



AssuredSAN 4004 Series Setup Guide

Abstract

This document describes initial hardware setup for Dot Hill AssuredSAN 4004 Series controller 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.

Copyright © 2013 Dot Hill Systems Corp. All rights reserved. Dot Hill Systems Corp., Dot Hill, the Dot Hill logo, AssuredSAN, AssuredSnap, AssuredCopy, AssuredRemote, R/Evolution, and the R/Evolution logo are trademarks of Dot Hill Systems Corp. All other trademarks and registered trademarks are proprietary to their respective owners.

The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, changes in the product design can be made without reservation and without notification to its users.



Adobe PostScript

Contents

About this guide	11
Overview	11
CNC ports used for host connection	11
HD mini-SAS ports used for host connection	12
Intended audience	12
Prerequisites	12
Related documentation	12
Document conventions and symbols	13
1 Components	15
Front panel components	15
24-drive enclosure front panel components	15
12-drive enclosure front panel components	16
Disk drives used in 4004 Series enclosures	16
Controller enclosure — rear panel layout	17
4824/4834 controller module — rear panel components	18
4524/4534 controller module — rear panel components	19
4124/4134 drive enclosure rear panel components	19
Component installation and replacement	19
Cache	20
CompactFlash	20
Supercapacitor pack	21
2 Installing the enclosures	23
Installation checklist	23
Network Equipment-Building System (NEBS) Level 3 compliance	23
Generic Requirements (GRs)	23
Exceptions to GRs	24
Product documentation requirements	24
Connecting the controller enclosure and drive enclosures	24
Connecting the 4004 Series controller to the SFF drive enclosure	25
Connecting the 4004 Series controller to the LFF drive enclosure	25
Connecting the 4004 Series controller to mixed model drive enclosures	25
Cable requirements for storage enclosures	25
Summary of drive enclosure cabling illustrations	26
Testing enclosure connections	30
Powering on/powering off	30
AC PSU	31
DC and AC PSUs equipped with a power switch	32
Connect power cable to DC power supply	32
Connect power cord to legacy AC power supply	32
3 Connecting hosts	35
Host system requirements	35
Cabling considerations	35
Connecting the enclosure to hosts	35
CNC technology	35
Fibre Channel protocol	36
10GbE iSCSI protocol	36
1 Gb iSCSI protocol	37
HD mini-SAS technology	37
12 Gb mini-SAS ports	37
Connecting direct attach configurations	37
Fibre Channel host connection	37

10GbE iSCSI host connection	37
1 Gb iSCSI host connection	38
HD mini-SAS host connection	38
Single-controller configurations	38
Dual-controller configurations	39
Connecting switch attach configurations	40
Dual-controller configuration	41
Connecting a management host on the network	42
Connecting two storage systems to replicate volumes	42
Cabling for replication	43
CNC ports and replication	44
Single-controller configuration	44
Dual-controller configuration	45
Updating firmware	48
Obtaining IP values	48
Setting network port IP addresses using DHCP	48
Setting network port IP addresses using the CLI port and cable	48
Change the CNC port mode	51
Set CNC port mode to iSCSI	51
Set CNC port mode to FC and iSCSI	51
Configure the system	51
4 Basic operation	53
Accessing RAIDar	53
Configuring and provisioning the storage system	53
5 Troubleshooting	55
USB CLI port connection	55
Fault isolation methodology	55
Basic steps	55
Options available for performing basic steps	55
Use RAIDar	55
Use the CLI	56
Monitor event notification	56
View the enclosure LEDs	56
Performing basic steps	56
Gather fault information	56
Determine where the fault is occurring	56
Review the event logs	56
Isolate the fault	57
If the enclosure does not initialize	57
Correcting enclosure IDs	57
Stopping I/O	57
Diagnostic steps	58
Is the enclosure front panel Fault/Service Required LED amber?	58
Is the controller back panel FRU OK LED off?	59
Is the controller back panel Fault/Service Required LED amber?	59
Are both disk drive module LEDs off?	59
Is the disk drive module Fault LED amber?	59
Is a connected host port Host Link Status LED off?	60
Is a connected port Expansion Port Status LED off?	60
Is a connected port's Network Port link status LED off?	60
Is the power supply Input Power Source LED off?	61
Is the Voltage/Fan Fault/Service Required LED amber?	61
Controller failure in a single-controller configuration	61
If the controller has failed or does not start, is the Cache Status LED on/blinking?	61
Transporting cache via professional services	62
Isolating a host-side connection fault	62
Host-side connection troubleshooting featuring CNC ports	62

Host-side connection troubleshooting featuring SAS host ports	63
Isolating a controller module expansion port connection fault	64
Isolating AssuredRemote replication faults	65
Cabling for replication	65
Replication setup and verification.	65
Diagnostic steps for replication setup	66
Can you successfully use the AssuredRemote feature?	66
Can you view information about remote links?	66
Can you create a replication set?	67
Can you replicate a volume?	68
Can you view a replication image?	68
Can you view remote systems?	68
Resolving voltage and temperature warnings	69
Sensor locations	69
Power supply sensors	69
Cooling fan sensors	69
Temperature sensors.	70
Power supply module voltage sensors.	70
A LED descriptions	71
Front panel LEDs.	71
Enclosure bezels	71
Enclosure bezel attachment and removal	71
Enclosure bezel attachment	71
Enclosure bezel removal	72
24-drive enclosure front panel LEDs	73
12-drive enclosure front panel LEDs	74
Disk drive LEDs.	75
Controller enclosure — rear panel layout.	77
4824/4834 CNC controller module — rear panel LEDs	78
4524/4534 SAS controller module—rear panel LEDs	80
Power supply LEDs.	81
4124/4134 drive enclosure rear panel LEDs.	82
B Environmental requirements and specifications.	83
Safety requirements.	83
Site requirements and guidelines	83
Site wiring and AC power requirements	83
Site wiring and DC power requirements	84
Weight and placement guidelines	84
Electrical guidelines	84
Ventilation requirements	85
Cabling requirements	85
Management host requirements	85
Physical requirements	85
Environmental requirements	87
Electrical requirements.	87
Site wiring and power requirements.	87
Power cable requirements.	88
C Electrostatic discharge	89
Preventing electrostatic discharge	89
Grounding methods to prevent electrostatic discharge	89
D USB device connection	91
Rear panel USB ports	91
USB CLI port	91
Emulated serial port	91
Supported host applications	92
Command-line Interface	92

Device driver/special operation mode	92
Microsoft Windows	92
Obtaining the software download.	92
Linux	93
Setting parameters for the device driver.	93
Using the CLI port and cable—known issues on Windows.	93
Problem	93
Workaround.	93
E SFP option for CNC ports.	95
Locate the SFP transceivers	95
Install an SFP transceiver	95
Verify component operation.	95
Index	97

Figures

1	2U24 enclosure: front panel	15
2	2U12 enclosure: front panel	16
3	4004 Series controller enclosure: rear panel	17
4	4824/4834 controller module face plate (FC or 10GbE iSCSI).	18
5	4824/4834 controller module face plate (1 Gb RJ-45)	18
6	4524/4534 controller module face plate (HD mini-SAS)	19
7	CompactFlash card	20
8	Cabling connections between a controller enclosure and one drive enclosure	27
9	Fault-tolerant cabling between a dual-controller enclosure and four drive enclosures.	28
10	Cabling diagrams for maximum configuration	29
11	AC PSU	31
12	AC power cord	31
13	DC and AC PSUs with power switch	32
14	DC power cable featuring D-shell and lug connectors	32
15	Connecting hosts: direct attach—one server/one HBA/single path	38
16	Connecting hosts: direct attach—one server/one HBA/dual path	39
17	Connecting hosts: direct attach—two servers/one HBA per server/dual path	40
18	Connecting hosts: direct attach—four servers/one HBA per server/dual path	40
19	Connecting hosts: switch attach—two servers/two switches.	41
20	Connecting hosts: switch attach—four servers/multiple switches/SAN fabric.	41
21	Connecting two storage systems for AssuredRemote: one server/two switches/one location	44
22	Connecting two storage systems for AssuredRemote: multiple servers/one switch/one location	45
23	Connecting two storage systems for AssuredRemote: multiple servers/switches/one location	45
24	Connecting two storage systems for AssuredRemote: multiple servers/switches/two locations	46
25	Connecting two storage systems for AssuredRemote: multiple servers/SAN fabric/two locations	47
26	Connecting a USB cable to the CLI port	49
27	Front panel enclosure bezel: 24-drive enclosure (2U24)	71
28	Front panel enclosure bezel: 12-drive enclosure (2U12)	71
29	Partial assembly showing bezel alignment with 2U24 chassis	72
30	Partial assembly showing bezel alignment with 2U12 chassis	72
31	LEDs: 2U24 enclosure front panel	73
32	LEDs: 2U12 enclosure front panel	74
33	LEDs: Disk drive modules	75
34	4004 Series controller enclosure: rear panel	77
35	LEDs: 4824/4834 CNC controller module (FC and 10GbE SFPs)	78
36	LEDs: 4824/4834 CNC controller module (1 Gb RJ-45 SFPs)	79
37	LEDs: 4524/4534 SAS controller module (HD mini-SAS)	80
38	LEDs: Power supply units — rear panel.	81
39	LEDs: 4124/4134 drive enclosure — rear panel.	82
40	Rackmount enclosure dimensions	86
41	USB device connection — CLI port.	91
42	Install a qualified SFP option	95

Tables

1	Related documents	12
2	Document conventions	13
3	Installation checklist	23
4	Summary of cabling connections for 4004 Series enclosures	26
5	Terminal emulator display settings	49
6	Terminal emulator connection settings	49
7	Diagnostics LED status: Front panel "Fault/Service Required"	58
8	Diagnostics LED status: Rear panel "FRU OK"	59
9	Diagnostics LED status: Rear panel "Fault/Service Required"	59
10	Diagnostics LED status: Disk drives (LFF and SFF modules)	59
11	Diagnostics LED status: Disk drive fault status (LFF and SFF modules)	59
12	Diagnostics LED status: Rear panel "Host Link Status"	60
13	Diagnostics LED status: Rear panel "Expansion Port Status"	60
14	Diagnostics LED status: Rear panel "Network Port Link Status"	60
15	Diagnostics LED status: Rear panel power supply "Input Power Source"	61
16	Diagnostics LED status: Rear panel power supply "Voltage/Fan Fault/Service Required"	61
17	Diagnostics LED status: Rear panel "Cache Status"	62
18	Diagnostics for replication setup: Using AssuredRemote feature	66
19	Diagnostics for replication setup: Viewing information about remote links	66
20	Diagnostics for replication setup: Creating a replication set	67
21	Diagnostics for replication setup: Replicating a volume	68
22	Diagnostics for replication setup: Viewing a replication image	68
23	Diagnostics for replication setup: Viewing a remote system	68
24	Power supply sensor descriptions	69
25	Cooling fan sensor descriptions	69
26	Controller module temperature sensor descriptions	70
27	Power supply temperature sensor descriptions	70
28	Voltage sensor descriptions	70
29	LEDs: Disks in SFF and LFF enclosures	76
30	LEDs: Vdisks in SFF and LFF enclosures	76
31	Power requirements - AC Input	83
32	Power requirements - DC Input	84
33	Rackmount controller enclosure weights	86
34	Rackmount compatible drive enclosure weights (ordered separately)	87
35	Operating environmental specifications	87
36	Non-operating environmental specifications	87
37	Supported terminal emulator applications	92
38	USB vendor and product identification codes	92

About this guide

Overview

This guide provides information about initial hardware setup for the AssuredSAN™ 4004 Series storage enclosure products listed below:

- CNC (Converged Network Controller) controller enclosure: 4824/4834
 - Qualified Fibre Channel SFP option supporting (4/8/16 Gb)
 - Qualified Internet SCSI (10GbE) SFP option
 - Qualified Internet SCSI (1 Gb) Copper RJ-45 SFP option
- HD mini-SAS (12 Gb) controller enclosure: 4524/4534

AssuredSAN 4004 Series enclosures are designed to meet NEBS Level 3, MIL-STD-810G (storage requirements), and European Telco requirements. The 4004 Series supports both a large form factor (LFF 12-disk) 2U chassis and a small form factor (SFF 24-disk) 2U chassis. These chassis form factors support controller enclosures and expansion enclosures.

The 4004 Series controller enclosures can optionally be cabled to 4124/4134 drive enclosures for adding storage. The 4124 is an SFF 24-disk 2U expansion enclosure, and the 4134 is an LFF 12-disk 2U expansion enclosure. Storage enclosures can be equipped with single or dual I/O modules (IOMs); and they can be equipped with either two AC or two DC power supply modules.


See the Dot Hill web site for more information about specific storage product models and uses: <http://www.dothill.com>.


CNC ports used for host connection

AssuredSAN 4824/4834 models use Converged Network Controller (CNC) technology, allowing you to select the desired host interface protocol from the available Fibre Channel (FC) or Internet SCSI (iSCSI) host interface protocols supported by the system. You can use the Command-line Interface (CLI) to set all controller module CNC ports to use one of these host interface protocols:

- 16 Gb FC
- 8 Gb FC
- 4 Gb FC
- 10 GbE iSCSI
- 1 GbE iSCSI

Alternatively, you can use the CLI to set CNC ports to support a combination of host interface protocols. When configuring a combination of host interface protocols, host ports 0 and 1 are set to FC (either both 16 Gbit/s or both 8 Gbit/s), and host ports 2 and 3 must be set to iSCSI (either both 10GbE or both 1 Gbit/s), provided the CNC ports use the qualified SFP connectors and cables required for supporting the selected host interface protocol. See [CNC technology](#) on page 35 and [4824/4834 CNC controller module — rear panel LEDs](#) on page 78 for more information.

 **TIP:** See the “Configuring host ports” topic within the RAIDar User Guide for information about configuring CNC ports with host interface protocols of the same type or a combination of types.

 **IMPORTANT:** AssuredSAN 4824/4834 models ship with CNC ports initially configured for FC. When connecting CNC ports to iSCSI hosts, you must use the CLI (not RAIDar) to specify which ports will use iSCSI. It is best to do this before inserting the iSCSI SFPs into the CNC ports (see [Change the CNC port mode](#) on page 51 for instructions).

HD mini-SAS ports used for host connection

AssuredSAN 4524/4534 models provide four high-density mini-SAS (HD mini-SAS) ports per controller module. The HD mini-SAS host interface protocol uses the SFF-8644 external connector interface defined for SAS3.0 to support a link rate of 12 Gbit/s using the qualified connectors and cable options. See [4524/4534 SAS controller module—rear panel LEDs](#) on page 80 for more information.

Intended audience

This guide is intended for storage system administrators.

Prerequisites

Prerequisites for installing and using this product include knowledge of:

- Servers and computer networks
- Network administration
- Storage system installation and configuration
- Storage area network (SAN) management and direct attach storage (DAS)
- Fibre Channel (FC), Internet SCSI (iSCSI), Serial Attached SCSI (SAS), and Ethernet protocols

Related documentation

Table 1 Related documents

For information about	See
Enhancements, known issues, and late-breaking information not included in product documentation	Release Notes
Overview of product shipkit contents and setup tasks	Getting Started*
Using a rackmount bracket kit to install an enclosure into a rack	AssuredSAN Rackmount Bracket Kit Installation* or AssuredSAN 2-Post Rackmount Bracket Kit Installation*
Obtaining and installing a license to use licensed features	AssuredSAN 4004 Series Obtaining and Installing a License Certificate File
Using the web interface to configure and manage the product	AssuredSAN 4004 Series RAIDar User Guide
Using the command-line interface (CLI) to configure and manage the product	AssuredSAN 4004 Series CLI Reference Guide
Event codes and recommended actions	AssuredSAN 4004 Series Event Descriptions Reference Guide
Identifying and installing or replacing field-replaceable units (FRUs)	AssuredSAN 4004 Series FRU Installation and Replacement Guide

* Printed document included in product shipkit.

For additional information, see Dot Hill's Customer Resource Center web site: <http://crc.dothill.com>.

Document conventions and symbols

Table 2 Document conventions

Convention	Element
Blue text	Cross-reference links and e-mail addresses
Blue, underlined text	Web site addresses
Bold text	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italic</i> text	Text emphasis
Monospace text	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic</i> text	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold text	Emphasis of file and directory names, system output, code, and text typed at the command-line

△ **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

📄 **IMPORTANT:** Provides clarifying information or specific instructions.

NOTE: Provides additional information.

💡 **TIP:** Provides helpful hints and shortcuts.

1 Components

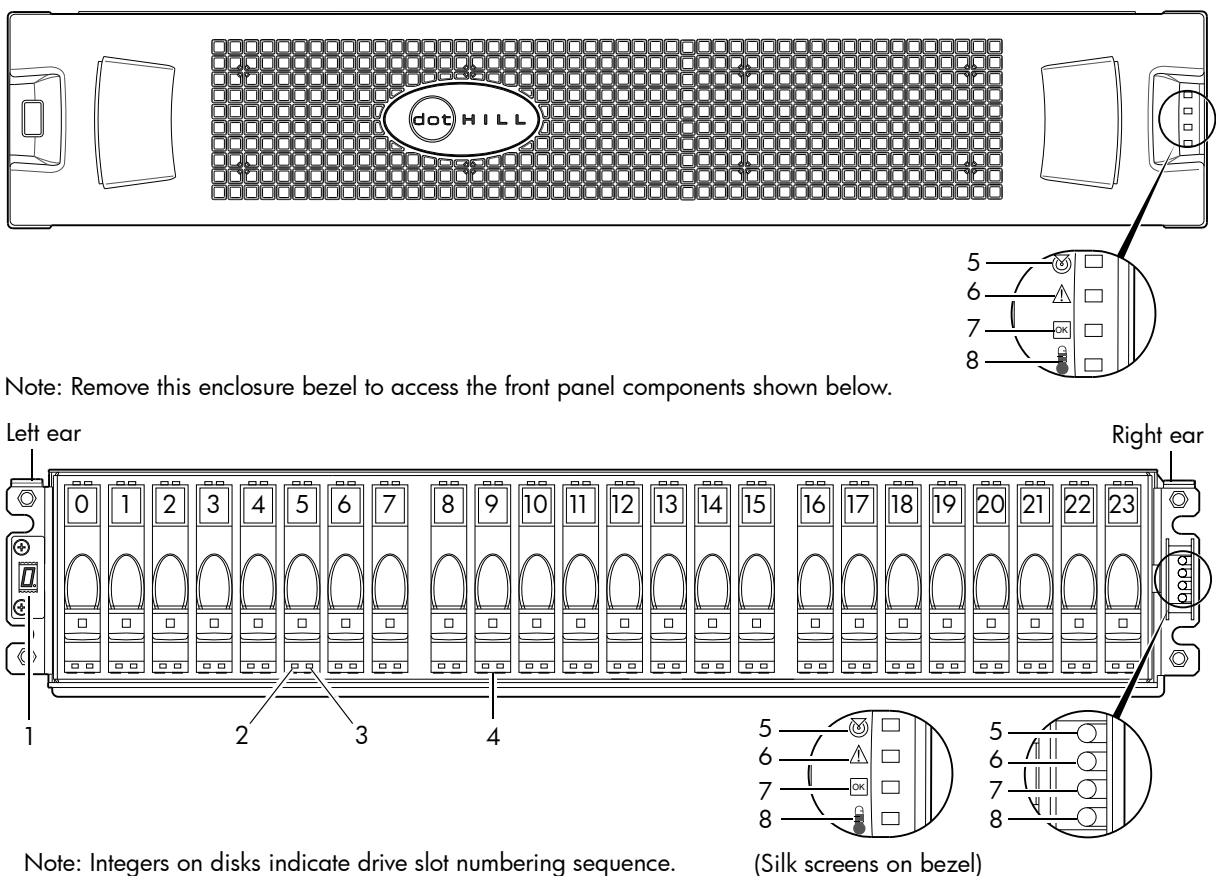
Front panel components

AssuredSAN 4004 Series supports 2U24 and 2U12 enclosures. The 2U24 chassis—configured with 24 2.5" small form factor (SFF) disks—is used as either a controller enclosure or expansion enclosure. The 2U12 chassis—configured with 12 3.5" large form factor (LFF) disks—is also used as either a controller enclosure or expansion enclosure.

Supported expansion enclosures are used for adding storage. The 4134 12-drive enclosure is the LFF drive enclosure used for storage expansion. The 4124 24-drive enclosure is the SFF drive enclosure used for storage expansion.

Storage enclosures support single or dual I/O modules (IOMs), and they can be equipped with either two redundant AC or two redundant DC power supply modules.

24-drive enclosure front panel components



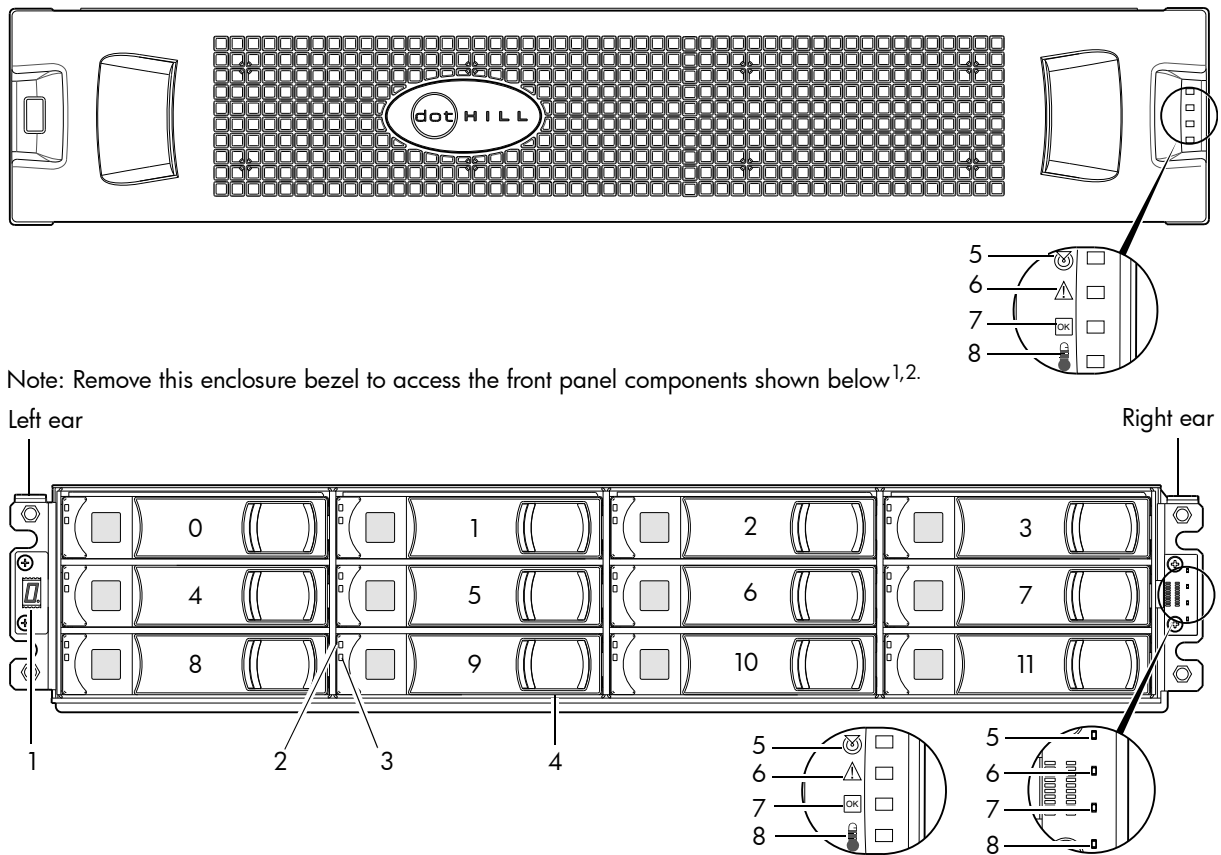
- | | |
|---|--|
| 1 Enclosure ID LED | 5 Enclosure status LED: Unit Locator |
| 2 Disk drive status LED: OK to Remove | 6 Enclosure status LED: Fault/Service Required |
| 3 Disk drive status LED: Power/Activity/Fault | 7 Enclosure status LED: FRU OK |
| 4 2.5" disk or drive blank (typical 24 slots) | 8 Enclosure status LED: Temperature Fault |

Figure 1 2U24 enclosure: front panel

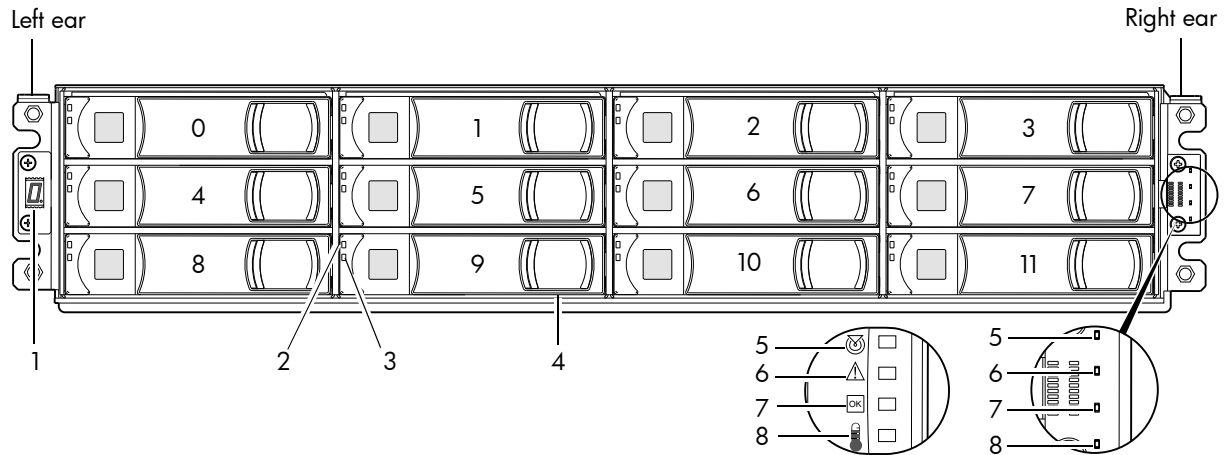
TIP: See [Enclosure bezel attachment and removal](#) on page 71 and [Figure 29](#) on page 72 (2U24).

NOTE: Front and rear panel LEDs for controller enclosures are described in [LED descriptions](#).

12-drive enclosure front panel components



Note: Remove this enclosure bezel to access the front panel components shown below^{1,2}.



Note: Integers on disks indicate drive slot numbering sequence.

(Silk screens on bezel)

- | | |
|---|--|
| 1 Enclosure ID LED | 5 Enclosure status LED: Unit Locator |
| 2 Disk drive status LED: OK to Remove | 6 Enclosure status LED: Fault/Service Required |
| 3 Disk drive status LED: Power/Activity/Fault | 7 Enclosure status LED: FRU OK |
| 4 3.5" disk or drive blank (typical 12 slots) | 8 Enclosure status LED: Temperature Fault |

¹This bezel might optionally include a removable air filter that can be serviced or replaced. Hard copy instructions for attaching or removing the bezel, and for servicing or replacing the air filters, are provided in the shipping container of a new enclosure.

²Alternatively, you can access the *AssuredSAN 12-drive Enclosure Bezel Kit Installation* document online. See Dot Hill's customer resource center (CRC) web site for additional information: <http://crc.dothill.com>.

Figure 2 2U12 enclosure: front panel

TIP: See [Enclosure bezel attachment and removal](#) on page 71 and [Figure 30](#) on page 72 (2U12).

