



Hewlett Packard
Enterprise

HPE MSA 2070/2072 Installation Guide

Abstract

This guide describes initial hardware setup for HPE MSA 2070/2072 controller enclosures and disk enclosures, and is intended for use by storage system administrators familiar with servers and computer networks, network administration, storage system installation and configuration, storage area network management, and relevant protocols.

Notices

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

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

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

Acknowledgments

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.

VMware®, VMware NSX®, VMware vCenter®, and VMware vSphere® are registered trademarks or trademarks of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.

Revision History

20-MSAG7-IG-ED1, 1st edition
Initial HPE release.

December 2024

Contents

1 Overview	8
MSA 2070/2072 Storage models	8
MSA 2070/2072 enclosure user interfaces	8
MSA 2070/2072 controllers	8
Features and benefits	9
Product QuickSpecs	9
Related MSA documentation	9
2 Components	11
Front panel components	11
Attach the enclosure bezel	11
24-drive controller enclosure or expansion enclosure	12
12-drive controller enclosure or expansion enclosure	13
Disks used in storage enclosures	14
Controller enclosure—rear panel layout	15
MSA 2070/2072 controller module—rear panel components	16
Disk enclosures	17
Cache	18
Non-volatile memory	19
Supercapacitor pack	19
3 Installing the enclosures	20
Installation checklist	20
FDE considerations	20
Connecting controller and disk enclosures	21
Verify enclosure connections	23
Powering on/powering off	23
4 Connecting hosts	27
Host system requirements	27
Host interface protocols	27
Fibre Channel protocol	27
iSCSI protocol	27
SAS protocol	28
About data host connection	28
MSA 2070 and MSA 2072 Storage	28
Fibre Channel host connect	28
iSCSI host connect	29
10GBase-T iSCSI host connect	29
12Gb mini-SAS HD host connect	29
Connecting the enclosure to data hosts	29
Connecting direct attach configurations	29
Connecting switch attach configurations	31
Connecting management hosts over an Ethernet network	32
Connecting two storage systems to replicate volumes	33
Cabling for replication	34
Host ports and replication	34
Updating firmware	36
5 Connecting to the controller CLI port	37
Device description	37
Emulated serial port	37
Preparing a Linux system for cabling to the CLI port	37
Preparing a Windows system for cabling to the CLI port	38
Obtaining IP values	38
Setting network port IP addresses using DHCP	38
Setting network port IP addresses using the CLI port and cable	39
Using the CLI port and cable — known issues on Windows	42

Problem	42
Workaround	42
6 Basic operation	43
Accessing the SMU	43
Configuring and provisioning the storage system	43
7 Troubleshooting	44
USB CLI port connection	44
Fault isolation methodology	44
Basic steps	44
Options available for performing basic steps	44
Performing basic steps	46
If an expansion enclosure does not initialize	47
Correcting enclosure IDs	47
Stopping I/O	48
Diagnostic steps	48
Controller failure	52
Isolating a host side connection fault	53
Host-side connection troubleshooting featuring FC and iSCSI host ports	53
Host-side connection troubleshooting featuring SAS host ports	54
Isolating a controller module expansion port connection fault	55
Isolating Remote Snap replication faults	56
Replication setup and verification	56
Diagnostic steps for replication setup	57
Can you successfully use the Remote Snap feature?	58
Can you create a replication set?	58
Can you replicate a volume?	59
Has a replication run successfully?	59
Resolving voltage and temperature warnings	59
Sensor locations	60
Power supply sensors	60
Cooling fan sensors	60
Temperature sensors	60
Power and cooling module voltage sensors	61
8 Support and other resources	62
Accessing Hewlett Packard Enterprise Support	62
Accessing updates	62
Remote support	63
Warranty information	63
Regulatory information	63
Additional regulatory information	63
Documentation feedback	63
A LED descriptions	64
Front panel LEDs	64
Enclosure bezel	64
24-drive controller enclosure or supported expansion enclosure	65
12-drive controller enclosure or supported expansion enclosure	66
Ear covers and hubcaps	67
Disk drive LEDs	68
Rear panel LEDs	69
Controller enclosure—rear panel layout	69
MSA 2070/2072 FC controller module—rear panel LEDs	70
MSA 2070/2072 iSCSI controller module—rear panel LEDs	71
MSA 2070/2072 10GBase-T iSCSI controller module—rear panel LEDs	72
MSA 2070/2072 SAS controller module—rear panel LEDs	73
Cache Status LED details	74
MSA 2070/2072 power and cooling modules—rear panel layout	74
MSA 2070/2072 drive enclosure—rear panel layout	76

B Specifications and requirements	78
Safety requirements	78
Site requirements and guidelines	78
Site wiring and AC power requirements	78
Site wiring and DC power requirements	78
Weight guidelines	79
Electrical guidelines	79
Ventilation requirements	79
Cabling requirements	80
Management host requirements	80
Physical requirements	80
Environmental requirements	81
Electrical requirements	81
Site wiring and power requirements	81
C Electrostatic discharge	82
Preventing electrostatic discharge	82
Grounding methods to prevent electrostatic discharge	82
Index	83

Figures

Figure 1	Bezel used with MSA 2070/2072 Storage enclosures: front panel	11
Figure 2	Attaching/removing the enclosure front bezel	12
Figure 3	24-drive enclosure shown with hubcaps only (no bezel)	12
Figure 4	24-drive controller or expansion enclosure: front panel with hubcaps removed	13
Figure 5	12-drive enclosure shown with hubcaps only (no bezel)	13
Figure 6	12-drive controller or expansion enclosure: front panel	14
Figure 7	Controller enclosure: rear panel	15
Figure 8	MSA 2070/2072 controller module face plate (SFP FC)	16
Figure 9	MSA 2070/2072 controller module face plate (SFP iSCSI)	16
Figure 10	MSA 2070/2072 controller module face plate (10GBase-T iSCSI)	17
Figure 11	MSA 2070 controller module face plate (12Gb mini-SAS HD)	17
Figure 12	Disk enclosure supporting either LFF or SFF disks	18
Figure 13	Cabling connections between controller and single drive enclosure	22
Figure 14	Cabling connections between controller and drive enclosures	22
Figure 15	AC power and cooling module	24
Figure 16	DC power and cooling module	25
Figure 17	DC power cable section featuring lug connectors	25
Figure 18	Host connect: direct attach—FC or iSCSI—one server/one HBA/dual path	30
Figure 19	Host connect: direct attach—SAS—one server/one HBA/dual path	30
Figure 20	Host connect: direct attach—FC or iSCSI—two servers/one HBA per server/dual path	30
Figure 21	Host connect: direct attach—SAS—two servers/one HBA per server/dual path	30
Figure 22	Host connect: direct attach—FC or iSCSI—four servers/one HBA per server/dual path	31
Figure 23	Host connect: direct attach—SAS—four servers/one HBA per server/dual path	31
Figure 24	Host connect: switch attach—two servers/two switches	32
Figure 25	Host connect: switch attach—four servers/multiple switches/SAN fabric	32
Figure 26	Connecting two storage systems for Remote Snap: multiple servers/one switch/one location	35
Figure 27	Connecting two storage systems for Remote Snap: multiple servers/switches/one location	35
Figure 28	Connecting two storage systems for Remote Snap: multiple servers/switches/two locations	35
Figure 29	Bezel used with MSA 2070/2072 enclosures: front panel	64
Figure 30	Partial exploded view showing alignment of bezel components	64
Figure 31	Details showing backside of bezel fitted to hubcaps	65
Figure 32	LEDs: 24-drive controller or expansion enclosure—front panel	66
Figure 33	LEDs: 12-drive controller or expansion enclosure—front panel	67
Figure 34	Cover details for enclosure ears	67
Figure 35	LEDs: Disk drive combinations — enclosure front panel	68
Figure 36	MSA 2070/2072: rear panel	69
Figure 37	LEDs: MSA 2070/2072 FC controller module	70
Figure 38	LEDs: MSA 2070/2072 iSCSI controller module	71
Figure 39	LEDs: MSA 2070/2072 10GBase-T iSCSI controller module	72
Figure 40	LEDs: MSA 2070/2072 SAS controller module	73
Figure 41	LEDs: MSA 2070/2072 power and cooling module (AC or DC model)	75
Figure 42	Expansion enclosure rear panel: 12-drive and 24-drive models	76
Figure 43	LEDs: MSA 2070/2072 drive enclosure rear panel	77

Tables

Table 1	Related MSA documentation	9
Table 2	Installation checklist	20
Table 3	Supported terminal emulator applications	37
Table 4	Terminal emulator display settings	37
Table 5	Terminal emulator display settings	40
Table 6	Terminal emulator connection settings	40
Table 7	Diagnostics LED status: Front panel "Fault/Service Required"	49
Table 8	Diagnostics LED status: Rear panel "FRU OK"	49
Table 9	Diagnostics LED status: Rear panel "Fault/Service Required"	49
Table 10	Diagnostics LED status: Front panel disks "Online/Activity" and "Fault/UID"	49
Table 11	Diagnostics LED status: Front panel disks "Fault/UID"	50
Table 12	Diagnostics LED status: Front panel disks "Fault/UID"	50
Table 13	Diagnostics LED status: Rear panel "Host Link Status"	51
Table 14	Diagnostics LED status: Rear panel "Expansion Port Status"	51
Table 15	Diagnostics LED status: Rear panel "Network Port Link Status"	51
Table 16	Diagnostics LED status: Rear panel power supply module "PCM OK"	52
Table 17	Diagnostics LED status: Rear panel power supply module "AC Fail/Fan Fail/DC Fail"	52
Table 18	Diagnostic LED status: Rear panel "Cache Status"	53
Table 19	Diagnostics for replication setup: Using Remote Snap feature	58
Table 20	Diagnostics for replication setup: Creating a replication set	58
Table 21	Diagnostics for replication setup: Replicating a volume	59
Table 22	Diagnostics for replication setup: Checking for a successful replication	59
Table 23	Power supply sensor descriptions	60
Table 24	Controller platform temperature sensor descriptions	61
Table 25	PCM temperature sensor descriptions	61
Table 26	PCM voltage sensor descriptions	61
Table 27	Cache Status LED — power on behavior	74
Table 28	PCM LED states	75
Table 29	LEDs: MSA 2070/2072 expansion activity states	77
Table 30	Rackmount enclosure dimensions	80
Table 31	Rackmount enclosure weights	81

1 Overview

HPE MSA Storage models are storage solutions combining outstanding performance with high reliability, availability, flexibility, and manageability.

MSA 2070/2072 Storage models

The MSA enclosures are Storage Bridge Bay (SBB) compliant. The 2U12 enclosure supports 12 large form factor (LFF) disks in a chassis, and the 2U24 enclosure supports 24 small form factor (SFF) disks in a chassis, using either AC power supplies or DC power supplies.

NOTE For additional information about these controller enclosures, see the following subsections:

- ["Controller enclosure—rear panel layout" on page 15](#)
- ["Rear panel LEDs" on page 69](#)

The MSA 2070/2072 enclosures support virtual storage. For virtual storage, a group of disks with an assigned RAID level is called a *disk group*.

MSA 2070/2072 enclosure user interfaces

MSA enclosures are managed by the Storage Management Utility (SMU), which is a web-based application for configuring, monitoring, and managing the storage system. Both the SMU and the command-line interface (CLI) are briefly described.

- The SMU is the web interface that manages the storage system.
- The CLI manages the storage system using command syntax entered via the keyboard or scripting, and is the only method available for accessing many advanced features.

NOTE For more information about the SMU, see the *HPE MSA 2070/2072 Storage Management Guide* or online help. For more information about the CLI, see the *HPE MSA 2070/2072 CLI Reference Guide*. See also ["Related MSA documentation" on the facing page](#).

MSA 2070/2072 controllers

The MSA 2070/2072 controller enclosures are pre-configured at the factory to support one of these host interface protocols:

- SFP FC
- 10GBase-T iSCSI
- SFP iSCSI
- 12Gb mini-SAS HD

For Fibre Channel (FC) host interfaces, a small form-factor pluggable (SFP) transceiver is used. MSA 2070/2072 SFP iSCSI configurations can use either SFP transceivers, Direct Attach Copper (DAC) cables, or Active Optical Cables (AOCs).

For MSA controllers requiring SFPs, DAC cables, or AOCs, you must purchase and install them into the host interface ports. MSA controller enclosures do not allow you to change the host interface protocol. Always use qualified SFP transceivers, DACs, and AOCs for supporting the host interface protocol as described in your product's QuickSpecs.

For more information, see "Product QuickSpecs" below.

NOTE See *HPE MSA Transceiver Replacement Instructions* at <https://www.hpe.com/info/msadocs> when installing qualified SFPs into FC and iSCSI controller modules.

For the mini-SAS HD host interface, use qualified SAS cable options as described in your product's QuickSpecs (see "Product QuickSpecs" below for more information). Host connection for mini-SAS HD controller modules are described by cabling diagrams in "Connecting hosts" on page 27.

MSA SAS controllers provide four (MSA 2070/2072) high density mini-SAS (mini-SAS HD) ports per controller module. The mini-SAS HD host interface protocol uses the SFF-8644 external connector interface defined for SAS 3.0 to support a link rate of 12 Gb/s using the qualified connectors and cable options.

Features and benefits

Product features and supported options are subject to change. Online documentation describes the latest product and product family characteristics, including currently supported features, options, technical specifications, configuration data, related optional software, and product warranty information. For more information, see "Related MSA documentation" below and "Support and other resources" on page 62.

Product QuickSpecs

Check the QuickSpecs for a complete list of supported servers, operating systems, and options. See:

- <https://www.hpe.com/support/MSA2070QuickSpecs>
- <https://www.hpe.com/support/MSA2072QuickSpecs>

Related MSA documentation

Related support information is provided in "Support and other resources" on page 62. Product documentation titles pertaining to management interfaces are shown in the table below.

Table 1 Related MSA documentation

For information about	See
Using the Storage Management Utility (SMU) web interface to configure and manage the product	HPE MSA 2070/2072 Storage Management Guide
Using the command-line interface (CLI) to configure and manage the product	HPE MSA 2070/2072 CLI Reference Guide
Events codes and recommended actions	HPE MSA 2070/2072 Event Descriptions Reference Guide

To access the above MSA documentation and additional documentation, see <https://www.hpe.com/info/msadocs>.

NOTE The table above provides titles of related MSA documents used with this guide. These documents are informally referenced within this guide as follows:

- Storage Management Guide
 - CLI Reference Guide
 - Event Descriptions Reference Guide
-

2 Components

Front panel components

HPE MSA 2070/2072 Storage enclosures support 2U12 and 2U24 enclosure configurations as specified in the **Note** below. The 2U12 supports 12 LFF 3.5" disks and the 2U24 supports 24 SFF 2.5" disks. The disk modules are accessed from the enclosure front panel. See also the topics about disk modules:

- ["24-drive controller enclosure or expansion enclosure" on the next page](#)
- ["12-drive controller enclosure or expansion enclosure" on page 13](#)
- ["Disks used in storage enclosures" on page 14](#)

NOTE Supported storage enclosure configurations:

- MSA 2070/2072 supports 2U24 and 2U12 chassis as controller enclosures and disk enclosures.
 - MSA 2072 uses two SSD drives pre-installed in drive slots 1 and 2.
 - MSA 2070/2072 controller enclosures support only MSA 12Gb disk enclosures that are described in this guide. Earlier MSA 6Gb LFF and SFF disk enclosures are incompatible.
-

The enclosure front panel provides a passive, non-replaceable status panel mounted on the left ear flange. This panel provides enclosure status LEDs, and it is protected by a cover.

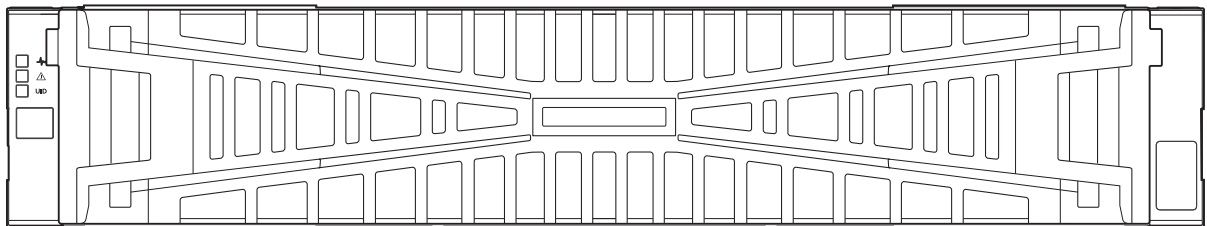


Figure 1 Bezel used with MSA 2070/2072 Storage enclosures: front panel

A flexible cable connects the panel to the midplane. The panel provides the functions described in the 24-drive and 12-drive front panel illustrations and their tables. See also the topic about front panel LEDs in ["LED descriptions" on page 64](#). Hubcaps protect enclosure ears. When the optional enclosure bezel is attached to the hubcaps as shown, the disks are hidden from view.

Attach the enclosure bezel

A generic version of the MSA enclosure bezel assembly is shown above. The geometry applies to all product models. Labels and icons may vary slightly between product models. Ear circuitry is protected by a plastic ear cover attached to the ear flange. Plastic hubcaps snap onto the left and right ear covers. The hubcap for the left ear provides icons identifying enclosure status LEDs. The hubcap for the right ear includes a logo and product model on the front face. The right hubcap used on 12-drive enclosures also includes a disk slot index diagram on its left face. The bezel component snaps into the left and right hubcaps.

You can attach or remove the optional enclosure bezel. Note that the left end of the bezel includes a release latch.

1. Verify that the left and right hubcaps are properly fitted over their ear covers.
2. Hook the right end of the bezel into the right hubcap.
3. Insert the left end of the bezel into the securing slot until the release latch snaps into place.

To observe disk LEDs during enclosure operation, you must remove the enclosure bezel. Optionally, you can monitor disk activity using management interfaces when the bezel is attached.

NOTE A partial assembly view shows bezel insertion into the right ear hubcap slot. Simplified conceptual graphics illustrate the enclosure bezel attachment procedure.

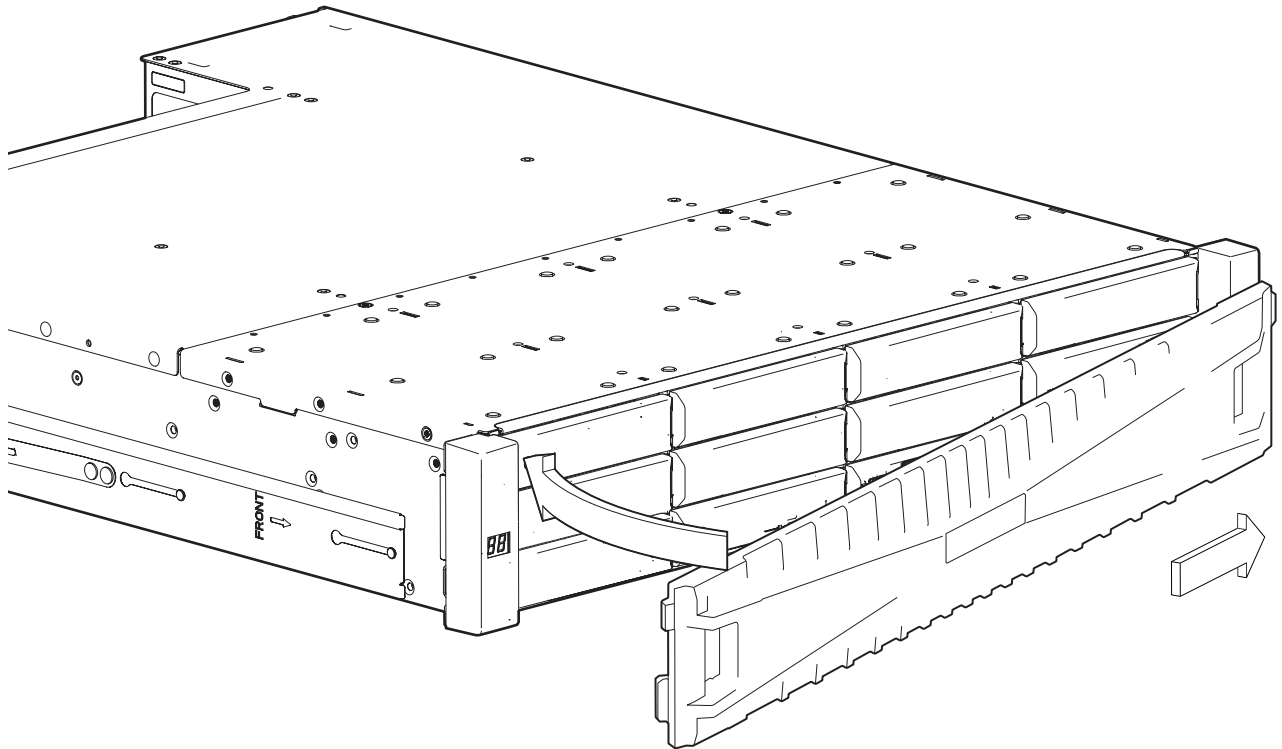



Figure 2 Attaching/removing the enclosure front bezel

 **TIP** To remove the bezel from the enclosure, reverse the order of the steps previously provided.

See also, "Enclosure bezel assembly" on page 64 for a partial exploded view showing alignment of enclosure bezel components.

The front panel illustrations that follow show the enclosures with the bezel removed, revealing disk modules.

24-drive controller enclosure or expansion enclosure

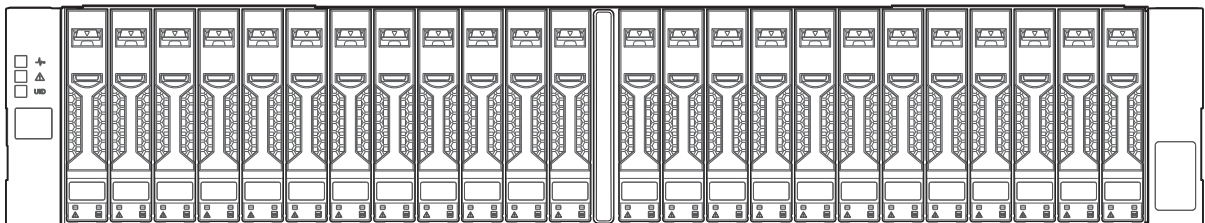
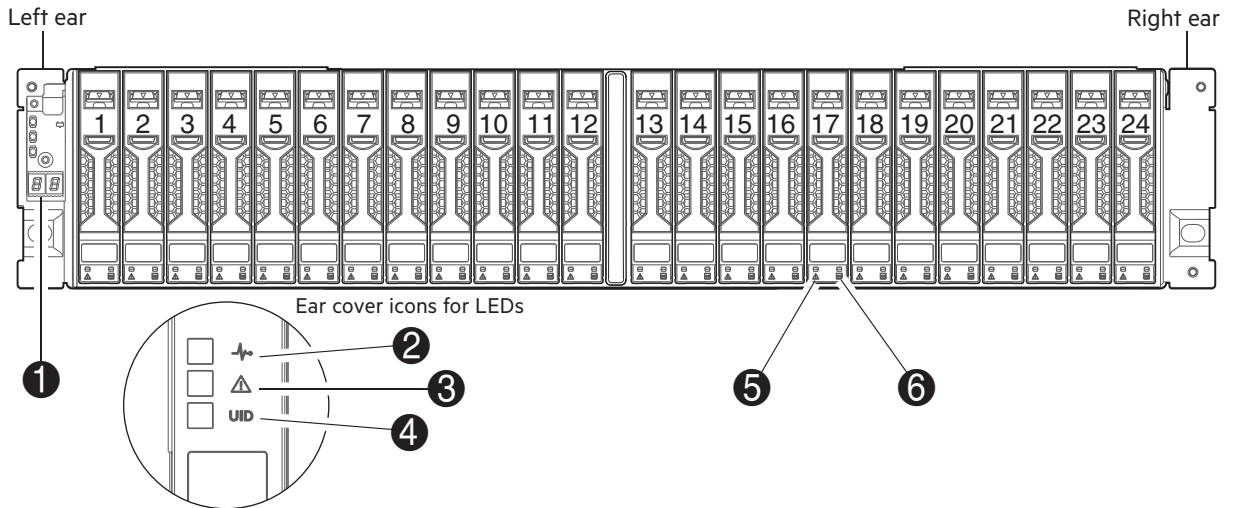


Figure 3 24-drive enclosure shown with hubcaps only (no bezel)

The figure above shows the enclosure with the bezel removed and the disks visible. The following figure shows the enclosure with both the bezel and the hubcaps removed. The enlarged inset in that figure is a detail view showing the icons pertaining to enclosure status LEDs located on the left ear.



Notes:

Integers on disks indicate drive slot numbering sequence.

The enlarged detail view at left shows LED icons from the left ear cover that correspond to the chassis LEDs.

