



AssuredSAN 3004 Series Setup Guide

For firmware release G222

Abstract

This document describes initial hardware setup for Dot Hill AssuredSAN 3004 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 © 2016 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	9
Overview	9
AssuredSAN 3004 Series enclosure user interfaces	9
CNC ports used for host connection	9
HD mini-SAS ports used for host connection	10
Intended audience	10
Prerequisites	10
Related documentation	10
Document conventions and symbols	11
1 Components	13
Front panel components	13
24-drive enclosure front panel components	13
12-drive enclosure front panel components	14
Disk drives used in 3004 Series enclosures	14
Controller enclosure — rear panel layout	15
3824/3834 controller module — rear panel components	16
3524/3534 controller module — rear panel components	17
J6G24/J6G12 drive enclosure rear panel components	17
Component installation and replacement	17
Cache	18
CompactFlash	18
Supercapacitor pack	19
2 Installing the enclosures	20
Installation checklist	20
Connecting the controller enclosure and drive enclosures	20
Connecting the 3004 Series controller to the SFF drive enclosure	21
Connecting the 3004 Series controller to the LFF drive enclosure	21
Connecting the 3004 Series controller to mixed model drive enclosures	21
Cable requirements for storage enclosures	21
Summary of drive enclosure cabling illustrations	23
Testing enclosure connections	24
Powering on/powering off	25
AC PSU	25
DC and AC PSUs equipped with a power switch	26
Connect power cable to DC power supply	27
Connect power cord to legacy AC power supply	27
3 Connecting hosts	29
Host system requirements	29
Cabling considerations	29
Connecting the enclosure to hosts	29
CNC technology	29
Fibre Channel protocol	30
10GbE iSCSI protocol	30
1 Gb iSCSI protocol	31
HD mini-SAS technology	31
12 Gb HD mini-SAS ports	31
Connecting direct attach configurations	31
Fibre Channel host connection	31
10GbE iSCSI host connection	32
1 Gb iSCSI host connection	32
HD mini-SAS host connection	32

Single-controller configurations	33
Dual-controller configurations	34
Connecting switch attach configurations	35
Dual-controller configuration.	35
Connecting a management host on the network	36
Connecting two storage systems to replicate volumes	36
Cabling for replication	37
CNC ports and replication	38
Single-controller configuration	38
Dual-controller configuration.	38
Updating firmware	39
Obtaining IP values	40
Setting network port IP addresses using DHCP.	40
Setting network port IP addresses using the CLI port and cable	40
Change the CNC port mode.	43
Set CNC port mode to iSCSI	43
Configure the system	44
4 Basic operation	45
Accessing the SMC or RAIDar	45
Configuring and provisioning the storage system	45
5 Troubleshooting	46
USB CLI port connection	46
Fault isolation methodology	46
Basic steps	46
Options available for performing basic steps	46
Use the SMC or RAIDar.	47
Use the CLI	47
Monitor event notification	47
View the enclosure LEDs	47
Performing basic steps	47
Gather fault information.	47
Determine where the fault is occurring.	47
Review the event logs	48
Isolate the fault	48
If the enclosure does not initialize	48
Correcting enclosure IDs.	48
Stopping I/O.	49
Diagnostic steps	49
Is the enclosure front panel Fault/Service Required LED amber?	50
Is the controller back panel FRU OK LED off?	50
Is the controller back panel Fault/Service Required LED amber?	50
Are both disk drive module LEDs off?	50
Is the disk drive module Fault LED amber?	51
Is a connected host port Host Link Status LED off?	51
Is a connected port Expansion Port Status LED off?	51
Is a connected port's Network Port link status LED off?	52
Is the power supply Input Power Source LED off?	52
Is the Voltage/Fan Fault/Service Required LED amber?	52
Controller failure in a single-controller configuration	52
If the controller has failed or does not start, is the Cache Status LED on/blinking?	53
Transporting cache	53
Isolating a host-side connection fault	53
Host-side connection troubleshooting featuring CNC ports	53
Host-side connection troubleshooting featuring SAS host ports	54
Isolating a controller module expansion port connection fault	55
Isolating replication faults	56
Cabling for replication	56