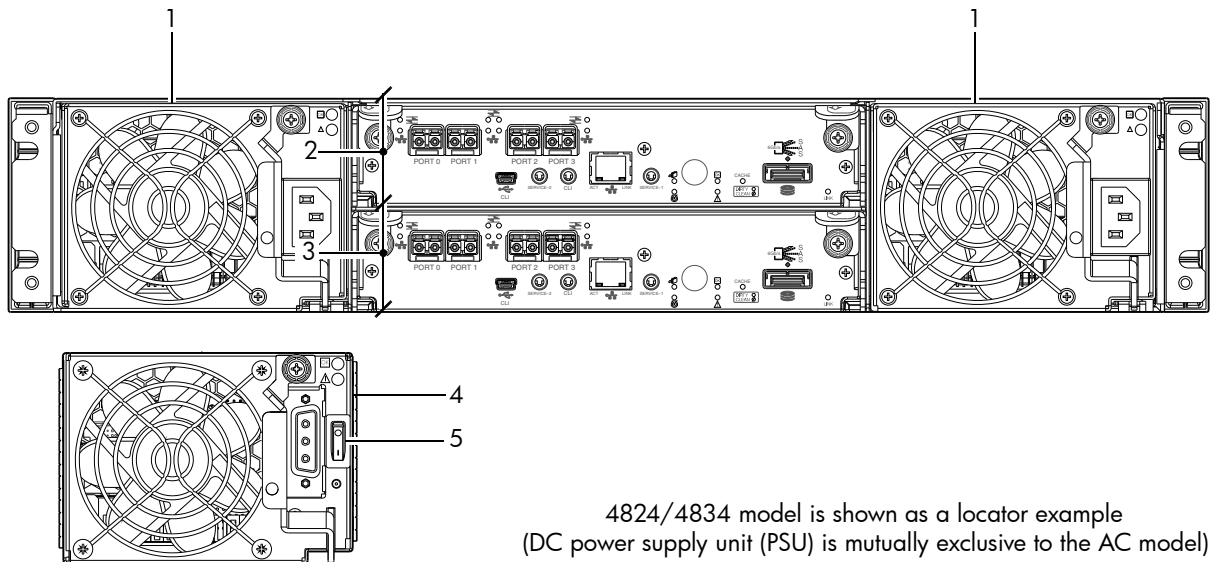
NOTE: Front and rear panel LEDs for controller enclosures are described in [LED descriptions](#).

Disk drives used in 4004 Series enclosures

4004 Series enclosures support LFF/SFF Midline SAS, LFF/SFF Enterprise SAS, and SFF SSD disks. For information about creating vdisks and adding spares using different disk drive types, see the *AssuredSAN 4004 Series RAIDar User Guide* or online help.

Controller enclosure — rear panel layout

The diagram and table below display and identify important component items that comprise the rear panel layout of an AssuredSAN 4004 Series controller enclosure. The 4824/4834 is shown as a representative example of controller enclosure models included in the product series.



- | | |
|---|---|
| 1 AC power supplies | 4 DC power supply (2) — (DC model only) |
| 2 Controller module A (see face plate detail figures) | 5 DC power switch |
| 3 Controller module B (see face plate detail figures) | |

4824/4834 model is shown as a locator example
(DC power supply unit (PSU) is mutually exclusive to the AC model)

Figure 3 4004 Series controller enclosure: rear panel

A controller enclosure accommodates two power supply FRUs of the same type—either both AC or both DC—within the two power supply slots (see two instances of callout No.1 above). The controller enclosure accommodates up to two controller module FRUs of the same type within the I/O module (IOM) slots (see callouts No.2 and No.3 above).

IMPORTANT: If the 4004 Series controller enclosure is configured with a single controller module, the controller module must be installed in the upper slot (see callout No.2 above), and an I/O module blank must be installed in the lower slot (see callout No.3 above). This configuration is required to allow sufficient air flow through the enclosure during operation.

The diagrams with tables that immediately follow provide descriptions for the different controller modules and power supply modules that can be installed into the rear panel of a 4004 Series controller enclosure. Showing controller modules and power supply modules separately from the enclosure enables 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 4004 Series controller enclosures for expanding storage capacity.

NOTE: 4004 Series enclosures support hot-plug replacement of redundant controller modules, fans, power supplies, and expansion modules. Hot-add replacement of drive enclosures is also supported.

4824/4834 controller module — rear panel components

Figure 4 shows CNC ports configured with SFPs supporting either 4/8/16 Gb FC or 10GbE iSCSI. The SFPs look identical. Refer to the CNC LEDs that apply to the specific configuration of your CNC ports.

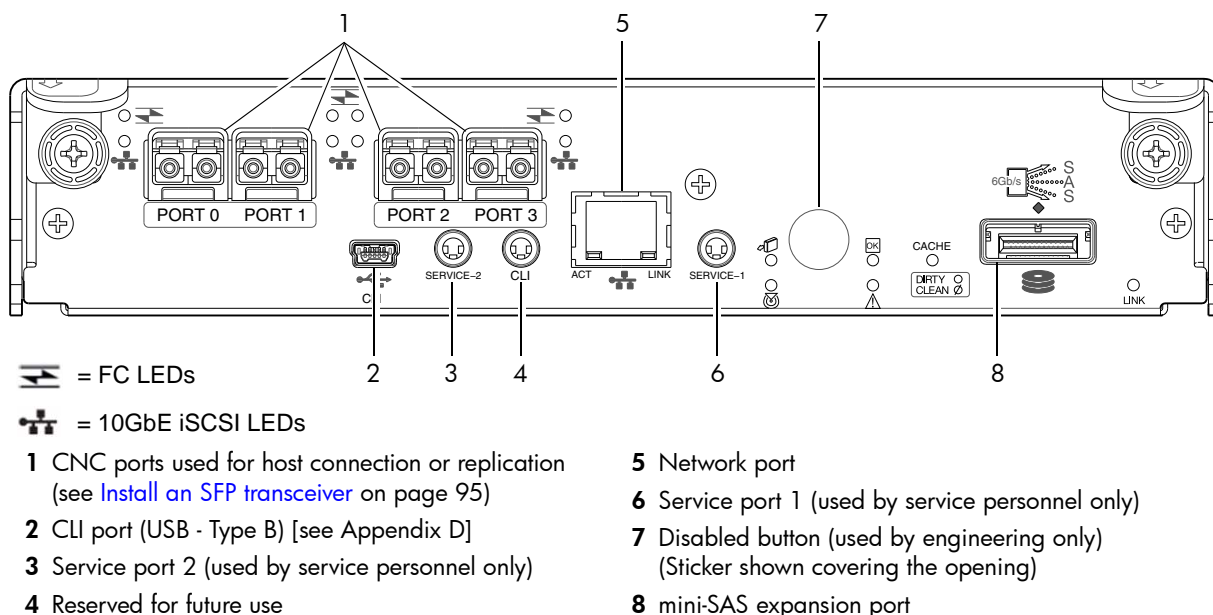


Figure 4 4824/4834 controller module face plate (FC or 10GbE iSCSI)

Figure 5 shows CNC ports configured with 1 Gb RJ-45 SFPs.

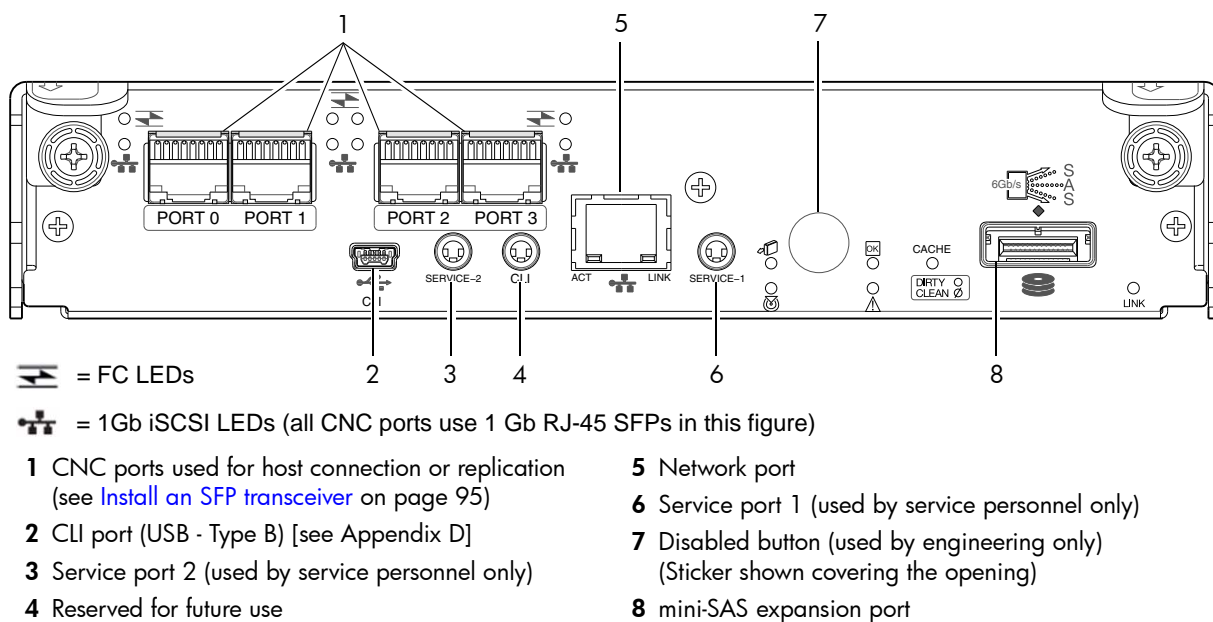
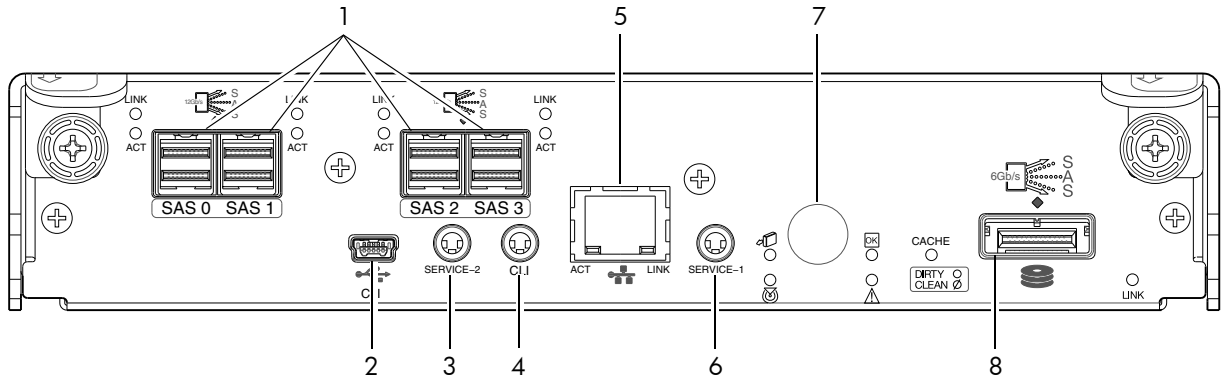


Figure 5 4824/4834 controller module face plate (1 Gb RJ-45)

NOTE: See [CNC ports used for host connection](#) on page 11 for more information about CNC technology. For CNC port configuration, see the “Configuring host ports” topic within the RAIDar User Guide or online help.

4524/4534 controller module — rear panel components

Figure 6 shows host ports configured with 12 Gbit/s HD mini-SAS (SFF-8644) connectors.

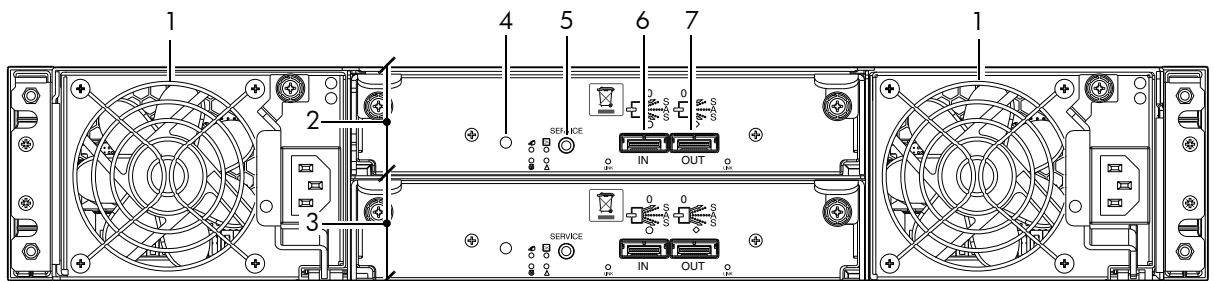


- | | |
|---|--|
| 1 HD mini-SAS ports used for host connection | 6 Service port 1 (used by service personnel only) |
| 2 CLI port (USB - Type B) [see Appendix D] | 7 Disabled button (used by engineering only)
(Sticker shown covering the opening) |
| 3 Service port 2 (used by service personnel only) | 8 mini-SAS expansion port |
| 4 Reserved for future use | |
| 5 Network port | |

Figure 6 4524/4534 controller module face plate (HD mini-SAS)

4124/4134 drive enclosure rear panel components

AssuredSAN 4004 Series controller enclosures support SFF 4124 24-disk and LFF 4134 12-disk drive enclosures for expansion of storage capacity. These drive enclosures use mini-SAS (SFF-8088) connectors to facilitate backend SAS expansion. See [Cable requirements for storage enclosures](#) on page 25 for cabling information.



- | | |
|---|---|
| 1 Power supplies (AC shown) | 5 Service port (used by service personnel only) |
| 2 Expansion module A | 6 SAS In port |
| 3 Expansion module B | 7 SAS Out port |
| 4 Disabled button (used by engineering/test only) | |

Component installation and replacement

Installation and replacement of 4004 Series FRUs (field-replaceable units) is addressed in the *AssuredSAN 4004 Series FRU Installation and Replacement Guide* within the “Procedures” chapter.

FRU procedures facilitate replacement of a damaged chassis or chassis component:

- Replacing a controller or expansion module
- Replacing a disk drive module
- Replacing a power supply unit (AC and DC units with integrated cooling fans)
- Replacing ear bezels
- Replacing a Fibre Channel transceiver

- Replacing a 10GbE SFP+ transceiver
- Replacing a 1 Gb SFP transceiver
- Replacing a controller enclosure chassis

See Dot Hill's Customer Resource Center web site for additional information: <http://crc.dothill.com>.

Select **AssuredSAN & R/Evolution Products > 4004 Series** to download the FRU I&R guide.

Cache

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

- Write-back or write-through caching. The controller writes user data into the cache memory in 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 data access, reads ahead into the next sequence of data—based upon settings—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.

TIP: See the “About volume cache options” and “Changing system cache settings” topics in the RAIDar User Guide for setting options.

CompactFlash

During a power loss or controller failure, data stored in cache is saved off to non-volatile memory (CompactFlash). The data is restored to cache, and then written to disk after the issue is corrected. To protect against writing incomplete data to disk, the image stored on the CompactFlash is verified before committing to disk.

The CompactFlash card is located at the midplane-facing end of the controller module as shown below. Do not remove the card; it is used for cache recovery only.

Controller module pictorial
(Midplane-facing rear view)

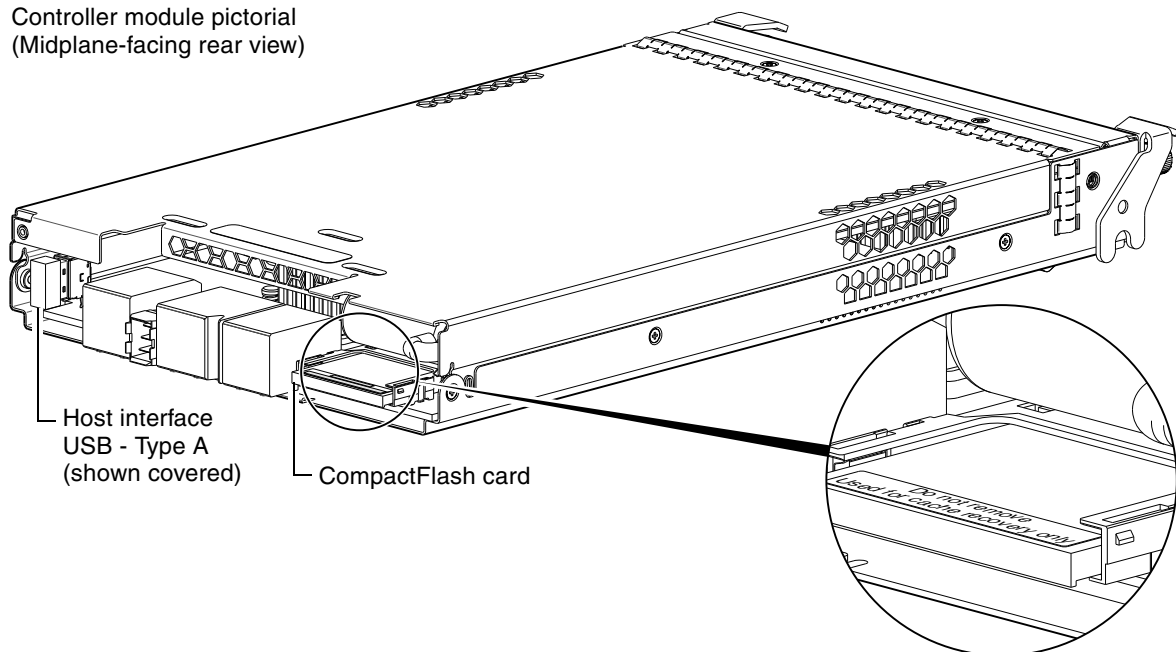



Figure 7 CompactFlash card

In single-controller configurations, if the controller has failed or does not start, and the Cache Status LED is on or blinking, the CompactFlash will need to be transported to a replacement controller to recover data

not flushed to disk (see [Controller failure in a single-controller configuration](#) on page 61 for more information).

 **IMPORTANT:** Customer removal of CompactFlash will void the product warranty.

 **IMPORTANT:** In dual-controller configurations featuring one healthy partner controller, there is no need to transport failed controller cache to a replacement controller because the cache is duplicated between the controllers (subject to volume write optimization setting).

Supercapacitor pack

To protect controller module cache in case of power failure, each controller enclosure model is equipped with supercapacitor technology, in conjunction with CompactFlash memory, built into each controller module to provide extended cache memory backup time. The supercapacitor pack provides energy for backing up unwritten data in the write cache to the CompactFlash, in the event of a power failure. Unwritten data in CompactFlash memory is automatically committed to disk media when power is restored. In the event of power failure, while cache is maintained by the supercapacitor pack, the Cache Status LED flashes at a rate of 1/10 second on and 9/10 second off.

2 Installing the enclosures

Installation checklist

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

Table 3 Installation checklist

Step	Task	Where to find procedure
1.	Install the controller enclosure and optional drive enclosures in the rack, and attach the enclosure bezel. ¹	See the rack-mount bracket kit installation instructions pertaining to your enclosure. Also refer to the bezel attachment instructions for your enclosure
2.	Connect controller enclosure and optional drive enclosures.	See Connecting the controller enclosure and drive enclosures on page 24.
3.	Connect power cords.	See Powering on/powering off on page 30.
4.	Test enclosure connectivity.	See Testing enclosure connections on page 30.
5.	Install required host software.	See Host system requirements on page 35.
6.	Connect hosts. ²	See Connecting the enclosure to hosts on page 35.
7.	Connect remote management hosts. ²	See Connecting a management host on the network , page 42.
8.	Obtain IP values and set network port IP properties on the controller enclosure.	See Obtaining IP values on page 48. For USB CLI port and cable use, see Appendix D. Also see the ship kit CD.
9.	Use the CLI to set the host interface protocol.	See CNC technology on page 35. The 4824/4834 models allow you to set the host interface protocol for your qualified SFP option. Use the <code>set host-port-mode</code> command as described in the CLI Reference Guide or online help.
10.	Perform initial configuration tasks ³ : <ul style="list-style-type: none">• Sign-in to the web-browser interface (RAIDar) to access the application GUI.• Verify firmware revisions and update if necessary.• Initially configure and provision the system using RAIDar.	Topics below correspond to bullets at left: See "Getting Started" in the web-posted <i>AssuredSAN 4004 Series RAIDar User Guide</i> . See Updating firmware on page 48. Also see the same topic in the <i>AssuredSAN 4004 Series RAIDar User Guide</i> . See "Configuring the System" and "Provisioning the System" topics in the RAIDar User Guide or online help.

¹ See the *AssuredSAN 4004 Series FRU Installation and Replacement Guide* for illustrations and narrative describing attachment of enclosure bezels to 2U24 and 2U12 chassis. See also [Enclosure bezel attachment and removal](#) on page 71.

² For more about hosts, see the "About hosts" topic in the *AssuredSAN 4004 Series RAIDar User Guide*.

³ RAIDar is introduced in [Accessing RAIDar](#) on page 53. See the RAIDar User Guide or online help for additional information.

NOTE: Additional installation notes:

- Controller modules within the same enclosure must be of the same type.
- For optimal performance, do not mix 6 Gb and 3 Gb disk drives within the same enclosure.

Network Equipment-Building System (NEBS) Level 3 compliance

Generic Requirements (GRs)

Meets the NEBS requirement of GR-1089-CORE Issue 5, port types 2, 7 & 8.

Meets the NEBS requirements of GR-63-CORE Issue 3, for the product's intended use.

NOTE: Table 4 on page 26 shows NEBS-compliance for individual storage enclosures.

Exceptions to GRs

Exceptions to the overall NEBS GR-63-CORE Issue 3 requirements include:

- Heat Dissipation: Environmental Criteria Section 4.1.6, Operational Requirement O4-20. This product exceeds the Optional Requirements shown in Table 4-5 for Forced-Air Fan Shelf equipment.
- Airborne Contaminants: This product is designed for indoor use only, and has not been tested for Outdoor Contaminant Levels (Table 4-11); per Requirement R4-86 (Environmental Criteria section 4.5.2.2).
- Equipment — Fan Filters: Environmental Criteria Section 4.5.4. This product does not have a fan filter, and has not been tested by any requirements in section 4.5.4. The following requirements have not been tested: R4-87 [138]; R4-88 [139]; R4-89 [176]; R4-90 [140]; R4-91 [141]; R4-92 [142]; R4-93 [143]; O4-94 [144] and O4-95 [145].
- This product does not meet the requirements of Spatial Requirements, Section 2.

Exceptions to the overall NEBS GR-1089-CORE Issue 5 requirements include:

- None reported

Product documentation requirements

NEBS product documentation requirements applying to AssuredSAN 4004 Series controller and drive enclosures are listed beneath “NEBS (Level 3)” in the Index — under either GR-1089-CORE Issue 5 or GR-63-CORE Issue 3 — together with adjacent page locations. NEBS topics are *integrated* within the overall content of this setup guide. The requirement designators in the Index have been codified for use within index marker tags according to the following example:

NEBS generic requirement number “R2-7 [7]” appears as “R2-7.7” within the Index.

Each codified string (e.g., R2-7.7) is followed by a hyphen and brief description of the requirement. Within the Index, click on the [blue page number](#) link to navigate to the corresponding NEBS topic.

Connecting the controller enclosure and drive enclosures

AssuredSAN 4004 Series controller enclosures—available in 24-drive (2.5") or 12-drive (3.5") chassis—support up to eight enclosures (including the controller enclosure), or a maximum of 192 disk drives. The 4004 Series enclosures support both *straight-through* and *reverse* SAS cabling. Reverse cabling allows any drive enclosure to fail—or be removed—while maintaining access to other enclosures. Fault tolerance and performance requirements determine whether to optimize the configuration for high availability or high performance when cabling. AssuredSAN 4004 Series controller modules support both 3-Gbps and 6-Gbps internal disk drive speeds together with 3-Gbps and 6-Gbps expander link speeds.

△ **CAUTION:** Some 6-Gbps disks might not consistently support a 6-Gbps transfer rate. If this happens, the system automatically adjusts transfers to those disks to 3 Gbps, increasing reliability and reducing error messages with little impact on system performance. This rate adjustment persists until the controller is restarted or power-cycled.

Cabling diagrams in this section show fault-tolerant cabling patterns. Controller and expansion modules are identified by <enclosure-ID><controller-ID>. When connecting multiple drive enclosures, use reverse cabling to ensure the highest level of fault tolerance, enabling controllers to access remaining drive enclosures if a drive enclosure fails.

For example, the illustration on the left in [Figure 9](#) on page 28 shows reverse cabling, wherein controller 0A (i.e., enclosure-ID = 0; controller-ID = Able) is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller 0B is connected to the lower expansion module (B) of the last drive enclosure in the chain, with connections moving in the opposite direction (green). Several cabling examples are provided on the following pages.

Connecting the 4004 Series controller to the SFF drive enclosure

The SFF 4124 24-drive enclosure, supporting 6 Gb internal disk drive and expander link speeds, can be attached to a 4004 Series controller enclosure using supported mini-SAS to mini-SAS cables of 0.5 m (1.64') to 2 m (6.56') length (see [Figure 8](#) on page 27).

Connecting the 4004 Series controller to the LFF drive enclosure

The LFF 4134 24-drive enclosure, supporting 6 Gb internal disk drive and expander link speeds, can be attached to a 4004 Series controller enclosure using supported mini-SAS to mini-SAS cables of 0.5 m (1.64') to 2 m (6.56') length (see [Figure 8](#) on page 27).


Connecting the 4004 Series controller to mixed model drive enclosures

The 4004 Series controllers support cabling of 6 Gb SAS link-rate SFF and LFF expansion modules—in mixed model fashion—as shown in [Figure 9](#) on page 28. The simplified rear-panel views of the 4124 and 4134 are identical.

Cable requirements for storage enclosures

The 4004 Series enclosures support 6-Gbps or 3-Gbps expansion port data rates. Use only AssuredSAN or OEM-qualified cables, and observe the following guidelines (see [Table 4](#) below):

- When installing SAS cables to expansion modules, use only supported mini-SAS x4 cables with SFF-8088 connectors supporting your 6 Gb application.
- Qualified mini-SAS to mini-SAS 0.5 m (1.64') cables are used to connect cascaded enclosures in the rack. The “mini-SAS to mini-SAS” cable designator connotes SFF-8088 to SFF-8088 connectors.
- The maximum expansion cable length allowed in any configuration is 2 m (6.56').
- Cables required, if not included, must be separately purchased.
- When adding more than two drive enclosures, you may need to purchase additional 1 m or 2 m cables, depending upon number of enclosures and cabling method used:
 - Spanning 3, 4, or 5 drive enclosures requires 1 m (3.28') cables.
 - Spanning 6 or 7 drive enclosures requires 2 m (6.56') cables.
- You may need to order additional or longer cables when reverse-cabling a fault-tolerant configuration (see [Figure 10](#) on page 29).
- Use only AssuredSAN or OEM-qualified cables for host connection:
 - Qualified Fibre Channel SFP and cable options
 - Qualified 10GbE iSCSI SFP and cable options
 - Qualified 1 Gb RJ-45 SFP and cable options
 - Qualified HD mini-SAS cable options supporting SFF-8644 and SFF-8088 host connectionA qualified SFF-8644 to SFF-8644 cable option is used for connecting to a 12 Gbit/s enabled host; whereas a qualified SFF-8644 to SFF-8088 cable option is used for connecting to a 6 Gbit/s enabled host.

 **TIP:** Requirements for cabling 4004 Series controller enclosures and supported drive enclosures are summarized in [Table 4](#) on page 26.

[Table 4](#) summarizes key characteristics of controller enclosures and compatible drive (expansion) enclosures relative to cabling, including: the cable type needed for attaching one specific enclosure model to another specific enclosure model; internal disk drive speeds; number of disks of given size (SFF or LFF) supported per enclosure model; and SAS expander data rates. Enclosure form factor (2U24/2U12) and NEBS compliance information are also provided.