- | | | | |
|---|------------------|---|--------------------------------|
| 1 | Enclosure ID LED | 4 | Unit Identification (UID) LED |
| 2 | System Power LED | 5 | Disk drive Fault/UID LED |
| 3 | Module Fault LED | 6 | Disk drive Online/Activity LED |

Figure 4 24-drive controller or expansion enclosure: front panel with hubcaps removed

12-drive controller enclosure or expansion enclosure

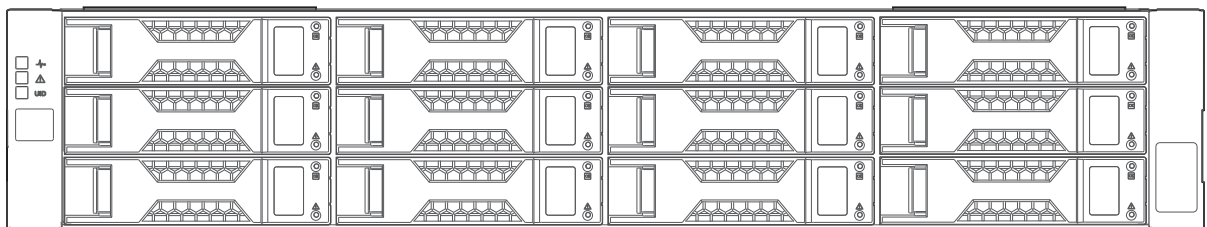
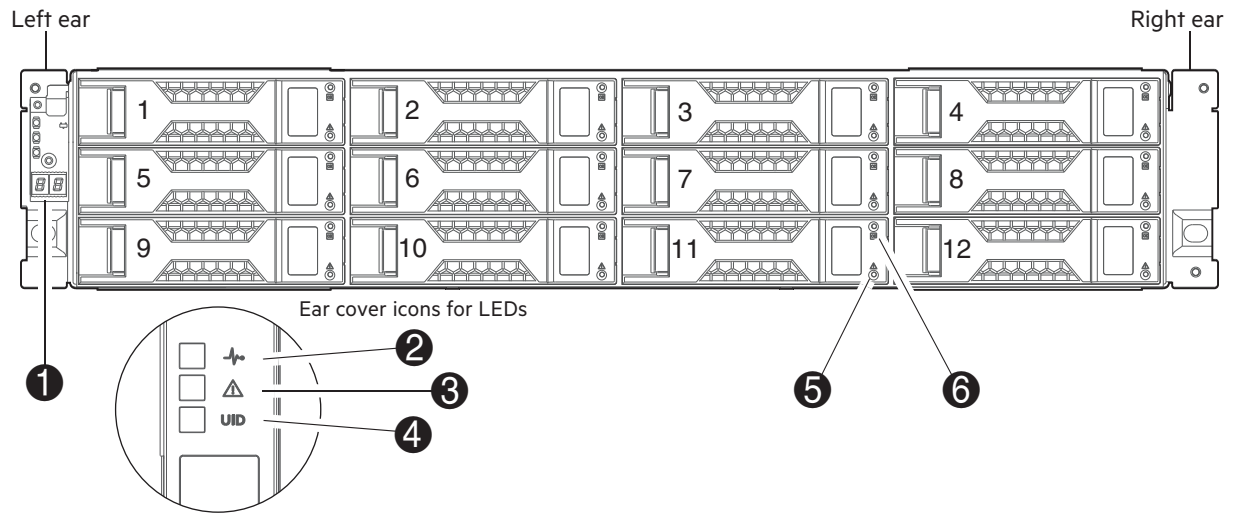


Figure 5 12-drive enclosure shown with hubcaps only (no bezel)

The figure above shows the enclosure with the bezel removed and the disks visible. The following figure shows the enclosure with both the bezel and the hubcaps removed. The enlarged inset in that figure is a detail view showing the icons pertaining to enclosure status LEDs located on the left ear.



Notes:
 Integers on disks indicate drive slot numbering sequence.
 The enlarged detail view at left shows LED icons from the left ear that correspond to the chassis LEDs.

1	Enclosure ID LED	4	Unit Identification (UID) LED
2	System Power LED	5	Disk drive Fault/UID LED
3	Module Fault LED	6	Disk drive Online/Activity LED

Figure 6 12-drive controller or expansion enclosure: front panel

NOTE The hubcaps/ear covers must be attached to the left and right ear flanges on the enclosure front panel to protect the front status panel and circuitry. Optionally, the bezel can also be attached between the two hubcaps.

Disks used in storage enclosures

Supported disk types are described below. For information about creating disk groups and adding spares using these different disk types, see the Storage Management Guide.

MSA 2070 enclosures

Enclosures support LFF Midline SAS, SFF Enterprise SAS, and LFF/SFF SSD disks. They also support LFF Midline SAS and SFF Enterprise and LFF/SFF SSD self-encrypting disks that work with the full disk encryption (FDE) feature.

MSA 2072 enclosures

These enclosures support the same disk types supported by MSA 2070 enclosures. A notable configuration exception is that for these enclosures, two SSDs are pre-installed. One SSD is installed in drive slot 1 and the other SSD is installed in drive slot 2.

NOTE Disk modules used in MSA 2070/2072 enclosures:

- In addition to the front views of SFF and LFF disk modules shown above, see "[Disk drive LEDs](#)" on page 68 for pictorial views.
- Storage enclosures may or may not ship with disks pre-installed, depending on order configuration terms.
- For information about installing or replacing disks, see *HPE MSA 2070/2072 Maintenance Guide*.

Controller enclosure—rear panel layout

The diagram and table below display and identify important component items comprising the rear panel layout of a representative controller enclosure (4-port Fibre Channel host interface protocol is shown in the example). For a given host interface protocol, the rear panel view of an LFF controller enclosure and SFF controller enclosure are identical.

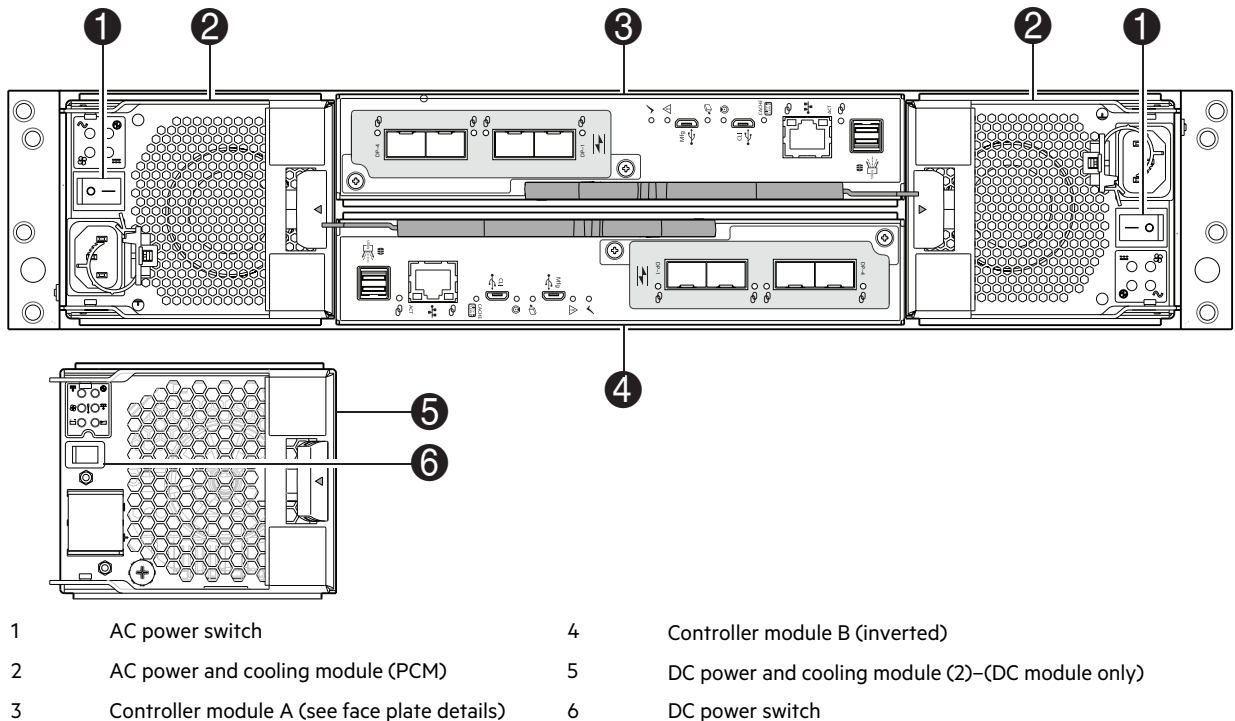


Figure 7 Controller enclosure: rear panel

A controller enclosure accommodates two PCM Field Replaceable Units (FRUs) of the same type—either both AC or both DC—within the PCM slots (see two instances of callout 2 above). The controller enclosure accommodates two controller module FRUs of the same type within the controller module slots (see callouts 3 and 4 above).

TIP The PCMs and controller modules are rotated 180° from their counterparts to align with their respective midplane connectors, as shown in the figure above.

IMPORTANT HPE MSA enclosures support dual-controller configurations only. If a partner controller fails, the array will fail over and run on a single controller until the redundancy is restored. A controller module must be installed in each controller module slot to ensure sufficient airflow through the enclosure during operation.

IMPORTANT Operation of the enclosure with any plug-in modules missing will disrupt the airflow, and the disks will not receive sufficient cooling. It is essential that all slots are fitted with appropriate plug-in modules before powering on the enclosure.

The diagrams with tables that immediately follow provide descriptions of the different controller modules and PCMs that can be installed into the rear panel of a controller enclosure. Showing controller modules and PCMs separately from

the enclosure provides improved clarity in identifying the component items called out in the diagrams and described in the tables. Descriptions are also provided for optional disk enclosures for expanding storage capacity.

NOTE Storage enclosures support hot-swap replacement of controller modules, PCMs, disk modules, and I/O modules. Hot-add of disk enclosures is also supported.

MSA 2070/2072 controller module—rear panel components

The figure below shows four host interface ports configured with FC SFP transceivers. See *HPE MSA Transceiver Replacement Instructions* at <https://www.hpe.com/info/msadocs> when installing qualified SFPs into FC controller modules.

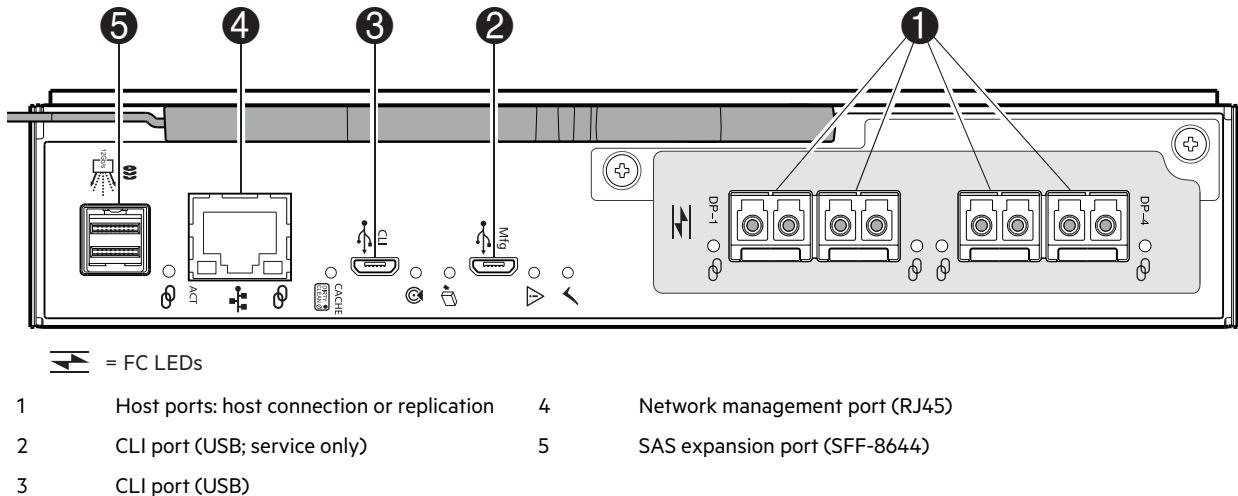


Figure 8 MSA 2070/2072 controller module face plate (SFP FC)

The figure below shows four host interface ports configured with iSCSI SFP transceivers. See *HPE MSA Transceiver Replacement Instructions* at <https://www.hpe.com/info/msadocs> when installing qualified SFPs into iSCSI controller modules.

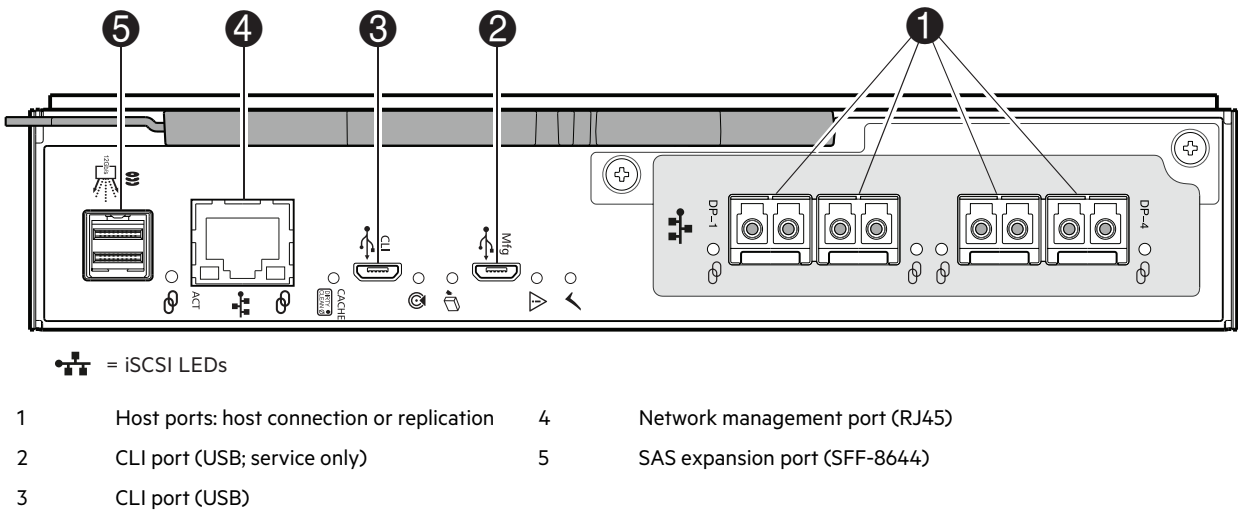
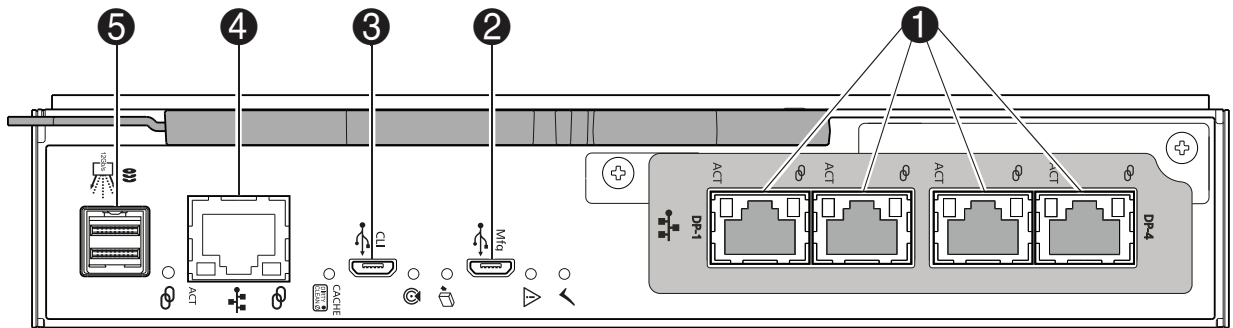



Figure 9 MSA 2070/2072 controller module face plate (SFP iSCSI)

The figure below shows four host interface ports configured with 10GBase-T iSCSI connectors.

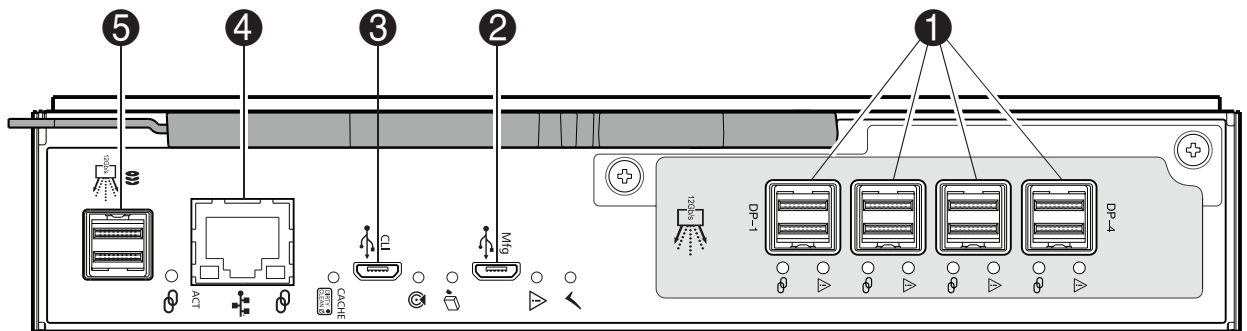



 = 10GBase-T iSCSI LEDs

- | | | | |
|---|--|---|--------------------------------|
| 1 | Host ports: host connection or replication | 4 | Network management port (RJ45) |
| 2 | CLI port (USB; service only) | 5 | SAS expansion port (SFF-8644) |
| 3 | CLI port (USB) | | |

Figure 10 MSA 2070/2072 controller module face plate (10GBase-T iSCSI)

The figure below shows four host interface ports configured with 12Gb/s mini-SAS HD (SFF-8644) connectors.



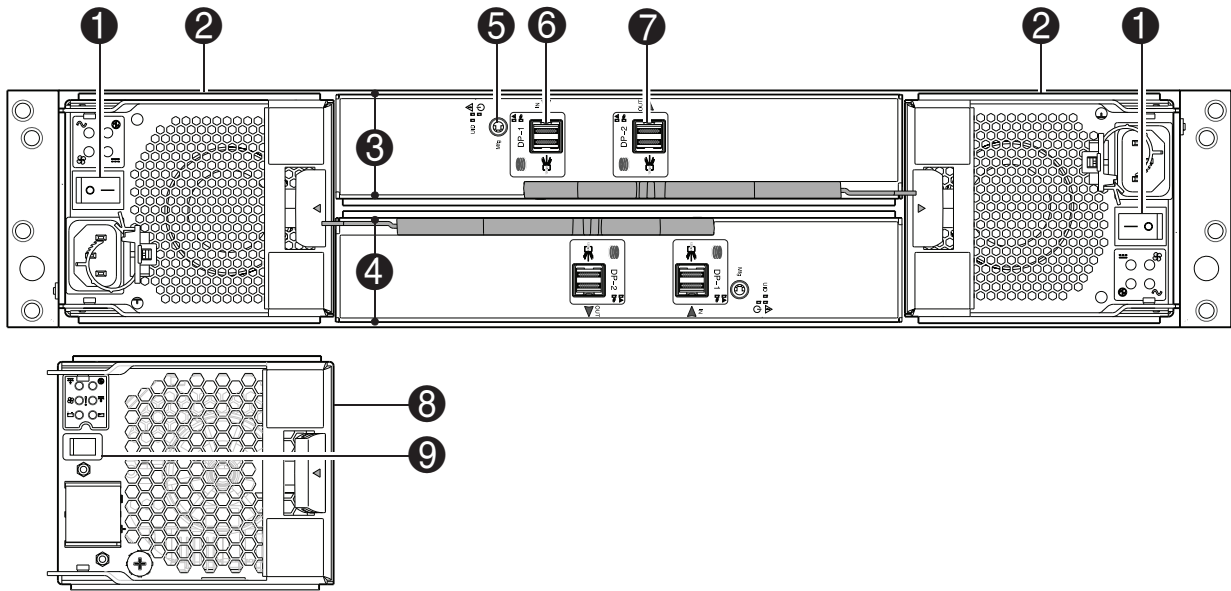
 = SAS LEDs

- | | | | |
|---|--|---|--------------------------------|
| 1 | Host ports: host connection or replication | 4 | Network management port (RJ45) |
| 2 | CLI port (USB; service only) | 5 | SAS expansion port (SFF-8644) |
| 3 | CLI port (USB) | | |

Figure 11 MSA 2070 controller module face plate (12Gb mini-SAS HD)

Disk enclosures

Disk enclosure expansion modules attach to controller modules via the mini-SAS HD expansion port, allowing addition of disks to the storage system. Controller enclosures support attachment of 12Gb disk enclosures using 2U12 and 2U24 form factors. The 2U12 chassis supports 12 LFF 3.5" disks and the 2U24 chassis supports 24 SFF 2.5" disks. The rear panel view of a disk enclosure representing both the 2U12 and the 2U24 is shown in the following figure.



- | | | | |
|---|-----------------------------------|---|--|
| 1 | AC power switch | 6 | Data port, in |
| 2 | AC power and cooling module (PCM) | 7 | Data port, out |
| 3 | Expansion module A | 8 | DC power and cooling module (2)-(DC module only) |
| 4 | Expansion module B (inverted) | 9 | DC power switch |
| 5 | Service port | | |

Figure 12 Disk enclosure supporting either LFF or SFF disks

NOTE Disk enclosure characteristics:

- Only HPE MSA qualified disks are supported by MSA 2070/2072 disk enclosures.
- Disk enclosures are equipped with two expansion modules.
- Disk enclosures are equipped with two PCMs of the same type (both AC or both DC).
- The rear panel views of an LFF disk enclosure and SFF disk enclosure used with MSA 2070/2072 controller enclosures are identical.
- The LFF disk enclosures and SFF disk enclosures can be intermixed, and are supported by MSA 2070/2072 controller enclosures.
- See the topic about connecting controller and disk enclosures for configuration limits when cabling disk enclosures.

For details about qualified disks and compatibility information pertaining to MSA 2070/2072 enclosures, see the Single Point of Connectivity Knowledge (SPOCK) storage compatibility matrix: <https://www.hpe.com/storage/spock>.

See also "[Front panel components](#)" on page 11. See the bullet note entitled "**Note** Supported storage enclosure configurations" for details pertaining to disk enclosures.

Cache

To enable faster data access from disk storage, the following types of caching are performed:

- Write-back caching. The controller writes user data in the cache memory on the controller module, rather than directly to the disks. Later, when the storage system is either idle or aging—and continuing to receive new I/O data—the controller writes the data to the disks.

- Read-ahead caching. The controller detects sequential access, reads ahead into the next sequence of data, and stores the data in the read-ahead cache. Then, if the next read access is for cached data, the controller immediately loads the data into the system memory, avoiding the latency of a disk access.

NOTE See the Storage Management Guide for more information about volume cache options.

Non-volatile memory

During a power loss or controller failure, data stored in cache is saved off to non-volatile memory (multi-channel eMMC daughterboard in the controller module). The data is then written to disk after the issue is corrected. To protect against writing incomplete data to disk, the image stored in the eMMC card is verified before committing to disk. The eMMC plugs into a slot on the controller module baseplane. Given that the controller module is a sealed component, the eMMC is not accessible.

NOTE In dual-controller configurations featuring a healthy partner controller, the cache is duplicated between the controllers provided that volume cache is set to standard on all volumes in the pool owned by the failed controller.

Supercapacitor pack

To protect RAID controller cache in case of power failure, HPE MSA controller modules are equipped with supercapacitor technology, which in conjunction with internal non-volatile memory, provides extended cache memory backup time. The supercapacitor pack provides energy for backing up unwritten data in the write cache to the non-volatile memory in the event of a power failure. Unwritten data in non-volatile memory is automatically committed to disk media when power is restored. While the cache is being maintained by the supercapacitor, the Cache Status LED flashes at a rate of 1/10 second on and 9/10 second off.

3 Installing the enclosures

Installation checklist

The following table outlines the steps required to install the enclosures and initially configure the system. To ensure a successful installation, perform the tasks in the order they are presented.

Table 2 Installation checklist

Step	Task	Where to find procedure
1	Install the controller enclosure and optional drive enclosures into the rack, and attach the hubcaps. Optionally, attach the bezel.	See the <i>HPE MSA 2070/2072 Quick Start Instructions</i> .
	Optional step: For enclosures using small form pluggable SFP transceivers, install the SFPs.	See <i>HPE MSA Transceiver Replacement Instructions</i> for 4-port FC and 4-port iSCSI controller modules.
2	Connect the controller enclosure and drive enclosures.	See "Connecting controller and disk enclosures" on the facing page.
3	Connect the power cords.	See "Powering on/powering off" on page 23.
4	Verify enclosure connections.	See "Verify enclosure connections" on page 23.
5	Install required host software.	See "Host system requirements" on page 27.
6	Connect data hosts.	See "Connecting the enclosure to data hosts" on page 29. If using optional Remote Snap feature, see also "Connecting two storage systems to replicate volumes" on page 33.
7	Connect management hosts.	See "Connecting management hosts over an Ethernet network" on page 32.
8	Obtain IP values and set management port IP properties on the controller enclosure.	See "Obtaining IP values" on page 38. See "Connecting to the controller CLI port" on page 37, which contains information for both Linux and Windows.
9	Perform system setup tasks: <ul style="list-style-type: none">• Sign in to the web-based Storage Management Utility (SMU).• Follow the wizard to perform preboarding and onboarding to initially configure and provision the storage system using the SMU.	See getting-started topics in the Storage Management Guide. See topics about configuring storage, provisioning storage, and adding data protection in the Storage Management Guide or help.

FDE considerations

The full disk encryption feature available via the management interfaces requires use of self-encrypting disks (SED) which are also referred to as FDE-capable disk drive modules. If using the FDE feature, ensure that all disks are FDE-capable. When installing FDE-capable disk drive modules, follow the same procedures for installing the disks that do not support FDE.

The procedures for using the FDE feature, such as securing the system, viewing the disk FDE status, and clearing and importing keys are performed using the SMU or CLI commands (see the Storage Management Guide or CLI Reference Guide for more information).

