FIFO to CRB
   - Enabling or disabling TPM
   - Clearing the TPM
8. Enable TPM functionality in the OS, such as Microsoft Windows BitLocker or measured boot.

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

Enabling the Trusted Platform Module as TPM 1.2

Procedure

1. During the startup sequence, press the **F9** key to access **System Utilities**.
2. From the System Utilities screen select **System Configuration** > **BIOS/Platform Configuration (RBSU)** > **Server Security** > **Trusted Platform Module options**.
3. Change the "TPM Mode Switch Operation" to **TPM 1.2**.
4. Verify "TPM Visibility" is **Visible**.
5. Press the **F10** key to save your selection.
6. When prompted to save the change in System Utilities, do one of the following:

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

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

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

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

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

Retaining the recovery key/password

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

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

- Always store the recovery key/password in multiple locations.
- Always store copies of the recovery key/password away from the system.
- Do not save the recovery key/password on the encrypted hard drive.

HPE Software and Configuration utilities

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

Active Health System

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

The Active Health System provides:

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

For more information about the Active Health System, see *iLO user guide* on the Hewlett Packard Enterprise website.

HPE iLO 5

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

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

For more information about iLO, see *iLO user guide* on the Hewlett Packard Enterprise website.

HPE Smart Storage Administrator

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

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

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

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

Accessing HPE SSA in the offline environment

IMPORTANT:

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

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

Accessing HPE SSA in the online environment

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

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

Websites

General websites

Hewlett Packard Enterprise Information Library

www.hpe.com/info/EIL

Single Point of Connectivity Knowledge (SPOCK) Storage compatibility matrix

www.hpe.com/storage/spock

Storage white papers and analyst reports

www.hpe.com/storage/whitepapers

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

Support and other resources

Accessing Hewlett Packard Enterprise Support

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

  http://www.hpe.com/assistance

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

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

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

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

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

- To subscribe to eNewsletters and alerts:

  www.hpe.com/support/e-updates

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

  www.hpe.com/support/AccessToSupportMaterials

ⓘ **IMPORTANT:**

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

Customer self repair

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

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

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

Remote support

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

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

Remote support and Proactive Care information

HPE Get Connected

www.hpe.com/services/getconnected

HPE Proactive Care services

www.hpe.com/services/proactivecare

HPE Proactive Care service: Supported products list

www.hpe.com/services/proactivecaresupportedproducts

HPE Proactive Care advanced service: Supported products list

www.hpe.com/services/proactivecareadvancedsupportedproducts

Proactive Care customer information

Proactive Care central

www.hpe.com/services/proactivecarecentral

Proactive Care service activation

www.hpe.com/services/proactivecarecentralgetstarted

Warranty information

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

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

Additional warranty information

HPE ProLiant and x86 Servers and Options

www.hpe.com/support/ProLiantServers-Warranties

HPE Enterprise Servers

www.hpe.com/support/EnterpriseServers-Warranties

HPE Storage Products

www.hpe.com/support/Storage-Warranties

HPE Networking Products

www.hpe.com/support/Networking-Warranties

Regulatory information

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

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

Additional regulatory information

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

www.hpe.com/info/reach

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

www.hpe.com/info/ecodata

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

www.hpe.com/info/environment

Documentation feedback

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

Appendix

Roles And Features	Installed
Active Directory Lightweight Directory Services	
DHCP Server	
DNS Server	
File And Storage Services	Yes
File and iSCSI Services	Yes
File Server	Yes
BranchCache for Network Files	Yes
Data Deduplication	Yes
DFS Namespaces	Yes
DFS Replication	Yes
File Server Resource Manager	Yes
File Server VSS Agent Service	Yes
iSCSI Target Server	Yes
Work Folders	Yes
iSCSI Target Storage Provider (VDS and V	Yes
Server for NFS	Yes
Storage Services	Yes
Hyper-V	
Print and Document Services	Yes
Print Server	Yes
Distributed Scan Server	
Internet Printing	
LPD Service	
Web Server (IIS)	Yes
Web Server	Yes
Common HTTP Features	Yes
Default Document	Yes
Directory Browsing	Yes
HTTP Errors	Yes
Static Content	Yes
HTTP Redirection	Yes

Table Continued

WebDAV Publishing	
Health and Diagnostics	Yes
HTTP Logging	Yes
Custom Logging	
Logging Tools	Yes
ODBC Logging	
Request Monitor	Yes
Tracing	Yes
Performance	Yes
Static Content Compression	Yes
Dynamic Content Compression	
Security	Yes
Request Filtering	Yes
Basic Authentication	Yes
Centralized SSL Certificate Support	
Client Certificate Mapping Authentic	
Digest Authentication	
IIS Client Certificate Mapping Authe	
IP and Domain Restrictions	
URL Authorization	
Windows Authentication	Yes
Application Development	Yes
.NET Extensibility 3.5	
.NET Extensibility 4.5	Yes
Application Initialization	
ASP	Yes
ASP.NET 3.5	
ASP.NET 4.5	Yes
CGI	
ISAPI Extensions	Yes
ISAPI Filters	Yes
Server Side Includes	
WebSocket Protocol	
FTP Server	
FTP Service	