Table 4 Summary of cabling connections for 4004 Series enclosures

Model	Form	Host connect	NEBS	SFF 24-disk drive enclosure	LFF 12-disk drive enclosure
4824 ^{1,2}	2U24	FC (8/16 Gb) SFP option	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4834 ^{1,2}	2U12	FC (8/16 Gb) SFP option	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4824 ^{1,2}	2U24	10GbE iSCSI SFP option	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4834 ^{1,2}	2U12	10GbE iSCSI SFP option	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4824 ^{1,2}	2U24	1 Gb iSCSI SFP option	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4834 ^{1,2}	2U12	1 Gb iSCSI SFP option	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4524 ^{1,3}	2U24	HD mini-SAS connector	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4534 ^{1,3}	2U12	HD mini-SAS connector	Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4124	2U24		Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
4134	2U12		Note 4	mini-SAS to mini-SAS	mini-SAS to mini-SAS
Enclosure chassis designators: 2U24: Enclosure measuring two rack units high, providing 24 SFF (2.5") sledded disk drive modules. 2U12: Enclosure measuring two rack units high, providing 12 LFF (3.5") sledded disk drive modules.					
See Physical requirements on page 85 for more information about 2U24 and 2U12 enclosures.					

¹These compatible product models feature 6 Gbit/s internal disk and SAS expander link speeds.

²See [CNC technology](#) on page 35 for information about locating and installing qualified SFP options into CNC ports.

³See [12 Gb mini-SAS ports](#) on page 37 for information about host connection using SFF-8644 high-density mini-SAS connectors.

⁴The 4004 Series is designed for NEBS compliance.

Summary of drive enclosure cabling illustrations

The following illustrations show both *reverse* and *straight-through* cabling examples featuring 4004 Series controller enclosures and compatible 4124 (2U24) and 4134 (2U12) drive enclosures. The rear-panel views of the 4124 and 4134 are identical. All storage enclosures use mini-SAS connectors for expansion.

NOTE: The 4004 Series controller enclosures and compatible drive enclosures support mini-SAS SFF-8088 connectors for adding storage. See [Table 4](#) for SAS cable requirements.

NOTE: For clarity, the schematic diagrams show only relevant details such as face plate outlines and expansion ports. For detailed illustrations, see [Controller enclosure — rear panel layout](#) on page 17. Also see the controller module face plate illustrations that follow the rear panel layout.

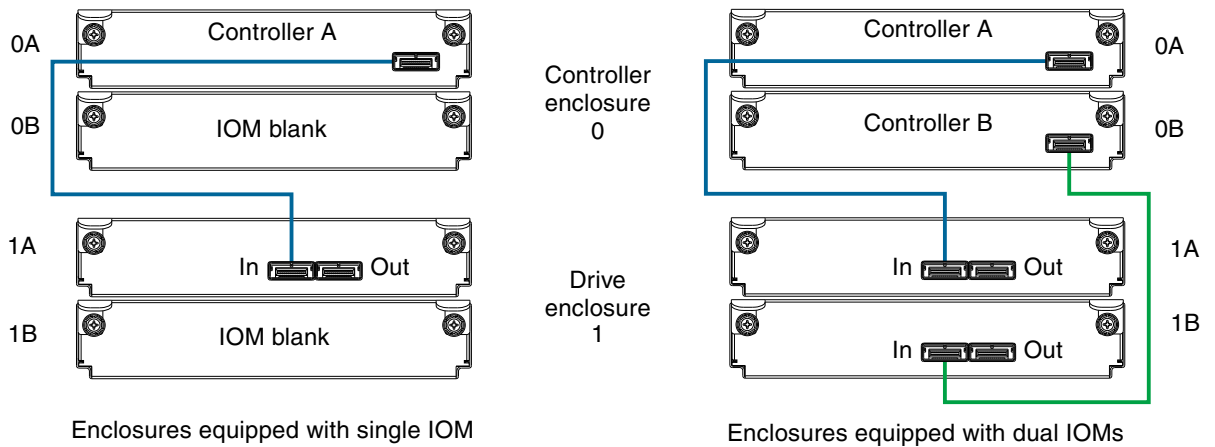


Figure 8 Cabling connections between a controller enclosure and one drive enclosure

The figure above shows examples of a 4004 Series controller enclosure cabled to a single drive enclosure. The illustration on the left shows cabling of enclosures equipped with a single I/O module (IOM). The empty IOM slot in each of the enclosures is covered with an IOM blank to ensure sufficient air flow during enclosure operation.

The illustration on the right shows cabling of enclosures equipped with dual IOMs. The remaining illustrations in the section feature enclosures equipped with dual IOMs.

IMPORTANT: If the 4004 Series controller enclosure is configured with a single controller module, the controller module must be installed in the upper slot, and an I/O module blank must be installed in the lower slot (shown above). This configuration is required to allow sufficient air flow through the enclosure during operation.

See the “Replacing a controller or expansion module” topic within the *AssuredSAN 4004 Series FRU Installation and Replacement Guide* for additional information.

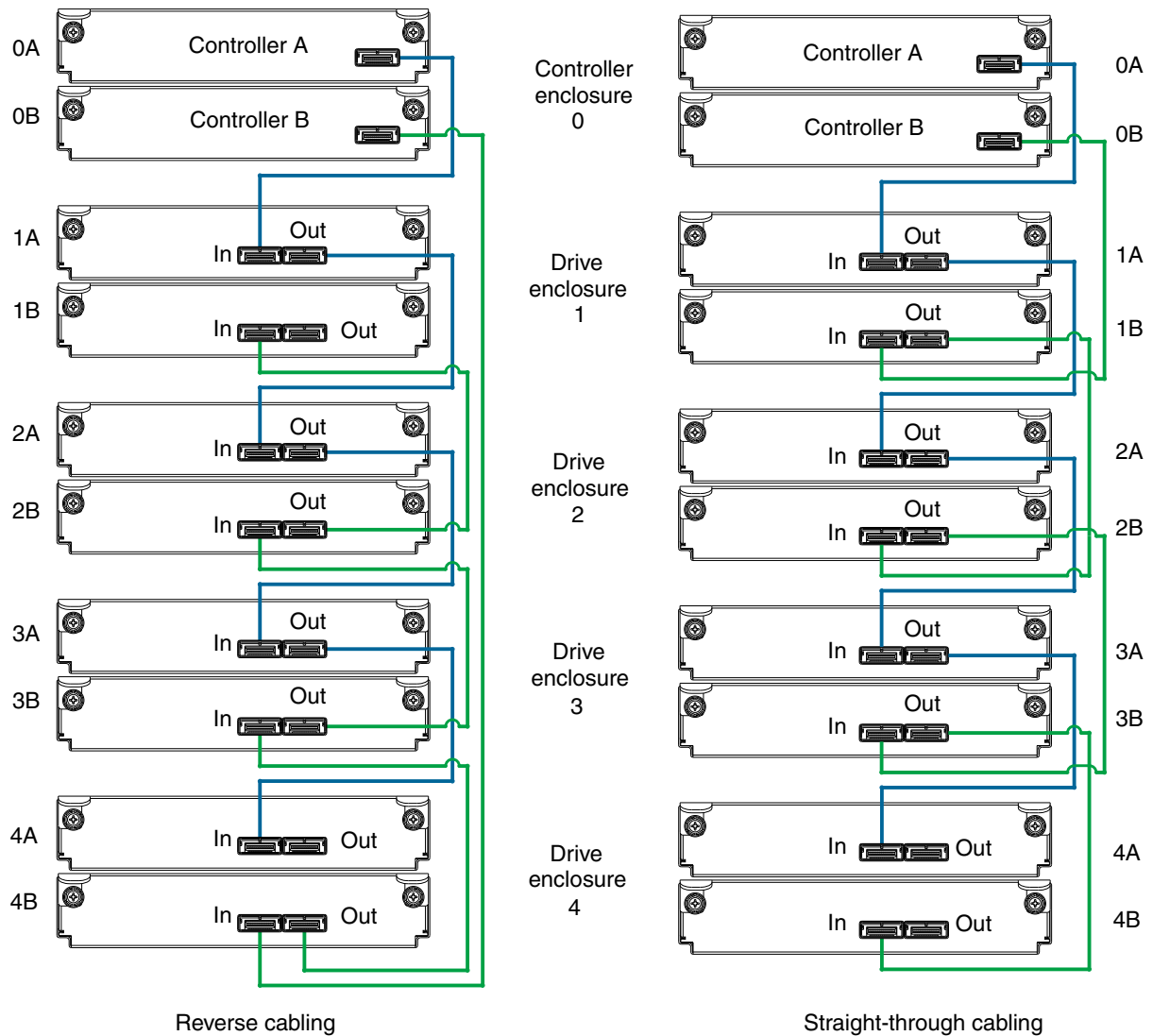


Figure 9 Fault-tolerant cabling between a dual-controller enclosure and four drive enclosures

The diagram at left (above) shows reverse cabling of a 4004 Series dual-controller enclosure and 4124 or 4134 drive enclosures configured with dual-expansion modules. Controller module 0A is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller module 0B is connected to the lower expansion module (4B), of the last expansion enclosure, with connections moving in the opposite direction (green). Reverse cabling allows any expansion enclosure to fail—or be removed—while maintaining access to other enclosures.

The diagram at right (above) shows the same storage components connected using straight-through cabling. Using this method, if an expansion enclosure fails, the enclosures that follow the failed enclosure in the chain are no longer accessible until the failed enclosure is repaired or replaced.

The drive enclosures can either be of the same type (all 4124 models or all 4134 models) or they can be a mixture of the two models. Given that both drive enclosure models use 6 Gb SAS link-rate and SAS2.0 expanders, they can be ordered in desired sequence within the array, following the controller enclosure.

Refer to these diagrams when cabling multiple compatible drive enclosures together with the 4004 Series controller enclosure.

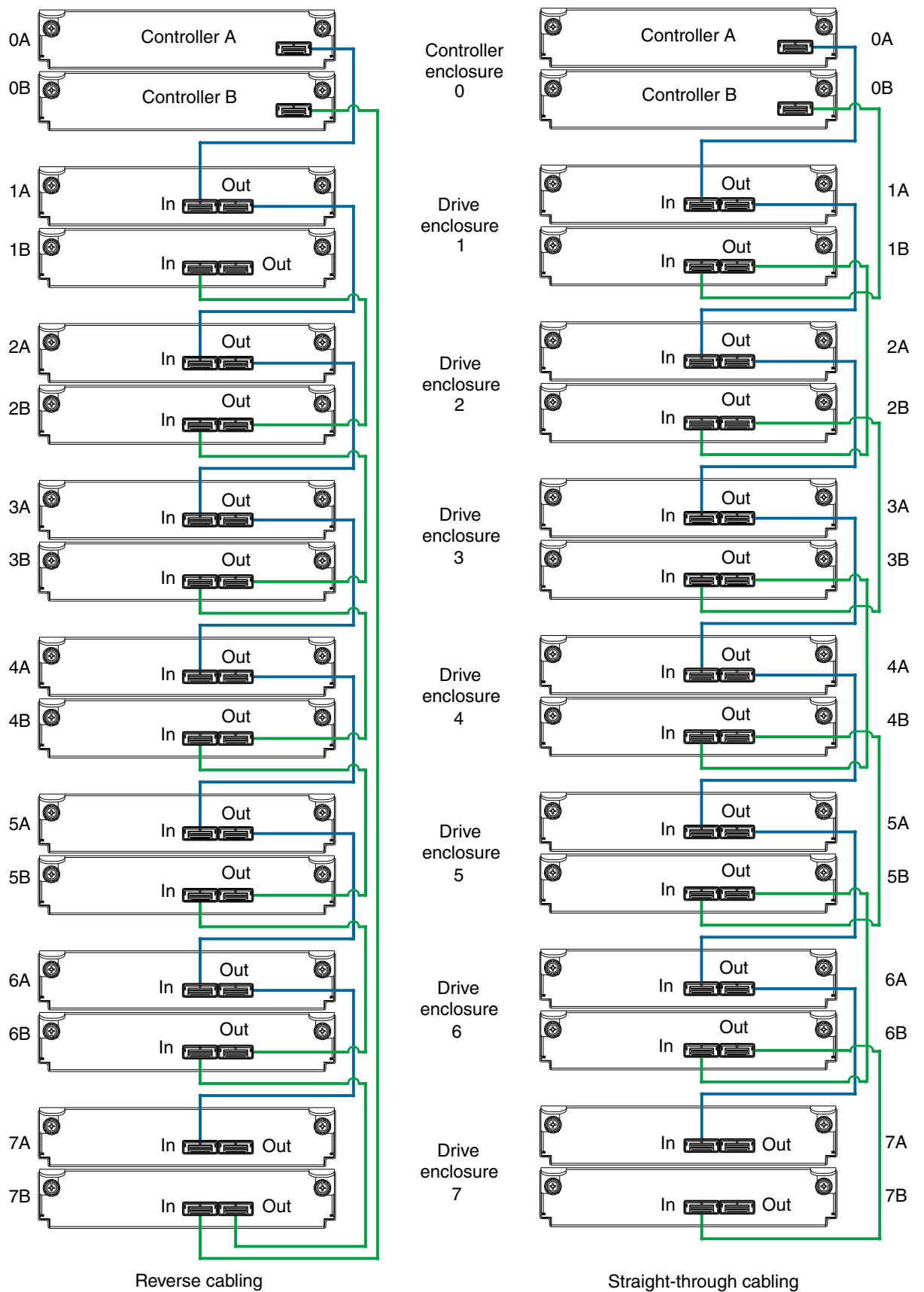


Figure 10 Cabling diagrams for maximum configuration

The diagrams above show dual-controller enclosures cabled to drive enclosures featuring dual-expansion modules. Cabling logic is explained in the narrative supporting [Figure 9](#) on page 28.

Testing enclosure connections

Power cycling procedures vary according to the type of power supply unit (PSU) provided with the enclosure. Some enclosure models are equipped with PSUs possessing power switches; whereas 4004 Series controller enclosures use PSUs that have no power switch.

NOTE: For NEBS applications, verify that you are using compatible PSUs and drive enclosures.

The following section, [Powering on/powering off](#), describes power cycling procedures relative to PSUs installed within enclosures. Once the power-on sequence succeeds, the storage system is ready to be connected to hosts as described in [Connecting the enclosure to hosts](#) on page 35.


Powering on/powering off

Before powering on the enclosure for the *first* time:


- Install all disk drives in the enclosure so the controller can identify and configure them at power-up.
- Connect the cables and power cords to the enclosure as described herein.

NOTE: Newer AC PSUs do not have power switches. *Switchless* PSUs power on when connected to a power source, and power off when disconnected.

- Generally, when powering up, make sure to power up the enclosures and associated data host in the following order:
 - 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. See [LED descriptions](#) on page 71 for descriptions of LED behavior.
 - 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.
 - Data host *last* (if powered down for maintenance purposes).

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

Power cycling procedures vary according to the type of power supply unit included within the enclosure. For controller and drive enclosures configured with switchless AC PSUs, refer to the procedure described under [AC PSU](#) on page 31. For procedures pertaining to a) controller enclosures configured with DC PSUs, or b) previously installed drive enclosures featuring power switches, see [DC and AC PSUs equipped with a power switch](#) on page 32.

 **IMPORTANT:** See the following PSU-specific subsections for more information about power cables supported by 4004 Series enclosures.

AC PSU

Controller and drive enclosures configured with switchless PSUs rely on the power cord for power cycling. Connecting the cord from the PSU power cord connector to the appropriate power source facilitates power on; whereas disconnecting the cord from the power source facilitates power off.

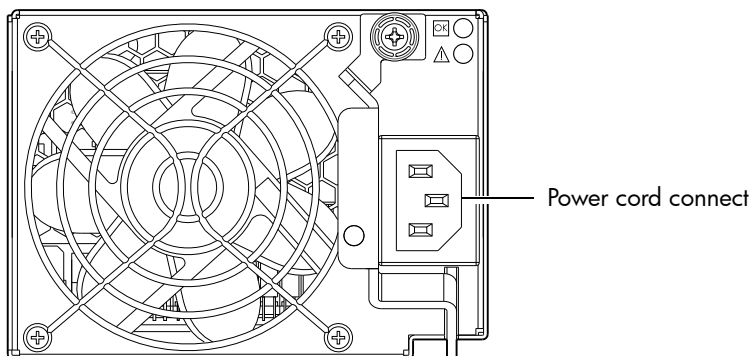


Figure 11 AC PSU

To power on the system:

1. Plug the power cord into the power cord connector on the back of the drive enclosure. Plug the other end of the power cord into the rack power source (see [Figure 11](#) and [Figure 12](#)). Wait several seconds to allow the disks to spin up.

Repeat this sequence for each switchless PSU within each drive enclosure.

2. Plug the power cord into the power cord connector on the back of the controller enclosure. Plug the other end of the power cord into the rack power source (see [Figure 11](#) and [Figure 12](#)).

Repeat the sequence for the controller enclosure's other switchless PSU.

Power cord facilitates power on/power off

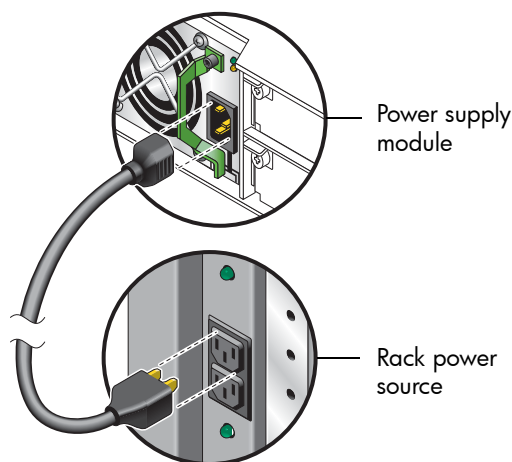


Figure 12 AC power cord

To power off the system:

1. Stop all I/O from hosts to the system (see [Stopping I/O](#) on page 57).
2. Shut down both controllers using *either* method described below:
 - Use RAIDar to shut down both controllers, as described in the online help and *AssuredSAN 4004 Series RAIDar User Guide*.
Proceed to [step 3](#).
 - Use the command-line interface (CLI) to shut down both controllers, as described in the *AssuredSAN 4004 Series CLI Reference Guide*.
3. Disconnect the power cord's male plug from the power source.
4. Disconnect the power cord's female plug from the power cord connector on the PSU.

DC and AC PSUs equipped with a power switch

DC and legacy AC power supplies—each equipped with a power switch—are shown below.

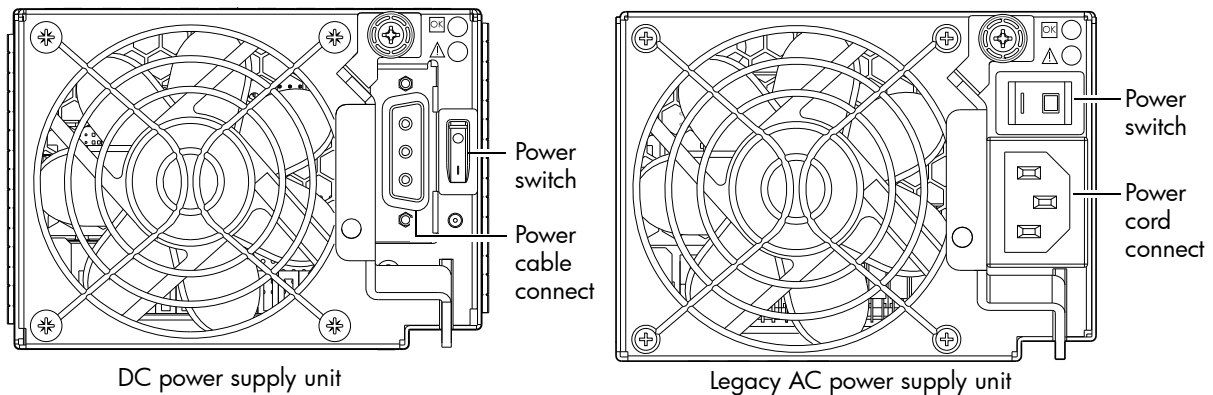


Figure 13 DC and AC PSUs with power switch

Connect power cable to DC power supply

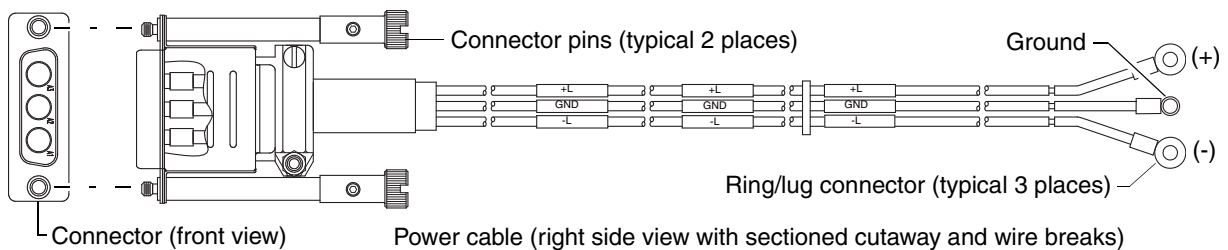
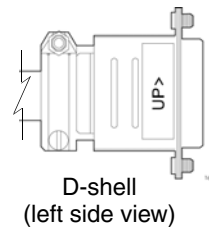


Figure 14 DC power cable featuring D-shell and lug connectors

See [Figure 14](#) and the illustration at left (in [Figure 13](#)) when performing the following steps:

1. Locate and use the provided DC power cables.
2. Verify that the enclosure's power switches are in the **Off** position.
3. Connect a DC power cable to each DC power supply using the D-shell connector. Use the **UP** arrow on the connector shell to ensure proper positioning (see adjacent left side view of D-shell connector).
4. Tighten the screws at the top and bottom of the shell, applying a torque between 1.7 N-m (15 in-lb) and 2.3 N-m (20 in-lb), to securely attach the cable to the DC power supply module.
5. 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.



CAUTION: Connecting to a DC power source outside the designated -48VDC nominal range (-36VDC to -72VDC) may damage the enclosure.

See [Power cycle](#) on page 33.

Connect power cord to legacy AC power supply

Obtain two suitable AC power cords: one for each AC power supply that will connect to a separate power source. See [Figure 12](#) on page 31 and the illustration at right in [Figure 13](#) when performing the following steps:

1. Verify that the enclosure's power switches are in the **Off** position.
2. Identify the power cord connector on the PSU, and locate the target power source.
3. Using the AC power cords provided, plug one end of the cord into the power cord connector on the PSU. Plug the other end of the power cord into the rack power source.
4. Verify connection of primary power cords from the rack to separate external power sources.
See [Power cycle](#).

Power cycle

To power on the system:

1. Power up drive enclosure(s). Allow several seconds for disks to spin up.
Press the power switches at the back of each drive enclosure to the **On** position.
2. Power up the controller enclosure next.
Press the power switches at the back of the controller enclosure to the **On** position.

To power off the system:

1. Stop all I/O from hosts to the system (see [Stopping I/O](#) on page 57).
2. Shut down both controllers using *either* method described below:
 - Use RAIDar to shut down both controllers, as described in the online help and *AssuredSAN 4004 Series RAIDar User Guide*.
Proceed to [step 3](#).
 - Use the command-line interface (CLI) to shut down both controllers, as described in the *AssuredSAN 4004 Series CLI Reference Guide*.
3. Press the power switches at the back of the controller enclosure to the **Off** position.
4. Press the power switches at the back of each drive enclosure to the **Off** position.

3 Connecting hosts

Host system requirements

Hosts connected to an AssuredSAN 4004 Series controller enclosure must meet the following requirements:

- Depending on your system configuration, host operating systems may require that multipathing is supported.
If fault tolerance is required, then multipathing 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.
- Use native Microsoft MPIO DSM support with Windows Server 2008 and Windows Server 2013. Use either the Server Manager or the command-line interface (*mpclaim* CLI tool) to perform the installation.

See the following web sites for information about using native Microsoft MPIO DSM:

<http://support.microsoft.com/gp/assistsupport>

<http://technet.microsoft.com> (search the site for “multipath I/O overview”)

Cabling considerations


Common cabling configurations address hosts, controller enclosures, drive enclosures, and switches. Host interface ports on 4004 Series controller enclosures can connect to respective hosts via direct-attach or switch-attach. Cabling systems to enable use of the optional AssuredRemote™ feature—to replicate volumes—is yet another important cabling consideration. See [Connecting two storage systems to replicate volumes](#) on page 42. The 4824/4834 models can be licensed to support replication; whereas the 4524/4534 models do not support the feature.

Connecting the enclosure to hosts

A *host* identifies an external port to which the storage system is attached. Cable connections vary depending on configuration. This section describes host interface protocols supported by 4004 Series controller enclosures, while showing a few common cabling configurations.

NOTE: 4004 Series controllers use Unified LUN Presentation (ULP) — a controller feature enabling a host to access mapped volumes through any controller host port.


ULP can show all LUNs through all host ports on both controllers, and the interconnect information is managed by the controller firmware. ULP appears to the host as an active-active storage system, allowing the host to select any available path to access the LUN, regardless of vdisk ownership.

 **TIP:** See “Configuring the system > Using the Configuration Wizard” in the *AssuredSAN 4004 Series Series RAIDar User Guide* to initially configure the system or change system configuration settings (e.g., Configuring host ports).

CNC technology

AssuredSAN 4824/4834 models use Converged Network Controller technology, allowing you to select the desired host interface protocol(s) from the available FC or iSCSI host interface protocols supported by the system. The small form-factor pluggable (SFP transceiver or SFP) connectors used in CNC ports are further described in the subsections below. Also see [CNC ports used for host connection](#) on page 11 for more information concerning use of CNC ports.

NOTE: Controller modules are *not* shipped with pre-installed SFPs. Within your product kit, you will need to locate the qualified SFP options, and install them into the CNC ports. See [Install an SFP transceiver](#) on page 95.

 **IMPORTANT:** Use the `set host-port-mode` CLI command to set the host interface protocol for CNC ports using qualified SFP options. AssuredSAN 4824/4834 models ship with CNC ports configured for FC. When connecting CNC ports to iSCSI hosts, you must use the CLI (not RAIDar) to specify which ports will use iSCSI. It is best to do this before inserting the iSCSI SFPs into the CNC ports (see [Change the CNC port mode](#) on page 51 for instructions).

Fibre Channel protocol


AssuredSAN 4824/4834 controller enclosures support one or two controller modules using the Fibre Channel interface protocol for host connection. Each controller module provides four host ports designed for use with an FC SFP supporting data rates up to 16 Gbit/s. When configured with FC SFPs, 4824/4834 controller enclosures can also be cabled to support the optionally-licensed AssuredRemote replication feature via the FC ports.

The controller supports Fibre Channel Arbitrated Loop (public or private) or point-to-point topologies. Loop protocol can be used in a physical loop or in a direct connection between two devices. Point-to-point protocol is used to connect to a fabric switch. See the `set host-parameters` command within the *AssuredSAN 4004 Series CLI Reference Guide* for command syntax and details about 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 AssuredRemote 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 AssuredRemote replication feature, whereas the second option requires that the host computer supports FC and optionally, multipath I/O.

 **TIP:** Use the RAIDar Configuration Wizard to set FC port speed. Within the RAIDar Reference Guide, see “Configuring the system > Using the Configuration Wizard > Configuring host ports,” and scroll to FC port options. Use the `show host-parameters` or `show ports` CLI commands to view information about host ports.

10GbE iSCSI protocol

AssuredSAN 4824/4834 controller enclosures support one or two controller modules using the Internet SCSI interface protocol for host connection. Each controller module provides four host ports designed for use with a 10GbE iSCSI SFP supporting data rates up to 10 Gbit/s, using either one-way or mutual CHAP (Challenge-Handshake Authentication Protocol).

 **TIP:** See the “Configuring CHAP” topic in the RAIDar Reference Guide. Also see the important statement about CHAP preceding the “Using the Replication Setup Wizard” procedure within that guide.