! **IMPORTANT** The Fault/UID disk LED displays amber under the following conditions for FDE:

- If an FDE disk is inserted into the storage enclosure in a secured locked state. The disk is unusable by the system, and must either be unlocked or repurposed.

- If a non-FDE disk is installed into an FDE-secured storage system. The disk is unusable by the system, and must be replaced with an FDE disk.
-

Connecting controller and disk enclosures

MSA 2070/2072 controller enclosures support up to ten enclosures (including the controller enclosure). You can cable disk enclosures of the same type or of mixed 12-drive and 24-drive model type.

The LFF Disk Enclosure and SFF Disk Enclosure can be attached to controller enclosures using mini-SAS HD cables of 0.5 m (1.64') to 2 m (6.56') length. Each drive enclosure provides two 0.5 m (1.65') mini-SAS HD to mini-SAS HD cables. Longer cables may be desired or required, and can be purchased separately.

Cable requirements for MSA 2070/2072 disk enclosures

This section describes cabling requirements for adding storage to MSA 2070/2072 controller enclosures.

! **IMPORTANT** Cable requirements for attaching disk enclosures are summarized below:

- When installing SAS cables to expansion modules, use only mini-SAS HD cables with SFF-8644 connectors supporting your 12Gb application.
 - For information about which cables are provided with your MSA 2070/2072 products, check the appropriate QuickSpecs for your products (see links below).
 - The maximum cable length allowed in any configuration is 2 m (6.56').
 - When adding multiple disk enclosures, you may need to purchase additional 1 m or 2 m cables (see appropriate QuickSpecs for supported cables).
-

For additional information concerning cabling of MSA 2070/2072 controllers, visit:

<https://www.hpe.com/support/MSA2070QuickSpecs>

<https://www.hpe.com/support/MSA2072QuickSpecs>

<https://www.hpe.com/support/MSAGen7BestPractices>

NOTE For clarity, the schematic illustrations of controller and expansion modules shown in this section provide only relevant details such as expansion ports within the module face plate outline. For detailed illustrations showing all components, see "[Controller enclosure—rear panel layout](#)" on page 15.

- Only simplified controller module and expansion module face plates are shown for each enclosure. The top set of face plates represents the controller enclosure; the following sets of face plates in the cascade represent the expansion enclosures.
 - SAS expansion ports showing the **In** descriptor are labeled DP-1, and those showing the **Out** descriptor are labeled DP-2.
-

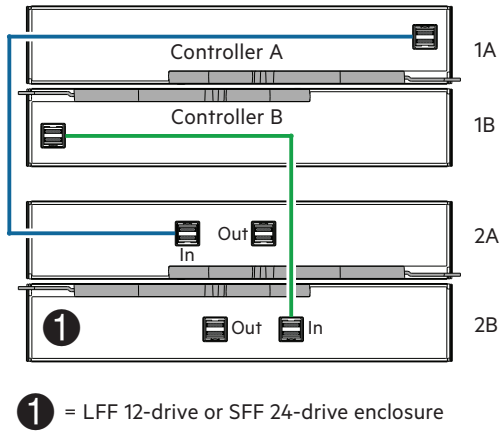


Figure 13 Cabling connections between controller and single drive enclosure

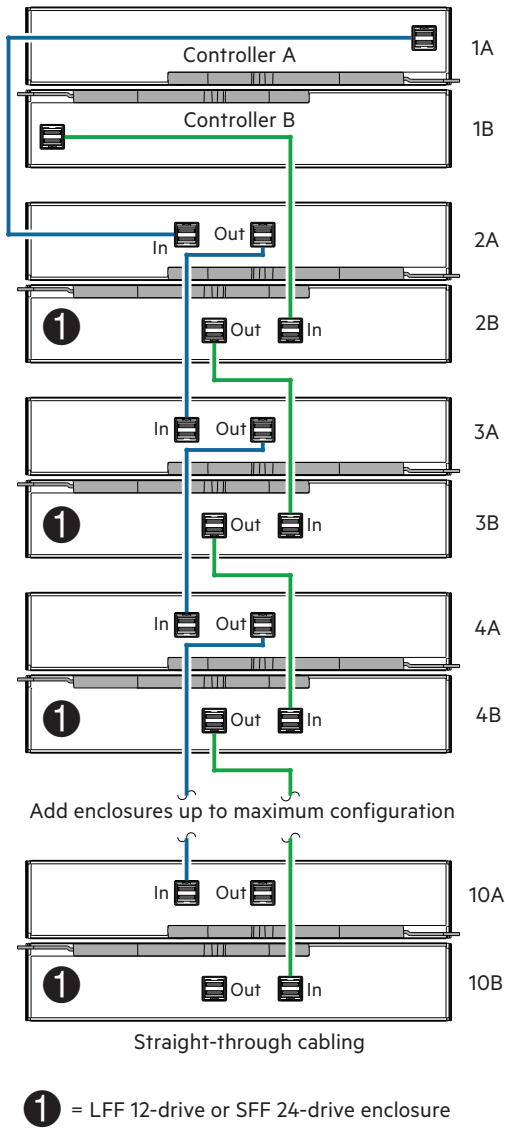


Figure 14 Cabling connections between controller and drive enclosures

The preceding diagram shows a dual-controller enclosure cabled to either the LFF Disk Enclosure or the SFF Disk Enclosure featuring dual-expansion modules.

Controller module 1A is connected to the **In** port of expansion module 2A. The **Out** port of expansion module 2A connects to the **In** port of expansion module 3A—and so on—with a chain of connections cascading down (blue).

Controller module 1B is connected to the **In** port of expansion module 2B. The **Out** port of expansion module 2B connects to the **In** port of expansion module 3B—and so on—with a chain of connections cascading down (green).


Maximum enclosure configurations are listed in "[Cable requirements for MSA 2070/2072 disk enclosures](#)" on page 21 within the **Important** bullets.

Verify enclosure connections

The "[Connecting controller and disk enclosures](#)" on page 21 section describes cabling of optional disk enclosures to a controller enclosure to add storage. Ensure proper routing and securely seated connections for the SAS cabling between the controller modules and the expansion modules, before proceeding to power connection and powering on steps.

NOTE After the power-on sequence succeeds, the storage system is ready to be connected as described in "[Connecting the enclosure to data hosts](#)" on page 29.

Powering on/powering off


 **CAUTION** Do not operate the enclosure system until the ambient temperature is within the specified operating range described in "[Environmental requirements](#)" on page 81. If disks have been recently installed, make sure they have had time to adjust to the environmental conditions before they are used with production data for I/O.

Power on the powered-down system by connecting the power cables from the PCMs to the Power Distribution Unit (PDU), and moving the power switch on each PCM to the on position.

The System Power LED on the front panel should be lit green when the enclosure power is activated.

1. Ensure the power switch on the PCM is in the off position.
2. Connect the power cables.
3. When powering on, make sure to power up the enclosures and associated data host in the following order:
 - a. Drive enclosures *first*. This ensures that the disks in the drive enclosure have enough time to completely spin up before being scanned by the controller modules within the controller enclosure. While enclosures power up, their LEDs blink. After the LEDs stop blinking—if no LEDs on the front and back of the enclosure are amber—the power on sequence is complete, and no faults have been detected.
 - b. Controller enclosure *next*. Depending upon the number and type of disks in the system, it may take several minutes for the system to become ready.
 - c. Data host *last* (if powered down for maintenance purposes).

 **TIP** When powering off, you will reverse the order of steps used for powering on.

 **IMPORTANT** If main power is lost for any reason, upon restoration of power, the system will restart automatically if the power switches on the PCMs are in the on position.

See "[Front panel LEDs](#)" on page 64 and related fault conditions for more details.

NOTE Guidelines for consideration when power cycling:

- Move the PCM power switch to the off position before connecting or disconnecting an AC or DC power cable.
 - Remove the AC or DC power cable before inserting or removing a PCM.
 - Allow 15 seconds between powering off and powering on the PCM.
 - Allow 15 seconds before powering on one PCM and powering off another PCM.
 - Powering off a PCM while any amber LED is lit on the partner PCM may result in complete loss of power to the cabled enclosures, and a loss of access to data.
-

! **IMPORTANT** See the topic about power cable requirements and the QuickSpecs for more information about power cables used by MSA 2070/2072 enclosures.

AC power supply

The AC power and cooling module (PCM) is shown in the following figure. This PCM is supported by all MSA 2070/2072 enclosures.

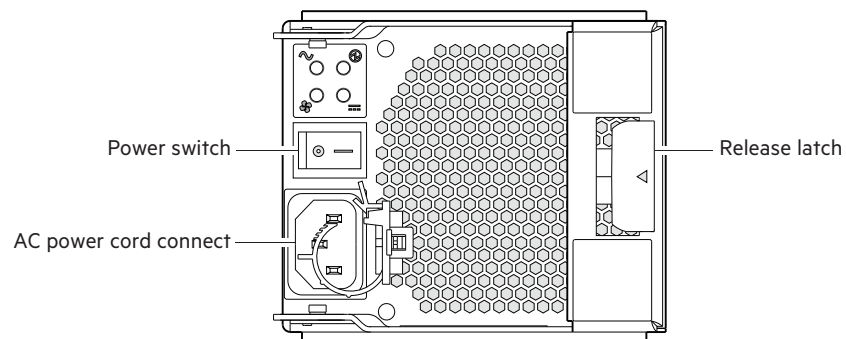


Figure 15 AC power and cooling module

Connect AC power cord to AC PDU and AC PCM

Access the enclosure rear panel when making power cord connections.

1. Obtain a suitable AC power cord for each AC PCM that will connect to a power source.
2. Verify that the power switch on each redundant PCM is in the **Off** position.
3. Plug the power cord into the power cord connector on PCM (see figure above). Plug the other end of the power cord into the rack power source, such as a PDU.

Repeat this sequence for the redundant AC PCM within the enclosure.

4. Repeat the procedure for the remaining AC enclosures in the array.

DC power supply

The DC power and cooling module is shown in the figure below. This PCM option is supported by MSA 2070 enclosures.

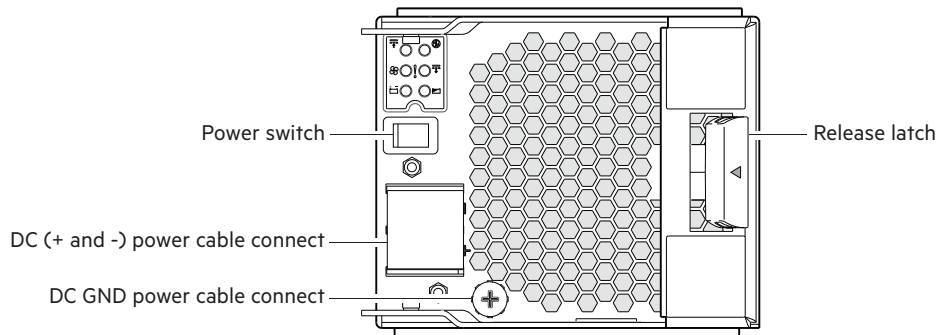


Figure 16 DC power and cooling module

Connect DC power cable to DC power supply and DC PCM

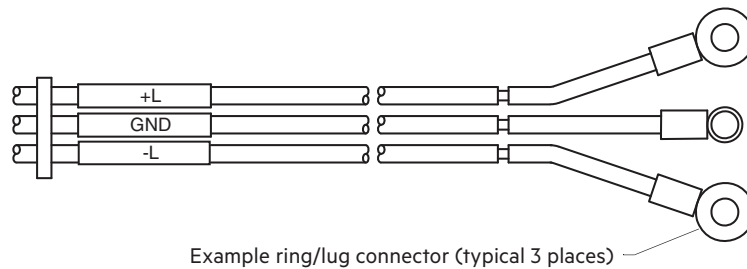


Figure 17 DC power cable section featuring lug connectors


Connection of individual DC cable wires requires a No.2 phillips screwdriver. Access the enclosure rear panel when making power cable connections.

1. Obtain a suitable DC power cable for each DC PCM that will connect to a DC power source.
2. Verify that the power switch on each redundant PCM is in the **Off** position.
3. Remove the DC PCM cable connect cover to provide access to the positive (+) and negative (-) connectors.
4. Attach the black wire to the (+) connector on the PCM (see DC PCM figure above):
 - a. Using a No.2 phillips screwdriver or flat blade, remove the screw with square washer from the (+) connection hole.
 - b. Align the black wire lug over the (+) connection hole.
 - c. Reinstall the screw with square washer to secure the lug connector in place, applying a torque between 1.7 N-m (15 in-lb) and 2.3 N-m (20 in-lb).
5. Attach the red wire to the (-) connector on the PCM (see DC PCM figure above):
 - a. Using a No.2 phillips screwdriver or flat blade, remove the screw with square washer from the (-) connection hole.
 - b. Align the red wire lug over the (-) connection hole.
 - c. Reinstall the screw with washer to secure the lug connector in place, applying a torque between 1.7 N-m (15 in-lb) and 2.3 N-m (20 in-lb).
 - d. Reattach the cable connect cover to the DC PCM.

6. Attach the green wire to the ground connector on the PCM (see DC PCM figure above).
 - a. Using a No.2 phillips screwdriver, remove the screw and lock washer from the ground connection hole.
 - b. Align the green wire lug over the ground connection hole.
 - c. Reinstall the screw with lock washer to secure the lug connector in place, applying a torque between 1.7 N-m (15 in-lb) and 2.3 N-m (20 in-lb).
7. To complete the DC connection, secure the other end of each cable wire component of the DC power cable to the target DC power source.

Check the three individual DC cable wire colors before connecting each cable wire lug to its proper location on the DC power source. The black cable attaches to the positive connection. The red cable attaches to the negative connection. The green cable attaches to the ground connection.

8. Repeat steps 3–7 for the redundant DC PCM installed in the enclosure.
9. Repeat the procedure for the remaining DC enclosures in the array.

 **CAUTION** Connecting to a DC power source outside the designated -48V DC nominal range (-35V DC to -72V DC) may damage the enclosure.

Power cycle AC or DC enclosures

Access the enclosure rear panel when powering on or powering off.

To power on the system:

1. Power up drive enclosure(s): Press the power switches on the back of each drive enclosure to the **On** position. Allow two minutes for the disks to spin up.
2. Power up the controller enclosure: Press the power switches on the back of the controller enclosure to the **On** position. Allow several seconds for the disks to spin up.
3. Check management interfaces or enclosure front and rear panel LEDs for fault conditions. See also "[Fault isolation methodology](#)" on page 44.

To power off the system:

1. Stop all I/O from hosts to the system.
2. Shut down both controllers using one of the methods described below:
 - Use the SMU to shut down both controllers, as described in the online help and the Storage Management Guide.
 - Use the CLI to shut down both controllers, as described in the CLI Reference Guide.
3. Press the power switch on each controller enclosure PCM to the **Off** position.
4. Press the power switch on each disk enclosure PCM to the **Off** position.

4 Connecting hosts

Host system requirements

Data hosts connected to HPE MSA 2070/2072 Storage systems must meet requirements described herein. Depending on your system configuration, data host operating systems may require that multipathing is supported.

If fault-tolerance is required, then multi-pathing software may be required. Host-based multipath software should be used in any configuration where two logical paths between the host and any storage volume may exist at the same time. This would include most configurations where there are multiple connections to the host or multiple connections between a switch and the storage.

For details about supported operating systems, multi-pathing enablement, and compatibility matrix information pertaining to MSA 2070/2072 enclosures, see <https://www.hpe.com/storage/spock>.

Host interface protocols


Fibre Channel protocol

MSA 2070/2072 FC controller enclosures support point-to-point or Fibre Channel Arbitrated Loop (public or private) technologies. Point-to-point protocol is used to connect to a fabric switch. Point-to-point protocol can also be used for direct connection, and it is the only option supporting direct connection at 16Gb/s or greater. Loop protocol can be used in a physical loop or in a direct connection between two devices. See the `set host-parameters` command within the CLI Reference Guide for command syntax and details about connection mode parameter settings relative to supported link speeds.

Fibre Channel ports are used in either of two capacities:


- To connect two storage systems through a Fibre Channel switch for use of Remote Snap replication.
- For attachment to FC hosts directly, or through a switch used for the FC traffic.

The first usage option requires valid licensing for the Remote Snap replication feature, available with the HPE MSA Advanced Data Services license, whereas the second option requires that the host computer supports FC and optionally, multipath I/O.

 **TIP** Use the SMU to view or change FC port settings, as described in the Storage Management Guide. Use the `set host-parameters` CLI command to set FC port parameters for communication with hosts, and use the `show ports` CLI command to view information about host ports in each controller module. See the CLI guide for information about commands and syntax.

iSCSI protocol


MSA 2070/2072 iSCSI controller enclosures support Internet SCSI (Small Computer System Interface). CHAP (Challenge Handshake Authentication Protocol) is supported for protecting the storage system from unauthorized access.

 **TIP** See the topics about configuring CHAP and about CHAP and replication in the Storage Management Guide.

The iSCSI ports are used in either of two capacities:

- To connect two storage systems through a switch for use of Remote Snap replication.
- For attachment to iSCSI hosts directly, or through a switch used for the iSCSI traffic.

The first usage option requires valid licensing for the Remote Snap replication feature, available with the HPE MSA Advanced Data Services license, whereas the second option requires that the host computer supports iSCSI and optionally, multipath I/O.

 **TIP** Use the SMU to view or change iSCSI port settings, as described in the Storage Management Guide. Alternatively, the following CLI commands can be used:

- Use the `set host-parameters` CLI command to set iSCSI port parameters for communication with hosts.
- Use the `show ports` CLI command to view information about host ports in each controller module.
- Use the `set iscsi-parameters` CLI command to change system-wide parameters for iSCSI ports.
- Use the `show iscsi-parameters` CLI command to show system-wide parameters for iSCSI ports.

See the CLI guide for information about commands, syntax, and important information concerning command usage.

SAS protocol

MSA 2070/2072 SAS controller enclosures support SAS (Serial Attached SCSI), which is a point-to-point serial protocol for moving data to and from storage devices. SAS uses the standard SCSI command set. SAS host interface ports connect to server HBAs using direct attach or a SAS interconnect if using blade systems. SAS host interface ports are used for I/O traffic and do not support the HPE MSA Remote Snap replication feature.

About data host connection

An initiator identifies an external port to which the storage system is attached. The external port may be a port in an I/O adapter (such as an FC HBA) in a server, or a connected switch. Cable connections vary depending on configuration. Common cabling configurations for the host interface protocols previously described are shown in the following sections. Supporting diagrams describe direct attach, switch-connect, and storage expansion configuration options for MSA 2070/2072 products. For specific information about qualified host cabling options for your product, see the appropriate QuickSpecs:

- <https://www.hpe.com/support/MSA2070QuickSpecs>
- <https://www.hpe.com/support/MSA2072QuickSpecs>

MSA 2070 and MSA 2072 Storage


MSA 2070/2072 Storage systems support FC, iSCSI, and SAS host interface protocols. The MSA 2070/2072 FC and iSCSI controller modules use small form-factor pluggable (SFP transceiver or SFP) connectors and cable options. The fibre-optic interface cable is plugged into the SFP, which is plugged into a host port.

The MSA 2070/2072 SAS controller modules use qualified mini-SAS HD external connectors. The MSA2070/2072 10GBase-T iSCSI controller modules use Cat-6 or above cables with RJ45 connectors.

Fibre Channel host connect


FC controller modules use Fibre Channel interface protocol for host connection. Each controller module provides four host ports designed for use with a qualified FC SFP. MSA 2070/2072 FC controller enclosures can also be cabled to

support the Remote Snap replication feature via the FC ports. See also "[Fibre Channel protocol](#)" on page 27.

 **TIP** Locate the SFP transceivers for your controller modules. See *HPE MSA Transceiver Replacement Instructions* for guidance.

iSCSI host connect

iSCSI controller modules use the Internet SCSI interface protocol for host connection. Each controller module provides four host ports designed for use with a qualified iSCSI SFP or qualified DAC or AOC cable option. MSA 2070/2072 iSCSI controller enclosures can also be cabled to support the Remote Snap replication feature via the iSCSI ports. See also "[iSCSI protocol](#)" on page 27.

 **TIP** Locate the SFP transceivers for your controller modules. See *HPE MSA Transceiver Replacement Instructions* for guidance.

10GBase-T iSCSI host connect

The 10GBase-T iSCSI controller modules use an Internet SCSI interface protocol for host connection. Each controller module provides four host ports designed for use with a qualified 10GBase-T cable option, which supports data rates up to 10Gb/s. The MSA 2070 iSCSI controller enclosures can also be cabled to support the HPE MSA Remote Snap replication feature via the iSCSI ports. See also "[iSCSI protocol](#)" on page 27.

NOTE This controller module supports Cat-6 and above cables with RJ45 connectors as described in <https://www.hpe.com/support/MSA2070QuickSpecs> and <https://www.hpe.com/support/MSA2072QuickSpecs>.

12Gb mini-SAS HD host connect

SAS controller modules use mini-SAS HD interface protocol for host connection. Each controller module provides four host ports designed for use with SFF-8644 connectors supporting data rates up to 12Gb/s. MSA 2070/2072 SAS controller enclosures connect to hosts for processing I/O; they are not used for replication. See also "[SAS protocol](#)" on [the previous page](#).

Connecting the enclosure to data hosts

Connecting direct attach configurations

MSA 2070/2072 controller enclosures support dual-controller configurations only. If a partner controller fails, the array will fail over and run on a single controller until the redundancy is restored. A controller module must be installed in each IOM slot to ensure sufficient airflow through the enclosure during operation.

NOTE Not all operating systems support direct-connect. For more information, see the Single Point of Connectivity Knowledge (SPOCK) storage compatibility matrix: <https://www.hpe.com/storage/spock>.

NOTE The following diagrams use a single cabling example for FC and iSCSI 4-port controller modules, since port locations are identical, immediately followed by the SAS model.

One server/one HBA/dual path

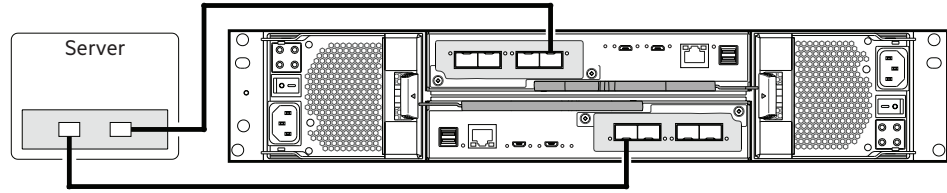


Figure 18 Host connect: direct attach—FC or iSCSI—one server/one HBA/dual path

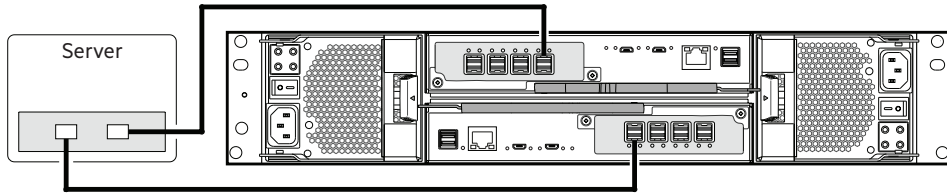


Figure 19 Host connect: direct attach—SAS—one server/one HBA/dual path

Two servers/one HBA per server/dual path

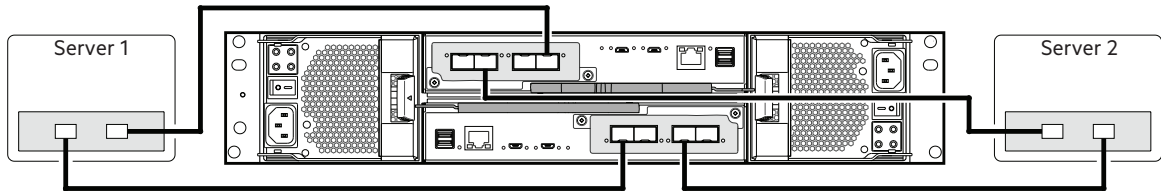


Figure 20 Host connect: direct attach—FC or iSCSI—two servers/one HBA per server/dual path

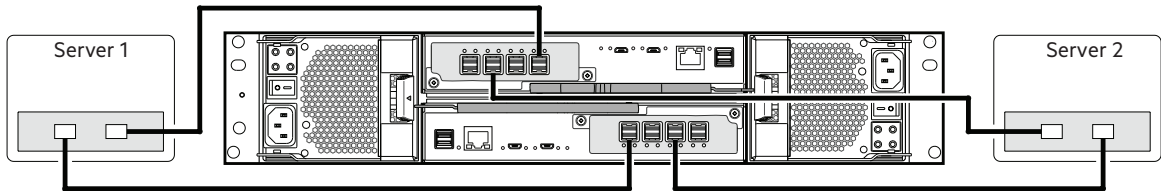


Figure 21 Host connect: direct attach—SAS—two servers/one HBA per server/dual path

Four servers/one HBA per server/dual path

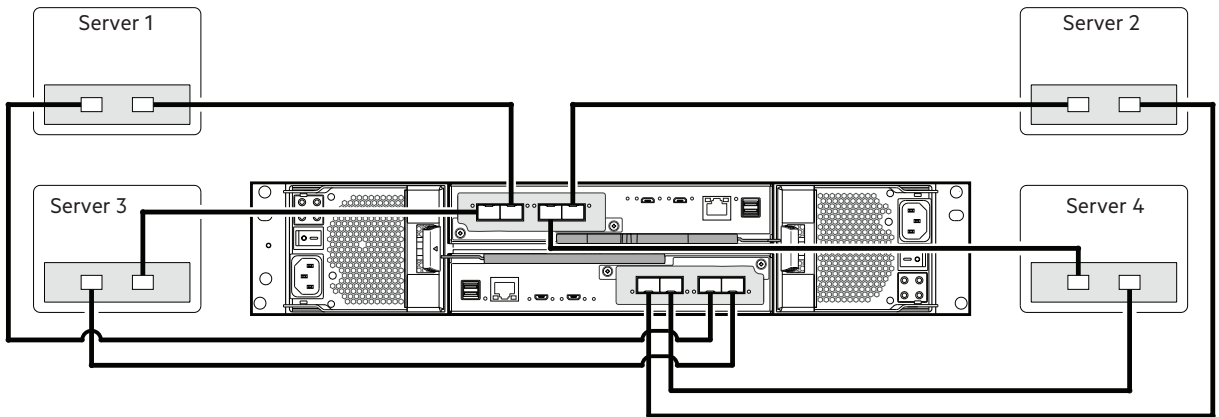


Figure 22 Host connect: direct attach—FC or iSCSI—four servers/one HBA per server/dual path

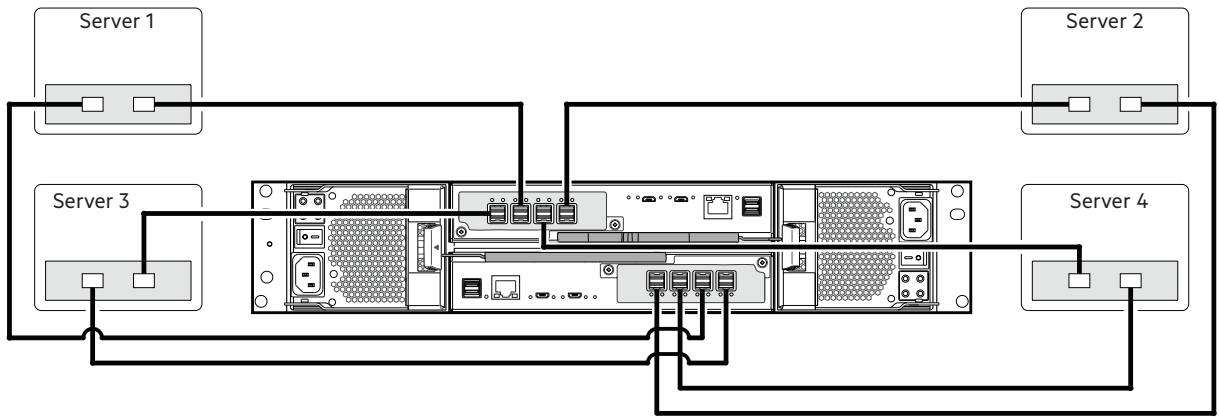


Figure 23 Host connect: direct attach—SAS—four servers/one HBA per server/dual path

Connecting switch attach configurations

NOTE Limit paths to a single LUN from a host to a total of eight (8) to align with software multipath best practices.