Replication setup and verification.	56
Diagnostic steps for replication setup	57
Virtual replication using the SMC	58
Linear replication using RAIDar.	61
Resolving voltage and temperature warnings	64
Sensor locations	64
Power supply sensors	64
Cooling fan sensors	64
Temperature sensors.	65
Power supply module voltage sensors.	66
A LED descriptions	67
Front panel LEDs.	67
Enclosure bezels	67
Enclosure bezel attachment and removal	67
Enclosure bezel attachment	67
Enclosure bezel removal	68
24-drive enclosure front panel LEDs	69
12-drive enclosure front panel LEDs	70
Disk drive LEDs.	71
Controller enclosure — rear panel layout.	73
3824/3834 CNC controller module — rear panel LEDs	74
3524/3534 SAS controller module—rear panel LEDs	76
Cache Status LED details	77
Power supply LEDs.	77
J6G24/J6G12 drive enclosure rear panel LEDs	78
B Specifications and requirements	79
Safety requirements.	79
Site requirements and guidelines	79
Site wiring and AC power requirements	79
Site wiring and DC power requirements	80
Weight and placement guidelines	80
Electrical guidelines	80
Ventilation requirements	81
Cabling requirements	81
Management host requirements	81
Physical requirements	81
Environmental requirements	83
Electrical requirements.	83
Site wiring and power requirements.	83
Power cable requirements.	84
C Electrostatic discharge	85
Preventing electrostatic discharge	85
Grounding methods to prevent electrostatic discharge	85
D USB device connection	86
Rear panel USB ports	86
USB CLI port	86
Emulated serial port	86
Supported host applications	87
Command-line Interface	87
Device driver/special operation mode	87
Microsoft Windows	87
Obtaining the software download.	87
Linux	88
Setting parameters for the device driver.	88
Using the CLI port and cable—known issues on Windows	88
Problem	88

Workaround	88
E SFP option for CNC ports	89
Locate the SFP transceivers	89
Install an SFP transceiver	89
Verify component operation	89
F SAS fan-out cable option	90
Locate the SAS fan-out cable	90
Install the SAS fan-out cable	90
Index	92

Figures

1	2U24 enclosure: front panel	13
2	2U12 enclosure: front panel	14
3	3004 Series controller enclosure: rear panel	15
4	3824/3834 controller module face plate (FC or 10GbE iSCSI).	16
5	3824/3834 controller module face plate (1 Gb RJ-45)	16
6	3524/3534 controller module face plate (HD mini-SAS)	17
7	J6G24/J6G12 expansion enclosure: rear panel	17
8	CompactFlash card	18
9	Cabling connections between a controller enclosure and one drive enclosure	23
10	Fault-tolerant cabling between a dual-controller enclosure and four drive enclosures.	24
11	AC PSU	25
12	AC power cord	26
13	DC and AC PSUs with power switch	26
14	DC power cable featuring D-shell and lug connectors	27
15	Connecting hosts: direct attach—one server/one HBA/single path	33
16	Connecting hosts: direct attach—two servers/two HBAs/dual path (fan-out)	33
17	Connecting hosts: direct attach—one server/one HBA/dual path	34
18	Connecting hosts: direct attach—two servers/one HBA per server/dual path	34
19	Connecting hosts: direct attach—four servers/one HBA per server/dual path (fan-out)	35
20	Connecting hosts: switch attach—two servers/two switches.	35
21	Connecting two storage systems for replication: one server/two switches/one location	38
22	Connecting two storage systems for replication: multiple servers/one switch/one location	39
23	Connecting two storage systems for replication: multiple servers/switches/one location	39
24	Connecting two storage systems for replication: multiple servers/switches/two locations	39
25	Connecting a USB cable to the CLI port	41
26	Front panel enclosure bezel: 24-drive enclosure (2U24)	67
27	Front panel enclosure bezel: 12-drive enclosure (2U12)	67
28	Partial assembly showing bezel alignment with 2U24 chassis	68
29	Partial assembly showing bezel alignment with 2U12 chassis	68
30	LEDs: 2U24 enclosure front panel	69
31	LEDs: 2U12 enclosure front panel	70
32	LEDs: Disk drive modules	71
33	3004 Series controller enclosure: rear panel	73
34	LEDs: 3824/3834 CNC controller module (FC and 10GbE SFPs)	74
35	LEDs: 3824/3834 CNC controller module (1 Gb RJ-45 SFPs)	75
36	LEDs: 3524/3534 SAS controller module (HD mini-SAS)	76
37	LEDs: Power supply units — rear panel	78
38	LEDs: J6G24/J6G12 drive enclosure — rear panel	78
39	Rackmount enclosure dimensions	82
40	USB device connection — CLI port	86
41	Install a qualified SFP option	89
42	HD mini-SAS to mini-SAS fan-out cable	90
43	HD mini-SAS to HD mini-SAS fan-out cable	91