 **TIP:** Use the RAIDar Configuration Wizard to set iSCSI port options. Within the RAIDar Reference Guide, see “Configuring the system > Using the Configuration Wizard > Configuring host ports,” and scroll to iSCSI port options. Use the `show host-parameters` or `show ports` CLI commands to view information about host ports.

The 10GbE iSCSI ports are used in either of two capacities:

- To connect two storage systems through a switch for use of AssuredRemote replication.
- For attachment to 10GbE iSCSI hosts directly, or through a switch used for the 10GbE iSCSI traffic.

The first usage option requires valid licensing for the AssuredRemote replication feature, whereas the second option requires that the host computer supports Ethernet, iSCSI, and optionally, multipath I/O.

1 Gb iSCSI protocol

AssuredSAN 4824/4834 controller enclosures support one or two controller modules using the Internet SCSI interface protocol for host port connection. Each controller module provides four iSCSI host ports configured with an RJ-45 SFP supporting data rates up to 1 Gbit/s, using either one-way or mutual CHAP.

TIP: See the “Configuring CHAP” topic in the RAIDar Reference Guide. Also see the admonition about CHAP preceding the “Using the Replication Setup Wizard” procedure within that guide.

TIP: Use the RAIDar Configuration Wizard to set iSCSI port options. Within the RAIDar Reference Guide, see “Configuring the system > Using the Configuration Wizard > Configuring host ports,” and scroll to iSCSI port options. Use the `show host-parameters` or `show ports` CLI commands to view information about host ports.

The 1 Gb iSCSI ports are used in either of two capacities:

- To connect two storage systems through a switch for use of AssuredRemote replication.
- For attachment to 1 Gb iSCSI hosts directly, or through a switch used for the 1 Gb iSCSI traffic.

The first usage option requires valid licensing for the AssuredRemote replication feature, whereas the second option requires that the host computer supports Ethernet, iSCSI, and optionally, multipath I/O.

HD mini-SAS technology

AssuredSAN 4524/4534 models use high-density mini-SAS (Serial Attached SCSI) interface protocol for host connection.

12 Gb mini-SAS ports

Each controller module provides four SFF-8644 HD mini-SAS host ports supporting data rates up to 12 Gbit/s. HD mini-SAS host ports connect to hosts or switches; they are not used for replication. Use a qualified SFF-8644 to SFF-8644 cable option when connecting to a 12 Gbit/s host. Use a qualified SFF-8644 to SFF-8088 option when connecting to a supported 6 Gbit/s host.

Connecting direct attach configurations

AssuredSAN 4004 Series controller enclosures support up to eight direct-connect server connections, four per controller module. Connect appropriate cables from the server’s HBAs to the controller module’s host ports as described below, and shown in the following illustrations.

Fibre Channel host connection

To connect 4824/4834 controller modules supporting (4/8/16 Gb) FC host interface ports to a server HBA or switch—using the controller’s CNC ports—select a qualified FC SFP option.

Qualified options support cable lengths of 1 m (3.28'), 2 m (6.56'), 5 m (16.40'), 15 m (49.21'), 30 m (98.43'), and 50 m (164.04') for OM4 multimode optical cables and OM3 multimode FC cables, respectively. A 0.5 m (1.64') cable length is also supported for OM3. In addition to providing host connection, these cables are used for connecting a local storage system to a remote storage system via a switch, to facilitate use of the optional AssuredRemote replication feature.

10GbE iSCSI host connection

To connect 4824/4834 controller modules supporting 10GbE iSCSI host interface ports to a server HBA or switch—using the controller’s CNC ports—select a qualified 10GbE SFP option.

Qualified options support cable lengths of 0.5 m (1.64'), 1 m (3.28'), 3 m (9.84'), 5 m (16.40'), and 7 m (22.97') for copper cables; and cable lengths of 0.65 m (2.13'), 1 m (3.28'), 1.2 m (3.94'), 3 m (9.84'), 5 m (16.40'), and 7 m (22.97') for direct attach copper (DAC) cables. In addition to providing host connection, these cables are used for connecting a local storage system to a remote storage system via a switch, to facilitate use of the optional AssuredRemote replication feature.

1 Gb iSCSI host connection

To connect 4824/4834 controller modules supporting 1Gb iSCSI host interface ports to a server HBA or switch—using the controller’s CNC ports—select a qualified 1 Gb RJ-45 copper SFP option supporting (CAT5-E minimum) Ethernet cables of the same lengths specified for 10GbE iSCSI above. In addition to providing host connection, these cables are used for connecting a local storage system to a remote storage system via a switch, to facilitate use of the optional AssuredRemote replication feature.

HD mini-SAS host connection

To connect 4524/4534 controller modules supporting SAS host interface ports to a server HBA or switch—using the controller’s SFF-8644 dual HD mini-SAS host ports—select a qualified HD mini-SAS cable option. A qualified SFF-8644 to SFF-8644 cable option is used for connecting to a 12 Gbit/s enabled host; whereas a qualified SFF-8644 to SFF-8088 cable option is used for connecting to a 6 Gbit/s host. Qualified SFF-8644 to SFF-8644 options support cable lengths of 0.5 m (1.64'), 1 m (3.28'), 2 m (6.56'), and 4 m (13.12'). Qualified SFF-8644 to SFF-8088 options support cable lengths of 1 m (3.28'), 2 m (6.56'), 3 m (9.84'), and 4 m (13.12').

NOTE: Supported qualified cable options for host connection are subject to change.

NOTE: The diagrams that follow use a single representation for each CNC cabling example. This is due to the fact that the CNC port locations and labeling are identical for each of the three possible interchangeable SFPs supported by the system.

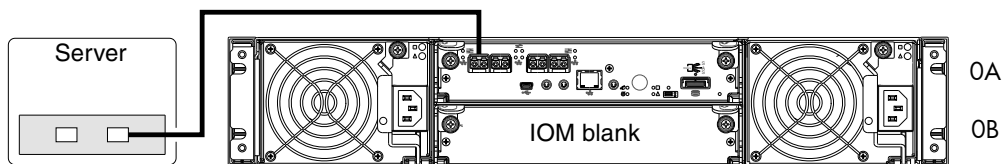
Within each cabling connection category, the HD mini-SAS model is shown beneath the CNC model.

Single-controller configurations

A single-controller configuration provides no redundancy in the event of controller failure. If the controller fails, the host loses access to the storage data. This configuration is suitable only in environments where high availability is not required, and loss of access to data can be tolerated until failure recovery actions are completed.

One server/one HBA/single path

4824/4834



4524/4534

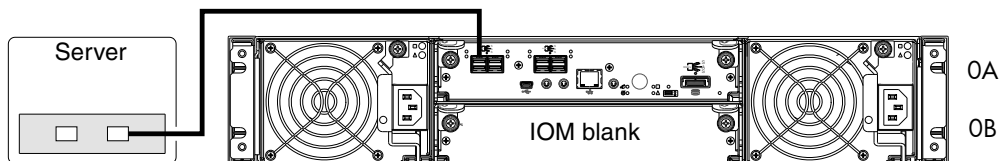


Figure 15 Connecting hosts: direct attach—one server/one HBA/single path

The two illustrations above show an IOM blank covering the bottom IOM slot (0B) on the controller enclosure. The remaining illustrations in the section feature enclosures equipped with dual IOMs.

IMPORTANT: If the 4004 Series controller enclosure is configured with a single controller module, the controller module must be installed in the upper slot, and an I/O module blank must be installed in the lower slot (shown above). This configuration is required to allow sufficient air flow through the enclosure during operation.

See the “Replacing a controller or expansion module” topic within the *AssuredSAN 4004 Series FRU Installation and Replacement Guide* for additional information about installing IOMs.

Dual-controller configurations

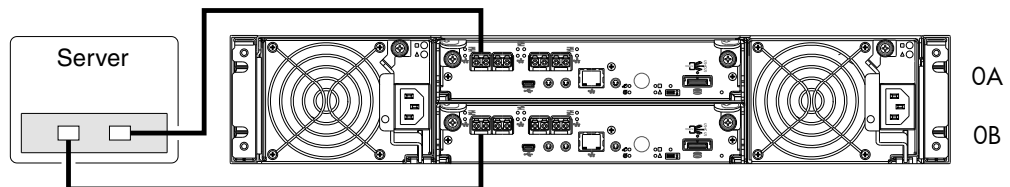
A dual-controller configuration improves application availability because in the event of a controller failure, the affected controller fails over to the partner controller with little interruption to data flow. A failed controller can be replaced without the need to shut down the storage system.

In a dual-controller system, hosts use LUN-identifying information from both controllers to determine that up to four paths are available to a given storage volume. Assuming MPIO software is installed, a host can use any available data path to access a volume owned by either controller. The path providing the best performance is through host ports on the volume’s owning controller. Both controllers share one set of 1,024 LUNs (0-1,023) for use in mapping volumes to hosts (see “ULP” in the *AssuredSAN 4004 Series RAIDar User Guide*).

The illustrations below show dual-controller configurations for 4004 Series controller enclosures equipped with either CNC ports or 12 Gb HD mini-SAS host ports.

One server/one HBA/dual path

4824/4834



4524/4534

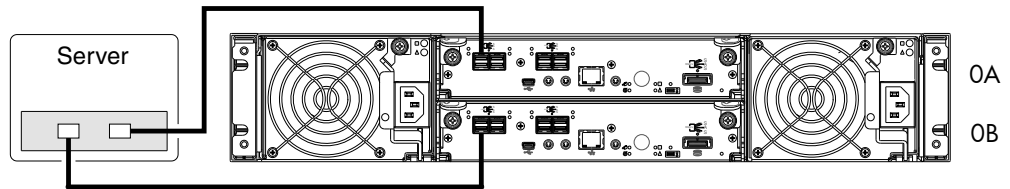
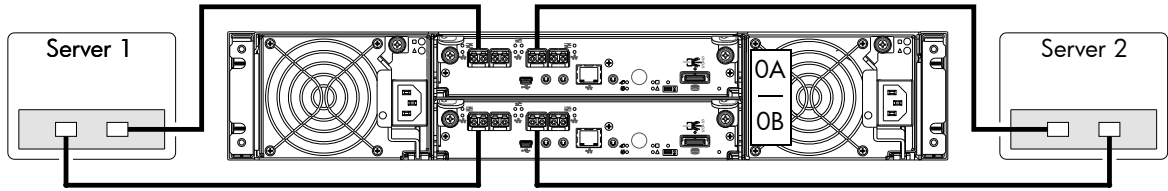


Figure 16 Connecting hosts: direct attach—one server/one HBA/dual path

Two servers/one HBA per server/dual path

4824/4834



4524/4534

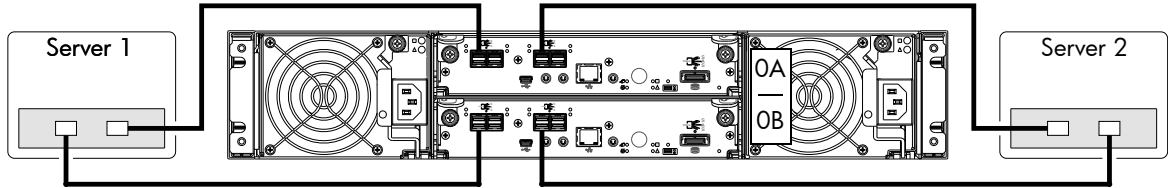
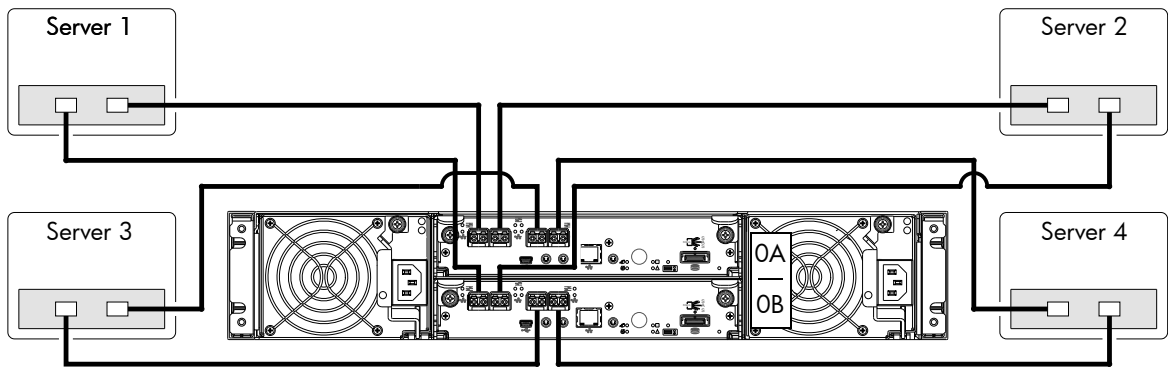


Figure 17 Connecting hosts: direct attach—two servers/one HBA per server/dual path

Four servers/one HBA per server/dual path

4824/4834



4524/4534

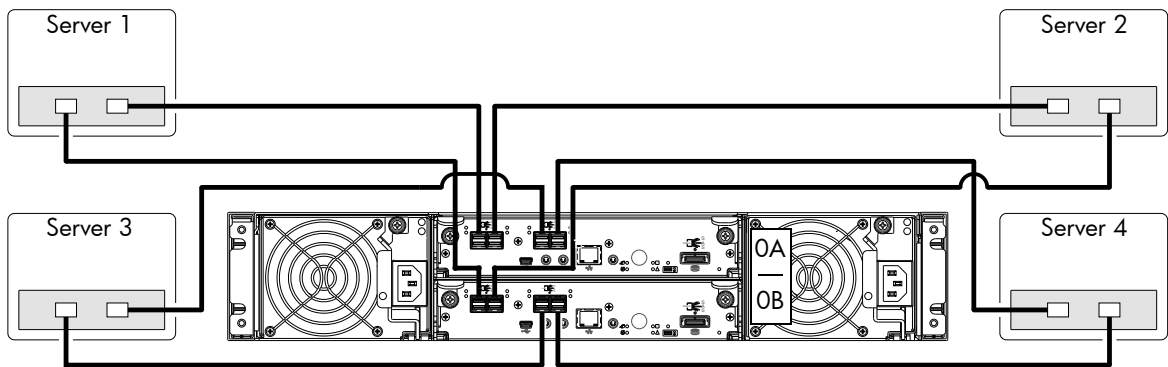


Figure 18 Connecting hosts: direct attach—four servers/one HBA per server/dual path

Connecting switch attach configurations

A switch attach solution—or SAN—places a switch between the servers and the controller enclosures. Using switches, a SAN shares a storage system among multiple servers, reducing the number of storage systems required for a particular environment. Using switches increases the number of servers that can be connected to the storage system. A 4004 Series controller enclosure supports 64 hosts.

Dual-controller configuration

Two servers/two switches

4824/4834

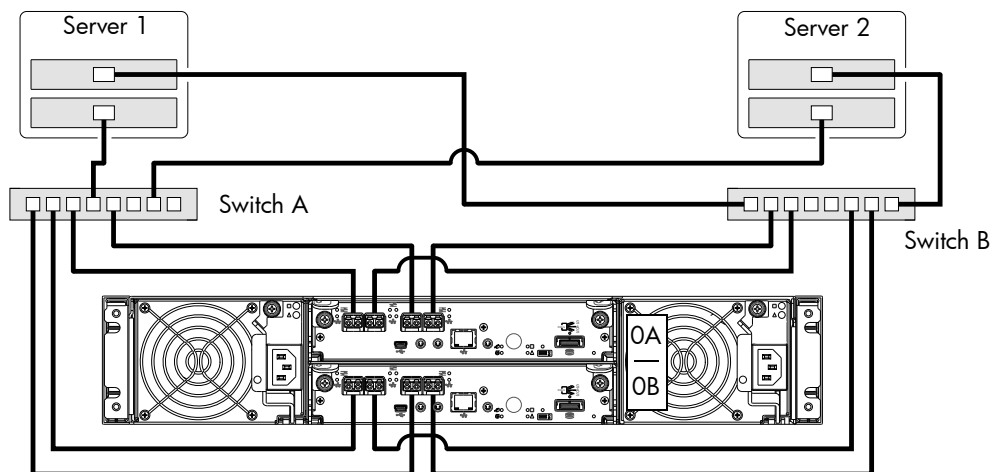


Figure 19 Connecting hosts: switch attach—two servers/two switches

Four servers/multiple switches/SAN fabric

4824/4834

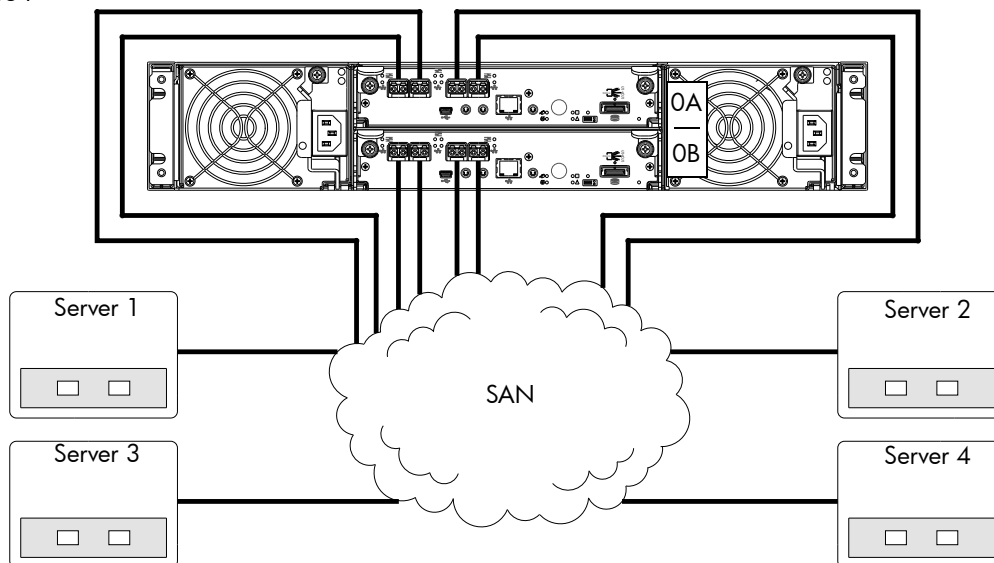


Figure 20 Connecting hosts: switch attach—four servers/multiple switches/SAN fabric

4004 Series controller enclosure iSCSI considerations

When installing a 4004 Series iSCSI controller enclosure, use at least three ports per server—two for the storage LAN, and one or more for the public LAN(s)—to ensure that the storage network is isolated from the other networks. The storage LAN is the network connecting the servers—via switch attach—to the controller enclosure (see [Figure 19](#) on page 41 and [Figure 20](#)).

IP address scheme for the controller pair — two iSCSI ports per controller

The 4824/4834 can use port 2 of each controller as one failover pair, and port 3 of each controller as a second failover pair for 1Gb iSCSI traffic. Port 2 of each controller must be in the same subnet, and port 3 of each controller must be in second subnet. See [Controller enclosure — rear panel layout](#) on page 17 for iSCSI port numbering.

For example (with a netmask of 255.255.255.0):

- Controller A port 2: 10.10.10.100
- Controller A port 3: 10.11.10.120

- Controller B port 2: 10.10.10.110
- Controller B port 3: 10.11.10.130

The 4824/4834 can use port 0 of each controller as one failover pair, and port 1 of each controller as a second failover pair. Port 0 of each controller must be in the same subnet, and port 1 of each controller must be in second subnet. See for iSCSI port numbering.

For example (with a netmask of 255.255.255.0):

- Controller A port 0: 10.10.10.100
- Controller A port 1: 10.11.10.120
- Controller B port 0: 10.10.10.110
- Controller B port 1: 10.11.10.130

IP address scheme for the controller pair — four iSCSI ports per controller

When all CNC ports are configured for iSCSI, the scheme is similar to the one described for two-ports above. See [Controller enclosure — rear panel layout](#) on page 17 for iSCSI port numbering.

For example (with a netmask of 255.255.255.0):

- Controller A port 0: 10.10.10.100
- Controller A port 1: 10.11.10.120
- Controller A port 2: 10.10.10.110
- Controller A port 3: 10.11.10.130
- Controller B port 0: 10.10.10.140
- Controller B port 1: 10.11.10.150
- Controller B port 2: 10.10.10.160
- Controller B port 3: 10.11.10.170

In addition to setting the port-specific options described above, you can also set common options. In RAIDar's Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**. See the "To change iSCSI host interface settings" topic within the RAIDar user guide or online help.

Connecting a management host on the network

The management host directly manages storage systems out-of-band over an Ethernet network.

1. Connect an RJ-45 Ethernet cable to the network port on each controller.
2. Connect the other end of each Ethernet cable to a network that your management host can access (preferably on the same subnet).

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 NEBS and FCC Rules and Regulations. See *AssuredSAN Product Regulatory Compliance and Safety* (included in your product's ship kit).

Alternatively, you can access the document online. See Dot Hill's customer resource center (CRC) web site for additional information: <http://crc.dothill.com>.

Select **AssuredSAN & R/Evolution Products > 4004 Series** to download the PRC&S document.

Connecting two storage systems to replicate volumes


AssuredRemote™ replication is a licensed disaster-recovery feature that performs asynchronous (batch) replication of block-level data from a volume on a local (primary) storage system to a volume that can be on the same system or a second, independent system. The second system can be located at the same site as the first system, or at a different site.

The two associated standard 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 AssuredRemote, and must be connected through switches to the same fabric or network (i.e., no direct attach). The server accessing the replication set need only 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 the CNC-based 4824/4834 systems on the same network, or on physically-split networks (4524/4534 SAS systems do not support replication). As you consider the physical connections of your system—specifically connections for replication—keep several important points in mind:

- Ensure that controllers have connectivity between systems, whether local or remote.
- Assign specific ports for replication whenever possible. By specifically assigning ports available for replication, you free the controller from scanning and assigning the ports at the time replication is performed.
- For remote replication, ensure that all ports assigned for replication are able to communicate appropriately with the remote replication system (see *verify remote-link* in the CLI Reference Guide for more information).
- Allow two ports to perform replication. This permits the system to balance the load across those ports as I/O demands rise and fall. On dual-controller enclosures, 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.
- Be sure of the desired link type before creating the replication set, because you cannot change the replication link type after creating the replication set.
- For the sake of system security, do not unnecessarily expose the controller module network port to an external network connection.

Conceptual cabling examples are provided addressing cabling on the same network and cabling relative to physically-split networks. Both single and dual-controller CNC environments support replication.

 **IMPORTANT:** AssuredRemote 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 AssuredRemote to perform replication tasks.

- AssuredSAN 4004 Series RAIDar User Guide
 - AssuredSAN 4004 Series CLI Reference Guide
-

Cabling for replication

This section shows example replication configurations for CNC-based 4824/4834 controller enclosures. The following illustrations provide conceptual examples of cabling to support AssuredRemote replication. Blue cables show I/O traffic and green cables show replication traffic.

NOTE: A simplified version of the controller enclosure rear panel is used in cabling illustrations to portray either FC or iSCSI host interface protocol. The rear panel layouts for the three CNC models are identical; only the external connectors used in the host interface ports differ.

Once the 4824/4834 systems are physically cabled, see the “AssuredSAN 4004 Series RAIDar User Guide” or online help for information about configuring, provisioning, and using the optional AssuredRemote feature.

NOTE: The RAIDar Replication Setup Wizard guides you through replication setup.

CNC ports and replication

CNC controller modules can use qualified SFP options of the same type, or they can use a combination of qualified SFP options supporting different interface protocols. If you use a combination of different protocols, then CNC ports 0 and 1 must be set to FC (either both 16 Gbit/s or both 8 Gbit/s), and CNC ports 2 and 3 must be set to iSCSI (either both 10GbE or both 1 Gbit/s). Each CNC port can perform I/O or replication. In combination environments one interface—for example FC—might be used for I/O, and the other interface type—10GbE or 1 Gb iSCSI—might be used for replication.

Single-controller configuration

One server/single network/two switches

The diagram below shows the rear panel of two 4824/4834 controller enclosures with both I/O and replication occurring on the same network. Each enclosure is equipped with a single controller module. The controller modules can use qualified SFP options of the same type, or they can use a combination of qualified SFP options supporting different interface protocols.

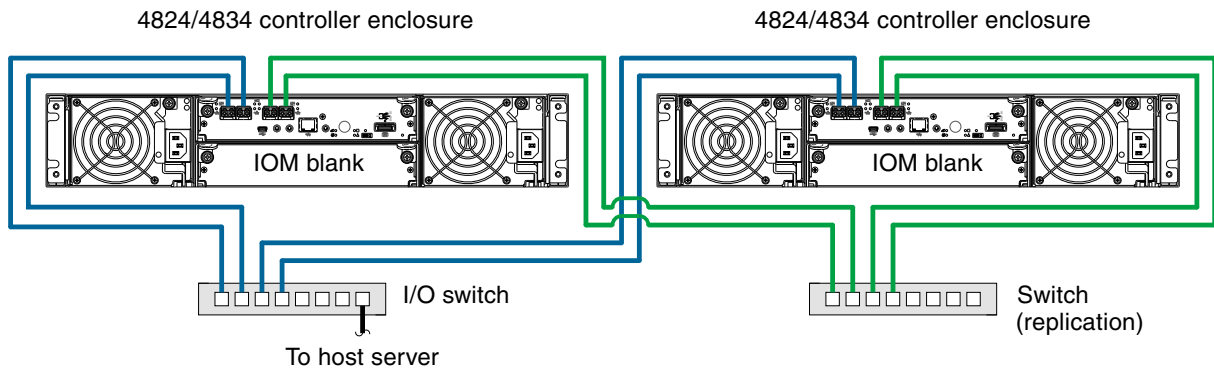


Figure 21 Connecting two storage systems for AssuredRemote: one server/two switches/one location

CNC ports used for replication must be connected to at least one switch. For optimal protection, use two switches, with one CNC replication port from each controller connected to the first switch, and the other CNC replication port from each controller connected to the second switch. Using two switches in tandem avoids the potential single point of failure inherent to using a single switch.

Dual-controller configuration

Each of the following diagrams show the rear panel of two 4824/4834 controller enclosures equipped with dual-controller modules. The controller modules can use qualified SFP options of the same type, or they can use a combination of qualified SFP options supporting different interface protocols.

Multiple servers/single network

The diagram below shows the rear panel of two 4824/4834 controller enclosures with both I/O and replication occurring on the same physical network.

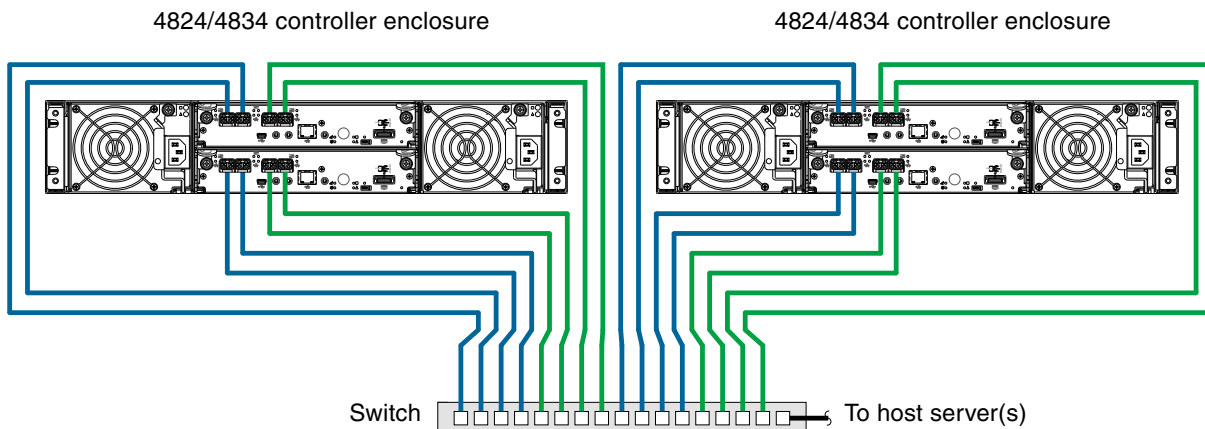


Figure 22 Connecting two storage systems for AssuredRemote: multiple servers/one switch/one location

The diagram below shows CNC host interface connections and CNC-based replication, with I/O and replication occurring on different networks. For optimal protection, use two switches. Connect two ports from each controller module to the first switch to facilitate I/O traffic, and connect two ports from each controller module to the second switch to facilitate replication. Using two switches in tandem avoids the potential single point of failure inherent to using a single switch; however, if one switch fails, either I/O or replication will fail, depending on which of the switches fails.