Two servers/two switches

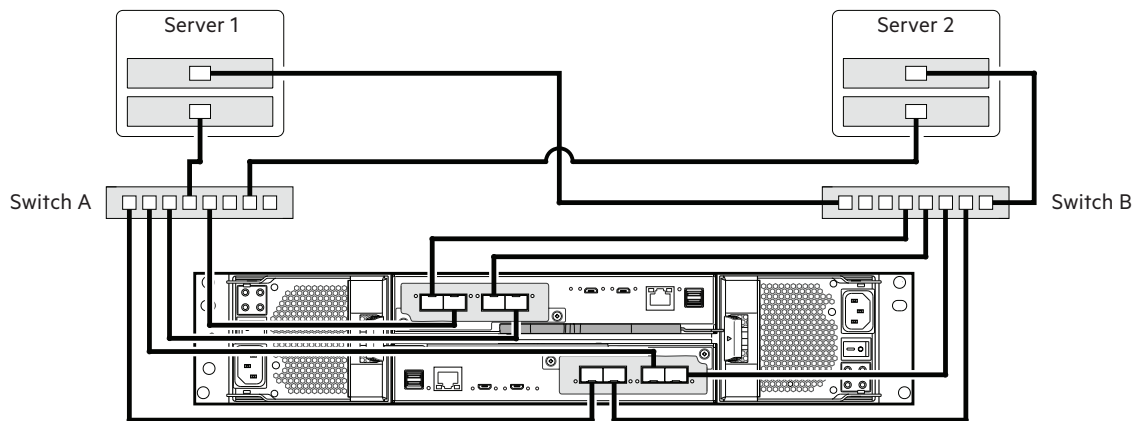


Figure 24 Host connect: switch attach—two servers/two switches

Four servers/multiple switches/SAN fabric

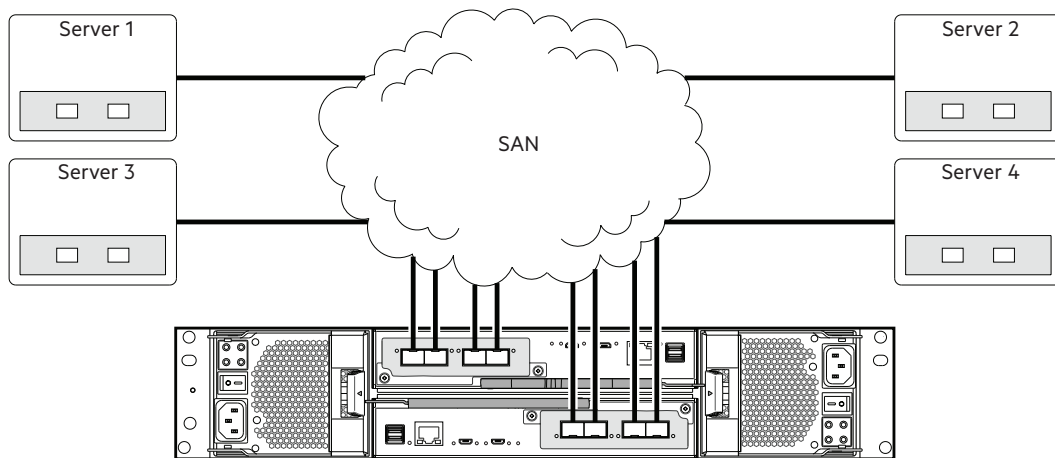


Figure 25 Host connect: switch attach—four servers/multiple switches/SAN fabric

Connecting management hosts over an Ethernet network

The management host manages MSA Storage systems out-of-band over an Ethernet network.

1. Connect an Ethernet cable with RJ45 connectors to the network management port on each controller module.
2. Connect the other end of each Ethernet cable to a network that your management host can access (preferably on the same subnet).
3. Set the network port IP addresses. For more information, see ["Obtaining IP values"](#) on page 38.

For the sake of system security, do not unnecessarily expose the controller module network port to an external network connection or to non-essential protocols.

NOTE Connections to this device must be made with shielded cables—grounded at both ends—with metallic RFI/EMI connector hoods, in order to maintain compliance with FCC Rules and Regulations.

NOTE Access via HTTPS and SSH is enabled by default, and access via HTTP and Telnet is disabled by default. See the Storage Management Guide for more information about suggested protocols.

Connecting two storage systems to replicate volumes

Remote Snap replication is a licensed feature for disaster-recovery. This feature performs asynchronous replication of block-level data from a volume in a primary system to a volume in a secondary system by creating an internal snapshot of the primary volume, and copying the changes to the data since the last replication to the secondary system via FC or iSCSI links.

The two associated volumes form a replication set, and only the primary volume (source of data) can be mapped for access by a server. Both systems must be licensed to use Remote Snap, and must be connected through switches to the same fabric or network (no direct attach). The server accessing the replication set must be connected to the primary system. If the primary system goes offline, a connected server can access the replicated data from the secondary system.

Replication configuration possibilities are many, and can be cabled—in switch attach fashion—to support MSA 2070/2072 FC storage systems or MSA 2070/2072 iSCSI storage systems on the same network, or on different networks (MSA 2070/2072 SAS storage systems do not support replication). As you consider the physical connections of your system—specifically the connections for replication—keep several important points in mind.

- Ensure that controllers have connectivity between systems, whether the destination system is co-located or remotely located.
- For MSA 2070/2072 Storage systems, qualified FC SFPs can be used for host I/O or replication, or both.
- For MSA 2070/2072 Storage systems, qualified 10GBase-T cable options can be used for host I/O or replication, or both.
- For MSA 2070/2072 Storage systems, qualified iSCSI SFP, DAC, and AOC cable options can be used for host I/O or replication, or both.
- The storage system does not provide for specific assignment of ports for replication. However, this can be accomplished by using virtual LANs for iSCSI and zones for FC, or by using physically separate infrastructure.
- For remote replication, ensure that all ports used for replication are able to communicate appropriately with the remote replication system by using:
 - The `query peer-connection` CLI command (see the CLI Reference Guide for more information) or
 - The SMU > Settings > Peer Connections panel (see the Storage Management Guide for more information)
- Allow a sufficient number of ports to perform replication. This permits the system to balance the load across those ports as I/O demands rise and fall. If some of the volumes replicated are owned by controller A and others are owned by controller B, then allow at least one port for replication on each controller module—and possibly more than one port per controller module—depending on replication traffic load.

Conceptual cabling examples address cabling on the same network and cabling relative to different networks.

! **IMPORTANT** Remote Snap must be licensed on all systems configured for replication, and the controller module firmware must be compatible on all systems licensed for replication.

NOTE Systems must be correctly cabled before performing replication. See the following documents for more information about using Remote Snap to perform replication tasks:

- HPE MSA Remote Snap Software Technical white paper
- HPE MSA 2070/2072 Best Practices
- HPE MSA 2070/2072 Storage Management Guide
- HPE MSA 2070/2072 CLI Reference Guide
- HPE MSA 2070/2072 Event Descriptions Reference Guide

To access MSA documentation, see: <https://www.hpe.com/info/msadocs>.

Cabling for replication

This section shows example replication configurations.

Example illustrations provide conceptual examples of cabling to support Remote Snap replication.

NOTE Simplified versions of controller enclosures are used in cabling illustrations to show host ports used for I/O or replication, given that only the external connectors used in the host interface ports differ.

- Replication supports FC and iSCSI host interface protocols.
- Each controller supports a single host interface protocol, whether used for replication, host I/O, or both.
- Colored cables indicate usage:
 - Orange shows replication
 - Blue shows I/O traffic on the source array
 - Tan shows I/O traffic on the destination array

After the storage systems are physically cabled, see the MSA 2070/2072 Storage Management Guide or online help for information about configuring, provisioning, and using the optional Remote Snap feature.

Host ports and replication

Multiple servers/single network

The diagram below shows the rear panel of two MSA 2070/2072 FC or two MSA 2070/2072 iSCSI controller enclosures with both I/O and replication occurring on the same physical network. With the replication configuration shown below, Virtual Local Area Network (VLAN) and zoning could be employed to provide separate networks for iSCSI and FC, respectively:

- Create a VLAN or zone for I/O traffic on the source array (blue cables).
- Create a VLAN or zone for I/O traffic on the destination array (tan cables).
- Create a VLAN or zone for replication to isolate I/O traffic from replication traffic (orange cables).

The configuration would appear physically as a single network, while logically, it would function as multiple networks.

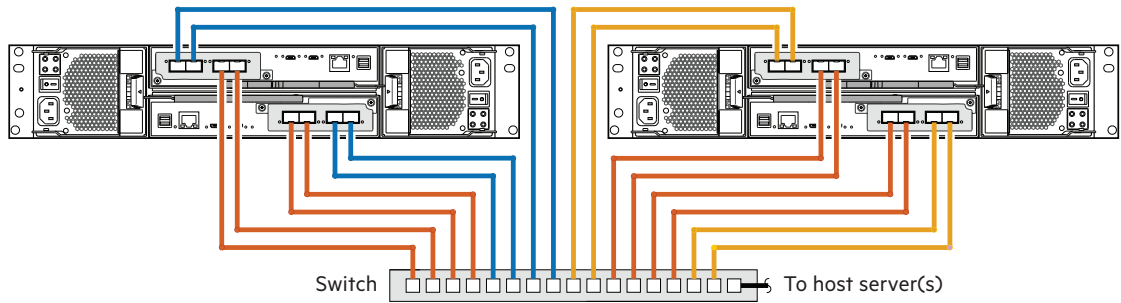


Figure 26 Connecting two storage systems for Remote Snap: multiple servers/one switch/one location

The diagram that follows shows the rear panel of two MSA 2070/2072 FC or two MSA 2070/2072 iSCSI controller enclosures with I/O and replication occurring on different physical networks. Use three switches to enable host I/O and replication. Connect two ports from each controller module in the left storage enclosure to the left switch. Connect two ports from each controller module in the right storage enclosure to the right switch. Connect two ports from each controller module in each enclosure to the middle switch.

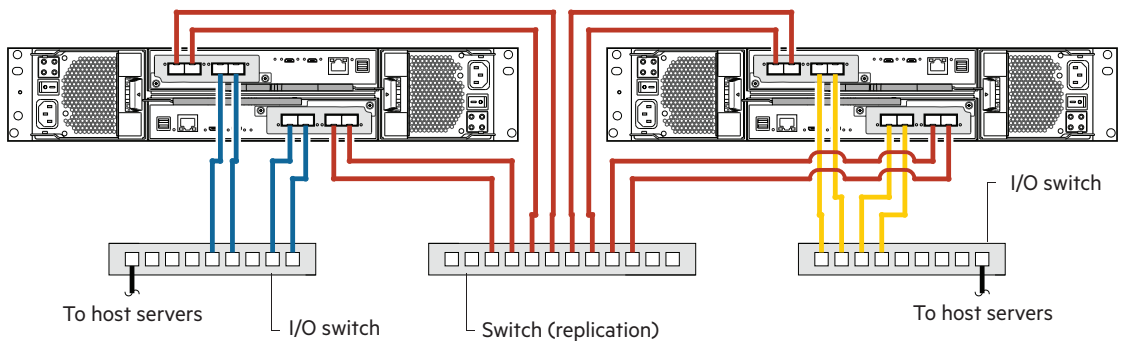


Figure 27 Connecting two storage systems for Remote Snap: multiple servers/switches/one location

Multiple servers/different networks/multiple switches

The diagram below shows the rear panel of two MSA 2070/2072 FC or two MSA 2070/2072 iSCSI controller enclosures with I/O and replication occurring on different networks.

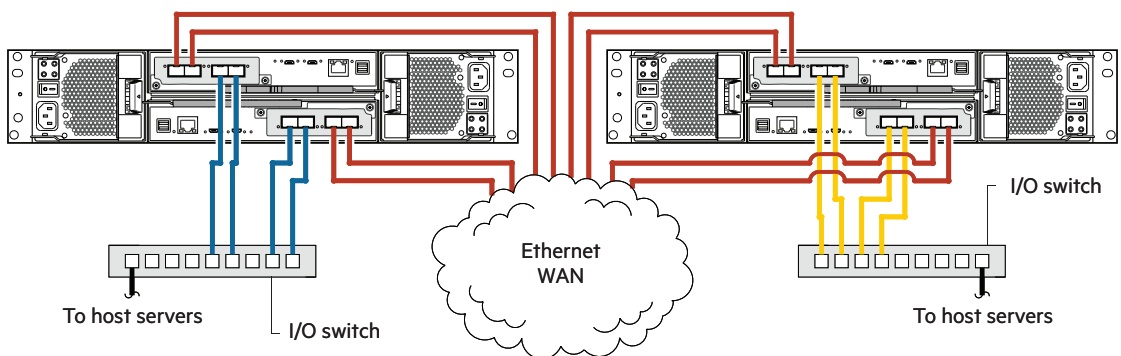


Figure 28 Connecting two storage systems for Remote Snap: multiple servers/switches/two locations

Updating firmware

After installing the hardware and powering on the storage system components for the first time, verify that the controller modules, expansion modules, and disk drives are using the current firmware release. When using the SMU, the preboarding process checks installed firmware versions, and provides for uploading and activating firmware if necessary.

NOTE Update component firmware by installing a firmware file obtained from the HPE web download site as described in "Accessing updates " on page 62. To install a Smart Component, follow the directions on the HPE website: <https://www.hpe.com/storage/msafirmware>. Follow the drive firmware support matrix link near the bottom of the page for disk drive firmware.

! **IMPORTANT** The storage system's management interfaces can check for firmware updates. See the topics about updating firmware within the Storage Management Guide before performing a firmware update.

NOTE To locate and download the latest software and firmware updates for your product, go to <https://www.hpe.com/support/downloads>.

5 Connecting to the controller CLI port

Device description

The MSA 2070/2072 controllers feature a command-line interface port used to cable directly to the controller and initially set IP addresses, or perform other configuration tasks. This port employs a micro-USB Type B form factor, requiring a cable that is supplied with the system, and additional support described herein, so that a server or other computer running a Linux or Windows operating system can recognize the controller enclosure as a connected device. Without this support, the computer might not recognize that a new device is connected, or might not be able to communicate with it.

For Linux systems, no new driver files are needed, but depending on the version of operating system, a Linux configuration file may need to be created or modified. For Windows computers, if you are using an operating system predating Windows 10/Server 2016, the Windows USB device driver must be downloaded from the HPE website, and installed on the computer that will be cabled directly to the controller command-line interface port (see also <https://www.hpe.com/support/downloads>).

NOTE Directly cabling to the CLI port is an out-of-band connection because it communicates outside the data paths used to transfer information from a computer or network to the controller enclosure.

Emulated serial port

After the CLI cable is attached to the controller module, the management computer should detect a new USB device. Using the Emulated Serial Port interface, the controller presents a single serial port using a vendor ID and product ID. Effective presentation of the emulated serial port assumes the management host previously had a terminal emulator installed (see [Table 3](#)). MSA 2070/2072 controllers support the following applications to facilitate connection.

Table 3 Supported terminal emulator applications

Application	Operating system
HyperTerminal, TeraTerm, PuTTY	Microsoft Windows (all versions)
Minicom	Linux (all versions)

Certain operating systems require a device driver or special mode of operation. Vendor and product identification are provided in [Table 4](#).

Table 4 Terminal emulator display settings

USB vendor identification code type	Code
USB vendor identification	0x210c
USB product identification	0xa4a7

Preparing a Linux system for cabling to the CLI port

You can determine if the operating system recognizes the USB (ACM) device by entering a command:

```
cat /proc/devices/ |grep -i "ttyACM"
```

If a device driver is discovered, the output will display:

```
ttyACM(and a device number)
```

You can query information about USB buses and the devices connected to them by entering a command:

lsusb

If a USB device driver is discovered, the output will display:

```
ID 210c:a4a7
```

The ID above is comprised of vendor ID and product ID terms as shown in the **Code** column of the preceding table.

ⓘ **IMPORTANT** Although Linux systems do not require installation of a device driver, on some operating system versions, certain parameters must be provided during driver loading to enable recognition of the MSA 2070/2072 controllers. To load the Linux device driver with the correct parameters on these systems, the following command is required:

```
modprobe usbserial vendor=0x210c product=0xa4a7 use_acm=1
```

Optionally, the information can be incorporated into the `/etc/modules.conf` file.

Preparing a Windows system for cabling to the CLI port

A Windows USB device driver is used for communicating directly with the controller command-line interface port using a USB cable to connect the controller enclosure and the management computer.

ⓘ **IMPORTANT** If using Windows 10/Server 2016 or newer, the operating system provides a native USB serial driver that supports the controller module's USB CLI port. However, if using an older version of Windows, you should download and install the USB device driver from your HPE MSA support page at <https://www.hpe.com/support/downloads>.

Obtaining IP values

You can manually set static IP address parameters for network ports, or you can specify that IP values be set automatically, using DHCP (Dynamic Host Configuration Protocol) for IPv4 or DHCPv6 or SLAAC (Stateless address auto-configuration) for IPv6.

Setting network port IP addresses using DHCP

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one is available. If a DHCP server is unavailable, current addressing is unchanged.

1. Look in the DHCP server's pool of leased addresses for two IP addresses assigned to the enclosure WWID followed by a controller ID (A or B).

The unique string is derived using the last 6 characters of the MAC address.

NOTE If you set up a DNS Hostname, the DHCP server will register that name instead of the string derived from the MAC address.

2. Use a ping broadcast to try to identify the device through the ARP table of the host.

If you do not have a DHCP server, you will need to ask your system administrator to allocate two IP addresses, and set them using the command-line interface during initial configuration (described below).

3. Use the CLI port and cable to determine the network information assigned by DHCP.
 - For IPv4, enter the **show network-parameters** CLI command.
 - For IPv6, enter the **show ipv6-network-parameters** CLI command.

NOTE For more information, see the topic about network configuration in the Storage Management Guide.

Setting network port IP addresses using the CLI port and cable

You can set network port IP addresses manually using the command-line interface port and cable. If you have not done so already, you need to enable your system for using the command-line interface port (see also ["Using the CLI port and cable — known issues on Windows" on page 42](#)).

For Linux systems, see ["Preparing a Linux system for cabling to the CLI port" on page 37](#). For Windows systems, see ["Preparing a Windows system for cabling to the CLI port" on the previous page](#).

Network ports on controller module A and controller module B are configured with the following factory-default IPv4 IP settings:

- **IP Address:** 10.0.0.2 (Controller A), 10.0.0.3 (Controller B)
- **IP Subnet Mask:** 255.255.255.0
- **Gateway IP Address:** 10.0.0.1

Network ports on controller module A and controller module B are configured with the following factory-default IPv6 IP settings:

Controller A

- **Autoconfig:** Enabled
- **Gateway:** ::
- **Link-Local Address:** fe80::2c0:ffff:fe44:952f
- **Autoconfig IP:** 6::2c0:ffff:fe44:952f

Controller B

- **Autoconfig:** Enabled (controller B)
- **Gateway:** ::
- **Link-Local Address:** fe80::2c0:ffff:fe44:7010
- **Autoconfig IP:** 6::2c0:ffff:fe44:7017

If the default IP addresses are not compatible with your network, you must set a valid IP address for each network port using the command-line interface.

Use the CLI commands described in the steps below to set the IP address for the network port on each controller module. After new IP addresses are set, you can change them as needed using the SMU.

NOTE Changing IP settings can cause management hosts to lose access to the storage system.

1. From your network administrator, obtain an IP address, subnet mask, and gateway address for controller A, and another for controller B.

Record these IP addresses so that you can specify them whenever you manage the controllers using the SMU or the CLI.

2. Use the provided USB cable to connect controller A to a USB port on a host computer. The USB micro-B male connector plugs into the CLI port.
3. Enable the CLI port for subsequent communication.

If the USB device is supported natively by the operating system, proceed to step 4.

- Linux customers should enter the command syntax provided in "Preparing a Linux system for cabling to the CLI port" on page 37.
 - Windows customers should locate the downloaded device driver described in "Preparing a Windows system for cabling to the CLI port" on page 38, and follow the instructions provided for proper installation.
4. Start and configure a terminal emulator using the display settings in Table 5 and the connection settings in Table 6 (also, see the note following this procedure).

Table 5 Terminal emulator display settings

Parameter	Value
Terminal emulator mode	VT-100 or ANSI (for color support)
Font	Terminal
Translations	None
Columns	80

Table 6 Terminal emulator connection settings

Parameter	Value
Connector	COM3 (for example) ^{1,2}
Baud rate	115,200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

1—Your server or laptop configuration determines which COM port is used for Disk Array USB Port.
2—Verify the appropriate COM port for use with the CLI.

5. In the terminal emulator, connect to controller A.
6. Press `Enter` to display the CLI.

The CLI displays the system version, OS version, MC version, serial number, and login prompt:

- To log in to the system for the first time, enter username **setup** and follow the on-screen directions to create a user account. After the new user account is created, the user session is closed.
 - To log in to the system again and make additional changes, use the user account credentials that were just created.
7. At the prompt, type the following command to set the values you obtained in step 1 on page 44 for each network port, first for controller A and then for controller B:

```
set network-parameters ip <address> netmask <netmask> gateway <gateway> controller a|b
```

where:

- <address> is the IP address of the controller
- <netmask> is the subnet mask
- <gateway> is the IP address of the subnet router
- a|b specifies the controller whose network parameters you are setting

For example:

```
# set network-parameters ip 192.168.0.10 netmask 255.255.255.0 gateway 192.168.0.1
controller a
```

```
# set network-parameters ip 192.168.0.11 netmask 255.255.255.0 gateway 192.168.0.1
controller b
```

NOTE See the CLI Reference Guide for information about IPv6, and the commands used to add IPv6 addresses and set IPv6 network parameters. The **ipv6** term is included within each relevant command name.

8. Type the following command to verify the new IP address:
 - For IPv4, enter the **show network-parameters** CLI command.
 - For IPv6, enter the **show ipv6-network-parameters** CLI command.

Network parameters, including the IP address, subnet mask, and gateway address are displayed for each controller.

9. Use the ping command to verify network connectivity.

For example, to ping the gateway in the examples above:

```
# ping 192.168.0.1
Info: Pinging 192.168.0.1 with 4 packets.
Success: Command completed successfully. - The remote computer responded with 4
packets.
```

10. In the host computer's command window, type the following command to verify connectivity, first for controller A and then for controller B:

```
ping <controller-IP-address>
```

If you cannot access your system for at least three minutes after changing the IP address, your network might require you to restart the Management Controller(s) using the CLI port. When you restart a Management Controller, communication with the MC is temporarily lost until it successfully restarts.