Table Continued

FTP Extensibility	
Management Tools	Yes
IIS Management Console	Yes
IIS 6 Management Compatibility	Yes
IIS 6 Metabase Compatibility	Yes
IIS 6 Management Console	
IIS 6 Scripting Tools	
IIS 6 WMI Compatibility	
IIS Management Scripts and Tools	
Management Service	
.NET Framework 3.5 Features	Yes
.NET Framework 3.5 (includes .NET 2.0 and 3.0)	Yes
HTTP Activation	
Non-HTTP Activation	
.NET Framework 4.5 Features	Yes
.NET Framework 4.5	Yes
ASP.NET 4.5	Yes
WCF Services	Yes
HTTP Activation	
Message Queuing (MSMQ) Activation	
Named Pipe Activation	
TCP Activation	
TCP Port Sharing	Yes
Background Intelligent Transfer Service (BITS)	Yes
IIS Server Extension	
Compact Server	
BitLocker Drive Encryption	Yes
BranchCache	Yes
Client for NFS	
Data Center Bridging	
Direct Play	
Enhanced Storage	Yes
Failover Clustering	Yes
Group Policy Management	
IIS Hostable Web Core	

Table Continued

Ink and Handwriting Services	
Internet Printing Client	
IP Address Management (IPAM) Server	
iSNS Server service	
LPR Port Monitor	
Management OData IIS Extension	
Media Foundation	
Message Queuing	
Message Queuing Services	
Message Queuing Server	
Directory Service Integration	
HTTP Support	
Message Queuing Triggers	
Multicasting Support	
Routing Service	
Message Queuing DCOM Proxy	
Multipath I/O	Yes
Network Load Balancing	
Peer Name Resolution Protocol	
Quality Windows Audio Video Experience	
RAS Connection Manager Administration Kit (CMAK)	
Remote Assistance	
Remote Differential Compression	
Remote Server Administration Tools	Yes
Feature Administration Tools	Yes
SMTP Server Tools	
BitLocker Drive Encryption Administration	Yes
BitLocker Drive Encryption Tools	Yes
BitLocker Recovery Password Viewer	Yes
BITS Server Extensions Tools	Yes
Failover Clustering Tools	Yes
Failover Cluster Management Tools	Yes
Failover Cluster Module for Windows PowerShell	Yes
Failover Cluster Automation Server	Yes
Failover Cluster Command Interface	Yes

Table Continued

IP Address Management (IPAM) Client	
Network Load Balancing Tools	
SNMP Tools	Yes
WINS Server Tools	
Role Administration Tools	Yes
AD DS and AD LDS Tools	
Active Directory module for Windows	
AD DS Tools	
AD DS Snap-Ins and Command-Line	Yes
Server for NIS Tools	
AD LDS Snap-Ins and Command-Line Tools	
Hyper-V Management Tools	
Hyper-V GUI Management Tools	
Hyper-V Module for Windows PowerShell	
Remote Desktop Services Tools	
Remote Desktop Gateway Tools	
Remote Desktop Licensing Diagnose	
Remote Desktop Licensing Tools	
Windows Server Update Services Tools	
API and PowerShell cmdlets	
User Interface Management Console	
Active Directory Certificate Services Tools	
Certification Authority Management	
Online Responder Tools	
Active Directory Rights Management	
DHCP Server Tools	
DNS Server Tools	
Fax Server Tools	
File Services Tools	Yes
DFS Management Tools	Yes
File Server Resource Manager Tools	Yes
Services for Network File System	Yes
Share and Storage Management Tool	
Network Policy and Access Services Tools	
Print and Document Services Tools	Yes

Table Continued

Remote Access Management Tools	
Remote Access GUI and Command-Line	
Remote Access module for Windows	
Volume Activation Tools	
Windows Deployment Services Tools	
RPC over HTTP Proxy	
Simple TCP/IP Services	
SMB 1.0/CIFS File Sharing Support	Yes
SMB Bandwidth Limit	
SMTP Server	
SNMP Service	Yes
SNMP WMI Provider	Yes
Subsystem for UNIX-based Applications	
Telnet Client	
TFTP Client	
Telnet Server	
User Interfaces and Infrastructure	Yes
Graphical Management Tools and Infrastructure	Yes
Desktop Experience	
Server Graphical Shell	Yes
Windows Biometric Framework	
Windows Feedback Forwarder	
Windows Identity Foundation 3.5	
Windows Internal Database	
Windows PowerShell	Yes
Windows PowerShell 4.0	Yes
Windows PowerShell 2.0 Engine	Yes
Windows PowerShell ISE	Yes
Windows PowerShell Web Access	
Windows Process Activation Service	Yes
Process Model	Yes
.NET Environment 3.5	
Configuration APIs	Yes
Windows Search Service	
Windows Server Backup	Yes

Table Continued

Windows Server Migration Tools	Yes
Windows Standards-Based Storage Management	Yes
Windows TIFF IFilter	
WinRM IIS Extension	
WINS Server	
Wireless LAN Service	
WoW64 Support	Yes
XPS Viewer	
2. IIS extension AD DS tools	Yes