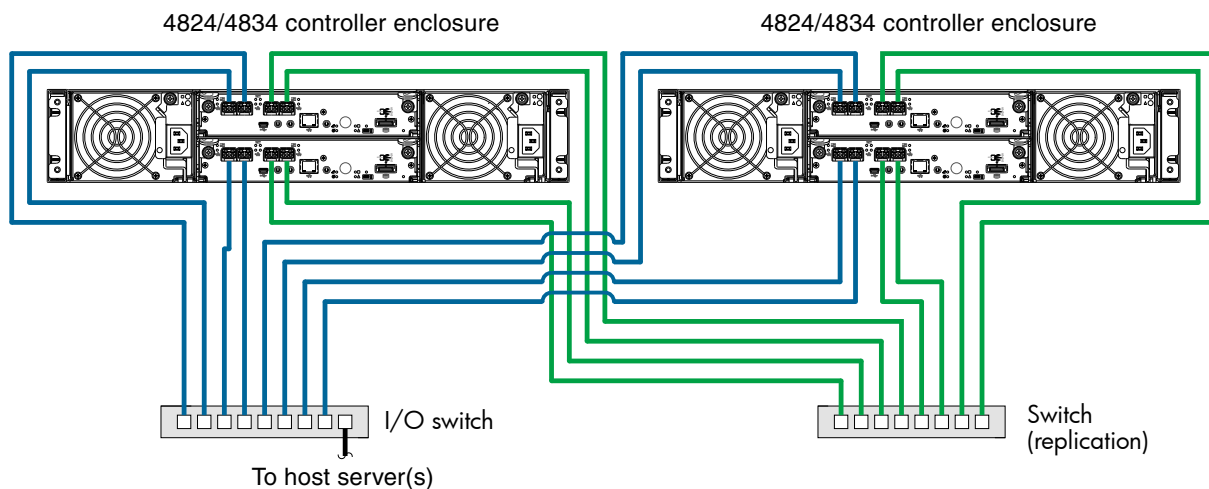


Figure 23 Connecting two storage systems for AssuredRemote: multiple servers/switches/one location

Virtual Local Area Network (VLAN) and zoning can be employed to provide separate networks for iSCSI and FC, respectively. Whether using a single switch or multiple switches for a particular interface, you can create a VLAN or zone for I/O and a VLAN or zone for replication to isolate I/O traffic from replication traffic. Since each switch would include both VLANs or zones, the configuration would function as multiple networks.

Multiple servers/different networks/multiple switches

The diagram below shows the rear panel of two 4824/4834 controller enclosures with I/O and replication occurring on different networks.

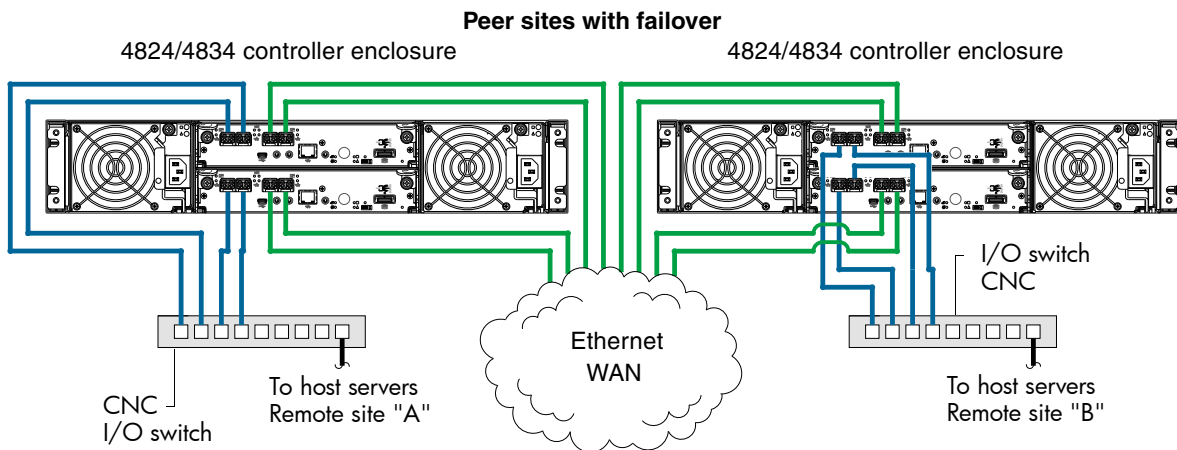
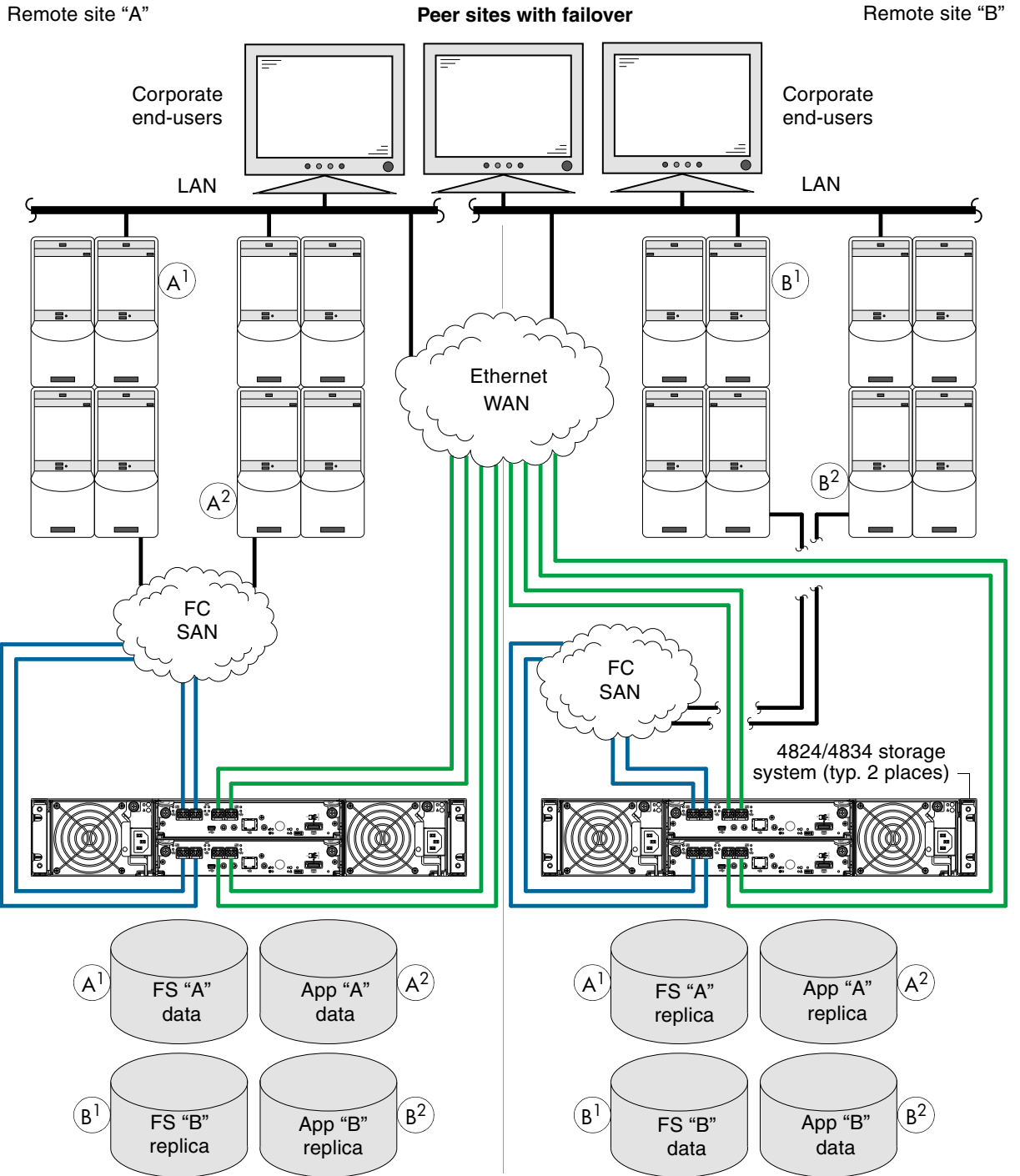


Figure 24 Connecting two storage systems for AssuredRemote: multiple servers/switches/two locations

The diagram entitled "[Connecting two storage systems for AssuredRemote: multiple servers/SAN fabric/two locations](#)" (Figure 25 on page 47) shows the rear-panel of two 4824/4834 controller enclosures with both I/O and replication occurring on different networks.

This diagram represents two branch offices cabled to enable disaster recovery and backup. In case of failure at either the local site or the remote site, you can fail over the application to the available site.



Key — Server Codes:

- A¹ = "A" File servers
- A² = "A" Application servers
- B¹ = "B" File servers
- B² = "B" Application servers

Data Restore Modes:

- Replicate back over WAN
- Replicate via physical media transfer


Failover Modes

- VMware
- Hyper V failover to servers

Figure 25 Connecting two storage systems for AssuredRemote: multiple servers/SAN fabric/two locations
 Although not shown in the preceding cabling examples, you can cable replication-enabled 4824/4834 systems and compatible 3000 Series systems—via switch attach—for performing replication tasks.


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. Using RAIDar, right-click the system in the Configuration View panel, and select **Tools > Update Firmware**. The Update Firmware panel displays the currently installed firmware versions, and allows you to update them. Optionally, you can update firmware using FTP (File Transfer Protocol) as described in the *AssuredSAN 4004 Series RAIDar User Guide*.

 **IMPORTANT:** See the “Updating firmware” topic in the *AssuredSAN 4004 Series RAIDar User Guide* before performing a firmware update.

Obtaining IP values

You can configure addressing parameters for each controller module’s network port. You can set static IP values or use DHCP.

 **TIP:** See the “Configuring network ports” topic in the *AssuredSAN 4004 Series RAIDar User Guide*.

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. You must have some means of determining what addresses have been assigned, such as the list of bindings on the DHCP server.

Because DHCP is disabled by default in 4004 Series systems, you must either use the CLI (Command-line Interface) to change controller IP address settings, or use RAIDar’s Configuration Wizard as described in the Using the Configuration Wizard topic in the RAIDar User Guide or online help.

Setting network port IP addresses using the CLI port and cable

If you did not use DHCP to set network port IP values, set them manually (default method) as described below. If you are using the USB CLI port and cable, you will need to enable the port for communication (also see [Using the CLI port and cable—known issues on Windows](#) on page 93).

Network ports on controller module A and controller module B are configured with the following default values:

- **Network port 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

If the default IP addresses are not compatible with your network, you must set an IP address for each network port using the CLI embedded in each controller module. The CLI enables you to access the system using the USB (Universal Serial Bus) communication interface and terminal emulation software.

NOTE: If you are using the mini USB CLI port and cable, see Appendix D - [USB device connection](#):

- Windows customers should download and install the device driver as described in [Obtaining the software download](#) on page 92.
 - Linux customers should prepare the USB port as described in [Setting parameters for the device driver](#) on page 93.
-

Use the CLI commands described in the steps below to set the IP address for the network port on each controller module.

Once new IP addresses are set, you can change them as needed using RAIDar. Be sure to change the IP address via RAIDar before changing the network configuration. See [Accessing RAIDar](#) on page 53 for more information concerning the web-based storage management application.

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 you can specify them whenever you manage the controllers using RAIDar or the CLI.
2. Use the provided USB cable to connect controller A to a USB port on a host computer. The USB mini 5 male connector plugs into the CLI port as shown in [Figure 26](#) on page 49 (generic 4004 Series controller module shown).

Connect USB cable to CLI port on controller face plate

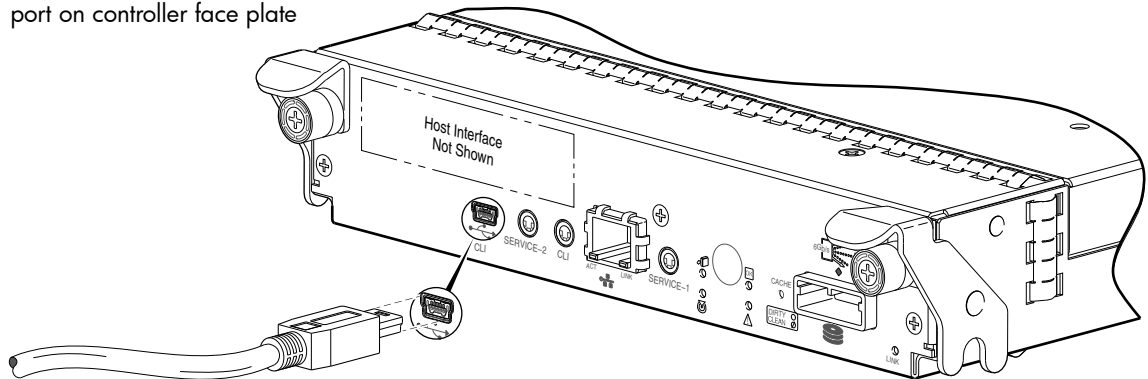


Figure 26 Connecting a USB cable to the CLI port

3. Enable the CLI port for subsequent communication:
 - Linux customers should enter the command syntax provided in [Setting parameters for the device driver](#) on page 93.
 - Windows customers should locate the downloaded device driver described in [Obtaining the software download](#) on page 92, and follow the instructions provided for proper installation.
4. Start and configure a terminal emulator, such as HyperTerminal or VT-100, 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 emulation 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

¹Your server or laptop configuration determines which COM port is used for Disk Array USB Port.

²Verify 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 prompt (#).

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

a. At the login prompt, enter the default user `manage`.

b. Enter the default password `!manage`.

If the default user or password — or both — have been changed for security reasons, enter the secure login credentials instead of the defaults shown above.

7. At the prompt, enter the following command to set the values you obtained in [step 1](#) 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
```

8. Enter the following command to verify the new IP addresses:

```
show network-parameters
```

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

9. Use the `ping` command to verify connectivity to the gateway address.

For example:

```
# 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. (2011-12-19 10:20:37)
```

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, you might need to restart the Management Controller(s) using the serial CLI.

When you restart a Management Controller, communication with it is temporarily lost until it successfully restarts.

Enter the following command to restart the Management Controller in both controllers:

```
restart mc both
```

 **IMPORTANT:** When configuring an iSCSI system or a system using a combination of FC and iSCSI SFPs, do *not* restart the Management Controller or exit the terminal emulator session until configuring the CNC ports as described in [Change the CNC port mode](#) on page 51.

11. When you are done using the CLI, exit the emulator.

12. Retain the IP addresses (recorded in step 1) for accessing and managing the controllers using either RAIDar or the CLI.

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

On a host computer connected to a controller module's mini-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 telnet rather than the mini-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 mini-USB CLI cable as described in [step 2](#) and [Figure 26](#) on page 49.

Change the CNC port mode

This subsection applies to 4824/4834 models only. While the USB cable is still connected and the terminal emulator session remains active, perform the following steps to change the CNC port mode from the default setting (FC), to either iSCSI or FC-and-iSCSI used in combination.

When using FC SFPs and iSCSI SFPs in combination, host ports 0 and 1 are set to FC (either both 16 Gbits/s or both 8 Gbit/s), and host ports 2 and 3 must be set to iSCSI (either both 10GbE or both 1 Gbit/s).

Set CNC port mode to iSCSI

To set the CNC port mode for use with iSCSI SFPs, run the following command at the command prompt:

```
set host-port-mode iSCSI
```

The command notifies you that it will change host port configuration, stop I/O, and restart both controllers. When asked if you want to continue, enter **y** to change the host port mode to use iSCSI SFPs.

Once the `set host-port-mode` command completes, it will notify you that the specified system host port mode was set, and that the command completed successfully.

Continue with [step 11](#) of [Setting network port IP addresses using the CLI port and cable](#).

Set CNC port mode to FC and iSCSI

To set the CNC port mode for use with FC SFPs and iSCSI SFPs in combination, run the following command at the command prompt:

```
set host-port-mode FC-and-iSCSI
```

The command notifies you that it will change host port configuration, stop I/O, and restart both controllers. When asked if you want to continue, enter **y** to change the host port mode to use FC and iSCSI SFPs.

Once the `set host-port-mode` command completes, it will notify you that the specified system host port mode was set, and that the command completed successfully.

Continue with [step 11](#) of [Setting network port IP addresses using the CLI port and cable](#).

Configure the system

NOTE:

- After using either of the CLI command sequences shown above, you may see events stating that the SFPs installed are not compatible with the protocol set for the host ports. The new host port mode setting will be synchronized with the qualified SFP option once the controller modules restart.
 - See [Appendix E—SFP option for CNC ports](#) for instructions about locating and installing your qualified SFP transceivers within the CNC ports.
-


After changing the CNC port mode, you can invoke RAIDar and use the Configuration Wizard to initially configure the system, or change system configuration settings as described in the *AssuredSAN 4004 Series RAIDar User Guide* and [Basic operation](#).

4 Basic operation


Verify that you have successfully completed the sequential “Installation Checklist” instructions in [Table 3](#) on page 23. Once you have successfully completed steps 1 through 8 therein, you can access the management interfaces using your web-browser, to complete the system setup.

Accessing RAIDar

Upon completing the hardware installation, you can access the controller module’s web-based management interface, RAIDar, to configure, monitor, and manage the storage system. Invoke your web browser, and enter the IP address of the controller module’s network port in the address field (obtained during completion of “Installation Checklist” step 8), then press Enter. To sign-in to RAIDar, use the default user name **manage** and password **!manage**. If the default user or password—or both—have been changed for security reasons, enter the secure login credentials instead of the defaults shown above. *This brief Sign In discussion assumes proper web browser setup.*

 **IMPORTANT:** For detailed information on accessing and using RAIDar, see the “Getting Started” section in the web-posted *AssuredSAN 4004 Series RAIDar User Guide*.

In addition to summarizing the processes to configure and provision a new system for the first time—using the wizards—the Getting Started section provides instructions for signing in to RAIDar, introduces key system concepts, addresses browser setup, and provides tips for using the main window and the help window.


 **TIP:** After signing-in to RAIDar, you can use online help as an alternative to consulting the user guide.

Configuring and provisioning the storage system

Once you have familiarized yourself with RAIDar, use it to configure and provision the storage system. If you are licensed to use the optional AssuredRemote feature, you may also need to set up the storage systems for replication. Refer to the following chapters within the RAIDar user guide or online help:

- Getting started
- Configuring the system
- Provisioning the system
- Using AssuredRemote to replicate volumes

NOTE: See the “Installing a license” topic within the RAIDar User Guide for instructions about creating a temporary license, or installing a permanent license.

 **IMPORTANT:** If the system is used in a VMware environment, set the system’s Missing LUN Response option to use its Illegal Request setting. To do so, see either the configuration topic “Changing the missing LUN response” in the RAIDar user guide or the command topic “set-advanced-settings” in the CLI Reference Guide.

5 Troubleshooting

USB CLI port connection

AssuredSAN 4004 Series controllers feature a CLI port employing a mini-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 Appendix D for more information.

Fault isolation methodology

AssuredSAN 4004 Series storage systems provide many ways to isolate faults. This section presents the basic methodology used to locate faults within a storage system, and to identify the pertinent FRUs (Field Replaceable Units) affected.

As noted in [Basic operation](#) on page 53, use RAIDar to configure and provision the system upon completing the hardware installation. As part of this process, configure and enable event notification so the system will notify you when a problem occurs that is at or above the configured severity (see “Using the Configuration Wizard > Configuring event notification” within the *AssuredSAN 4004 Series RAIDar User Guide*). With event notification 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:

- Gather fault information, including using system LEDs (see [Gather fault information](#) on page 56)
- Determine where in the system the fault is occurring (see [Determine where the fault is occurring](#) on page 56)
- Review event logs (see [Review the event logs](#) on page 56)
- If required, isolate the fault to a data path component or configuration (see [Isolate the fault](#) on page 57)

Cabling systems to enable use of the licensed AssuredRemote feature—to replicate volumes—is another important fault isolation consideration pertaining to initial system installation. See [Isolating AssuredRemote replication faults](#) on page 65 for 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 RAIDar 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 RAIDar and the CLI provide recommended-action text online. Options for performing basic steps are listed according to frequency of use:

- Use RAIDar
- Use the CLI
- Monitor event notification
- View the enclosure LEDs

Use RAIDar

RAIDar uses health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. RAIDar 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 RAIDar’s GUI to drill down to

find each component that has a problem, and follow actions in the component Health Recommendations field to resolve the problem.

Use the CLI

As an alternative to using RAIDar, 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.

Monitor event notification

With event notification configured and enabled, you can view event logs to monitor the health of the system and its components. 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 RAIDar or the CLI. Using RAIDar, you would view the event log and then click on the event message to see detail about that event. Using the CLI, you would run the `show events detail` command (with additional parameters to filter the output) to see the detail for an event.

View the enclosure LEDs

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

Performing basic steps

You can use any of the available options described above 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, or power supply unit?*

By isolating the fault to *one* of the components within the storage system, you will be able to determine the necessary corrective action more quickly.

Determine where the fault is occurring

Once you have an understanding of the reported fault, review the enclosure LEDs. The enclosure LEDs are designed to immediately alert users of any system faults, and might be what alerted the user to a fault in the first place.

When a fault occurs, the Fault ID status LED on an enclosure's right ear illuminates (see the diagram pertaining to your product's front panel components on [page 16](#)). 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.

Use RAIDar to verify any faults found while viewing the LEDs. RAIDar is also a good tool to use in determining where the fault is occurring if the LEDs cannot be viewed due to the location of the system. RAIDar provides you with a visual representation of the system and where the fault is occurring. It can also provide more detailed information about FRUs, data, and faults.

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. 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.

See the *AssuredSAN Event Descriptions Reference Guide* for information about specific events.

See Dot Hill's Customer Resource Center web site for additional information: <http://crc.dothill.com>. Select **AssuredSAN & R/Evolution Products > 4004 Series** to download the Event Descriptions guide.

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 virtual disk 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, or data host.

If the enclosure does not initialize

It may take up to two minutes for all enclosures to initialize. If an enclosure does not initialize:

- Perform a rescan
- Power cycle the system
- Make sure the power cord is properly connected, and check the power source to which it is connected
- Check the event log for errors

Correcting enclosure IDs

When installing a system with drive enclosures attached, the enclosure IDs might not agree with the physical cabling order. This is because the controller might have been previously attached to enclosures in a different configuration, and it 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 RAIDar or the CLI. This will reorder the enclosures, but can take up to two minutes for the enclosure IDs to be corrected.

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