Type the following command to restart the management controller on both controllers:

```
restart mc both
```

11. When you are done using the CLI, exit the emulator.
12. Retain the new IP addresses to access and manage the controllers, using either the SMU or the CLI.

NOTE Using HyperTerminal with the CLI on a Microsoft Windows host:

On a host computer connected to a controller module's micro-USB CLI port, incorrect command syntax in a HyperTerminal session can cause the CLI to hang. To avoid this problem, use correct syntax, use a different terminal emulator, or connect to the CLI using SSH rather than the micro-USB cable.

Be sure to close the HyperTerminal session before shutting down the controller or restarting its Management Controller. Otherwise, the host's CPU cycles may rise unacceptably.

If communication with the CLI is disrupted when using an out-of-band cable connection, communication can sometimes be restored by disconnecting and reattaching the micro-USB cable as described in step 2 above.

NOTE If using a Windows operating system version older than Windows 10/Server 2016, access the USB device driver download from the HPE MSA support website at <https://www.hpe.com/support/downloads>.

Using the CLI port and cable — known issues on Windows

When using the CLI port and cable for setting controller IP addresses and other operations, be aware of the following known issues on Microsoft Windows platforms.

Problem

On Windows operating systems, the USB CLI port may encounter issues preventing the terminal emulator from reconnecting to storage after the Management Controller (MC) restarts or the USB cable is unplugged and reconnected.

Workaround

To restore a hung connection after restarting the MC:

1. For any hung connection, quit the terminal emulator program.
2. In the Windows Device Manager, right-click on the problem COM port and select **Disable**.
3. Confirm the COM port disabled status.
4. Right-click on COM port you just disabled and select **Enable** to re-enable it.
5. Start the terminal emulator program and connect to the COM port.
6. Validate the port settings.

NOTE When using Windows 10/Server 2016 with PuTTY, the XON/XOFF setting must be disabled, or the COM port will not open.

6 Basic operation

Verify that you have completed the sequential instructions in "Installation checklist" on page 20. After you have successfully completed steps 1 through 8 therein, you can access the management interface using your web browser to complete the system setup.

Accessing the SMU

Upon completing the hardware installation, you can access the Storage Management Utility (SMU)—the web-based management interface—from the controller module to monitor and manage the storage system. Invoke your web browser, and enter the `https://<IP-address>` of the controller module's network port in the address field (obtained during completion of "Installation checklist" on page 20), then press `Enter`. When signing in to the SMU for the first time, you will be required to create a user if you have not already done so. Follow the on-screen directions to complete setting up your system. After you complete the preboarding and onboarding steps, you will be taken to the system Dashboard. From here, you will begin to use the SMU to monitor and manage the storage system.

! **IMPORTANT** For detailed information about accessing and using the SMU, see the topic about getting started in the Storage Management Guide. This topic provides directions for signing-in to the SMU, introduces key concepts, addresses browser setup, and provides tips for using the system Dashboard and accessing help.

💡 TIP After signing in to the SMU—and completing preboarding and onboarding—you can use online help and available tool tips as an alternative to consulting the Storage Management Guide.

Configuring and provisioning the storage system

Use the SMU to configure and provision the storage system. If the configuration and provisioning steps have not been completed when you access the storage system, the wizard will guide you through these processes. If you are licensed to use the optional Remote Snap feature, you may also need to set up storage systems for replication.

See the following topics within the Storage Management Guide or SMU online help:

- Configuring the system settings
- Provisioning the system
- Using Remote Snap to replicate volumes

! **IMPORTANT** Some features within the storage system require a license. The license is specific to the controller enclosure and firmware version. See the topic about installing a license within the Storage Management Guide for directions about viewing the status of licensed features and installing a license.

! **IMPORTANT** If the system is used in a VMware environment, set the system Missing LUN Response option to use its Illegal Request setting. To do so, see either the topic about changing the missing LUN response in the Storage Management Guide, or the topic about the `set advanced-settings` command in the CLI Reference Guide.

7 Troubleshooting

These procedures are intended to be used only during initial configuration, for the purpose of verifying that hardware setup is successful. They are not intended to be used as troubleshooting procedures for configured systems using production data and I/O.

USB CLI port connection

MSA 2070/2072 controllers feature a CLI port employing a micro-USB Type B form factor. If you encounter problems communicating with the port after cabling your computer to the USB device, you may need to either download a device driver (Windows), or set appropriate parameters via an operating system command (Linux). See ["Connecting to the controller CLI port" on page 37](#) for more information. You may need to unplug and reconnect the CLI cable if the terminal emulator application cannot access the COM port.

Fault isolation methodology

MSA 2070/2072 controllers provide many ways to isolate faults. This section presents the basic methodology used to locate faults within a storage system, and to identify the associated Field Replaceable Units (FRUs) affected.

As noted in ["Basic operation" on page 43](#), use the SMU to configure and provision the system upon completing the hardware installation. As part of this process, configure and enable event and/or alert notification so the system will notify you when a problem occurs that is at or above the configured severity (as described in the Storage Management Guide). With notifications configured and enabled, you can follow the recommended actions in the notification message to resolve the problem, as further discussed in the options presented below.

Basic steps

The basic fault isolation steps are listed below and described in ["Performing basic steps" on page 46](#):

- Gather fault information, including using system LEDs.
- Determine where in the system the fault is occurring.
- Review event logs.
- If required, isolate the fault to a data path component or configuration.

Cabling systems to enable use of the licensed Remote Snap feature—to replicate volumes—is another important fault isolation consideration pertaining to initial system installation. See ["Isolating Remote Snap replication faults" on page 56](#) more information about troubleshooting during initial setup.

Options available for performing basic steps

When performing fault isolation and troubleshooting steps, select the option or options that best suit your site environment. Use of any option (four options are described below) is not mutually exclusive to the use of another option. You can use the SMU to check the health icons/values for the system and its components to ensure that everything is okay, or to drill down to a problem component. If you discover a problem, both the SMU and the CLI provide recommended action text online. Options for performing basic steps are listed according to frequency of use:

- Monitor event or alert notification.
- Use the SMU.

- Use the CLI.
- View the enclosure LEDs.

Monitor notifications

With notifications configured and enabled, you can view alerts or event logs to monitor the health of the system and its components. Alerts inform the user of conditions requiring action to maintain availability and prevent potential loss of data. Timely alert notification compels user acknowledgment via the SMU, leading to resolution. In contrast, events are logged for many different storage system activities, and the event logs can be viewed by category using different access methods. These complimentary notification subsystems are further described herein.

Alerts

You can view information about alerts using either the SMU or the CLI. Using the SMU, you can access the Alerts panel from the system Dashboard to view the scrollable list of alerts. This panel allows you to drill down to acknowledge and resolve alerts. The Alerts panel allows for compact or expanded views with tables showing the status of active alerts and alert history. Using the CLI, you can run the `show alerts` command (with additional parameters to filter the output) to see detail for a storage system component. You can also run the `show alert-condition-history` CLI command to view a log history of alert conditions that have generated alerts.

Events

If a message tells you to check whether an event has been logged, or to view information about an event in the log, you can do so using either the SMU or the CLI. Using the SMU, you can view the event log and then click on the event message to see detail about that event. Using the CLI, you can run the `show events detail` command (with additional parameters to filter the output) to see the detail for an event.

Typical log data that can be written to a compressed file on the network include device status summary, the event log from each controller, the debug log from each controller, the boot log from each controller, and critical error dumps from each controller, if critical errors have occurred. Alternative methods for obtaining log data are to use the Collect Logs action (Maintenance > Support) in the SMU or the `get logs` command in the FTP or SFTP interface. These methods transfer the entire contents of a log file without changing its capacity-status level. Use of Collect Logs or `get logs` is expected as part of providing information for a technical support request.

Use the SMU

The SMU's Dashboard provides access to an Alerts panel listing current issues you should be aware of. You can acknowledge alerts and determine how to resolve them. Once an alert is acknowledged and resolved, it is removed from the scrollable list.

The SMU uses health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. The SMU enables you to monitor the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown. Use the SMU to drill down to find each component that has a problem, and follow actions in the Recommendation field for the component to resolve the problem.

Use the CLI

As an alternative to using the SMU, you can run the `show system` command in the CLI to view the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown, and those components will be listed as Unhealthy Components. Follow the recommended actions in the component Health Recommendation field to resolve the problem.

View the enclosure LEDs

You can view the LEDs on the hardware (while referring to ["LED descriptions" on page 64](#) for your enclosure model) to identify component status. If a problem prevents access to either the SMU or the CLI, this is the only option available. However, monitoring/management is often done using the SMU interface rather than relying on line-of-sight to LEDs of racked hardware components.

Performing basic steps

You can use any of the available options in performing the basic steps comprising the fault isolation methodology.

Gather fault information

When a fault occurs, it is important to gather as much information as possible. Doing so will help you determine the correct action needed to remedy the fault.

Begin by reviewing the reported fault:

- Is the fault related to an internal data path or an external data path?
- Is the fault related to a hardware component such as a disk drive module, controller module, expansion module, or PCM?

Determine where the fault is occurring

When a fault occurs, the management interfaces report the condition using alerts and event logs. The Fault ID status LED on the enclosure left ear (see ["Front panel components" on page 11](#)) also illuminates.

Use the SMU to verify any faults found.

- Alerts indicate where the fault is occurring. Observing enclosure components in the **Maintenance > Hardware** and **Maintenance > About > Hardware Information** panels can provide additional context for resolving the reported failure or fault. See also ["Monitor notifications" on the previous page](#) and ["Review alerts" below](#).
- Event logs contain storage system information classified by event category. See also ["Monitor notifications" on the previous page](#) and ["Review the event logs" on the facing page](#).

The SMU is useful in determining where the fault is occurring, especially if the LEDs cannot be viewed due to the location of the system. The SMU provides you with a visual representation of the system—including front and rear enclosure views—and indicates where the fault is occurring. It provides detailed information about FRUs, data, and faults.

If the SMU is unavailable, observe the enclosure LEDs. The enclosure LEDs are designed to alert users of any system faults. Check the LEDs on the back of the enclosure to narrow the fault to a FRU, connection, or both. The LEDs also help you identify the location of a FRU reporting a fault.

Review alerts

Alerts report system faults, and they are used to monitor system health and track the resolution of reported system health issues.

You can access alerts from the Alerts panel on the system Dashboard. The Active Alerts table provides a scrollable list of active health alerts in the system. For each alert, the table shows the following:

- How long the alert has been active
- Severity of the alert
- Affected system component

- Description of the problem
- Whether the alert has been acknowledged, and whether it has been resolved

Additional controls provide greater detail and recommended actions for alert resolution, if applicable. For more information about managing alerts, see the Storage Management Guide or the online help provided in the SMU.

Review the event logs

The event logs record all system events. Each event has a numeric code that identifies the type of event that occurred, and has one of the following severities:

- Critical. A failure occurred that may cause a controller to shut down or place data at risk. Correct the problem immediately.
- Error. A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
- Warning. A problem occurred that may affect system stability, but not data integrity. Evaluate the problem and correct it if necessary.
- Informational. A configuration or state change occurred, or a problem occurred that the system corrected. No immediate action is required.
- Resolved. A condition that caused an event to be logged has been resolved. No action is required.

For information about specific events, see the Event Descriptions Reference Guide, located on the Hewlett Packard Enterprise Information Library website: <https://www.hpe.com/info/msadocs>.

The event logs record all system events. It is very important to review the logs, not only to identify the fault, but also to search for events that might have caused the fault to occur. For example, a host could lose connectivity to a disk group if a user changes channel settings without taking the storage resources assigned to it into consideration. In addition, the type of fault can help you isolate the problem to either hardware or software.

Isolate the fault

Occasionally it might become necessary to isolate a fault. This is particularly true with data paths, due to the number of components comprising the data path. For example, if a host-side data error occurs, it could be caused by any of the components in the data path: controller module, cable, connectors, switch, or data host (HBA/NIC).

If an expansion enclosure does not initialize

It may take up to two minutes for the enclosures in the storage system to initialize. If an expansion enclosure within the storage system does not initialize:

- Make sure the power cord is properly connected, and check the power source that it is connected to.
- Verify that the expansion cabling connections for the enclosure are correct.
- Perform a rescan to force a rediscovery of disks and enclosures in the storage system.
- Power cycle the system.
- Check the event log for errors.

Correcting enclosure IDs

When installing a system with disk enclosures attached, the enclosure IDs might not match the physical cabling order. This is because the controller might have been previously attached to some of the same enclosures during factory testing, and attempts to preserve the previous enclosure IDs if possible. To correct this condition, make sure that both controllers are up, and perform a rescan using the SMU or the CLI. This will reorder the enclosures, but can take up to

two minutes for the enclosure IDs to be corrected. The rescan temporarily pauses all I/O processes, then resumes normal operation.

To perform a rescan using the CLI, type the following command:

```
rescan
```

To rescan using the SMU:

1. Verify that both controllers are operating normally.
2. Select **Maintenance > Hardware > <enclosure-ID> > Actions > Rescan All Disks**.
3. Click **Rescan**.

Stopping I/O

When troubleshooting disk drive and connectivity faults, stop I/O to all volumes in the pool with the affected disk group, from all hosts and remote systems as a data protection precaution. As an additional data protection precaution, it is recommended to conduct regularly scheduled backups of your data.

! **IMPORTANT** Stopping I/O to a disk group is a host-side task, and falls outside the scope of this document.

When on-site, you can verify there is no I/O activity by briefly monitoring the system LEDs. When accessing the storage system remotely, this is not possible. Remotely, you can use the `show disk-group-statistics` CLI command to determine if input and output has stopped. Perform these steps:

1. Using the CLI, run the `show disk-group-statistics` command.

The `Reads` and `Writes` outputs show the number of these operations that have occurred since the statistic was last reset, or since the controller was restarted.

Record the numbers displayed.

2. Run the `show disk-group-statistics` command a second time.

This provides you a specific window of time (the interval between requesting the statistics) to determine if data is being written to or read from the disk group. Record the numbers displayed.

3. To determine if any reads or writes occur during this interval, subtract the set of numbers you recorded in step 1 from the numbers you recorded in step 2.

If the resulting difference is zero, then I/O has stopped.

If the resulting difference is not zero, a host is still reading from or writing to this disk group. Continue to stop I/O from hosts, and repeat step 1 and step 2 until the difference in step 3 is zero.

Diagnostic steps

This section describes possible reasons and actions to take when an LED indicates a fault condition during initial system setup. See "[LED descriptions](#)" on page 64 for descriptions of all LED statuses.

In addition to monitoring LEDs via line-of-sight observation of racked hardware components when performing diagnostic steps, you can also monitor the health of the system and its components using the management interfaces. Be mindful of this when reviewing the Actions column in the diagnostics tables, and when reviewing the step procedures provided in this chapter.

Is the enclosure front panel Fault/Service Required LED amber?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	A fault condition exists/occurred. If installing an I/O module FRU, the module has not gone online and likely failed its self-test.	<ul style="list-style-type: none"> Check the LEDs on the back of the controller enclosure to narrow the fault to a FRU, connection, or both. Check the event log for specific information regarding the fault. Follow any recommended actions. If installing an IOM FRU, try removing and reinstalling the new IOM, and check the event log for errors. If the above actions do not resolve the fault, isolate the fault and contact an authorized service provider for assistance. Replacement may be necessary.

Table 7 Diagnostics LED status: Front panel "Fault/Service Required"

Is the enclosure rear panel FRU OK LED off?

This table pertains to the controller module FRU OK LED (not the PCM OK LED).

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Blinking	System is booting.	Wait for the system to boot.
Yes	The controller module is not powered on. The controller module has failed.	<ul style="list-style-type: none"> Verify the controller module is fully inserted and latched in place, and that the enclosure is powered on. Check the event log for specific information regarding the failure.

Table 8 Diagnostics LED status: Rear panel "FRU OK"

Is the enclosure rear panel Fault/Service Required LED amber?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes (blinking)	One of the following errors occurred: <ul style="list-style-type: none"> Hardware-controller power-up error Cache flush error Cache self-refresh error 	<ul style="list-style-type: none"> Restart this controller from the other controller using the SMU or CLI. If the above action does not resolve the fault, remove the controller module and reinsert it. If the above action does not resolve the fault, contact an authorized service provider for assistance. It may be necessary to replace the controller module.

Table 9 Diagnostics LED status: Rear panel "Fault/Service Required"

Are both disk drive module LEDs off (Online/Activity and Fault/UID)?

Answer	Possible reasons	Actions
Yes	<ul style="list-style-type: none"> There is no power. The disk is offline. The disk is not configured. 	Verify that the disk drive module is fully inserted and latched in place, and that the enclosure is powered on.

Table 10 Diagnostics LED status: Front panel disks "Online/Activity" and "Fault/UID"

NOTE See "Disks used in storage enclosures" on page 14.

Is the disk drive module Fault/UID LED blinking amber?


Answer	Possible reasons	Actions
Yes, 1 second on and 1 second off, and the Activity LED is blinking.	The disk drive is rebuilding.	No action required.  CAUTION Do not remove a disk drive that is reconstructing. Removing a reconstructing disk drive might terminate the current operation and cause data loss.
Yes, 3 seconds on and 1 second off, and the Activity LED is flickering.	The disk drive is identified.	No action required.

Table 11 Diagnostics LED status: Front panel disks "Fault/UID"

NOTE See "FDE considerations" on page 20.

Is the disk drive module Fault/UID LED amber?

Answer	Possible reasons	Actions
Yes, and the Activity LED is off.	The disk drive is offline. A predictive failure alert may have been received for this device.	<ul style="list-style-type: none"> • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance.
Yes, and the Activity LED is blinking.	The disk drive is active, but a predictive failure alert may have been received for this device.	<ul style="list-style-type: none"> • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance.

Table 12 Diagnostics LED status: Front panel disks "Fault/UID"

NOTE See "FDE considerations" on page 20.

Is a connected host port Host Link Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • Inspect cables for damage. Replace cable if necessary. • Swap cables to determine if the fault is caused by a defective cable. Replace the cable if necessary. • Verify that the switch, if any, is operating properly. If possible, test with another port. • Verify that the HBA is fully seated, and that the PCI slot is powered on and operational. • In the SMU, review event logs for indicators of a specific fault in a host data path component. Follow any recommended actions. • Contact an authorized service provider for assistance. • See "Isolating a host side connection fault" on page 53.

Table 13 Diagnostics LED status: Rear panel "Host Link Status"

Is a connected host port Expansion Port Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • Inspect cables for damage. Replace cable if necessary. • Swap cables to determine if the fault is caused by a defective cable. Replace the cable if necessary. • In the SMU, review event logs for indicators of a specific fault in a host data path component. Follow any recommended actions. • Contact an authorized service provider for assistance. • See "Isolating a controller module expansion port connection fault" on page 55.

Table 14 Diagnostics LED status: Rear panel "Expansion Port Status"

Is a connected port Network Port Link Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • Inspect cables for damage. Replace cable if necessary. • Swap cables to determine if the fault is caused by a defective cable. Replace cable if necessary. • Verify that the switch, if any, is operating properly. If possible, test with another port. • Verify that the HBA is fully seated, and that the PCI slot is powered on and operational. • In the SMU, review event logs for indicators of a specific fault in a network component. Follow any recommended actions. • Use standard networking troubleshooting procedures to isolate faults on the network.

Table 15 Diagnostics LED status: Rear panel "Network Port Link Status"

Is the power supply PCM OK LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The power supply module is not receiving adequate power.	<ul style="list-style-type: none"> Verify that the power cable is properly connected, and check the power source to which it connects. Verify that the PCM is firmly locked into position within the PCM slot. In the SMU, review event logs for specific information regarding a PCM fault. Follow any recommended actions. If the above action does not resolve the fault, isolate the fault, and contact an authorized service provider for assistance.

Table 16 Diagnostics LED status: Rear panel power supply module "PCM OK"

Is the power supply AC Fail/Fan Fail/DC Fail LED amber?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The power supply unit or a fan is operating at an unacceptable voltage/RPM level, or has failed.	<p>When isolating faults in the power supply module, remember that the fans in both modules receive power through a common bus on the midplane, so if a power supply unit fails, the fans continue to operate normally.</p> <ul style="list-style-type: none"> Verify that the power supply module is firmly locked into position within the PCM slot. Verify that the power cable is connected to a power source. Verify that the power cable is connected to the power supply module.

Table 17 Diagnostics LED status: Rear panel power supply module "AC Fail/Fan Fail/DC Fail"

Controller failure

Cache memory is flushed to nonvolatile memory in the case of a controller failure or power loss. During the write to nonvolatile memory process, only the components needed to write the cache to nonvolatile memory are powered by the supercapacitor. This process typically takes 60 seconds per 1 Gbyte of cache. After the cache is copied to nonvolatile memory, the remaining power left in the supercapacitor is used to refresh the cache memory. While the cache is being maintained by the supercapacitor, the Cache Status LED flashes momentarily slowly.

If the controller has failed or does not start, is the Cache Status LED on/blinking?

Answer	Actions
No, the Cache Status LED is off, and the controller does not boot.	Replace the controller module.
No, the Cache Status LED is off, and the controller boots.	The system has flushed data to disks. If the problem persists, replace the controller module.
Yes, at a strobe 1:10 rate – 1 Hz, and the controller does not boot.	Replace the controller module.
Yes, at a strobe 1:10 rate – 1 Hz, and the controller boots.	The system is in self-refresh mode. If the problem persists, replace the controller module.

Table 18 Diagnostic LED status: Rear panel "Cache Status"

Answer	Actions
Yes, at a blink 1:1 rate – 1 Hz, and the controller does not boot.	Replace the controller module.
Yes, at a blink 1:1 rate – 1 Hz, and the controller boots.	The system is flushing data to nonvolatile memory. If the problem persists, replace the controller module.

Table 18 Diagnostic LED status: Rear panel "Cache Status" (continued)

NOTE See also ["Cache Status LED details" on page 74.](#)

Isolating a host side connection fault

During normal operation, when a controller module host port is connected to a data host, the port's host link status/link activity LED is green. If there is I/O activity, the LED blinks green. If data hosts are having trouble accessing the storage system, and you cannot locate a specific fault or cannot access the event logs, use the following procedure. This procedure requires scheduled downtime.

! **IMPORTANT** Do not perform more than one step at a time. Changing more than one variable at a time can complicate the troubleshooting process.

Host-side connection troubleshooting featuring FC and iSCSI host ports

The procedure below applies to MSA 2070/2072 controller enclosures using small form factor pluggable (SFP) transceivers in Fibre Channel or iSCSI host interface ports. It also applies to qualified cable options used for 10GBase-T and DAC. In the following procedure, "cable option" is used to refer to any of the qualified cable options supporting host interface ports used for I/O or replication.

NOTE When experiencing difficulty diagnosing performance problems with enclosures using SFPs, consider swapping out one SFP at a time to see if performance improves.

1. Halt all I/O from hosts to the system (see ["Stopping I/O" on page 48](#)).
2. Check the host link status/link activity LED.
If there is activity, halt all applications that access the storage system.
3. Check the Cache Status LED to verify that the controller cached data is flushed to the disk drives.
 - Solid – Cache contains data yet to be written to the disk.
 - Blinking – Cache data is being written to nonvolatile memory.
 - Flashing at 1/10 second on and 9/10 second off – Cache is being refreshed by the supercapacitor.
 - Off – Cache is clean (no unwritten data).
4. Remove the cable option and inspect for damage.
5. Reseat the cable option.
Is the host link status/link activity LED on?
 - Yes – Monitor the status to ensure there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
 - No – Proceed to the next step.
6. Move the cable option to a port with a known good link status.
This isolates the problem to the external data path (SFP if used, host cable, and host-side devices) or to the controller

module port.

Is the host link status/link activity LED on?

- Yes – You now know that the cable option and host-side devices are functioning properly. Return the cable option to the original port. If the link status/link activity LED remains off, you have isolated the fault to the controller module port. Replace the controller module.
 - No – Proceed to the next step.
7. For enclosures using SFPs, swap the SFP with the known good one.
Is the host link status/link activity LED on?
- Yes – You have isolated the fault to the SFP. Replace the SFP.
 - No – Proceed to the next step.
8. For enclosures using SFPs, re-insert the original SFP and swap the cable with a known good one.
Is the host link status/link activity LED on?
- Yes – You have isolated the fault to the cable. Replace the cable.
 - No – Proceed to the next step.
9. For enclosures using cable options without SFPs, swap the cable option with a known good one.
Is the host link status/link activity LED on?
- Yes – You have isolated the fault to the cable. Replace the cable.
 - No – Proceed to the next step.
10. If a switch is being used as part of the data path, verify it is operating properly. If possible, test with another port.
11. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
12. Replace the HBA with a known good HBA, or move the host side cable and SFP to a known good HBA.
Is the host link status/link activity LED on?
- Yes – You have isolated the fault to the HBA. Replace the HBA.
 - No – It is likely that the controller module must be replaced.
13. Move the cable option back to its original port.
Is the host link status/link activity LED on?
- No – The controller module port has failed. Replace the controller module.
 - Yes – Monitor the connection for a period of time. It may be an intermittent problem, which can occur with damaged SFPs, host cables, and HBAs.

Host-side connection troubleshooting featuring SAS host ports

The procedure below applies to MSA 2070/2072 controller enclosures employing 12Gb SFF-8644 connectors in mini-SAS HD host interface ports used for I/O.