```
rescan
```


To rescan using RAIDar:

1. Verify that controllers are operating normally
2. In the Configuration View panel, right-click the system and select **Tools > Rescan Disk Channels**
3. Click **Rescan**

NOTE: The reordering enclosure IDs action only applies to Dual Controller mode. If only one controller is available, due to either Single Controller configuration or controller failure, a manual rescan will not reorder the drive enclosure IDs.

Stopping I/O

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

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

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

1. Using the CLI, run the `show vdisk-statistics` command.
The `Number of Reads` and `Number of Writes` outputs show the number of these operations that have occurred since the statistic was last reset, or since the controller was restarted.
2. Run the `show vdisk-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.
3. If any reads or writes occur during this interval, a host is still reading from or writing to this vdisk.
Continue to stop IOPS from hosts, and repeat [step 1](#) until the `Number of Reads` and `Number of Writes` statistics are zero.

NOTE: See *AssuredSAN 4004 Series CLI Reference Guide* for additional information.

Diagnostic steps

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

NOTE: Once event notification is configured and enabled using RAIDar, you can view event logs to monitor the health of the system and its components using the GUI.

In addition to monitoring LEDs via line-of-sight observation of the racked hardware components when performing diagnostic steps, you can also monitor the health of the system and its components using the management interfaces previously discussed. Bear this in mind when reviewing the **Actions** column in the following diagnostics tables, and when reviewing the step procedures provided later 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 gone online and likely failed its self-test.	<ul style="list-style-type: none">• Check the LEDs on the back of the controller 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 controller back panel FRU OK LED off?

Answer	Possible reasons	Actions
No (blinking)	System functioning properly. System is booting.	No action required. Wait for system to boot.
Yes	The controller module is not powered on. The controller module has failed.	<ul style="list-style-type: none"> • Check that 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 controller back 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-controlled power-up error • Cache flush error • Cache self-refresh error 	<ul style="list-style-type: none"> • Restart this controller from the other controller using RAIDar or the 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?

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

Table 10 Diagnostics LED status: Disk drives (LFF and SFF modules)

Is the disk drive module Fault LED amber?

Answer	Possible reasons	Actions
Yes, and the online/activity LED is off .	The disk drive is offline. An event message 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 online/activity LED is blinking .	The disk drive is active, but an event message 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 11 Diagnostics LED status: Disk drive fault status (LFF and SFF modules)

Is a connected host port Host Link Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required (see Link LED note: page 80).
Yes	The link is down.	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • Inspect cable for damage. • Swap cables to determine if 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 RAIDar, review event logs for indicators of a specific fault in a host data path component. • Contact an authorized service provider for assistance. • See Isolating a host-side connection fault on page 62.

Table 12 Diagnostics LED status: Rear panel “Host Link Status”

Is a connected 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 cable for damage. Replace cable if necessary. • Swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. • In RAIDar, review the event logs for indicators of a specific fault in a host data path component. • Contact an authorized service provider for assistance. • See Isolating a controller module expansion port connection fault on page 64.

Table 13 Diagnostics LED status: Rear panel “Expansion Port Status”

Is a connected port’s Network Port link status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	Use standard networking troubleshooting procedures to isolate faults on the network.

Table 14 Diagnostics LED status: Rear panel “Network Port Link Status”

Is the power supply Input Power Source LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The power supply is not receiving adequate power.	<ul style="list-style-type: none"> Verify that the power cord is properly connected, and check the power source to which it connects. Check that the power supply FRU is firmly locked into position. Check the event log for specific information regarding the fault. If the above action does not resolve the fault, isolate the fault, and contact an authorized service provider for assistance.

Table 15 Diagnostics LED status: Rear panel power supply “Input Power Source”

Is the Voltage/Fan Fault/Service Required 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, 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 FRU is firmly locked into position. Verify that the power cable is connected to a power source. Verify that the power cable is connected to the enclosure’s power supply unit.

Table 16 Diagnostics LED status: Rear panel power supply “Voltage/Fan Fault/Service Required”

Controller failure in a single-controller configuration

Cache memory is flushed to CompactFlash in the case of a controller failure or power loss. During the write to CompactFlash process, only the components needed to write the cache to the CompactFlash are powered by the supercapacitor. This process typically takes 60 seconds per 1 Gbyte of cache. After the cache is copied to CompactFlash, 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 at a rate of 1/10 second on and 9/10 second off.

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


Answer	Actions
No, the Cache LED status is off, and the controller does not boot.	If valid data is thought to be in Flash, see Transporting cache via professional services ; otherwise, 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.	See Transporting cache via professional services .
Yes, at a strobe 1:10 rate - 1 Hz, and the controller boots.	The system is flushing data to CompactFlash. If the problem persists, replace the controller module.

Answer	Actions
Yes, at a blink 1:1 rate - 1 Hz, and the controller does not boot.	See Transporting cache via professional services .
Yes, at a blink 1:1 rate - 1 Hz, and the controller boots.	The system is in self-refresh mode. If the problem persists, replace the controller module.


Table 17 Diagnostics LED status: Rear panel “Cache Status” (continued)

NOTE: See also [Cache Status LED details](#) on page 81.

Transporting cache via professional services


 **IMPORTANT:** Transportable cache only applies to single-controller configurations. In dual-controller configurations, there is no need to transport a failed controller’s cache to a replacement controller because the cache is duplicated between the partner controllers (subject to volume write optimization setting).

To preserve the existing data stored in the CompactFlash, you must transport the CompactFlash from the failed controller to a replacement controller. To transport cache, you must return the controller module to a maintenance depot for servicing by qualified personnel.

 **CAUTION:** Transporting of cache must be performed by a qualified service technician.

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 host activity 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 CNC ports

The procedure below applies to AssuredSAN 4004 Series controller enclosures employing small form factor pluggable (SFP) transceiver connectors in 4/8/16 Gb FC, 10GbE iSCSI, or 1 Gb iSCSI host interface ports. In the following procedure, “SFP and host cable” is used to refer to any of the qualified SFP options supporting CNC ports used for I/O or replication.

1. Halt all I/O to the storage system (see [Stopping I/O](#) on page 57).
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 CompactFlash.
 - 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 SFP and host cable and inspect for damage.

5. Reseat the SFP and host cable.
Is the host link status/link activity LED on?
 - Yes – Monitor the status to ensure that 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 SFP and host cable to a port with a known good link status.
This step isolates the problem to the external data path (SFP, 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 SFP, host cable, and host-side devices are functioning properly. Return the cable to the original port. If the link status LED remains off, you have isolated the fault to the controller module's port. Replace the controller module.
 - No – Proceed to the next step.
7. 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. 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. Verify that the switch, if any, is operating properly. If possible, test with another port.
10. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
11. 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 needs to be replaced.
12. Move the cable and SFP 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, cables, and HBAs.

Host-side connection troubleshooting featuring SAS host ports

The procedure below applies to 4524/4534 controller enclosures employing 12 Gb SFF-8644 connectors in the HD mini-SAS host ports used for I/O. These models do not support AssuredRemote replication.

1. Halt all I/O to the storage system (see [Stopping I/O](#) on page 57).
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 CompactFlash.
 - 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 LED on?
 - Yes – Monitor the status to ensure that 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 step 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 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 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 the switch, if any, is operating properly. If possible, test with another port.
 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 LED on?
 - Yes – You have isolated the fault to the HBA. Replace the HBA.
 - No – It is likely that the controller module needs to be replaced.
 9. Move the host cable back to its original port.
Is the host link status 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 cables and HBAs.

Isolating a controller module expansion port connection fault

During normal operation, when a controller module's 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 (see [Stopping I/O](#) on page 57).
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 CompactFlash.
 - 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 step isolates the problem to the expansion cable or to the controller module's 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's expansion port. Replace the controller module.

- No – Proceed to the next step.
- 6. Move 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’s 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 AssuredRemote replication faults

Cabling for replication

AssuredRemote replication is a licensed feature for disaster-recovery. This feature performs asynchronous (batch) replication of block-level data from a volume on a local storage system to a volume that can be on the same system, or a second, independent system. The second system can be located at the same site as the first system, or at a different site. See [Connecting two storage systems to replicate volumes](#) on page 42 for host connection information concerning AssuredRemote.

Replication setup and verification

After storage systems and hosts are cabled for replication, you can use RAIDar’s Replication Setup Wizard to prepare to use the AssuredRemote feature. Alternatively, you can use telnet to access the IP address of the controller module and access the optional AssuredRemote feature using the CLI.

NOTE: Refer to the following manuals for more information about replication setup:

- See *AssuredSAN 4004 Series RAIDar User Guide* for procedures to setup and manage replications.
 - See *AssuredSAN 4004 Series CLI Reference Guide* for replication commands and syntax.
 - See *AssuredSAN 4004 Series Event Descriptions Reference Guide* for replication event reporting.
-

Basic information for enabling the 4004 Series controller enclosures for replication supplements the troubleshooting procedures that follow.

- Familiarize yourself with AssuredRemote by reviewing the “Getting started” and “Using AssuredRemote to replicate volumes” chapters in the RAIDar User Guide.
- Use RAIDar’s **Wizards > Replication Setup Wizard** to prepare to replicate an existing volume to another vdisk in the primary system or secondary system.

Follow the wizard to select the primary volume, replication mode, and secondary volume, and to confirm your replication settings. The wizard verifies the communication links between the primary and secondary systems. Once setup is successfully completed, you can initiate replication from RAIDar or the CLI.

- For descriptions and replication-related events, see the Event Descriptions guide.

Diagnostic steps for replication setup

Can you successfully use the AssuredRemote feature?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	AssuredRemote is not licensed on each controller enclosure used for replication.	<p>Verify licensing of the optional feature per system:</p> <ul style="list-style-type: none"> In the Configuration View panel in RAIDar, right-click on the system, and select View > Overview. Within the System Overview table, select the Licensed Features component to display the status of licensed features. If the Replication feature is not enabled, obtain and install a valid license for AssuredRemote. <hr/> <p>NOTE: AssuredRemote is not supported by 4004 Series SAS controller enclosures.</p> <hr/>
No	Compatible firmware revision supporting AssuredRemote is not running on each system used for replication.	<p>Perform the following actions on each system used for replication:</p> <ul style="list-style-type: none"> In the Configuration View panel in RAIDar, right-click the system, and select Tools > Update Firmware. The Update Firmware panel displays currently installed firmware versions. If necessary, update the controller module firmware to ensure compatibility with the other systems.
No	Invalid cabling connection. (If multiple controller enclosures are used, check the cabling for each system.)	<p>Verify controller enclosure cabling:</p> <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 on the same fabric or network. Verify that cable connections are securely fastened. Inspect cables for damage and replace if necessary.

Table 18 Diagnostics for replication setup: Using AssuredRemote feature

Can you view information about remote links?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Invalid login credentials	<ul style="list-style-type: none"> Verify user name with Manage role on remote system. Verify user's password on remote system.
No	Communication link is down	<ul style="list-style-type: none"> Verify controller enclosure cabling (see Table 15). In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. Verify valid IP address of the network port on the remote system. In the Configuration View panel in RAIDar, right-click the remote system, and select Tools > Check Remote System Link. Click Check Links.

Table 19 Diagnostics for replication setup: Viewing information about remote links

Can you create a replication set?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Selected link type or port-to-link connections are incorrect.	<ul style="list-style-type: none"> Remote Replication mode: In the Configuration View panel in RAIDar, right-click the remote system, and select Tools > Check Remote System Link. Click Check Links to verify correct link type and remote host port-to-link connections. Local Replication mode: In the Configuration View panel in RAIDar, right-click the local system, and select Tools > Check Local System Link. Click Check Links to verify correct link type and local host port-to-link connections.
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), configure it as described in the RAIDar topics "Using the Replication Setup Wizard" or "Replicating a volume."
No	Unable to select the replication mode (Local or Remote)? ¹	<ul style="list-style-type: none"> In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. Follow any Recommended Actions. Local Replication mode replicates to a secondary volume residing in the local storage system. <ul style="list-style-type: none"> Verify valid links. <p>On dual-controller systems, verify that A ports can access B ports on the partner controller, and vice versa.</p> Verify existence of either a replication-prepared volume of the same size as the master volume, or a vdisk with sufficient unused capacity. Remote Replication mode replicates to a secondary volume residing in an independent storage system: <ul style="list-style-type: none"> Verify selection of a valid remote vdisk. Verify selection of valid remote volume on vdisk. Verify valid IP address of remote system network port. Verify user name with Manage role on remote system. Verify user password on remote system. <hr/> <p>NOTE: If the remote system has not been added, it cannot be selected.</p> <hr/>
No	Unable to select the secondary volume (the destination volume on the vdisk to which you will replicate data from the primary volume)? ¹	<ul style="list-style-type: none"> In RAIDar, 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"> Creation of the new volume on the vdisk Selection of replication-prepared volume
No	Communication link is down.	<ul style="list-style-type: none"> See actions described in Can you view information about remote links? on page 66.
<p>¹After ensuring valid licensing, valid cabling connections, and network availability, create the replication set using the Wizards > Replication Setup Wizard in RAIDar.</p>		

Table 20 Diagnostics for replication setup: Creating a replication set

Can you replicate a volume?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	AssuredRemote is not licensed on each controller enclosure used for replication.	See actions described in Can you successfully use the AssuredRemote feature? on page 66.
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 RAIDar Replication Setup Wizard to create one. In RAIDar, review event logs 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"> In RAIDar, review event logs for indicators of a specific fault in a replication data path component. Follow any Recommended Actions. In the Configuration View panel in RAIDar, right-click the secondary volume, and select View > Overview to display the Replication Volume Overview table: <ul style="list-style-type: none"> Check for replication interruption (suspended) status. Check for inconsistent status. Check for offline status. Replications that enter the suspended state must be resumed manually.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 66.

Table 21 Diagnostics for replication setup: Replicating a volume

Can you view a replication image?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Nonexistent replication image.	<ul style="list-style-type: none"> In the Configuration View panel in RAIDar, expand vdisks and subordinate volumes to reveal the existence of a replication image or images. If a replication image has not been successfully created, use RAIDar to create one as described in the “Using AssuredRemote to replicate volumes” topic within the RAIDar User Guide.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 66.

Table 22 Diagnostics for replication setup: Viewing a replication image

Can you view remote systems?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 66.

Table 23 Diagnostics for replication setup: Viewing a remote system

Resolving voltage and temperature warnings

1. Check that all of the fans are working by making sure the Voltage/Fan Fault/Service Required LED on each power supply module is off, or by using RAIDar to check enclosure health status. In the Configuration View panel, right click the enclosure and click **View > Overview** to view the health status of the enclosure and its components. The Enclosure Overview page enables you to see information about each enclosure and its physical components in front, rear, and tabular views—using graphical or tabular presentation—allowing you to view the health status of the enclosure and its components.
See [Options available for performing basic steps](#) on page 55 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 and that their latches are 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 slot open negatively affects the airflow and can cause the enclosure to overheat.
4. Try replacing each power supply one at a time.
5. Replace the controller modules 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. In each controller module and expansion module, the enclosure management processor (EMP) monitors the status of these sensors to perform SCSI enclosure services (SES) functions.

The following sections describe each element and its sensors.

Power supply sensors

Each enclosure has two fully redundant power supplies with load-sharing capabilities. The power supply sensors described in the following table monitor the voltage, current, temperature, and fans in each power supply. If the power supply sensors report a voltage that is under or over the threshold, check the input voltage.

Table 24 Power supply sensor descriptions

Description	Event/Fault ID LED condition
Power supply 1	Voltage, current, temperature, or fan fault
Power supply 2	Voltage, current, temperature, or fan fault

Cooling fan sensors

Each power supply includes two fans. The normal range for fan speed is 4,000 to 6,000 RPM. When a fan speed drops below 4,000 RPM, the EMP considers it a failure and posts an alarm in the storage system event log. The following table lists the description, location, and alarm condition for each fan. If the fan speed remains under the 4,000 RPM threshold, the internal enclosure temperature may continue to rise. Replace the power supply reporting the fault.

Table 25 Cooling fan sensor descriptions

Description	Location	Event/Fault ID LED condition
Fan 1	Power supply 1	< 4,000 RPM
Fan 2	Power supply 1	< 4,000 RPM
Fan 3	Power supply 2	< 4,000 RPM
Fan 4	Power supply 2	< 4,000 RPM

During a shutdown, the cooling fans do not shut off. This allows the enclosure to continue cooling.

Temperature sensors

Extreme high and low temperatures can cause significant damage if they go unnoticed. Each controller module has six temperature sensors. Of these, if the CPU or FPGA (Field-programmable Gate Array) temperature reaches a shutdown value, the controller module is automatically shut down. Each power supply has one temperature sensor.

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 26 Controller module temperature sensor descriptions

Description	Normal operating range	Warning operating range	Critical operating range	Shutdown values
CPU temperature	3°C–88°C	0°C–3°C, 88°C–90°C	> 90°C	0°C 100°C
FPGA temperature	3°C–97°C	0°C–3°C, 97°C–100°C	None	0°C 105°C
Onboard temperature 1	0°C–70°C	None	None	None
Onboard temperature 2	0°C–70°C	None	None	None
Onboard temperature 3 (Capacitor temperature)	0°C–70°C	None	None	None
CM temperature	5°C–50°C	≤ 5°C, ≥ 50°C	≤ 0°C, ≥ 55°C	None