1. Halt all I/O from hosts to the system (see ["Stopping I/O" on page 48](#)).
2. Check the host link status/link activity LED.
If there is activity, halt all applications that access the storage system.
3. Check the Cache Status LED to verify that the controller cached data is flushed to the disk drives.
 - Solid – Cache contains data yet to be written to the disk.
 - Blinking – Cache data is being written to nonvolatile memory.
 - Flashing at 1/10 second on and 9/10 second off – Cache is being refreshed by the supercapacitor.
 - Off – Cache is clean (no unwritten data).
4. Reseat the host cable and inspect for damage.
Is the host link status/link activity LED on?

- Yes – Monitor the status to ensure there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
 - No – Proceed to the next step.
5. Move the host cable to a port with a known good link status.
This isolates the problem to the external data path (host cable and host-side devices) or to the controller module port.
Is the host link status/link activity LED on?
- Yes – You now know that the host cable and host-side devices are functioning properly. Return the cable to the original port. If the link status/link activity LED remains off, you have isolated the fault to the controller module port. Replace the controller module.
 - No – Proceed to the next step.
6. Swap the host cable with a known good one.
Is the host link status/link activity LED on?
- Yes – You have isolated the fault to the cable. Replace the cable.
 - No – Proceed to the next step.
7. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
8. Replace the HBA with a known good HBA, or move the host side cable to a known good HBA.
Is the host link status/link activity LED on?
- Yes – You have isolated the fault to the HBA. Replace the HBA.
 - No – It is likely that the controller module must be replaced.
9. Move the host cable back to its original port.
Is the host link status/link activity LED on?
- No – The controller module port has failed. Replace the controller module.
 - Yes – Monitor the connection for a period of time. It may be an intermittent problem, which can occur with damage cables, and HBAs.

Isolating a controller module expansion port connection fault

During normal operation, when a controller module expansion port is connected to a drive enclosure, the expansion port status LED is green. If the connected port's expansion port LED is off, the link is down. Use the following procedure to isolate the fault.

This procedure requires scheduled downtime.

NOTE Do not perform more than one step at a time. Changing more than one variable at a time can complicate the troubleshooting process.

1. Halt all I/O to the storage system as described in ["Stopping I/O" on page 48](#).
2. Check the host activity LED.
If there is activity, halt all applications that access the storage system.
3. Check the Cache Status LED to verify that the controller cached data is flushed to the disk drives.
 - Solid – Cache contains data yet to be written to the disk.
 - Blinking – Cache data is being written to nonvolatile memory.

- Flashing at 1/10 second on and 9/10 second off – Cache is being refreshed by the supercapacitor.
 - Off – Cache is clean (no unwritten data).
4. Reseat the expansion cable, and inspect it for damage.
Is the expansion port status LED on?
 - Yes – Monitor the status to ensure there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
 - No – Proceed to the next step.
 5. Move the expansion cable to a port on the controller enclosure with a known good link status.
This isolates the problem to the expansion cable or to the controller module expansion port.
Is the expansion port status LED on?
 - Yes – You now know that the expansion cable is good. Return the cable to the original port. If the expansion port status LED remains off, you have isolated the fault to the controller module port. Replace the controller module.
 - No – Proceed to the next step.
 6. Verify that you have moved the expansion cable back to the original port on the controller enclosure.
 7. Move the expansion cable on the drive enclosure to a known good expansion port on the drive enclosure.
Is the expansion port status LED on?
 - Yes – You have isolated the problem to the drive enclosure port. Replace the expansion module.
 - No – Proceed to the next step.
 8. Replace the cable with a known good cable, ensuring the cable is attached to the original ports used by the previous cable.
Is the host link status LED on?
 - Yes – Replace the original cable. The fault has been isolated.
 - No – It is likely that the controller module must be replaced.

Isolating Remote Snap replication faults

Remote Snap replication is a licensed disaster-recovery feature that performs asynchronous replication of block-level data from a volume in a primary storage system to a volume in a secondary system. Remote Snap creates an internal snapshot of the primary volume, and copies changes to the data since the last replication to the secondary system via iSCSI or FC links. The primary volume exists in a primary pool in the primary storage system. Replication can be completed using either the SMU or CLI. See "[Connecting two storage systems to replicate volumes](#)" on page 33 for host connection information concerning Remote Snap.

Replication setup and verification

After storage systems and hosts are cabled for replication, you can use the SMU to prepare to use the Remote Snap feature. Optionally, you can use the CLI to access the Remote Snap feature.

NOTE See the following manuals for more information about replication setup:

- See *HPE MSA Remote Snap Software Technical white paper* for replication best practices.
 - See *HPE MSA 2070/2072 Storage Management Guide* for procedures to setup and manage replications.
 - See *HPE MSA 2070/2072 CLI Reference Guide* for replication commands and syntax.
 - See *HPE MSA Event Descriptions Reference Guide* for replication event reporting.
-

Basic information for enabling the controller enclosures for replication supplements the troubleshooting procedures that follow.

- Familiarize yourself with the replication feature overview provided in the Storage Management Guide.
- For best practices concerning replication-related tasks, see the *HPE MSA Remote Snap Software Technical white paper*.
- In order to replicate an existing volume to a pool on the peer, ensure both the primary and secondary systems have the MSA Advanced Data Services license installed and follow these steps:
 - Find the port address on the secondary system:
In the CLI, run the `show ports` command on the secondary system.
 - Verify that ports on the secondary system can be reached from the primary system using either method below:
 - In the CLI, run the `query peer-connection` command on the primary system, using a port address obtained from the output of the `show ports` command above.
 - In the SMU, select **Settings > Peer Connections** and view **Available Ports**. View **Current Peer Connections**. You can enter an IP address into the **Peer System IP Address** field and select the **Query Peer Connection** button to view the result.
 - Ensure a pool exists on both the primary and the secondary systems.
 - Create a peer connection and replication set, using either method below:
 - In the CLI, run the `create peer-connection` command and then run the `create replication-set` command.
 - In the SMU, select **Provisioning > Volumes > Data Protection > Add Data Protection > Remote Replication** and follow the on-screen directions to create the peer connection while creating the replication set.
 - Initiate replication.
 - In the CLI, run the `replicate` command.
 - In the SMU, select **Provisioning > Volumes** and select the slide-over to access the **Replications** panel. Click **Start Replication**.
- For descriptions of replication-related events, see the Event Descriptions Reference Guide.

Diagnostic steps for replication setup

The tables in this subsection show menu navigation for replication using the SMU.

! **IMPORTANT** Remote Snap must be licensed on all systems configured for replication via the HPE MSA Advanced Data Services license, and the controller module firmware must be compatible on all systems licensed for replication.

Can you successfully use the Remote Snap feature?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Remote Snap is not licensed on each controller enclosure used for replication.	Verify licensing on each enclosure used for replication: <ul style="list-style-type: none"> In the SMU, select Maintenance > Support > Licensing. If the replication feature is not enabled, obtain and install the MSA Advanced Data Services license. For more information on licensing, see the topic about installing a license in the Storage Management Guide.
No	Compatible firmware revision supporting Remote Snap is not running on each system used for replication.	Perform the following actions on each system used for replication: <ul style="list-style-type: none"> In the SMU, select Maintenance > Firmware. If necessary, obtain and install the controller module firmware, and activate it to ensure compatibility with other systems. For more information about compatible firmware, see the topic about updating firmware in the Storage Management Guide.
No	Invalid cabling connection. (check the cabling for each system)	Verify controller enclosure cabling: <ul style="list-style-type: none"> Verify use of proper cables. Verify proper cabling paths for host connections. Verify cabling paths between replication ports and switches are visible to one another. Verify that cable connections are securely fastened. Inspect cables for damage and replace if necessary.
No	A system does not have a pool configured.	Configure each system to have a storage pool.

Table 19 Diagnostics for replication setup: Using Remote Snap feature

Can you create a replication set?

! **IMPORTANT** Remote Snap must be licensed on all systems configured for replication, and the controller module firmware must be compatible on all systems licensed for replication.

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	On controller enclosures with iSCSI host interface ports, replication set creation fails due to use of CHAP.	If using CHAP (Challenge Handshake Authentication Protocol), see the topics about configuring CHAP and working in replications within the Storage Management Guide.
No	Unable to create the secondary volume (the destination volume on the pool to which you will replicate data from the primary volume)? ¹	<ul style="list-style-type: none"> Review event logs for indicators of a specific fault in a replication data path component. Follow any recommended actions. Verify valid specification of the secondary volume according to either of the following criteria: <ul style="list-style-type: none"> A conflicting volume does not already exist Available free space in the pool
No	Communication link is down.	Review alerts and event logs for indicators of a specific fault in a host or replication data path component.

¹After ensuring valid licensing, valid cabling connections, and network availability, create the replication set in the SMU using the Remote Replication actions provided in **Provisioning > Volumes > Data Protection > Add Data Protection**.

Table 20 Diagnostics for replication setup: Creating a replication set

Can you replicate a volume?

! **IMPORTANT** Remote Snap must be licensed on all systems configured for replication, and the controller module firmware must be compatible on all systems licensed for replication.


Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Remote Snap is not licensed on each controller enclosure used for replication.	Verify licensing: <ul style="list-style-type: none"> In the SMU, select Maintenance > Support > Licensing. If the replication feature is not enabled, obtain and install a valid license. For more information on licensing, see the topic about installing a license in the Storage Management Guide.
No	Nonexistent replication set.	<ul style="list-style-type: none"> Determine existence of primary or secondary volumes. If a replication set has not been successfully created, use the Remote Replication actions provided in Provisioning > Volumes > Data Protection > Add Data Protection of the SMU to create one. Review alerts for indicators of a specific fault in a replication data path component. Follow any recommended actions.
No	Network error occurred during in-progress replication.	<ul style="list-style-type: none"> Review alerts for indicators of a specific fault in a replication data path component. Follow any recommended actions. In the SMU, select Provisioning > Volumes, select the applicable volume, click the  icon, and select the Replications tab to see replication details. Replications that enter the suspended state can be resumed manually (see the Storage Management Guide for additional information).
No	Communication link is down.	Review event logs for indicators of a specific fault in a host or replication data path component.

Table 21 Diagnostics for replication setup: Replicating a volume

Has a replication run successfully?


Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Last Successful Run shows N/A.	<ul style="list-style-type: none"> In the SMU, select Provisioning > Volumes, select the applicable volume, click the  icon, and select the Replications tab to see Last Successful Run information. If a replication has not run successfully, use the SMU to replicate as described in the Storage Management Guide.
No	Communication link is down.	Review event logs for indicators of a specific fault in a host or replication data path component. Follow any recommended actions.

Table 22 Diagnostics for replication setup: Checking for a successful replication

Resolving voltage and temperature warnings

1. Check that all of the fans are working by making sure that the Fan Fail/AC Fail/DC Fail LEDs on each PCM are off, or by using the SMU to check enclosure health status.
See the topic about options available for performing basic fault isolation methodology steps for a description of

- health status icons and alternatives for monitoring enclosure health.
2. Make sure that all modules are fully seated in their slots with latches locked.
 3. Make sure that no slots are left open for more than two minutes.
If you need to replace a module, leave the old module in place until you have the replacement, or use a blank module to fill the slot. Leaving a plug-in module slot open negatively affects the airflow and can cause the enclosure to overheat.
 4. Make sure there is proper air flow, and no cables or other obstructions are blocking the front or rear of the array.
 5. Try replacing each PCM one at a time.

Sensor locations

The storage system monitors conditions at different points within each enclosure to alert you to problems. Power, cooling fan, temperature, and voltage sensors are located at key points in the enclosure. Controller modules actively manage the enclosure. Each module has a SAS expander with its own storage enclosure processor (SEP) to monitor the status of these sensors to perform SCSI enclosure services (SES) functions according to the ANSI SES Standard. If one of these modules fails, the other module will continue to operate.

See a module's specification or the SES interface specification for definitions of the module's functions and its SES control.

The following sections describe each element and its sensors.

Power supply sensors

Each enclosure has two fully redundant power and cooling modules (PCMs) with load-sharing capabilities. The power supply sensors described in the following table monitor power or system driven voltage, current, temperature, and fan status in each PCM. If the power supply sensors report a voltage that is under or over the threshold, check the input voltage.

Table 23 Power supply sensor descriptions

Description	Event/PCM fault LED condition
Power supply 1	Voltage, current, temperature, fan fault. Power or system driven.
Power supply 2	Voltage, current, temperature, fan fault. Power or system driven.

Cooling fan sensors

Each PCM includes two fans. The normal range for fan speed is 4,000 to 13,000 RPM. Under normal operation, the cooling fans are spinning with no fail states. When a fan speed is outside the allowable threshold, the enclosure management software records a failure and posts an alarm. Replace the PCM reporting the fan failure.

Temperature sensors

Extreme high and low temperatures can cause significant damage if they go unnoticed. When a temperature fault is reported, it must be remedied as quickly as possible to avoid system damage. This can be done by warming or cooling the installation location.

Table 24 Controller platform temperature sensor descriptions

Description	Normal operating range	Warning operating range	Failure threshold
CPU temperature (internal digital thermal sensor)	2°C–98°C	0°C–1°C, 99°C–104°C	>104°C
SAS3008 internal digital sensor	2°C–104°C	0°C–1°C, 105°C–115°C	<0°C, >115°C
Supercapacitor pack thermistor	0°C–50°C	None	None
SAS35x36 onboard temperature	2°C–104°C	0°C–1°C, 105°C–115°C	<0°C, >115°C*
ASIC onboard temperature	2°C–100°C	0°C–1°C, 101°C–105°C	<0°C, >110°C*
Controller module inlet	6°C–62°C	1°C–5°C, 63°C–67°C	<0°C, >68°C*
SAS 12Gb FRAMs	2°C–104°C	0°C–1°C, 105°C–115°C	<0°C, >115°C*
FC FRAMs	2°C–94°C	0°C–1°C, 95°C–105°C	<0°C, >105°C*
iSCSI FRAMs	2°C–94°C	0°C–1°C, 95°C–105°C	<0°C, >105°C*

* Shut down outside the operating range of the junction temperature specification for this device.

If a power supply sensor goes out of range, the fault LEDs on the PCM will illuminate amber, and the PCM OK LED will be off.

Table 25 PCM temperature sensor descriptions

Description	Normal operating range
Power supply 1 inlet	6°C–55°C
Power supply 1 hot spot	6°C–95°C
Power supply 2 inlet	6°C–55°C
Power supply 2 hot spot	6°C–95°C

Power and cooling module voltage sensors

Power and cooling module (PCM) voltage sensors ensure that the enclosure power supply voltage is within normal ranges. Each PCM has three voltage sensors.

Table 26 PCM voltage sensor descriptions

Description	Event/PCM fault LED condition
Power supply voltage sensor, 12V	<10V, >13V
Power supply voltage sensor, 5V	<4.2V, >5.6V
Power supply voltage sensor, 5Vsb	<4V, >5.6V

8 Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:
<https://www.hpe.com/info/assistance>
- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:
<https://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

<https://www.hpe.com/support/hpesc>

My HPE Software Center

<https://www.hpe.com/software/hpesoftwarecenter>

- To subscribe to eNewsletters and alerts:
<https://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:

<https://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 Account set up with relevant entitlements.

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 initiates a fast and accurate resolution based on the service level of your product. 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.

HPE Get Connected

<https://www.hpe.com/services/getconnected>

HPE Tech Care Service

<https://www.hpe.com/services/techcare>

HPE Complete Care Service

<https://www.hpe.com/services/completecure>

Warranty information

To view the warranty information for your product, see the [warranty check tool](#).

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:

<https://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:

<https://www.hpe.com/info/reach>

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

<https://www.hpe.com/info/ecodata>

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

<https://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, use the Feedback button and icons (at the bottom of an opened document) on the Hewlett Packard Enterprise Support Center portal (<https://www.hpe.com/support/hpesc>) to send any errors, suggestions, or comments. This process captures all document information.

A LED descriptions

Front panel LEDs

HPE MSA 2070/2072 models support small form factor (SFF) and large form factor (LFF) disks. For SFF storage, the chassis is configured with 24 2.5" disks. For LFF storage, the chassis is configured with 12 3.5" disks.

Enclosure bezel

The MSA 2070/2072 enclosures provide a removable bezel designed to cover the front panel during enclosure operation. The enclosure bezel covers the disk modules, and attaches to the left and right hubcaps. The bezel will not properly attach to the enclosure unless the hubcaps are installed. Enclosure bezel components are described in more detail below.

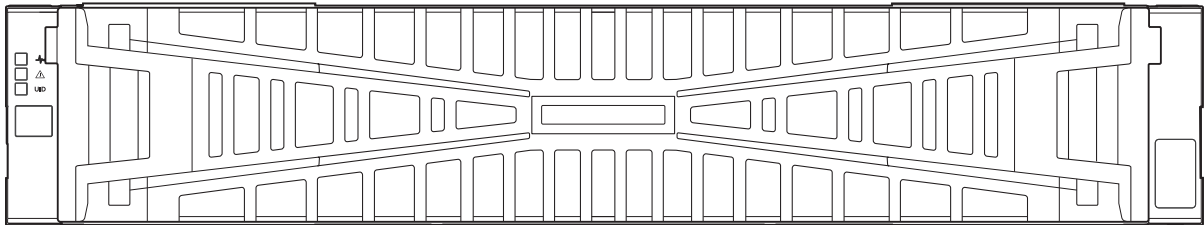


Figure 29 Bezel used with MSA 2070/2072 enclosures: front panel

Enclosure bezel assembly

The MSA 2070/2072 Storage enclosures provide a removable bezel option designed to cover the front panel during operation. If the enclosure bezel is not attached, you can attach it at any time. Ear covers protect the ears and circuitry. Hubcaps fit over the ear covers. The bezel snaps into the hubcaps. An empty 12-drive enclosure is shown in the following example.

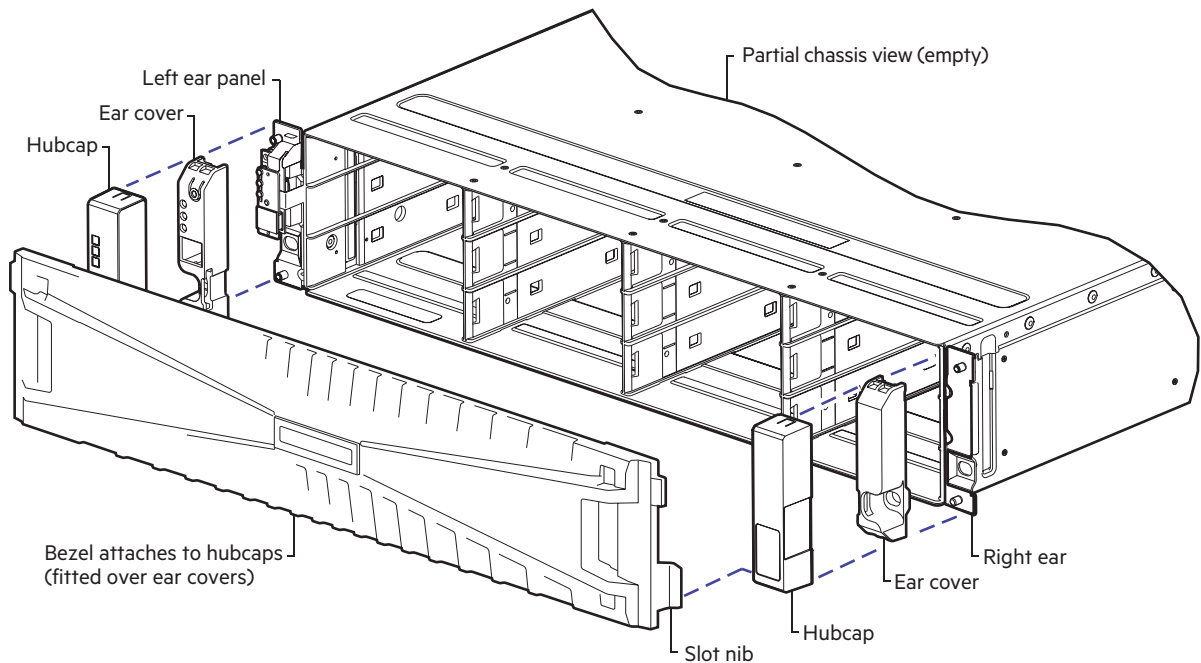


Figure 30 Partial exploded view showing alignment of bezel components

See also, the ["Attach the enclosure bezel" on page 11](#) topic, which provides a simple procedure for attaching the bezel to the hubcaps fitted over ear covers. The bezel slot nibs fit through the aligned slots in the hubcaps and ear covers.

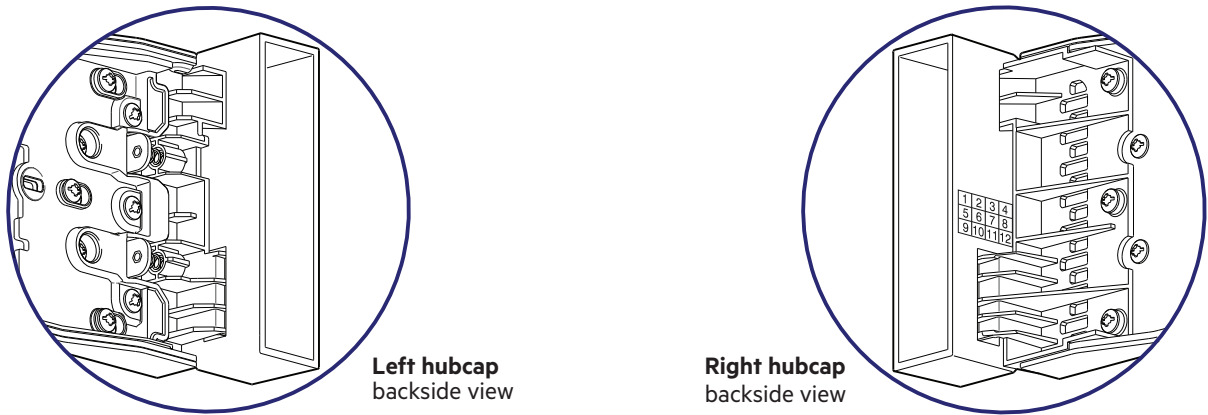


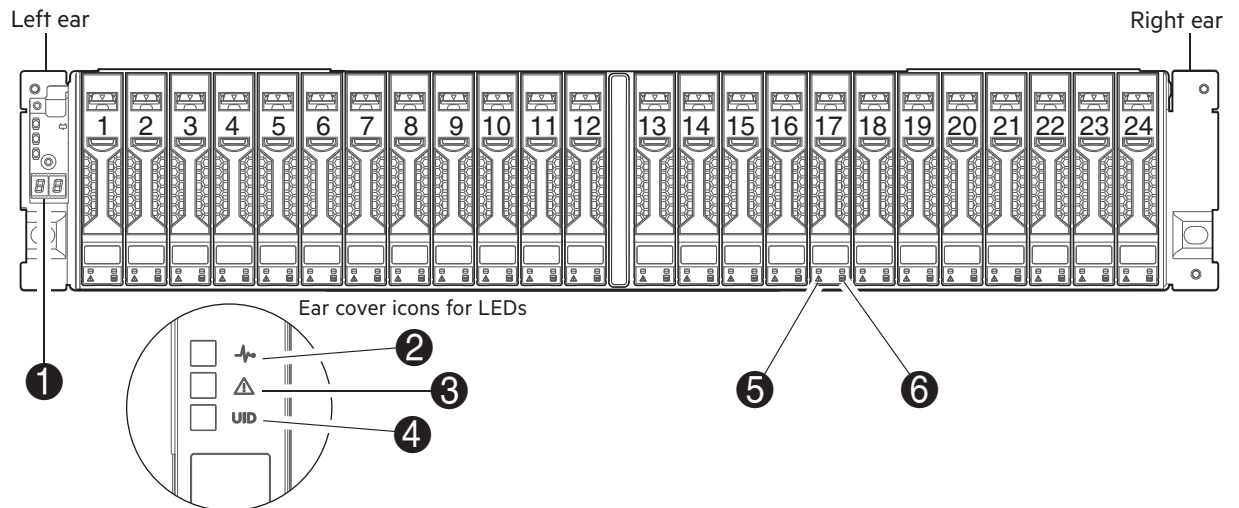
Figure 31 Details showing backside of bezel fitted to hubcaps

The details above are simplified for clarity. They show the slot locations at the base of each hubcap through which the bezel attaches. Only the hubcaps are shown. The ear covers over which they attach are factory installed to protect the ears. See also the exploded view above, which shows the hubcaps aligned to fit over the ear covers. The topic about ["Ear covers and hubcaps" on page 67](#) provides additional details about the left and right hubcaps.

Enclosure bezel removal

TIP To remove the bezel from the enclosure front panel, reverse the order of the steps provided in the attachment procedure. See also ["Attach the enclosure bezel" on page 11](#).