When a power supply sensor goes out of range, the Fault/ID LED illuminates amber and an event is logged to the event log.

Table 27 Power supply temperature sensor descriptions

Description	Normal operating range
Power supply 1 temperature	–10°C–80°C
Power supply 2 temperature	–10°C–80°C

Power supply module voltage sensors

Power supply voltage sensors ensure that an enclosure's power supply voltage is within normal ranges. There are three voltage sensors per power supply.

Table 28 Voltage sensor descriptions

Sensor	Event/Fault LED condition
Power supply 1 voltage, 12V	< 11.00V > 13.00V
Power supply 1 voltage, 5V	< 4.00V > 6.00V
Power supply 1 voltage, 3.3V	< 3.00V > 3.80V

A LED descriptions

Front panel LEDs

AssuredSAN 4004 Series supports 2U24 and 2U12 enclosures. The 2U24 chassis—configured with 24 2.5" small form factor (SFF) disks—is used as either a controller enclosure or expansion enclosure. The 2U12 chassis—configured with 12 3.5" large form factor (LFF) disks—is also used as either a controller enclosure or expansion enclosure.

Supported expansion enclosures are used for adding storage. The 4134 12-drive enclosure is the LFF drive enclosure used for storage expansion. The 4124 24-drive enclosure is the SFF drive enclosure used for storage expansion.

Enclosure bezels

Each AssuredSAN 4004 Series enclosure is equipped with a removable bezel designed to cover the front panel during enclosure operation. The bezels look very similar, but there are differences between the two models. The bezel fitting the 2U24 chassis provides two embossed pockets used during bezel removal ([Figure 27](#)); whereas the bezel fitting the 2U12 chassis provides two debossed pockets, is equipped with an EMI (Electromagnetic Interface) shield, and may or may not be equipped with the serviceable dust filtration air filter option ([Figure 28](#)).

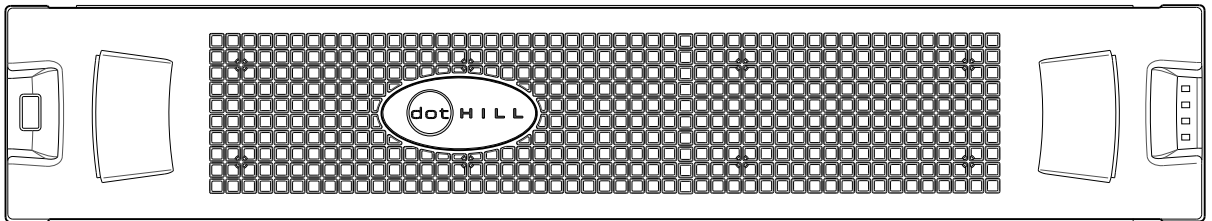


Figure 27 Front panel enclosure bezel: 24-drive enclosure (2U24)

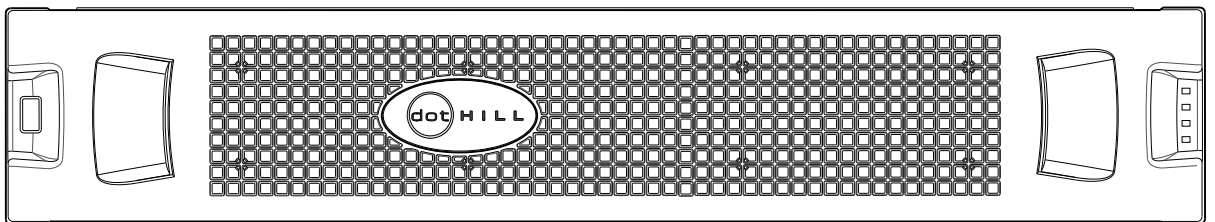


Figure 28 Front panel enclosure bezel: 12-drive enclosure (2U12)

Enclosure bezel attachment and removal

When you initially attach or remove the front panel enclosure bezel for the first time, refer to the appropriate pictorials for your enclosure(s) from the list below, and follow the instructions provided.

- Front view of 24-drive enclosure (2U24): [Figure 27](#)
- Front view of 12-drive enclosure (2U12): [Figure 28](#)
- Bezel alignment for 24-drive enclosure (2U24): [Figure 29](#) on page 72
- Bezel alignment for 12-drive enclosure (2U12): [Figure 30](#) on page 72

Enclosure bezel attachment

Orient the enclosure bezel to align its back side with the front face of the enclosure as shown in [Figure 29](#) on page 72 and [Figure 30](#) on page 72. Face the front of the enclosure, and while supporting the base of the bezel, position it such that the mounting sleeves within the integrated ear caps align with the ball studs, and then gently push-fit the bezel onto the ball studs to securely attach the bezel to the front of the enclosure.

Enclosure bezel removal

While facing the front of the enclosure, insert the index finger of each hand into the top of the respective (left or right) pocket opening, and insert the middle finger of each hand into the bottom of the respective opening, with thumbs on the bottom of the bezel face. Gently pull the top of the bezel while applying slight inward pressure below, to release the bezel from the ball studs.

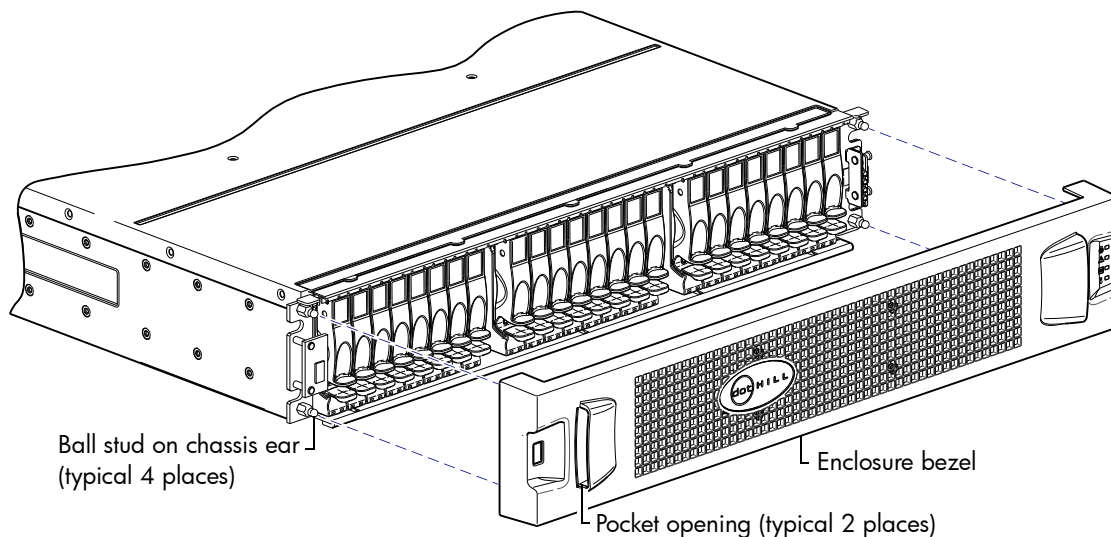


Figure 29 Partial assembly showing bezel alignment with 2U24 chassis

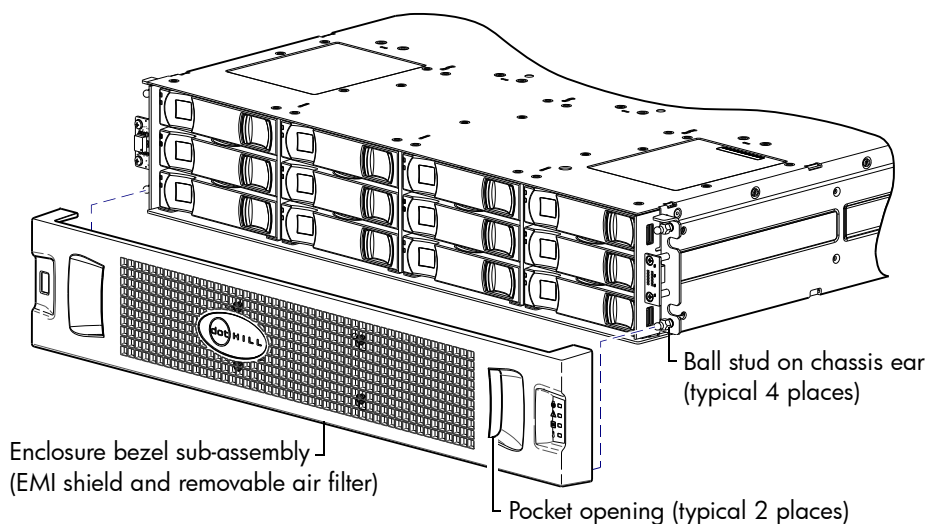


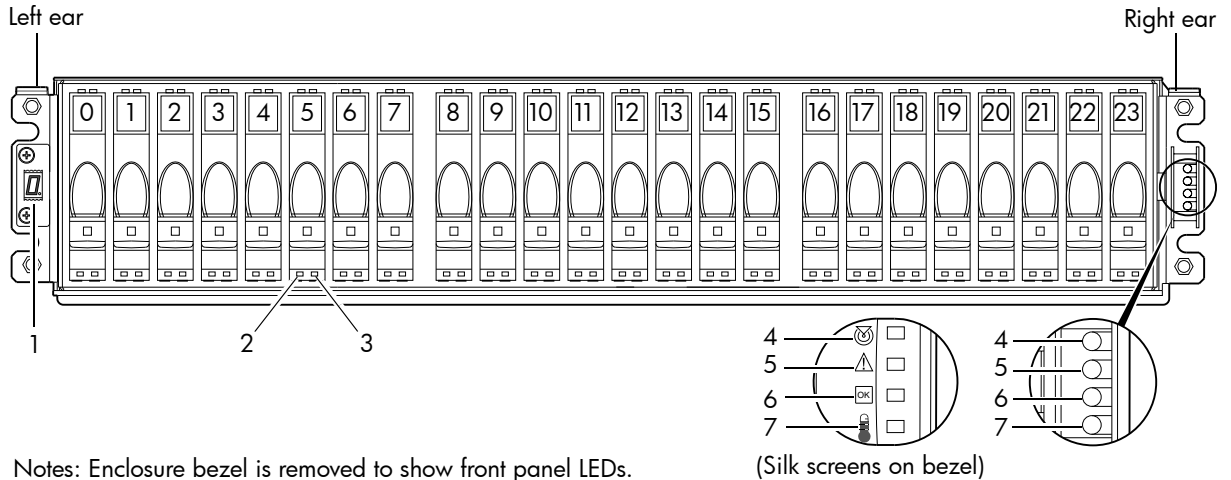
Figure 30 Partial assembly showing bezel alignment with 2U12 chassis

NOTE: For more information about servicing or replacing the removable air filter option for this particular bezel (Figure 30), refer to the *AssuredSAN 12-drive Enclosure Bezel Kit Installation* instructions included in your product ship kit.

NOTE: The enclosure front panel illustrations that follow assume that you have removed the enclosure bezel to reveal underlying components.

24-drive enclosure front panel LEDs

The enclosure bezel is removed to reveal the underlying 2U24 enclosure front panel LEDs. The front panel LEDs—including SFF disk LEDs—are described in the table below the illustration.



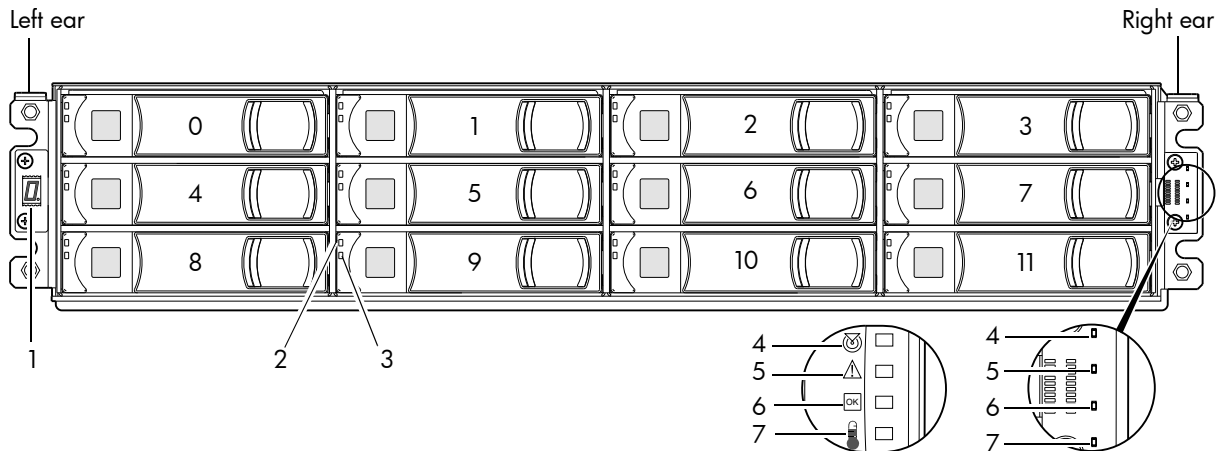
Notes: Enclosure bezel is removed to show front panel LEDs.
Integers on disks indicate drive slot numbering sequence.

LED	Description	Definition
1	Enclosure ID	Green — On Enables you to correlate the enclosure with logical views presented by management software. Sequential enclosure ID numbering of controller enclosures begins with the integer 0. The enclosure ID for an attached drive enclosure is nonzero.
2	Disk drive — Left LED	See Disk drive LEDs on page 75.
3	Disk drive — Right LED	See Disk drive LEDs on page 75.
4	Unit Locator	White blink — Enclosure is identified Off — Normal operation
5	Fault/Service Required	Amber — On Enclosure-level fault condition exists. The event has been acknowledged but the problem needs attention. Off — No fault condition exists.
6	FRU OK	Green — On The enclosure is powered on with at least one power supply operating normally. Off — Both power supplies are off; the system is powered off.
7	Temperature Fault	Green — On The enclosure temperature is normal. Amber — On The enclosure temperature is above threshold.

Figure 31 LEDs: 2U24 enclosure front panel

12-drive enclosure front panel LEDs

The enclosure bezel is removed to reveal the underlying 2U12 enclosure front panel LEDs. The front panel LEDs—including LFF disk LEDs—are described in the table below the illustration.



Notes: Enclosure bezel is removed to show front panel LEDs.
Integers on disks indicate drive slot numbering sequence.

(Silk screens on bezel)

LED	Description	Definition
1	Enclosure ID	Green — On Enables you to correlate the enclosure with logical views presented by management software. Sequential enclosure ID numbering of controller enclosures begins with the integer 0. The enclosure ID for an attached drive enclosure is nonzero.
2	Disk drive — Upper LED	See Disk drive LEDs on page 75.
3	Disk drive — Lower LED	See Disk drive LEDs on page 75.
4	Unit Locator	White blink — Enclosure is identified Off — Normal operation
5	Fault/Service Required	Amber — On Enclosure-level fault condition exists. The event has been acknowledged but the problem needs attention. Off — No fault condition exists.
6	FRU OK	Green — On The enclosure is powered on with at least one power supply operating normally. Off — Both power supplies are off; the system is powered off.
7	Temperature Fault	Green — On The enclosure temperature is normal. Amber — On The enclosure temperature is above threshold.

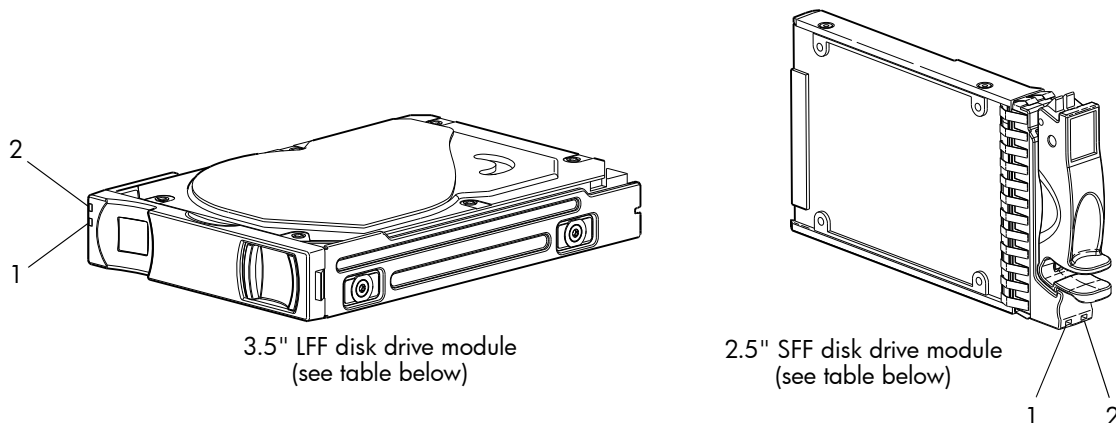
Figure 32 LEDs: 2U12 enclosure front panel

The enclosure bezel for this model provides the EMI protection for the LFF disk drive modules. The bezel should be securely attached to the enclosure during operation (see [Enclosure bezel attachment](#) on page 71 and [Figure 30](#) on page 72).

△ **CAUTION:** Whether configured with or without an air filter, to ensure adequate EMI protection for the LFF disk drives, the enclosure bezel should be properly installed while the enclosure is in operation.

Disk drive LEDs

You must remove the enclosure bezel to facilitate visual observation of disk LEDs. Alternatively, you can use management interfaces to monitor disk LED behavior.



LED No./Description	Color	State	Definition
1— Power/Activity	Green	On	The disk drive module is operating normally.
		Blink	The disk drive module is initializing; active and processing I/O; performing a media scan; or the vdisk is initializing or reconstructing.
		Off	If not illuminated and Fault is not illuminated, the disk is not powered on.
2— Fault	Amber	On	The disk has failed; experienced a fault; is a leftover; or the vdisk that it is associated with is down or critical.
		Blink	Physically identifies the disk; or locates a leftover (also see Blue).
	Off	If not illuminated and Power/Activity is not illuminated, the disk is not powered on.	
	Blue	Blink	Leftover disk from vdisk is located (alternates blinking amber).

Figure 33 LEDs: Disk drive modules

For information about disk drive types supported in 4004 Series LFF and SFF disk drive modules, see [Disk drives used in 4004 Series enclosures](#) on page 16.

For information about replacing a disk drive module in a 4004 Series controller enclosure or 4124/4134 drive enclosure, refer to the “Replacing a disk drive module” topic in the *AssuredSAN 4004 Series FRU Installation and Replacement Guide*. Instructions are provided for replacing LFF and SFF disk drive modules therein.

For information about creating a vdisk with volumes, and mapping the volumes to hosts, see the “Provisioning the system” topic within the *AssuredSAN 4004 Series RAIDar User Guide*.

NOTE: Additional information pertaining to disk drive LED behavior is provided in the supplementary tables on the facing page.

Table 29 LEDs: Disks in SFF and LFF enclosures

Disk drive module LED behavior		LFF/SFF disks	
Description	State	Color	Action
Disk drive OK, FTOL	Off	None	None
	On (operating normally)	Green	On
	OK to remove	Green	Blink
		Blue	On
	Identifying self — offline/online	Green ¹	On
		Amber	Blink
Disk drive I/O	Initializing	Green	Blink
	Active and processing I/O	Green	Blink
	Performing a media scan	Green	Blink
Disk drive leftover	Disk drive is a leftover	Amber	On
	Identifying a leftover	Amber	Blink
		Blue ¹	On
Disk drive failed	Fault or failure	Green ¹	On
		Amber	On
	Fault and remove disk drive	Green	On
		Amber	On
	Fault and identify disk drive	Green	On
		Amber	On
	Fault, identify, and remove disk drive	Green	On
		Amber	Blink
Blue	On		

¹This color may or may not illuminate.

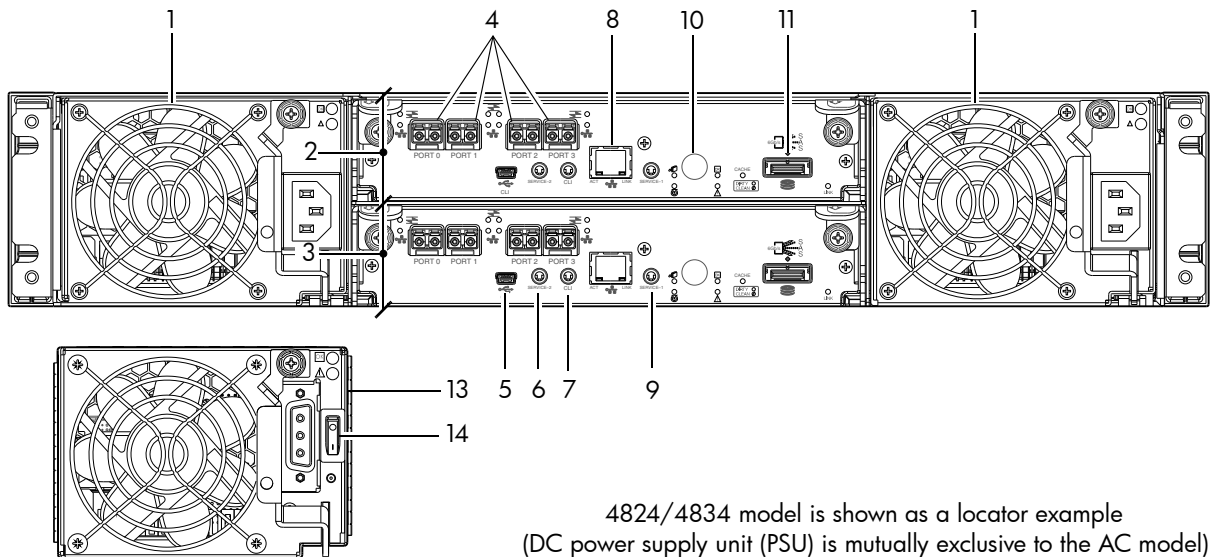
Table 30 LEDs: Vdisks in SFF and LFF enclosures

Vdisk LED behavior		LFF/SFF disks	
Description	State	Color	Action
FTOL	On (operating normally)	Green	On
Vdisk activity	Vdisk is reconstructing	Green	Blink
	Vdisk is initializing	Green	Blink
Vdisk degraded	Vdisk is critical/down	See note 1 below	

¹Individual disks will display fault LEDs

Controller enclosure — rear panel layout

The diagram and table below display and identify important component items that comprise the rear panel layout of an AssuredSAN 4004 Series controller enclosure. In [Figure 34](#) below, a 4824/4834 is shown as a representative example. Diagrams and tables on the following pages describe rear panel LED behavior. The rear panel layout applies to 2U24 and 2U12 chassis form factors.



- | | |
|--|--|
| 1 AC power supplies | 8 Network port |
| 2 Controller module A | 9 Service port 1 (used by service personnel only) |
| 3 Controller module B | 10 Disabled button (used by engineering/test only)
(Stickers shown covering the openings) |
| 4 CNC ports: used for host connection or replication | 11 SAS expansion port |
| 5 CLI port (USB - Type B) | 12 DC Power supply (2)—(DC model only) |
| 6 Service port 2 (used by service personnel only) | 13 DC Power switch |
| 7 Reserved for future use | |

Figure 34 4004 Series controller enclosure: rear panel

A controller enclosure accommodates two power supply FRUs of the same type—either both AC or both DC—within the two power supply slots (see two instances of callout No.1 above). The controller enclosure accommodates two controller module FRUs of the same type within the I/O module (IOM) slots (see callouts No.2 and No.3 above).

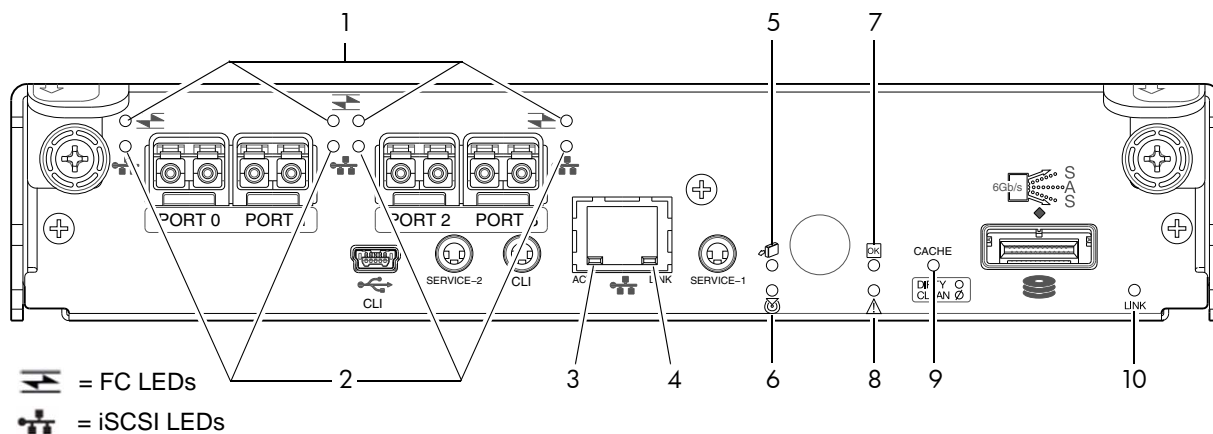
IMPORTANT: If the 4004 Series controller enclosure is configured with a single controller module, the controller module must be installed in the upper slot (see callout No.2 above) and the I/O module blank must be installed in the lower slot (see callout No.3 above). This configuration is required to allow sufficient air flow through the enclosure during operation (also see [Figure 8](#) on page 27).

The diagrams with tables that immediately follow provide descriptions for the different controller modules and power supply modules that can be installed into the rear panel of a 4004 Series controller enclosure. Showing controller modules and power supply modules separately from the enclosure enables improved clarity in identifying the component items called out in the diagrams and described in the tables.

LED descriptions are also provided for optional drive enclosures supported by the 4004 Series controller enclosures.

For information about replacing 4004 Series controller enclosure FRUs, refer to the appropriate FRU replacement procedure in the *AssuredSAN 4004 Series FRU Installation and Replacement Guide*.

4824/4834 CNC controller module — rear panel LEDs



LED	Description	Definition
1	Host 4/8/16 Gb 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 or replication activity.
2	Host 10GbE iSCSI ^{2,3} 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	Network Port Link Active Status	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to all negotiated link speeds).
4	Network Port Link Speed	Off — Link is up at 10/100base-T negotiated speeds. Amber — Link is up and negotiated at 1000base-T.
5	OK to Remove	Off — The controller module is not prepared for removal. Blue — The controller module is prepared for removal.
6	Unit Locator	Off — Normal operation. Blinking white — Physically identifies the controller module.
7	FRU OK	Off — Controller module is not OK. Blinking green — System is booting. Green — Controller module is operating normally.
8	Fault/Service Required	Amber — A fault has been detected or a service action is required. Blinking amber — Hardware-controlled power-up or a cache flush or restore error.
9	Cache Status	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 CompactFlash flush or cache self-refresh is in progress, indicating cache activity. See also Cache Status LED details on page 81.
10	Expansion Port Status	Off — The port is empty or the link is down. On — The port is connected and the link is up.

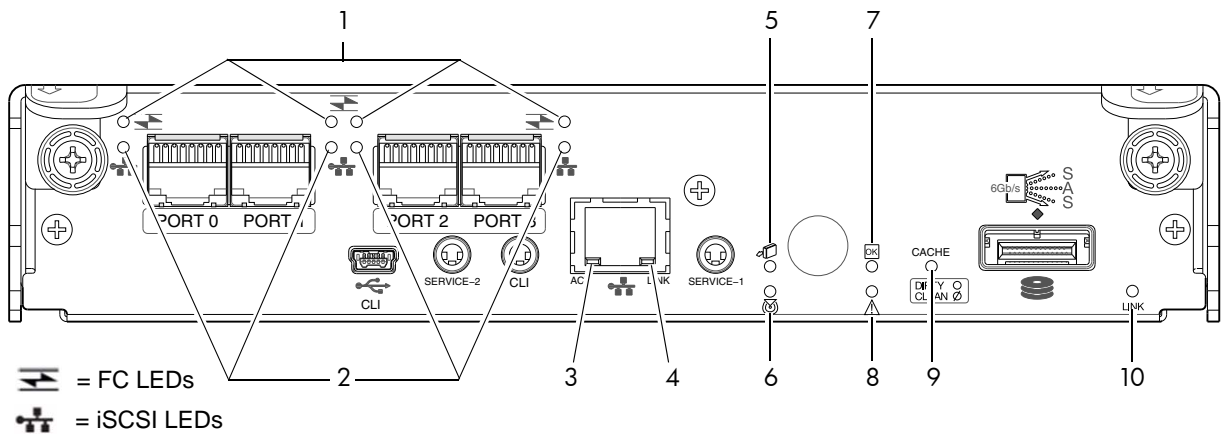
¹When in FC mode, the SFPs must be a qualified 8 Gb or 16 Gb fibre optic option. A 16 Gbit/s SFP can run at 16 Gbit/s, 8 Gbit/s, 4 Gbit/s, or auto-negotiate its link speed. An 8 Gbit/s SFP can run at 8 Gbit/s, 4 Gbit/s, or auto-negotiate its link speed.

²When in 10GbE iSCSI mode, the SFPs must be a qualified 10GbE iSCSI optic option.

³When powering up and booting, iSCSI LEDs will be on/blinking momentarily, then they will switch to the mode of operation.

Figure 35 LEDs: 4824/4834 CNC controller module (FC and 10GbE SFPs)

NOTE: For information about supported combinations of host interface protocols using CNC ports, see [CNC ports used for host connection](#) on page 11 and the “Configuring host ports topic” in the RAIDar User Guide.



LED	Description	Definition
1	Not used in example ¹	The FC SFP is not shown in this example (see Figure 35 on page 78).
2	Host 1 Gb iSCSI ^{2,3} 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	Network Port Link Active Status	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to all negotiated link speeds).
4	Network Port Link Speed	Off — link is up at 10/100base-T negotiated speeds. Amber — link is up and negotiated at 1000base-T.
5	OK to Remove	Off — The controller module is not prepared for removal. Blue — The controller module is prepared for removal.
6	Unit Locator	Off — Normal operation. Blinking white — Physically identifies the controller module.
7	FRU OK	Off — Controller module is not OK. Blinking green — System is booting. Green — Controller module is operating normally.
8	Fault/Service Required	Amber — A fault has been detected or a service action is required. Blinking amber — Hardware-controlled power-up or a cache flush or restore error.
9	Cache Status	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 CompactFlash flush or cache self-refresh is in progress, indicating cache activity. See also Cache Status LED details on page 81.
10	Expansion Port Status	Off — The port is empty or the link is down. On — The port is connected and the link is up.

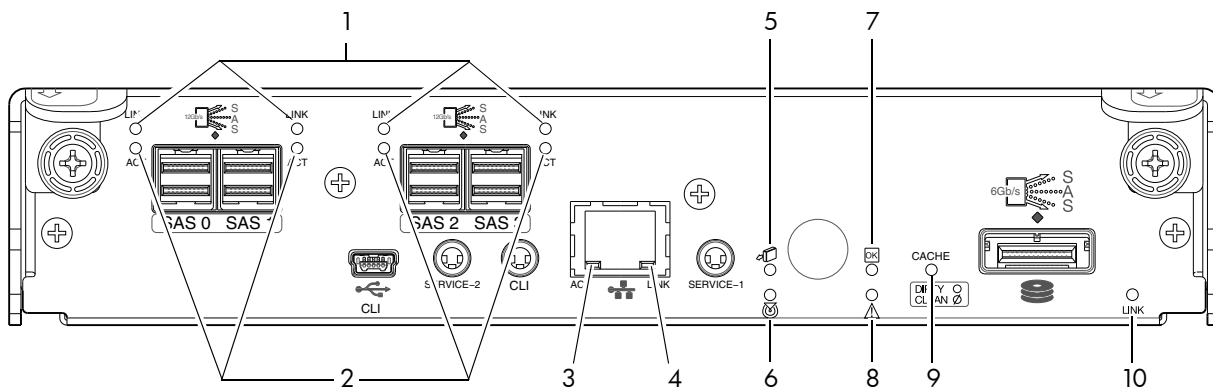
¹When in FC mode, the SFPs must be a qualified 8 Gb or 16 Gb fibre optic option. A 16 Gbit/s SFP can run at 16 Gbit/s, 8 Gbit/s, 4 Gbit/s, or auto-negotiate its link speed. An 8 Gbit/s SFP can run at 8 Gbit/s, 4 Gbit/s, or auto-negotiate its link speed.

²When in 1 GbE iSCSI mode, the SFPs must be a qualified 1 GbE iSCSI optic option.

³When powering up and booting, iSCSI LEDs will be on/blinking momentarily, then they will switch to the mode of operation.

Figure 36 LEDs: 4824/4834 CNC controller module (1 Gb RJ-45 SFPs)

4524/4534 SAS controller module—rear panel LEDs



LED	Description	Definition
1	Host 12 Gb SAS ¹⁻³ Link Status	Off — No link detected. Green — The port is connected and the link is up.
2	Host 12 Gb SAS ¹⁻³ Link Activity	Off — The link is idle. Blinking green — The link has I/O activity.
3	Network Port Link Active Status	Off — The Ethernet link is not established, or the link is down. Green — The Ethernet link is up (applies to all negotiated link speeds).
4	Network Port Link Speed	Off — Link is up at 10/100base-T negotiated speeds. Amber — Link is up and negotiated at 1000base-T.
5	OK to Remove	Off — The controller module is not prepared for removal. Blue — The controller module is prepared for removal.
6	Unit Locator	Off — Normal operation. Blinking white — Physically identifies the controller module.
7	FRU OK	Off — Controller module is not OK. Blinking green — System is booting. Green — Controller module is operating normally.
8	Fault/Service Required	Amber — A fault has been detected or a service action is required. Blinking amber — Hardware-controlled power-up or a cache flush or restore error.
9	Cache Status	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 CompactFlash flush or cache self-refresh is in progress, indicating cache activity. See also Cache Status LED details on page 81.
10	Expansion Port Status	Off — The port is empty or the link is down. On — The port is connected and the link is up.

¹Cables must be qualified HD mini-SAS host cable options.

²Use a qualified SFF-8644 to SFF-8644 cable option when connecting the 4524/4534 controller to a 12 Gb SAS HBA.

³Use a qualified SFF-8644 to SFF-8088 cable option when connecting the 4524/4534 controller to a 6 Gb SAS HBA.

Figure 37 LEDs: 4524/4534 SAS controller module (HD mini-SAS)

NOTE: Once a Link Status LED is lit, it remains so, even if the controller is shut down via RAIDar or CLI.

When a controller is shut down or otherwise rendered inactive—its Link Status LED remains illuminated—falsely indicating that the controller can communicate with the host. Though a link exists between the host

and the chip on the controller, the controller is not communicating with the chip. To reset the LED, the controller must be power-cycled (see [Powering on/powering off](#) on page 30).

Cache Status LED details

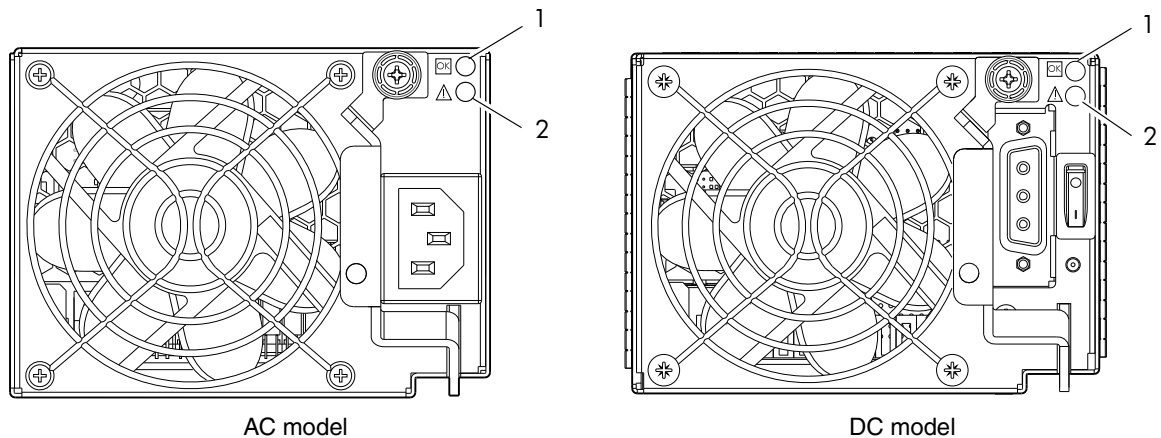
If the LED is blinking evenly, a cache flush is in progress. When a controller module loses power and write cache is dirty (contains data that has not been written to disk), the supercapacitor pack provides backup power to flush (copy) data from write cache to CompactFlash memory. When cache flush is complete, the cache transitions into self-refresh mode.

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 CompactFlash, 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 CompactFlash 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 the CompactFlash 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 CompactFlash.

Power supply LEDs

Power redundancy is achieved through two independent load-sharing power supplies. In the event of a power supply failure, or the failure of the power source, the storage system can operate continuously on a single power supply. Greater redundancy can be achieved by connecting the power supplies to separate circuits. DC power supplies are equipped with a power switch. AC power supplies may or may not have a power switch (model shown below has no power switch). Whether a power supply has a power switch is significant to powering on/off. Power supplies are used by controller and drive enclosures.



LED No./Description	Color	State	Definition
1 — Input Source Power Good	Green	On	Power is on and input voltage is normal.
		Off	Power is off, or input voltage is below the minimum threshold.
2 — Voltage/Fan Fault/Service Required	Amber	On	Output voltage is out of range, or a fan is operating below the minimum required RPM.
		Off	Output voltage is normal.

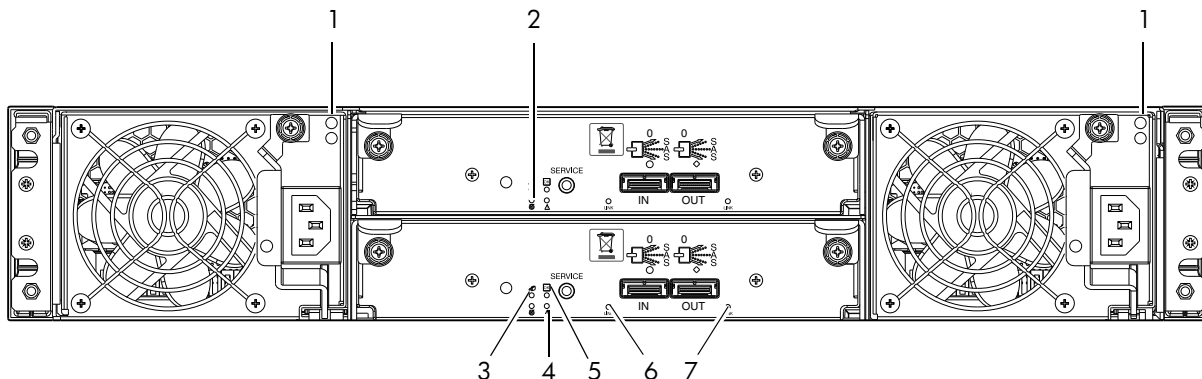
Figure 38 LEDs: Power supply units — rear panel

NOTE: See [Powering on/powering off](#) on page 30 for information on power-cycling enclosures.

4124/4134 drive enclosure rear panel LEDs

The rear panel layout of the 4124/4134 drive enclosure is shown below. Using mini-SAS (SFF-8088) external connectors, these drive enclosures support a 6-Gbps data rate for backend SAS expansion.

Newer models of these drive enclosures feature AC power supplies without power switches, as per the system shown. See [Powering on/powering off](#) on page 30 for more information.



LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 81.
2 — Unit Locator	White	Off Blink	Normal operation. Physically identifies the expansion module.
3 — OK to Remove	Blue	Off	Not implemented.
4 — Fault/Service Required	Amber	On Blink	A fault is detected or a service action is required. Hardware-controlled power-up.
5 — FRU OK	Green	On Off Blink	Expansion module is operating normally. Expansion module is not OK. System is booting.
6 — SAS In Port Status	Green	On Off	Port is connected and the link is up. Port is empty or link is down.
7 — SAS Out Port Status	Green	On Off	Port is connected and the link is up. Port is empty or link is down.

Figure 39 LEDs: 4124/4134 drive enclosure — rear panel

B Environmental requirements and specifications

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.

 **IMPORTANT:** Also see the hard copy *AssuredSAN Product Regulatory Compliance and Safety* document (included in your product ship kit).

Alternatively, you can access the document online. See Dot Hill's customer resource center (CRC) web site for additional information: <http://crc.dothill.com>.

Select **AssuredSAN & R/Evolution Products > 4004 Series** to download the PRC&S document.

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:

Table 31 Power requirements - AC Input

Measurement	Rating
Input power requirements	100-240 VAC, 50/60 Hz
Maximum input power	475 W maximum continuous
Heat dissipation	1,622 BTUs/hour

- 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).

Site wiring and DC power requirements

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

Table 32 Power requirements - DC Input

Measurement	Rating
Input power requirements	-40 to -72 VDC, -48/-60 V nominal
Maximum input power	475 W maximum continuous
Heat dissipation	1,622 BTUs/hour

The 4004 Series system is suitable for installation as part of the Common Bonding Network (CBN). The system's Battery Return (BR) Input Terminals are considered to be an Isolated DC Return (DC-I).

The following criteria are required for all installations:

- 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.

Weight and placement guidelines

Refer to [Physical requirements](#) on page 85 for detailed size and weight specifications.

- The weight of an enclosure depends on the number and type of modules installed.
- Ideally, use two people to lift an enclosure. However, one person can safely lift an enclosure if its weight is reduced by removing the power supply 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 installing enclosures in a rack, make sure that any surfaces over which you might move the rack can support the weight. To prevent accidents when moving equipment, especially on sloped loading docks and up ramps to raised floors, ensure you have a sufficient number of helpers. Remove obstacles such as cables 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 are shipped with a grounding-type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.
- 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

Refer to [Environmental requirements](#) on page 87 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 15.2 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 38.1 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.
- 4004 Series controller and drive enclosures are suitable for connection to intra-building or non-exposed wiring or cabling only.
- 4004 Series controller and drive enclosures are suitable for installation in Network Telecommunication Facilities and locations where the NEC applies. 4004 Series enclosures are not suitable for Outside Plant (OSP) installations.

Management host requirements

A local management host with at least one mini-USB 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 IP address, you then use a remote management host on an Ethernet network to 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 NEBS and FCC Rules and Regulations.

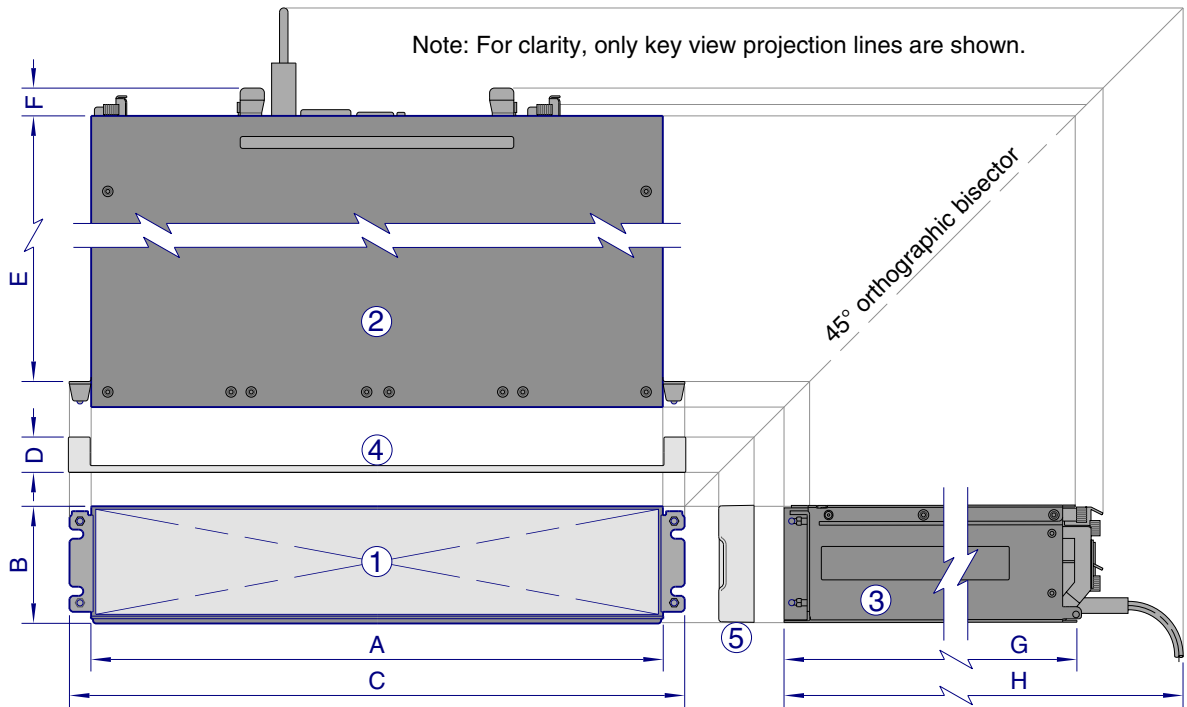
Physical requirements

The floor space at the installation site must be strong enough to support the combined weight of the rack, controller enclosures, drive enclosures, 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 chassis of a 4004 Series controller or drive enclosure is comprised of sheet steel that is bonded together using rivets, welding, and other forced contact methods. The metal surfaces are free from non-conductive coatings and paint.

[Figure 40](#) and [Table 33](#) on page 86 show enclosure dimensions and weights. Enclosure designators are described below. Enclosure weights assume the following configuration characteristics:

- 2U12 enclosure (LFF – also see [Table 4](#) on page 26):
 - “2U12” denotes the 3.5" 12-drive enclosure (with controller or expansion modules)
 - The 2U12 chassis is equipped with a disk in each disk drive slot
- 2U24 enclosure (SFF – also see [Table 4](#) on page 26):
 - “2U24” denotes the 2.5" 24-drive enclosure (with controller or expansion modules)
 - The 2U24 chassis is equipped with a disk in each disk drive slot
- Two controller modules or two expansion modules per enclosure
- Two power supply modules per enclosure



Key for generic enclosure diagram:

- ① – Enclosure front view without bezel or disks
- ② – Enclosure top view (section removed)
- ③ – Enclosure side view (section removed)
- ④ – Enclosure bezel top view (reference only)
- ⑤ – Enclosure bezel side view (reference only)
- A–H: Critical-fit dimensions (see table)

Form	A		B		C		D		E		F		G		H	
	cm	in	cm	in	cm	in	cm	in	cm	in	cm	in	cm	in	cm	in
2U24 ¹	44.7	17.6	8.9	3.5	47.9	18.9	2.5	.98	47.6	18.7	3.0	1.2	51.8	20.4	57.9	22.8
2U12 ²									52.7	20.5	3.0	1.2	54.9	21.6	59.9	23.6

¹The 2U24 enclosure uses 2.5" SFF disks. Remove the enclosure bezel to view disk drive module LEDs.

²The 2U12 enclosure uses 3.5" LFF disks. Remove the enclosure bezel to view disk drive module LEDs.

Figure 40 Rackmount enclosure dimensions

Table 33 Rackmount controller enclosure weights

Specifications	Rackmount
SFF controller enclosure (2U24)	8.6 kg (19.0 lb) [chassis]
• Chassis with FRUs (no disks) ¹⁻³	17.4 kg (38.4 lb)
• Chassis with FRUs (including disks) ¹⁻⁴	23.4 kg (51.6 lb)
LFF controller enclosure (2U12)	9.3 kg (20.6 lb) [chassis]
• Chassis with FRUs (no disks) ¹⁻³	18.1 kg (40.0 lb)
• Chassis with FRUs (including disks) ¹⁻⁴	27.7 kg (61.0 lb)

¹Weights shown are nominal, and subject to variances.

²Rail kits add between 2.8 kg (6.2 lb) and 3.4 kg (7.4 lb) to the aggregate enclosure weight.

³Weights may vary due to different power supplies, IOMs, and differing calibrations between scales.

⁴Weights may vary due to actual number and type of disk drives (SAS or SSD) and air management modules installed.

NOTE: The table below provides information about the optional drive enclosures that are compatible with the 4004 Series controller enclosure.

Table 34 Rackmount compatible drive enclosure weights (ordered separately)

Specifications	Rackmount
4124 (SFF 2.5" 24-drive enclosure)	8.6 kg (19.0 lb) [chassis]
<ul style="list-style-type: none"> Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	16.2 kg (35.8 lb) 22.2 kg (49.0 lb)
4134 (LFF 3.5" 12-drive enclosure)	8.5 kg (18.8 lb) [chassis]
<ul style="list-style-type: none"> Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	16.1 kg (35.6 lb) 25.6 kg (56.6 lb)

¹Weights shown are nominal, and subject to variances.

²Rail kits add between 2.8 kg (6.2 lb) and 3.4 kg (7.4 lb) to the aggregate enclosure weight.

³Weights may vary due to different power supplies and differing calibrations between scales.

⁴Weights may vary due to actual number and type of disk drives (SAS or SSD) and air management modules installed.

Environmental requirements

Table 35 Operating environmental specifications

Specification	Range
Altitude	To 3,000 meters (9,843 feet)
Temperature*	5°C to 40°C (41°F to 104°F)
Humidity	10% to 90% RH up to 40°C (104°F) non-condensing
Shock	3.0 g, 11 ms, ½ sine pulses, X, Y, Z
Vibration	(Shaped-spectrum) 5 Hz to 500 Hz, 0.14 G _{rms} total X, Y, Z

*Temperature is de-rated by 2°C (3.6°F) for every 1 km (3,281) feet above sea level.

Table 36 Non-operating environmental specifications

Specification	Range
Altitude	To 12,000 meters (39,370 feet)
Temperature	-40°C to 70°C (-40°F to 158°F)
Humidity	Up to 93% RH @ 104°F (40°C) non-condensing
Shock	15.0 g, 11 ms, ½ sine pulses, X, Y, Z
Vibration	(Shaped-spectrum) 2.8 Hz to 365.4 Hz, 0.852 G _{rms} total (horizontal) 2.8 Hz to 365.4 Hz, 1.222 G _{rms} total (vertical)

NOTE: For additional information about Telco and ruggedized products, see Dot Hill's web site: <http://www.dothill.com>.

Electrical requirements

Site wiring and power requirements

Each enclosure has two power supply modules for redundancy. If full redundancy is required, use a separate power source for each module. The AC power supply unit in each power supply module is auto-ranging and is automatically configured to an input voltage range from 88–264 VAC with an input frequency of 47–63 Hz. The power supply modules meet standard voltage requirements for both U.S. and

international operation. The power supply modules use standard industrial wiring with line-to-neutral or line-to-line power connections.

Power cable requirements

Each enclosure ships with two power cables designed for use with the enclosure power supply module. AC power cords ship with enclosures equipped with AC power supply modules. Each power cable connects one of the power supply modules to an independent, external power source. To ensure power redundancy, connect the two power cables to two separate circuits; for example, to one commercial circuit and one uninterruptible power source (UPS).

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.

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 about static electricity or assistance with product installation, contact an authorized reseller.

D USB device connection

Rear panel USB ports

AssuredSAN 4004 Series controllers contain two different USB (universal serial bus) management interfaces: a *Host* interface and a *Device* interface. Both interfaces pertain to the Management Controller (MC). The Device interface is accessed via a port on the controller module face plate. The Host interface (USB Type A)—reserved for future use—is accessible from the midplane-facing end of the controller module (see [Figure 7](#) on page 20), and its discussion is deferred.

This appendix describes the port labeled CLI (USB Type B), which enables direct connection between a management computer and the controller, using the command-line interface and appropriate cable (see [Figure 41](#)).

USB CLI port

Connect USB cable to CLI port on controller face plate

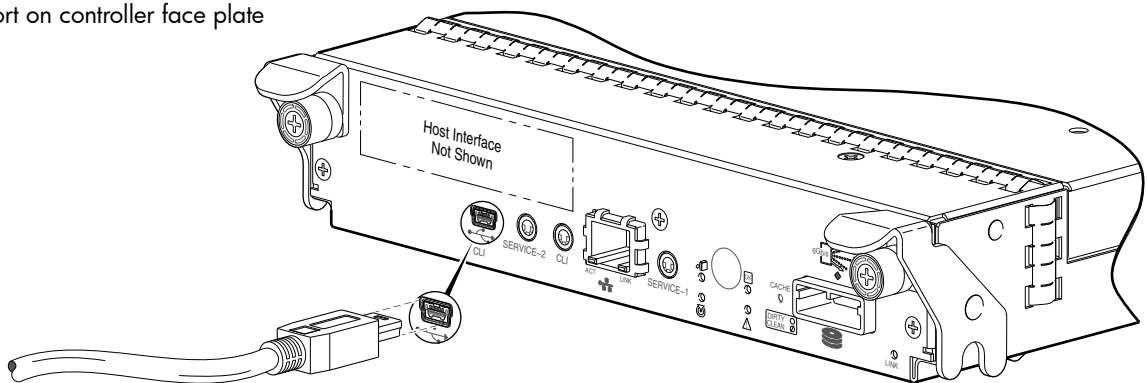


Figure 41 USB device connection — CLI port

AssuredSAN 4004 Series controllers feature a USB CLI port used to cable directly to the controller and initially set IP addresses, or perform other configuration tasks. The USB CLI port employs a mini-USB Type B form factor, and requires a specific cable and additional support, 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 computers, no new driver files are needed, but a Linux configuration file must be created or modified (see [Linux](#) on page 93). For Windows computers a special device driver file, `gserial.inf`, must be downloaded from a CD or web site, and installed on the computer that will be cabled directly to the controller's CLI port (see [Microsoft Windows](#) on page 92).

Emulated serial port

Once attached to the controller module, the management computer should detect a new USB device. Using the Emulated Serial Port interface, the 4004 Series controller presents a single serial port using a *customer vendor ID* and *product ID*. Effective presentation of the emulated serial port assumes the management computer previously had terminal emulator installed (see [Supported host applications](#)). Serial port configuration is unnecessary.

IMPORTANT: Certain operating systems require a device driver or special mode of operation to enable proper functioning of the USB CLI port (see [Device driver/special operation mode](#)).

Supported host applications

4004 Series controllers support the following applications to facilitate connection.

Table 37 Supported terminal emulator applications

Application	Operating system
HyperTerminal and TeraTerm	Microsoft Windows (all versions)
Minicom	Linux (all versions)
	Solaris
	HP-UX

Command-line Interface

Once the management computer detects connection to the USB-capable device, the Management Controller awaits input of characters from the host computer via the command-line. To see the command-line prompt, you must press *Enter*. The MC provides direct access to the CLI.

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

Device driver/special operation mode

Certain operating systems require a device driver or special mode of operation. Product and vendor identification information required for such setup is provided below.

Table 38 USB vendor and product identification codes

USB Identification code type	Code
USB Vendor ID	0x210c
USB Product ID	0xa4a7

Microsoft Windows

Microsoft Windows operating systems provide a USB serial port driver. However, the USB driver requires details for connecting to AssuredSAN 4004 Series controller enclosures. Dot Hill provides a device driver for use in the Windows environment. The USB device driver and installation instructions are provided on the ship kit CD. Alternatively, you can download this data.

Obtaining the software download

1. Verify that the management computer has Internet access.
2. See Dot Hill's customer resource center (CRC) web site <http://crc.dothill.com>.
 - a. Select **AssuredSAN & R/Evolution Products > Software Downloads**.
Peruse the list of articles for an entry pertaining to USB device driver.
 - b. Click on the underscored article title to view its content.
The screen reformats to display article content together with a supporting pane to the right of the article. This pane provides optional actions and attachments.
 - c. Click on the zip file icon under Attachments in the right pane adjacent to the article.
The File Download dialog displays.
 - d. From the File Download dialog, save the zip file locally to the management computer.
 - e. Follow the instructions accompanying the device driver, within the zip file or on the CD, to install the USB device driver.

Linux

Although Linux operating systems do not require installation of a device driver, certain parameters must be provided during driver loading to enable recognition of the AssuredSAN 4004 Series controller enclosures.


Setting parameters for the device driver

1. Enter the following command:

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

2. Press Enter to execute the command.

The Linux device driver is loaded with the parameters required to recognize the controllers.

 **NOTE:** Optionally, this information can be incorporated into the `/etc/modules.conf` file.

Using the CLI port and cable—known issues on Windows

When using the CLI port and cable for setting network port IP addresses, 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

Follow these steps when using the mini-USB cable and USB Type B CLI port to communicate out-of-band between the host and controller module for setting network port IP addresses.

To create a new connection or open an existing connection (HyperTerminal):

1. From the Windows Control Panel, select Device Manager.
2. Connect using the USB COM port and Detect Carrier Loss option.
 - a. Select **Connect To > Connect using:** > pick a COM port from the list.
 - b. Select the **Detect Carrier Loss** check box.

The Device Manager page should show “Ports (COM & LPT)” with an entry entitled “Disk Array USB Port (COM n)”—where n is your system’s COM port number.

3. Set network port IP addresses using the CLI (see procedure on [page 48](#)).

To restore a hung connection when the MC is restarted (any supported terminal emulator):

1. If the connection hangs, disconnect and quit the terminal emulator program.
 - a. Using Device Manager, locate the COM n port assigned to the Disk Array Port.
 - b. Right-click on the hung **Disk Array USB Port (COM n)**, and select **Disable**.
 - c. Wait for the port to disable.
2. Right-click on the previously hung—now disabled—**Disk Array USB Port (COM n)**, and select **Enable**.
3. Start the terminal emulator and connect to the COM port.
4. Set network port IP addresses using the CLI (see procedure on [page 48](#)).

E SFP option for CNC ports

Locate the SFP transceivers

Locate the qualified SFP option for your CNC controller module within your product ship kit. The SFP transceiver (SFP) should look similar to the generic SFP shown in the figure below. Follow the guidelines provided in [Electrostatic discharge](#) when installing an SFP.

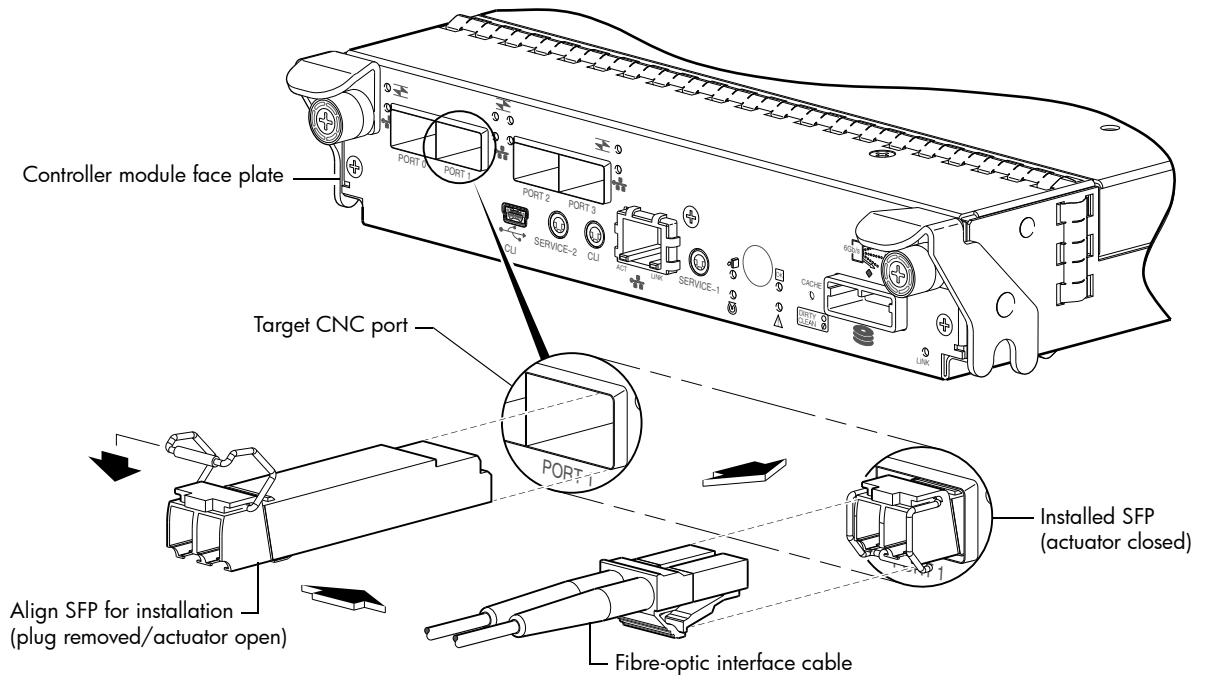


Figure 42 Install a qualified SFP option

Install an SFP transceiver

For each target CNC port, perform the following procedure to install an SFP. Refer to the figure above when performing the steps.

1. Orient the SFP as shown above, and align it for insertion into the target CNC port.
The SFP should be positioned such that the actuator pivot-hinge is on top.
2. If the SFP has a plug, remove it before installing the transceiver. Retain the plug.
3. Flip the actuator open as shown in the figure (near the left detail view).
The actuator on your SFP option may look slightly different than the one shown, and it may not open to a sweep greater than 90° (as shown in the figure).
4. Slide the SFP into the target CNC port until it locks into place.
5. Flip the actuator down, as indicated by the down-arrow next to the open actuator in the figure.
The installed SFP should look similar to the position shown in the right detail view.
6. When ready to attach to the host, obtain and connect a qualified fibre-optic interface cable into the duplex jack at the end of the SFP connector.

NOTE: To remove an SFP module, perform the above steps in *reverse* order.

Verify component operation

View the CNC port Link Status/Link Activity LED on the controller module face plate. A green LED indicates that the port is connected and the link is up (see [LED descriptions](#) for information about controller module LEDs).

Index

Numerics

2U12

3.5" 12-drive enclosure 85

2U24

2.5" 24-drive enclosure 85

A

accessing

CLI (Command-line Interface) 49

RAIDar (web-based management GUI) 53

AssuredRemote

licensed replication feature 42

audience 12

B

bezel

2U12 enclosure 71

2U24 enclosure 71

C

cables

FCC compliance statement 42, 85

shielded 42, 85

cabling

cable routing requirements 85

connecting controller and drive enclosures 24

considerations 35

direct attach configurations 37

switch attach configurations 40

cache

post-write 20

read-ahead 20

clearance requirements

service 85

ventilation 85

CNC ports

change port mode 51

locate and install SFPs 95

SFP transceivers 35

Command-line Interface

using to set controller IP addresses 48

CompactFlash

card location 20

transporting 62

components

12-drive enclosure front panel 16

4124/4134 rear panel 19

4524/4534 rear panel

12 Gb SAS ports 19

CLI (reserved for future use) 19

CLI port (USB) 19

expansion port 19

network port 19

service port 1 19

service port 2 19

4824/4834 rear panel

CLI (reserved for future use) 18

CLI port (USB) 18

CNC ports (1 Gb iSCSI) 18

CNC ports (FC/10GbE) 18

expansion port 18

network port 18

service port 1 18

service port 2 18

Power Supply Unit (PSU)

AC 17

DC 17

connecting

controller enclosures to hosts 35

to remote management hosts 42

connections

test 30

verify 30

console requirement 85

controller enclosures

connecting to hosts 35

connecting to remote management hosts 42

controller modules

4-port 1 Gb iSCSI (CNC) 11

4-port 10GbE iSCSI (CNC) 11

4-port 12 Gb SAS 11

4-port 8/16 Gb FC (CNC) 11

conventions

document 13

D

DHCP

obtaining IP addresses 48

server 48

direct attach configurations 35

disk drive

LEDs

general 75

specific states 76

document

conventions 13

prerequisite knowledge 12

related documentation 12

E

electrostatic discharge

grounding methods 89

precautions 89

enclosure

cabling 24

IDs, correcting 57

- initial configuration [23](#)
- input frequency requirement [87](#)
- input voltage requirement [87](#)
- installation checklist [23](#)
- site requirements [85](#)
- troubleshooting [57](#)
- weight [86](#), [87](#)

Ethernet cables requirements [42](#)

F

faults

- isolating
 - a host-side connection [62](#)
 - expansion port connection fault [64](#)
 - methodology [55](#)

H

host interface ports

- FC (8/16 Gb) [36](#)
- FC host interface protocol
 - loop topology [36](#)
 - point-to-point protocol [36](#)
- iSCSI (10GbE) [36](#)
- iSCSI (1Gb) [37](#)
- iSCSI host interface protocol
 - mutual CHAP [36](#), [37](#)
- SAS (12Gb) [37](#)
- SAS host interface protocol [37](#)

hosts

- defined [35](#)
- optional software [35](#)
- stopping I/O [58](#)
- system requirements [35](#)

humidity non-operating range [87](#)

humidity operating range [87](#)

I

IDs, correcting for enclosure [57](#)

Installing a license

- permanent [53](#)
- temporary [53](#)

IP addresses

- setting using DHCP [48](#)
- setting using the CLI [48](#)

L

LEDs

- 2U12 front panel
 - Disk drive [74](#)
 - Enclosure ID [74](#)
 - Fault/Service Required [74](#)
 - FRU OK [74](#)
 - Temperature Fault [74](#)
 - Unit Locator [74](#)
- 2U24 front panel
 - Disk drive [73](#)
 - Enclosure ID [73](#)

- Fault/Service Required [73](#)
- FRU OK [73](#)
- Temperature Fault [73](#)
- Unit Locator [73](#)

4004 Series controller enclosure rear panel [77](#)

4124/4134 face plate

- Fault/Service Required [82](#)
- FRU OK [82](#)
- OK to Remove [82](#)
- SAS In Port Status [82](#)
- SAS Out Port Status [82](#)
- Unit Locator [82](#)

Disk

- Fault [75](#)
- Power/Activity [75](#)

enclosure rear panel

- 4524/4534
 - 12 Gb Host Link Activity [80](#)
 - 12 Gb Host Link Status [80](#)
 - Cache Status [80](#)
 - Expansion Port Status [80](#)
 - Fault/Service Required [80](#)
 - FRU OK [80](#)
 - Network Port Link Active [80](#)
 - Network Port Link Speed [80](#)
 - OK to Remove [80](#)
 - Unit Locator [80](#)
- 4824/4834
 - 10GbE iSCSI Host Link Status/Link Activity [78](#)
 - 1Gb iSCSI Host Link Status/Link Activity [79](#)
 - Cache Status [78](#), [79](#)
 - Expansion Port Status [78](#), [79](#)
 - Fault/Service Required [78](#), [79](#)
 - FC Host Link Status/Link Activity [78](#)
 - FRU OK [78](#), [79](#)
 - Network Port Link Active [78](#), [79](#)
 - Network Port Link Speed [78](#), [79](#)
 - OK to Remove [78](#), [79](#)
 - Unit Locator [78](#), [79](#)

Power Supply Unit (PSU)

- AC [81](#)
- DC [81](#)

using to diagnose fault conditions [58](#)

local management host requirement [85](#)

M

MPIO DSM

- native Microsoft installation [35](#)
- see related documentation [35](#)

N

NEBS (Level 3)

- Exceptions to GR-63-CORE [24](#)
 - Airborne Contaminants [24](#)
 - Equipment - Fan Filters [24](#)
 - Heat Dissipation [24](#)
 - Spatial Requirements [24](#)

GR-1089-CORE Issue 5 [23](#)

R1-3.155 - hard copy Cautions and Warnings [83](#)

- R2-5.5 - documented ESD sensitivity [89](#)
- R2-6.6 - operating environmental specs [83](#), [84](#), [87](#)
- R2-7.7 - grounding to prevent ESD [89](#)
- R3-1.159 - emission and immunity criteria [42](#)
- R4-16.171 - suitable for intra-building cabling [85](#)
- R4-89.210 - surge protective device [83](#), [84](#)
- R9-10.79 - electrical continuity [85](#)
- R9-16.151 - BR input terminals are DC-I [84](#)
- R9-3.76 - suitable for installing as part of CBN [84](#)
- R9-6.213 - suitable installation sites [85](#)
- GR-63-CORE Issue 3 [23](#)
- R4-17.157 - fans and cooling units [19](#)
- NEBS (Network Equipment-Building System) [23](#)
- non-operating ranges, environmental [87](#)

O

- operating ranges, environmental [87](#)
- optional software [35](#)

P

- physical requirements [85](#)
- power cord requirements [88](#)
- power cycle
 - power off [33](#)
 - power on [31](#)
- power supply
 - AC power requirements [83](#)
 - DC power requirements [84](#)
 - site wiring requirements [83](#)
- prerequisite knowledge [12](#)

R

- RAIDar
 - web-based storage management interface [53](#)
- regulatory compliance
 - notices
 - shielded cables [42](#), [85](#)
 - see related document [83](#)
- related documentation [12](#)
- remote management [42](#)
- requirements
 - cabling [85](#)
 - clearance [85](#)
 - Ethernet cables [42](#)
 - host system [35](#)
 - physical [85](#)
 - ventilation [85](#)
- RFI/EMI connector hoods [42](#), [85](#)
- rugged chassis
 - European Telco compliant [11](#)
 - MIL-STD-810G (storage requirements) compliant [11](#)
 - NEBS Level 3 compliant [11](#)

S

- safety precautions [83](#)
- sensors
 - locating [69](#)
 - power supply [69](#)

- temperature [70](#)
- voltage [70](#)
- SFP transceivers
 - installing [95](#)
 - locating [95](#)
 - supported options [35](#)
 - verifying operation [95](#)
- shock non-operating range [87](#)
- shock operating range [87](#)
- site planning
 - local management host requirement [85](#)
 - physical requirements [85](#)
 - safety precautions [83](#)
- storage system setup
 - configuring [53](#)
 - getting started [53](#)
 - provisioning [53](#)
 - replicating [53](#)
- supercapacitor pack [21](#)
- switch attach configurations [40](#)

T

- temperature non-operating range [87](#)
- temperature operating range [87](#)
- troubleshooting [55](#)
 - controller failure, single controller configuration [61](#)
 - correcting enclosure IDs [57](#)
 - enclosure does not initialize [57](#)
 - expansion port connection fault [64](#)
 - host-side connection fault [62](#)
 - using event notification [56](#)
 - using RAIDar [55](#)
 - using system LEDs [56](#), [58](#)
 - using the CLI [56](#)

U

- Unified LUN Presentation [35](#)
- USB device connection
 - Command-line Interface (CLI) [92](#)
 - device driver [92](#)
 - emulated serial port [91](#)
 - rear panel USB ports [91](#)
 - supported host applications [92](#)
 - vendor and product ID codes [92](#)

V

- ventilation requirements [85](#)
- vibration non-operating range [87](#)
- vibration operating range [87](#)

W

- warnings
 - temperature [69](#)
 - voltage [69](#)
- web site
 - Dot Hill Systems Customer Resource Center [12](#), [20](#), [57](#)