24-drive controller enclosure or supported expansion enclosure



Notes:

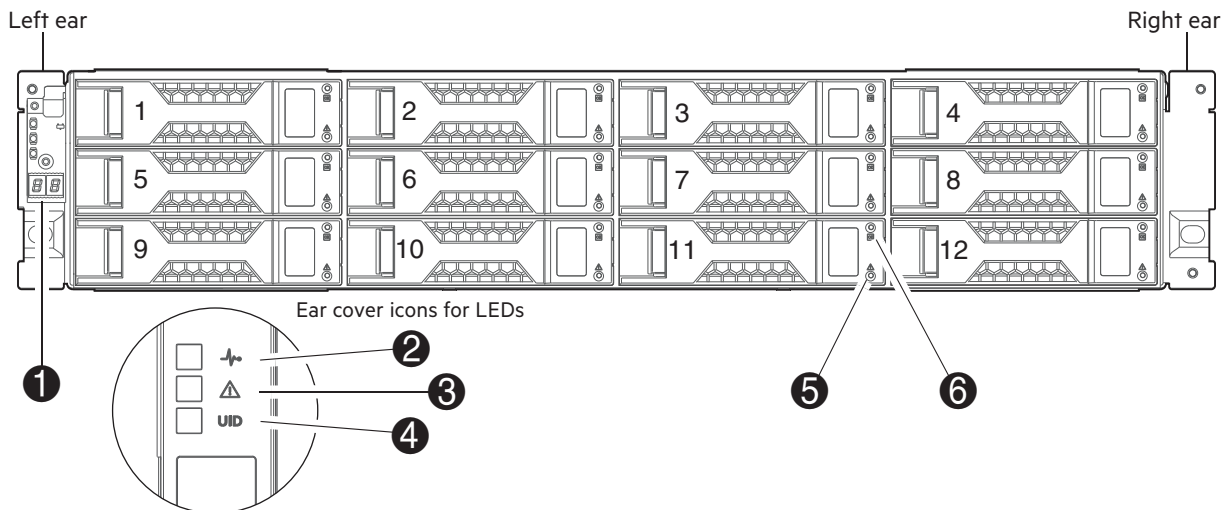
Integers on disks indicate drive slot numbering sequence.

The enlarged detail view at left shows LED icons from the left ear cover that correspond to the chassis LEDs.

LED	Description	Definition
1	Enclosure ID	Green — On The enclosure ID value is shown using 7-segment display. Enables you to correlate the enclosure with logical views presented by management software. Sequential enclosure ID numbering of controller enclosures begins with the integer 1. The enclosure ID for an attached drive enclosure is nonzero.
2	System Power	Green — The enclosure is powered on with at least one power supply operating normally. Off — Both power supplies are off; the system is powered off.
3	Module Fault	Amber — Fault condition exists. The event has been identified, but the problem needs attention. Off — No fault condition exists.
4	Unit Identification (UID)	Blue — Blinking The enclosure is identified. Off — Identity LED is not illuminated.
5	Disk drive Fault/UID	See "Disk drive LEDs" on page 68.
6	Disk drive Online/Activity	See "Disk drive LEDs" on page 68.

Figure 32 LEDs: 24-drive controller or expansion enclosure—front panel

12-drive controller enclosure or supported expansion enclosure



Notes:

Integers on disks indicate drive slot numbering sequence.

The enlarged detail view at left shows LED icons from the left ear that correspond to the chassis LEDs.

LED	Description	Definition
1	Enclosure ID	Green — On The enclosure ID value is shown using 7-segment display. Enables you to correlate the enclosure with logical views presented by management software. Sequential enclosure ID numbering of controller enclosures begins with the integer 1. The enclosure ID for an attached drive enclosure is nonzero.
2	System Power	Green — The enclosure is powered on with at least one power supply operating normally. Off — Both power supplies are off; the system is powered off.

LED	Description	Definition
3	Module Fault	Amber — Fault condition exists. The event has been identified, but the problem needs attention. Off — No fault condition exists.
4	Unit Identification (UID)	Blue — Blinking The enclosure is identified. Off — Identity LED is not illuminated.
5	Disk drive Fault/UID	See "Disk drive LEDs" on the next page.
6	Disk drive Online/Activity	See "Disk drive LEDs" on the next page.

Figure 33 LEDs: 12-drive controller or expansion enclosure—front panel

Ear covers and hubcaps

The enclosure is equipped with a plastic ear cover on each of the ears located on the front panel. A hubcap, in turn, fits over each of the ear covers. Slots at the base of each cover's inside face receive the mounting nibs on each end of the enclosure bezel. These mounting nibs insert through the respective slots of each overlaid ear cover and hubcap assembly. The enclosure can operate with or without the bezel attached, but the ears should be fitted with both sets of covers at minimum. Figure 42 callouts apply to the table portion of Figure 41. The front view of the enclosure bezel shows the assembled components.

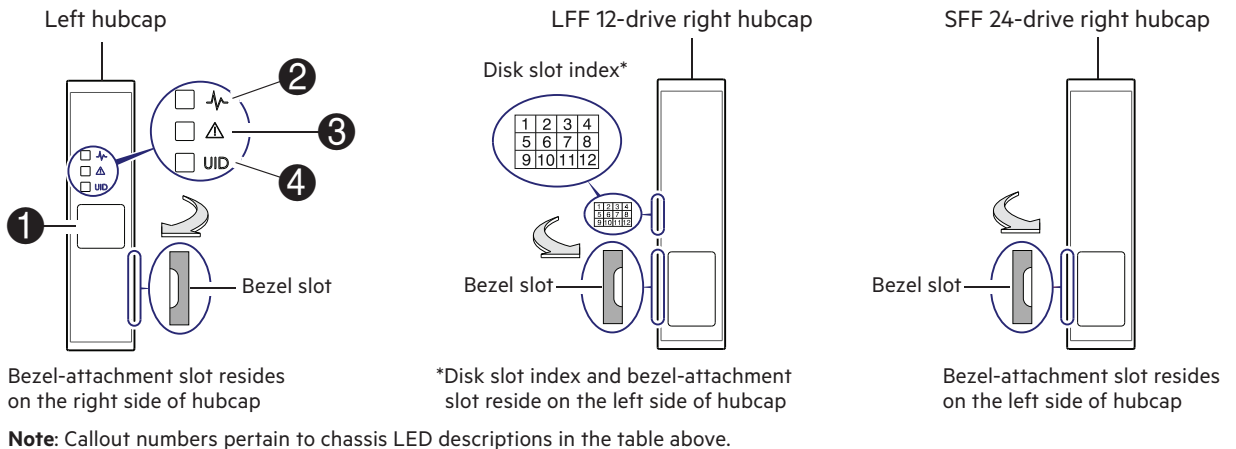
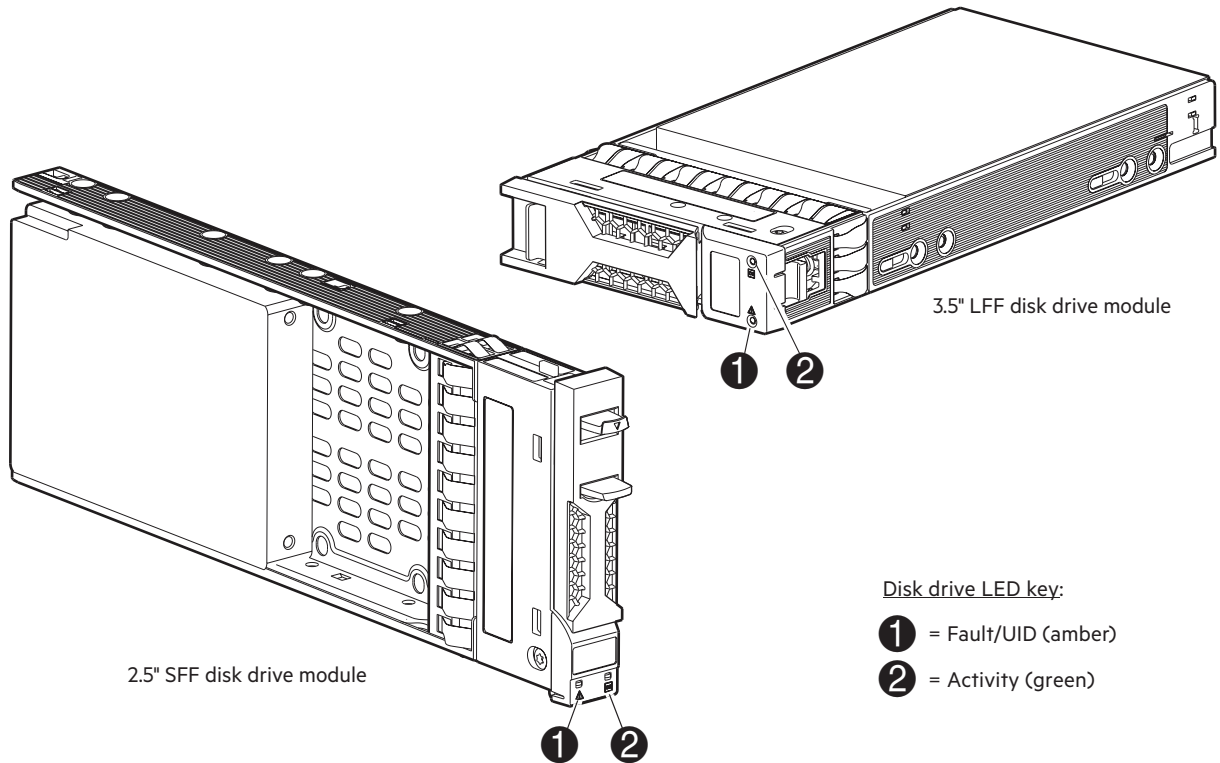


Figure 34 Cover details for enclosure ears

Disk drive LEDs



Activity LED (Green)	Fault LED (Amber)	Status/condition*
Off	Off	Either: <ul style="list-style-type: none"> Power is off (drive/enclosure)—if a supported drive is fully seated Not present or drive not recognized—if the drive slot is absent or the drive is not supported
Flicker with activity	Blinking: 3s on/1s off	Identify
Blink with activity	On	One Drive Link (PHY lane) down
Off	On	Fault (leftover/failed/locked-out both Drive Link (PHY lanes) down
Off: Blink with activity	Off	Available
Blink with activity	Off	Either: <ul style="list-style-type: none"> Storage system: Initializing Storage system: Fault tolerant Use the SMU or the CLI to determine the state.
Off: Blink with activity	Off	Storage system: Quarantined
Off: Blink with activity	Blink: (1s on/1s off) for the reconstructing drive only	Storage system: Reconstructing (Note: do not remove the disk drive)

*If multiple conditions occur simultaneously, the LED state will behave as indicated by the condition listed earliest in the table, as rows are read from top to bottom.

Figure 35 LEDs: Disk drive combinations — enclosure front panel

! **IMPORTANT** For information about self-encrypting disk (SED) drives, see the Storage Management Guide.

Rear panel LEDs

Controller enclosure—rear panel layout

The diagram and table below display and identify important component items comprising the rear panel layout of an MSA 2070/2072 controller enclosure. Diagrams and tables on the following pages further describe rear panel LED behavior for component field-replaceable units.

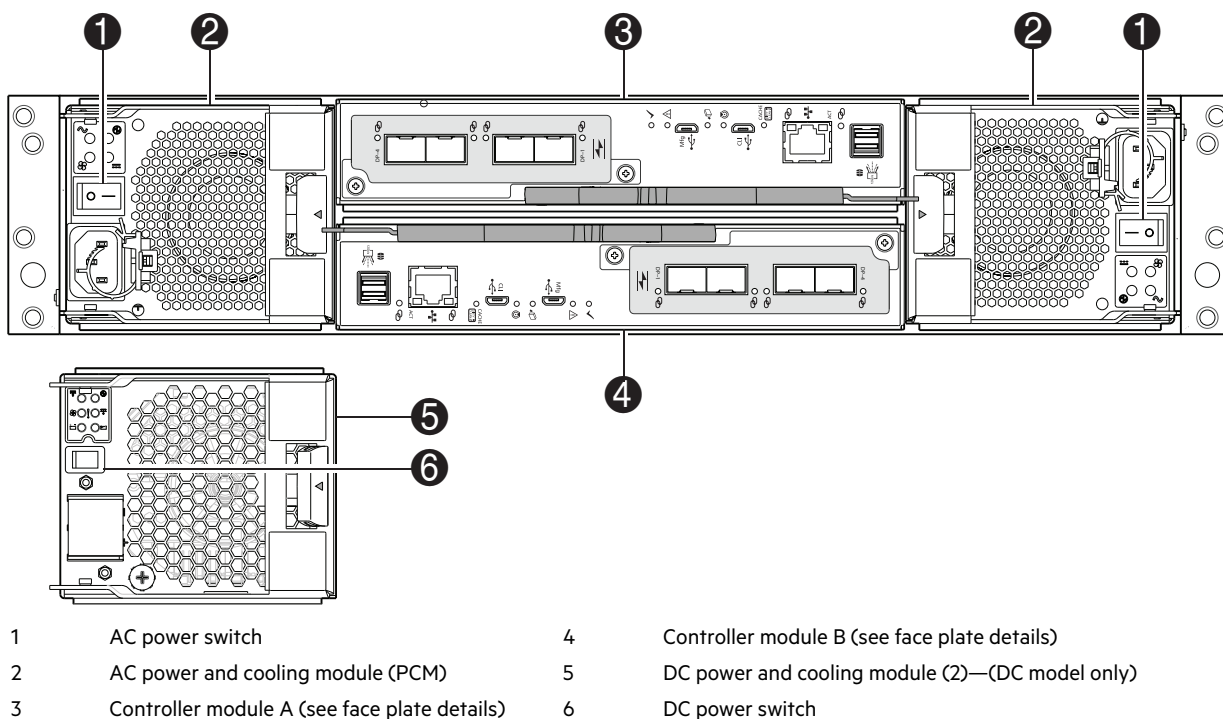


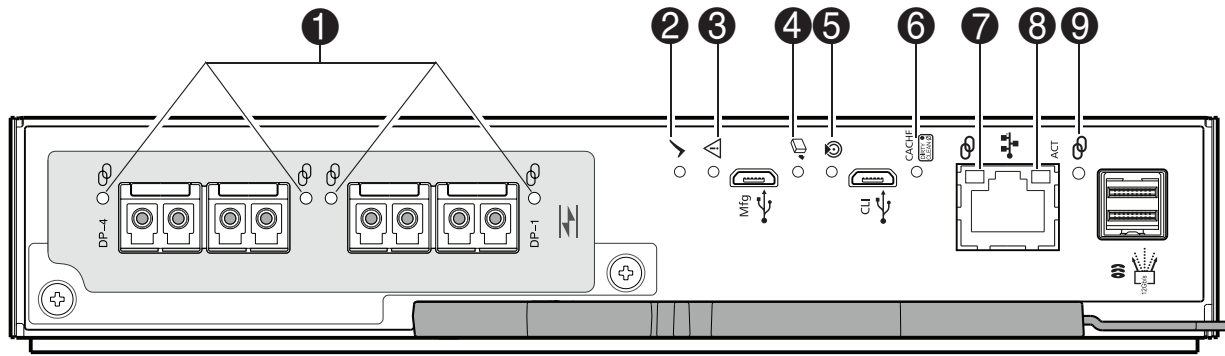
Figure 36 MSA 2070/2072: rear panel


A controller enclosure accommodates two PCMs of the same type—either both AC or both DC—within the PCM slots (see callout 2), and two controller modules of the same type within the controller module slots (see callouts 3 and 4).

! **IMPORTANT** MSA 2070/2072 controller enclosures support dual-controller configurations only. If a partner controller fails, the array will fail over and run on a single controller until the redundancy is restored. A controller module must be installed in each IOM slot to ensure sufficient airflow through the enclosure during operation.

The diagrams with tables that immediately follow provide descriptions of the different controller modules and power supply modules that can be installed into the rear panel of an MSA 2070/2072 controller enclosure. The controller module for your product uses the appropriate external connector for the selected host interface protocol. Showing controller modules and power supply modules separately from the enclosure provides improved clarity in identifying the component items called out in the diagrams and described in the tables. Descriptions are also provided for optional drive enclosures supported by MSA 2070/2072 controller enclosures for expanding storage capacity.

MSA 2070/2072 FC controller module—rear panel LEDs



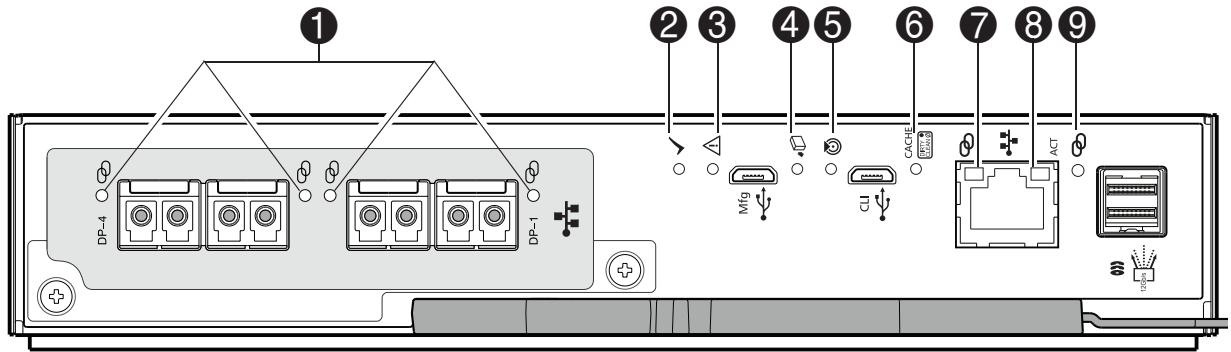
 = FC LEDs

LED	Description	Definition
1	Host FC ¹ Link Status/ Link Activity	Off — No link detected. Green — The port is connected and the link is up. Blinking green — The link has I/O activity.
2	OK	Green — The controller is operating normally. Blinking green — The system is booting. Off — The controller module is not OK, or is powered off.
3	Fault	Off — The controller is operating normally. Amber — A fault has been detected or a service action is required.
4	OK to Remove	Off — The controller module is not prepared for removal. White — The controller module is prepared for removal.
5	Identify	Blue — The controller module is being identified.
6	Cache Status ²	Green — Cache is dirty (contains unwritten data) and operation is normal. The unwritten information can be log or debug data that remains in the cache, so a green Cache Status LED does not, by itself, indicate that any user data is at risk or that any action is necessary. Off — In a working controller, cache is clean (contains no unwritten data). This is an occasional condition that occurs while the system is booting. Blinking green — A nonvolatile memory flush or cache self-refresh is in progress, indicating cache activity.
7	Network Port Link Speed ³	Off — Link is up at 10/100base-T negotiated speeds. Amber — Link is up and negotiated at 1000base-T.
8	Network Port Link Active ³	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to negotiated link speeds).
9	Expansion Port Link Status	Off — The port is empty or the link is down. Green — The port is connected and the link is up. Blinks with activity. Amber — Partial link up (one or more lanes down). Blinks with activity.

1—See the QuickSpecs for qualified FC SFPs and fiber optic cable options.
2—The Cache Status LED supports power on behavior and operational (cache status) behavior.
3—When the port is down, both LEDs are off.

Figure 37 LEDs: MSA 2070/2072 FC controller module

MSA 2070/2072 iSCSI controller module—rear panel LEDs



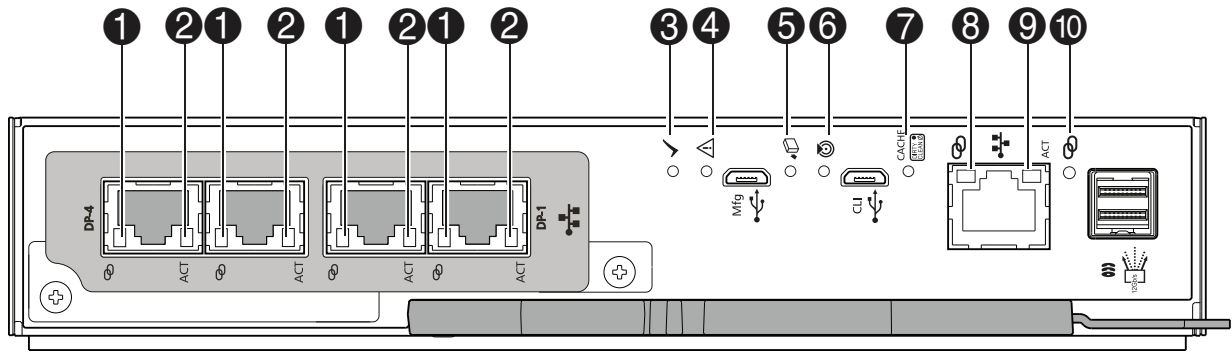
 = iSCSI LEDs


LED	Description	Definition
1	Host iSCSI ¹ Link Status/ Link Activity	Off — No link detected. Green — The port is connected and the link is up. Blinking green — The link has I/O activity.
2	OK	Green — The controller is operating normally. Blinking green — The system is booting. Off — The controller module is not OK, or is powered off.
3	Fault	Off — The controller is operating normally. Amber — A fault has been detected or a service action is required.
4	OK to Remove	Off — The controller module is not prepared for removal. White — The controller module is prepared for removal.
5	Identify	Blue — The controller module is being identified.
6	Cache Status ²	Green — Cache is dirty (contains unwritten data) and operation is normal. The unwritten information can be log or debug data that remains in the cache, so a green Cache Status LED does not, by itself, indicate that any user data is at risk or that any action is necessary. Off — In a working controller, cache is clean (contains no unwritten data). This is an occasional condition that occurs while the system is booting. Blinking green — A nonvolatile memory flush or cache self-refresh is in progress, indicating cache activity.
7	Network Port Link Speed ³	Off — Link is up at 10/100base-T negotiated speeds. Amber — Link is up and negotiated at 1000base-T.
8	Network Port Link Active ³	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to negotiated link speeds).
9	Expansion Port Link Status	Off — The port is empty or the link is down. Green — The port is connected and the link is up. Blinks with activity. Amber — Partial link up (one or more lanes down). Blinks with activity.

1—See the QuickSpecs for qualified iSCSI SFP options and DAC or AOC cable options.
2—The Cache Status LED supports power on behavior and operational (cache status) behavior.
3—When the port is down, both LEDs are off.

Figure 38 LEDs: MSA 2070/2072 iSCSI controller module

MSA 2070/2072 10GBase-T iSCSI controller module—rear panel LEDs



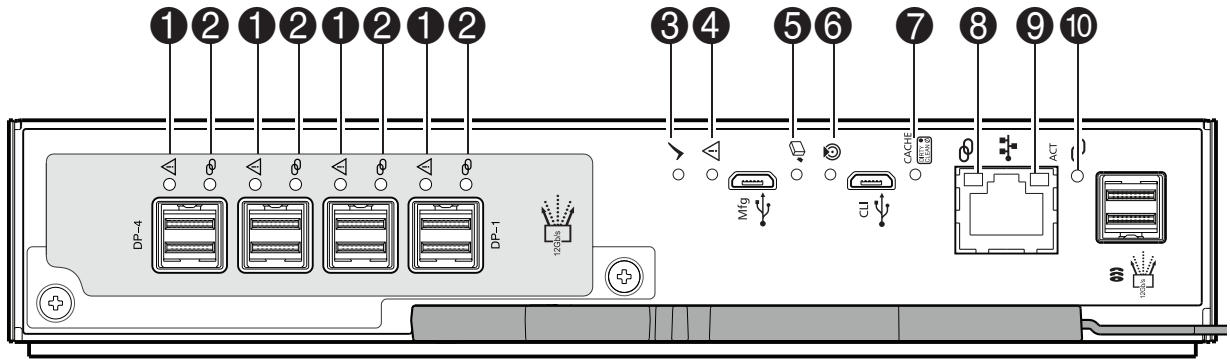
 = 10GBase-T iSCSI LEDs


LED	Description	Definition
1	Host 10GBase-T iSCSI ¹ Link Speed	Off — The link is not established, or the link is down. Green — The link is up at 10G negotiated speed. Amber — The link is up at 1G negotiated speed.
2	Host 10GBase-T iSCSI ¹ Link Status/Link Activity	Off — No link detected. Green — The port is connected and the link is up. Blinking green — The link has I/O or replication activity.
3	OK	Green — The controller is operating normally. Blinking green — The system is booting. Off — The controller module is not OK, or is powered off.
4	Fault	Off — The controller is operating normally. Amber — A fault has been detected or a service action is required.
5	OK to Remove	Off — The controller module is not prepared for removal. White — The controller module is prepared for removal.
6	Identify	Blue — The controller module is being identified.
7	Cache Status ²	Green — Cache is dirty (contains unwritten data) and operation is normal. The unwritten information can be log or debug data that remains in the cache, so a green Cache Status LED does not, by itself, indicate that any user data is at risk or that any action is necessary. Off — In a working controller, cache is clean (contains no unwritten data). This is an occasional condition that occurs while the system is booting. Blinking green — A nonvolatile memory flush or cache self-refresh is in progress, indicating cache activity.
8	Network Port Link Speed ³	Off — Link is up at 10/100base-T negotiated speeds. Amber — Link is up and negotiated at 1000base-T.
9	Network Port Link Active ³	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to negotiated link speeds).
10	Expansion Port Link Status	Off — The port is empty or the link is down. Green — The port is connected and the link is up. Blinks with activity. Amber — Partial link up (one or more lanes down). Blinks with activity.

1—See the QuickSpecs for qualified 10GBase-T iSCSI connector and cable options.
2—The Cache Status LED supports power on behavior and operational (cache status) behavior.
3—When the port is down, both LEDs are off.

Figure 39 LEDs: MSA 2070/2072 10GBase-T iSCSI controller module

MSA 2070/2072 SAS controller module—rear panel LEDs



 = SAS LEDs

LED	Description	Definition
1	Host 12Gb SAS ¹ Link Status/ Link Activity	Off — No link detected. Amber — The port is connected with partial link up (one or more lanes are down, or operating at a lower link speed inconsistent with other lanes). Blinking amber — The link has I/O activity.
2	Host 12Gb SAS ¹ Link Status/ Link Activity	Off — No link detected. Green — The port is connected and the link is up with all four SAS lanes active/operating at the same negotiated speed. Blinking green — The link has I/O activity.
3	OK	Green — The controller is operating normally. Blinking green — The system is booting. Off — The controller module is not OK, or is powered off.
4	Fault	Off — The controller is operating normally. Amber — A fault has been detected or a service action is required.
5	OK to Remove	Off — The controller module is not prepared for removal. White — The controller module is prepared for removal.
6	Identify	Blue — The controller module is being identified.
7	Cache Status ²	Green — Cache is dirty (contains unwritten data) and operation is normal. The unwritten information can be log or debug data that remains in the cache, so a green Cache Status LED does not, by itself, indicate that any user data is at risk or that any action is necessary. Off — In a working controller, cache is clean (contains no unwritten data). This is an occasional condition that occurs while the system is booting. Blinking green — A nonvolatile memory flush or cache self-refresh is in progress, indicating cache activity.
8	Network Port Link Speed ³	Off — Link is up at 10/100base-T negotiated speeds. Amber — Link is up and negotiated at 1000base-T.
9	Network Port Link Active ³	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to negotiated link speeds).
10	Expansion Port Link Status	Off — The port is empty or the link is down. Green — The port is connected and the link is up. Blinks with activity. Amber — Partial link up (one or more lanes down). Blinks with activity.

1-See the QuickSpecs for qualified SFF-8644 cable options.
2-The Cache Status LED supports power on behavior and operational (cache status) behavior.
3-When the port is down, both LEDs are off.

Figure 40 LEDs: MSA 2070/2072 SAS controller module

Cache Status LED details

Power on/off behavior

During power on, discrete sequencing for power on display states of internal components is reflected by blinking patterns displayed by the Cache Status LED as shown in the table.

Table 27 Cache Status LED — power on behavior

Item	Display states reported by Cache Status LED during power on sequence							
Display state	0	1	2	3	4	5	6	7
Component	VP	ASIC	SAS BE	SC	Host	Boot	Normal	Reset
Blink pattern	On 1/Off 7	On 2/Off 6	On 3/Off 5	On 4/Off 4	On 5/Off 3	On 6/Off 2	Solid/On	Steady

NOTE Component acronyms used for Cache Status LED states:


- VP = Voltage Plane (stage 0)
- ASIC = Application-specific Integrated Circuit (stage 1)
- SAS BE = Enclosure's backend SAS system interface (stage 2)
- SC = Storage controller: processor located in controller module (stage 3)

After the enclosure has completed the power on sequence, the Cache Status LED displays Solid/On (Normal), before assuming the operating state for cache purposes.

Cache status behavior


If the LED is blinking evenly, a cache flush is in progress. When a controller module loses power and write cache contains data that has not been written to disk, the supercapacitor pack provides backup power to flush (copy) data from write cache to nonvolatile memory. When cache flush is complete, the cache transitions into self-refresh mode. See also ["Supercapacitor pack" on page 19](#).

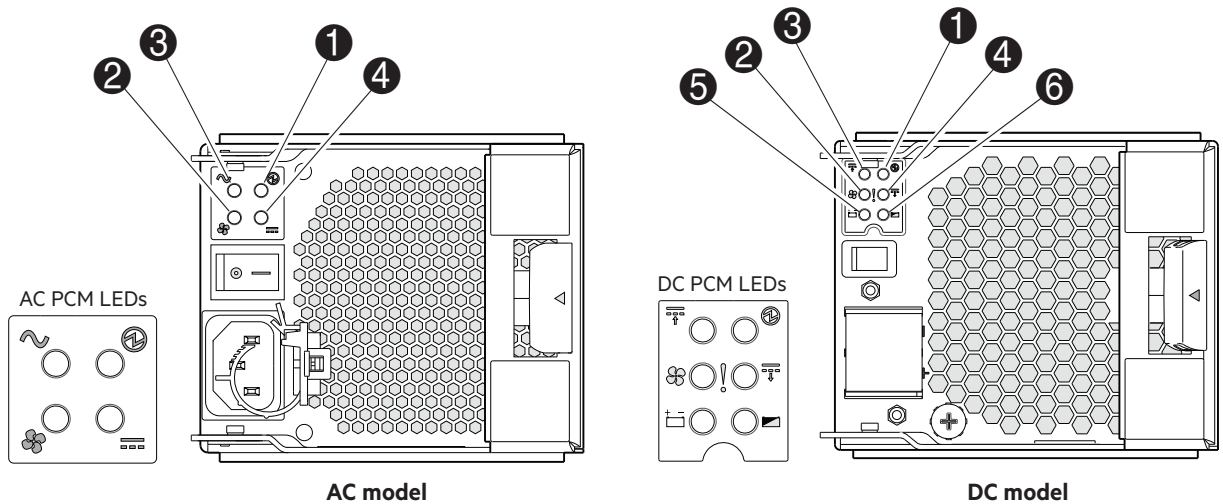
If the LED is blinking momentarily slowly, the cache is in a self-refresh mode. In self-refresh mode, if primary power is restored before the backup power is depleted (3–30 minutes, depending on various factors), the system boots, finds data preserved in cache, and writes it to disk. This means the system can be operational within 30 seconds, and before the typical host I/O time-out of 60 seconds, at which point system failure would cause host-application failure. If primary power is restored after the backup power is depleted, the system boots and restores data to cache from nonvolatile memory, which can take about 90 seconds. The cache flush and self-refresh mechanism is an important data protection feature; essentially four copies of user data are preserved: one in controller cache and one in nonvolatile memory of each controller. The Cache Status LED illuminates solid green during the boot-up process. This behavior indicates the cache is logging all POSTs, which will be flushed to nonvolatile memory the next time the controller shuts down.

 **CAUTION** If the Cache Status LED illuminates solid green—and you wish to shut-down the controller—do so from the user interface, so unwritten data can be flushed to nonvolatile memory.

MSA 2070/2072 power and cooling modules—rear panel layout

MSA 2070/2072 Storage enclosures support either two redundant AC power and cooling modules (PCMs) or two redundant DC PCMs as described below.

 **TIP** Cross reference the enlarged LED icon labels with the callout numbers when reading table entries.



LED	Description	Definition
1	PCM OK	Green—Power is on and input voltage is normal. Off—Power is off or input voltage is below the minimum threshold.
2	Fan Fail	Off—The PCM is operating normally. Amber — A fault has been detected or a service action is required.
3	AC Input Fail (AC PCM); or DC input Fail (DC PCM)	Off—PCM is operating normally. Amber—A fault has been detected or a service action is required.
4	PCM Fail	Off — The expansion module is operating normally. Amber — A fault has been detected or a service action is required.
5	Battery Good	Battery not installed / non-operative
6	Battery Fault	Battery not installed / non-operative

Figure 41 LEDs: MSA 2070/2072 power and cooling module (AC or DC model)

Under normal conditions, the PCM OK LEDs on redundant PCMs within the enclosure, will be illuminated solid green. When a fault occurs, the colors of the LEDs will display as shown below.

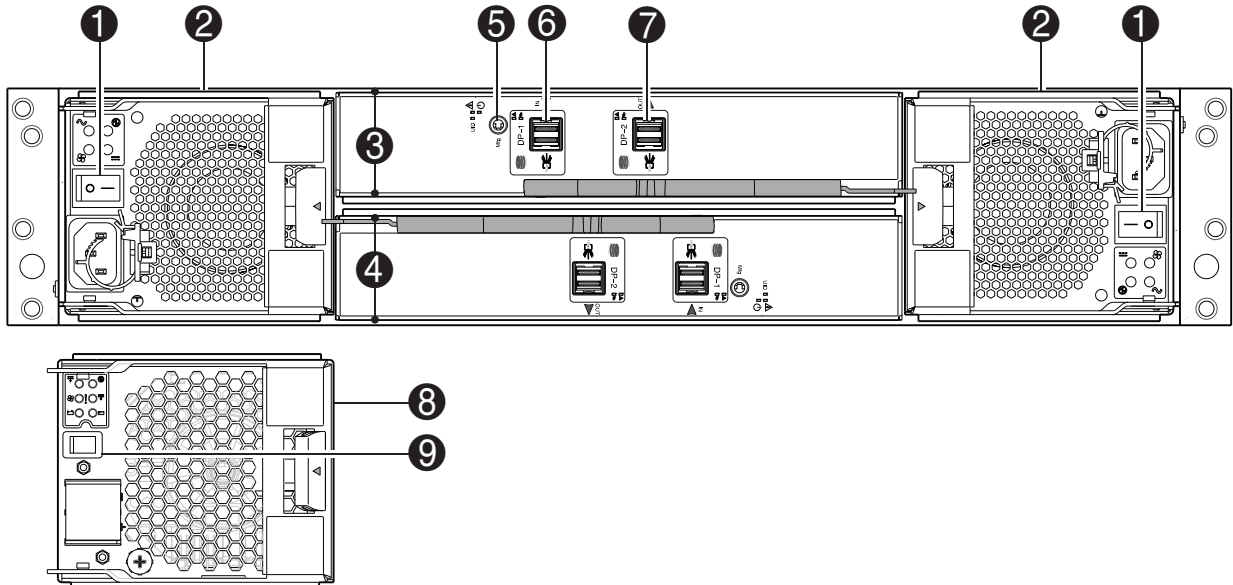
Table 28 PCM LED states

PCM OK (Green)	Fan Fail (Amber)	AC or DC Fail (Amber)	PCM Fail (Amber)	LED behavior status
Off	Off	Off	Off	No AC or DC power on any PCM.
Off	Off	On	On	No AC or DC power on this PCM only.
On	Off	Off	Off	AC or DC power is present; PCM is operating normally.
On	Off	Off	On	PCM fan speed is outside acceptable limits.
Off	On	Off	Off	PCM fan has failed.
Off	On	On	On	PCM fault (over temperature, over voltage, over current).
Off	Blinking	Blinking	Blinking	PCM firmware download is in progress.
Blinking	Off	Off	Off	Power is on, and in stand-by mode within the enclosure.

Battery condition LED states for the DC PCM are not provided because the battery is not installed or used by this configuration.

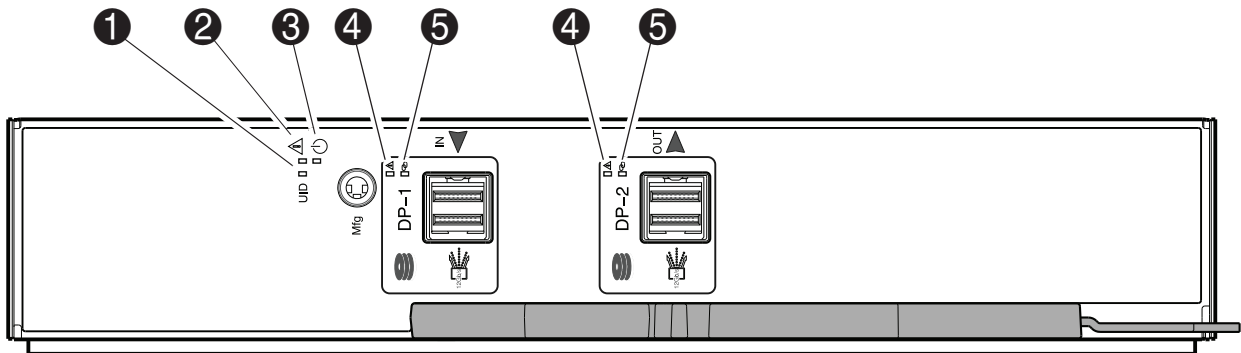
MSA 2070/2072 drive enclosure—rear panel layout

MSA 2070/2072 controllers support the 3.5" 12-drive expansion enclosure and the 2.5" 24-drive expansion enclosure for adding storage. The front panel of the 12-drive enclosure looks identical to the MSA 2070/2072 LFF front panels. The front panel of the 24-drive enclosure looks identical to the MSA 2070/2072 SFF front panels. The rear panel of the 12-drive and 24-drive expansion enclosures are identical.



- | | | | |
|---|---|---|--|
| 1 | AC power switch | 6 | Data port, in |
| 2 | AC power and cooling module (PCM) | 7 | Data port, out |
| 3 | Expansion module A (see face plate details) | 8 | DC power and cooling module (2)-(DC module only) |
| 4 | Expansion module B (see face plate details) | 9 | DC power switch |
| 5 | Service port | | |

Figure 42 Expansion enclosure rear panel: 12-drive and 24-drive models



LED	Description	Definition
1	Identify	Blue — The expansion module is being identified. Blinking blue — 1 second on, 1 second off to identify the expansion module.
2	Fault	Off — The expansion module is operating normally. Amber — A fault has been detected or a service action is required. Blinking amber — 1 second on, 1 second off for a non-critical fault.
3	OK	Green — The expansion module is operating normally. Blinking green — The system is booting. Off — The expansion module is powered off.
4	SAS Port Status (Fault)	Table below shows expansion LED behavior states.
5	SAS Port Status (Activity)	Table below shows expansion LED behavior states.

Figure 43 LEDs: MSA 2070/2072 drive enclosure rear panel

Condition	Activity (Green)	Fault (Amber)
No cable present	Off	Off
Cable present: all links up/no activity	On	Off
Cable present: all links up/with aggregate port activity	Blinking	Off
Non-critical fault: a fault that does not cause the connection to cease operation (e.g., not all links are established; over temperature)	Blinking	Blinking 1s on/1s off
Critical Fault: any fault causing operation of the cable to cease or fail to start (e.g., over current trip)	Off	On

Table 29 LEDs: MSA 2070/2072 expansion activity states

B Specifications and requirements

Safety requirements

Install the system in accordance with the local safety codes and regulations at the facility site. Follow all cautions and instructions marked on the equipment. Also, see the documentation included with your product ship kit.

Site requirements and guidelines

The following sections provide requirements and guidelines that you must address when preparing your site for the installation.

When selecting an installation site for the system, choose a location not subject to excessive heat, direct sunlight, dust, or chemical exposure. These conditions greatly reduce the system's longevity and might void your warranty.

Site wiring and AC power requirements

The following are required for all installations using AC power supplies:

- All AC mains and supply conductors to power distribution boxes for the rack-mounted system must be enclosed in a metal conduit or raceway when specified by local, national, or other applicable government codes and regulations.
- Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the equipment's electrical rating label.
- To ensure redundancy, provide two separate power sources for the enclosures. These power sources must be independent of each other, and each must be controlled by a separate circuit breaker at the power distribution point.
- The system requires voltages within minimum fluctuation. The customer-supplied facilities' voltage must maintain a voltage with not more than ± 5 percent fluctuation. The customer facilities must also provide suitable surge protection.
- Site wiring must include an earth ground connection to the AC power source. The supply conductors and power distribution boxes (or equivalent metal enclosure) must be grounded at both ends.
- Power circuits and associated circuit breakers must provide sufficient power and overload protection. To prevent possible damage to the AC power distribution boxes and other components in the rack, use an external, independent power source that is isolated from large switching loads (such as air conditioning motors, elevator motors, and factory loads).

NOTE For related information about power requirements, including AC power cords, see "[Product QuickSpecs](#)" on [page 9](#).

Site wiring and DC power requirements

The MSA 2070/2072 enclosure models support DC power supplies. The following are required for all installations using DC power supplies:

- All DC mains and supply conductors to power distribution boxes for the rack-mounted system must comply with local, national, or other applicable government codes and regulations.
- Ensure that the voltage of your power source matches the voltage inscribed on the equipment's electrical label.
- To ensure redundancy, provide two separate power sources for the enclosures. These power sources must be independent of each other, and each must be controlled by a separate circuit breaker at the power distribution point.

- The system requires voltages within minimum fluctuation. The customer-supplied facilities' voltage must maintain a voltage within the range specified on the equipment's electrical rating label. The customer facilities must also provide suitable surge protection.
- Site wiring must include an earth ground connection to the DC power source. Grounding must comply with local, national, or other applicable government codes and regulations.
- Power circuits and associated circuit breakers must provide sufficient power and overload protection.

NOTE For related information about power requirements, including DC power cables, see ["Product QuickSpecs" on page 9](#).

Weight guidelines

See ["Physical requirements" on the next page](#) for detailed weight and size specifications.

- The weight of an enclosure depends on the number and type of modules installed.
- Ideally, use two people to lift a storage enclosure. One person can safely lift an enclosure if its weight is reduced by removing the power and cooling modules and disk drive modules.
- Do not place enclosures in a vertical position. Always install and operate the enclosures in a horizontal/level orientation.
- When loading a rack with enclosures, fill the rack from bottom up; and empty the rack from top down to maintain optimal rack stability.
- When installing enclosures in the rack, make sure that any surface over which you might move the rack can support the weight. To prevent accidents when moving equipment—especially on sloped loading docs and up ramps to raised floors—ensure you have a sufficient number of helpers. Remove obstacles such as cables, packing, and other objects from the floor.
- To prevent the rack from tipping, and to minimize personnel injury in the event of a seismic occurrence, securely anchor the rack to a wall or other rigid structure that is attached to both the floor and to the ceiling of the room.

Electrical guidelines

- These enclosures work with single-phase power systems having an earth ground connection. To reduce the risk of electric shock, do not plug an enclosure into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.
- Enclosures fitted with AC PCMs use a grounding-type (three-wire) power cord. To reduce the risk of electric shock, always plug the AC power cord into a grounded power outlet.
- Enclosures fitted with DC PCMs use a DC power cable with positive (+), negative (-) and ground connections. Connect this cable as described in ["DC power supply" on page 25](#).
- Do not use household extension cords with the enclosures. Not all power cords have the same current ratings. Household extension cords do not have overload protection and are not meant for use with computer systems.

Ventilation requirements

See ["Environmental requirements" on page 81](#) for detailed environmental requirements.

- Do not block or cover ventilation openings at the front and rear of an enclosure. Never place an enclosure near a radiator or heating vent. Failure to follow these guidelines can cause overheating and affect the reliability and warranty of your enclosure.

- Leave a minimum of 15 cm (6 inches) at the front and back of each enclosure to ensure adequate airflow for cooling. No cooling clearance is required on the sides, top, or bottom of enclosures.
- Leave enough space in front and in back of an enclosure to allow access to enclosure components for servicing. Removing a component requires a clearance of at least 37 cm (15 inches) in front of and behind the enclosure.

Cabling requirements

- Keep power and interface cables clear of foot traffic. Route cables in locations that protect the cables from damage.
- Route interface cables away from motors and other sources of magnetic or radio frequency interference.
- Stay within the cable length limitations.

Management host requirements

A local management host with at least one USB Type B port connection is recommended for the initial installation and configuration of a controller enclosure. After you configure one or both of the controller modules with an Internet Protocol (IP) address, you then use a remote management host on an Ethernet network to configure, manage, and monitor.

NOTE Connections to this device must be made with shielded cables—grounded at both ends—with metallic RFI/EMI connector hoods, in order to maintain compliance with FCC Rules and Regulations.

Physical requirements

The floor space at the installation site must be strong enough to support the combined weight of the rack, controller enclosures, drive enclosures (expansion), a full complement of disk drives, and any additional equipment. The site also requires sufficient space for installation, operation, and servicing of the enclosures, together with sufficient ventilation to allow a free flow of air to all enclosures.

The tables below provide enclosure dimensions and weights. Weights are based on an enclosure having a full complement of disk drives, two controller or expansion modules, and two power and cooling modules installed.

Table 30 Rackmount enclosure dimensions

Specifications	Rackmount
Height (y-axis)	8.9 cm (3.5 inches)
Width (x-axis):	
• Chassis only	44.5 cm (17.5 inches)
• Chassis with bezel ear caps	48.3 cm (19.0 inches)
Depth (z-axis):	
• Back of chassis ear to controller latch	50.8 cm (20.0 inches)
• Front of chassis ear to back of cable bend	66.9 cm (26.4 inches)

The dimensions shown above apply to the 24-drive SFF enclosure and the 12-drive LFF enclosure.

Table 31 Rackmount enclosure weights

Specifications	Rackmount
MSA 2070/2072 LFF Enclosure <ul style="list-style-type: none">• Chassis empty• Controller enclosure (fully populated with FRUs and disks)• Expansion enclosure (fully populated with FRUs and disks)	5 kg (11 lb) 32 kg (71 lb) 28 kg (62 lb)
MSA 2070/2072 SFF Enclosure <ul style="list-style-type: none">• Chassis empty• Controller enclosure (fully populated with FRUs and disks)• Expansion enclosure (fully populated with FRUs and disks)	5 kg (11 lb) 30 kg (66 lb) 25 kg (55 lb)

Environmental requirements

NOTE For operating and non-operating environmental technical specifications, see "[Product QuickSpecs](#)" on page 9.

Electrical requirements

Site wiring and power requirements

Each enclosure has two power and cooling modules for redundancy. If full redundancy is required, use a separate power source for each module. AC-DC power is provided by up to two auto-ranging PCMs with integrated axial cooling fans. The enclosure's IOMs control fan speed.

The PCMs meet standard voltage requirements for both U.S. and international operation. The PCMs use standard industrial wiring with line-to-neutral or line-to-line power connections.

C Electrostatic discharge

Preventing electrostatic discharge

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

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-protected workstations.
- Place parts in a static-protected area before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.
- Remove clutter (plastic, vinyl, foam) from the static-protected workstation.

Grounding methods to prevent electrostatic discharge

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

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

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part. For more information on static electricity or assistance with product installation, contact an authorized reseller.

Index

#

- 2U12
 - large form factor (LFF) enclosure 80
- 2U24
 - small form factor (SFF) enclosure 80

A

- accessing
 - CLI (command-line interface) 39
 - SMU (Storage Management Interface) 43

B

- bezel
 - assembly view 64
 - attach/remove 12
 - exploded view 64

C

- cables
 - Ethernet 32
 - MSA 2070 iSCSI 29
 - MSA 2070/2072 FC 28
 - MSA 2070/2072 iSCSI 29
 - MSA 2070/2072 SAS 29
 - product QuickSpecs links 28
 - routing requirements 80
 - shielded 33, 80
- cabling
 - connecting controller and disk enclosures 21
 - direct attach configurations 29
 - switch attach configurations 31
 - to enable Remote Snap replication 34
- cache
 - read-ahead 19
 - self-refresh 74
 - write-back 18
- clearance requirements
 - service 80
 - ventilation 80
- command-line interface (CLI)
 - connecting USB cable to CLI port 40
 - using to set controller IP addresses 40
- components
 - controller enclosure rear panel 15
 - disk enclosure rear panel 17
 - enclosure front panel (LFF 12-drive) 13
 - enclosure front panel (SFF 24-drive) 12
- connections
 - verify 23
- controller enclosure
 - connecting to disk enclosures 21

- connecting to hosts 29
- connecting to remote management hosts 32

D

- data hosts
 - defined 27
 - optional software 27
 - system requirements 27

DHCP

- server (IPv4/IPv6) 38

disk slot numbering

- LFF 12-drive enclosure 14
- SFF 24-drive enclosure 13

E

- electrical guidelines 79
- electrostatic discharge
 - grounding methods 82
 - precautions 82
- enclosure
 - cabling 21
 - dimensions 80
 - IDs, correcting 47
 - installation checklist 20
 - safety requirements 78
 - site requirements 78
 - troubleshooting (basic steps) 44
 - web-browser based system setup 43
 - weight 81

F

- fault isolation
 - diagnostics for initial system setup 48
 - diagnostics for Remote Snap replication setup 57
 - expansion port connection fault 55
 - host-side connection 53
 - methodology 44

H

- host
 - defined 28
 - stopping I/O 48
- host interfaces
 - FC protocol 27
 - iSCSI protocol 27
 - SAS protocol 28

I

- installing enclosures
 - installation checklist 20

- IP addresses
 - setting using CLI port and cable 39
 - setting using DHCP 38

L

LEDs

- disk drive modules (SFF/LFF) 68
- enclosure front panel (LFF) 67
- enclosure front panel (SFF) 66
- enclosure rear panel (controller) 69
- enclosure rear panel (expansion) 76
- MSA 2070/2072 expansion module 77
- MSA 2070/2072 FC controller module 70
- MSA 2070/2072 iSCSI controller module 71
- MSA 2070/2072 PCMs (AC/DC) 75
- MSA 2070/2072 SAS controller module 73

P

- physical requirements 80

power cycle

- power off 26
- power on 26

power supply

- AC power requirements 78
- DC power requirements 78
- site wiring requirements 78

R

- regulatory/safety compliance 63

requirements

- electrical 81
- environmental 81
- management host 80
- physical 80
- safety 78
- site 78

- RFI/EMI connector hoods 33, 80

S

- safety precautions 78

sensors

- cooling fan 60
- locating 60
- PCM voltage 61
- power supply 60
- temperature 61

site planning

- requirements and guidelines 78

SMU

- accessing web-based management interface 43
- defined 43
- getting started 43

storage system setup

- configuring 43
- provisioning 43

- replicating 43

- supercapacitor pack 19

T

- technical support 62

troubleshooting system setup

- correcting enclosure IDs 48
- enclosure does not initialize 47
- expansion port connection fault 55
- host-side connection fault 53
- Remote Snap replication setup faults 56
- using event notification 45
- using system LEDs 46
- using the CLI 45
- using the SMU 45

V

- ventilation requirements 79

W

warnings

- voltage and temperature 59