Tables

1	Related documents	10
2	Document conventions	11
3	Installation checklist	20
4	Summary of cabling connections for 3004 Series enclosures.	22
5	Terminal emulator display settings	42
6	Terminal emulator connection settings.	42
7	Diagnostics LED status: Front panel "Fault/Service Required"	50
8	Diagnostics LED status: Rear panel "FRU OK"	50
9	Diagnostics LED status: Rear panel "Fault/Service Required"	50
10	Diagnostics LED status: Disk LEDs (LFF and SFF modules).	50
11	Diagnostics LED status: Disk drive fault status (LFF and SFF modules).	51
12	Diagnostics LED status: Rear panel "Host Link Status"	51
13	Diagnostics LED status: Rear panel "Expansion Port Status"	51
14	Diagnostics LED status: Rear panel "Network Port Link Status"	52
15	Diagnostics LED status: Rear panel power supply "Input Power Source"	52
16	Diagnostics LED status: Rear panel power supply "Voltage/Fan Fault/Service Required"	52
17	Diagnostics LED status: Rear panel "Cache Status"	53
18	Diagnostics for replication setup: Using the replication feature (v3).	58
19	Diagnostics for replication setup: Viewing information about remote links (v3).	59
20	Diagnostics for replication setup: Creating a replication set (v3)	59
21	Diagnostics for replication setup: Replicating a volume (v3)	59
22	Diagnostics for replication setup: Checking for a successful replication (v3)	60
23	Diagnostics for replication setup: Using the replication feature (v2)	61
24	Diagnostics for replication setup: Viewing information about remote links (v2).	61
25	Diagnostics for replication setup: Creating a replication set (v2)	62
26	Diagnostics for replication setup: Replicating a volume (v2)	63
27	Diagnostics for replication setup: Viewing a replication image (v2)	63
28	Diagnostics for replication setup: Viewing a remote system (v2).	63
29	Power supply sensor descriptions.	64
30	Cooling fan sensor descriptions.	65
31	Controller module temperature sensor descriptions.	65
32	Power supply temperature sensor descriptions	65
33	Voltage sensor descriptions.	66
34	LEDs: Disks in SFF and LFF enclosures	72
35	LEDs: Disk groups in SFF and LFF enclosures	72
36	Power requirements - AC Input	79
37	Power requirements - DC Input.	80
38	Rackmount controller enclosure weights	82
39	Rackmount compatible drive enclosure weights (ordered separately)	83
40	Operating environmental specifications	83
41	Non-operating environmental specifications	83
42	Supported terminal emulator applications	87
43	USB vendor and product identification codes	87

About this guide

Overview

This guide provides information about initial hardware setup for the AssuredSAN™ 3004 Series storage enclosure products listed below:

- CNC (Converged Network Controller) Controller enclosure: 3824/3834
 - 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: 3524/3534

The 3004 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 3004 Series controller enclosures can optionally be cabled to J6G24/J6G12 drive enclosures for adding storage. The J6G24 is an SFF 24-disk 2U expansion enclosure, and the J6G12 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>.

AssuredSAN 3004 Series enclosures support both traditional linear storage and new virtual storage, which uses paged-storage technology. For linear storage, a group of disks with an assigned RAID level is called a *vdisk* or *linear disk group*. For virtual storage, a group of disks with an assigned RAID level is called a *virtual disk group*. This guide uses the term *vdisk* when specifically referring to linear storage, and uses the term *disk group* otherwise.

AssuredSAN 3004 Series enclosure user interfaces

The 3004 Series enclosures support two versions of the web-based application for configuring, monitoring, and managing the storage system. Both web-based application GUI versions (v3 and v2), and the command-line interface are briefly described:

- Storage Management Console (SMC) is the *new* primary web interface (v3) for the enclosures, providing access to all common management functions for both linear and virtual storage.
- RAIDar is a secondary web interface (v2) for the enclosures, providing access to traditional linear storage functions. This legacy interface provides certain functionality that is not available in the primary interface.
- The command-line interface (CLI) enables you to interact with the storage system using command syntax entered via the keyboard or scripting. You can set a CLI preference to use v3 or v2 terminology in command output and system messages.

NOTE: For more information about enclosure user interfaces, see the following:


- *AssuredSAN Storage Management Guide* or online help
The guide describes SMC (v3) and RAIDar (v2) GUIs
 - *AssuredSAN CLI Reference Guide*
-


CNC ports used for host connection

AssuredSAN 3824/3834 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

3004 Series enclosures do not support SFPs for multiple host interface protocols in combination. You must select a common host interface protocol and SFP for use in all CNC ports within the controller enclosure. See [CNC technology](#) on page 29 and [3824/3834 CNC controller module — rear panel LEDs](#) on page 74 for more information.

 **TIP:** See the Storage Management Guide for information about configuring CNC ports with host interface protocols of the same type or a combination of types.

 **IMPORTANT:** AssuredSAN 3824/3834 models ship with CNC ports initially configured for FC. When connecting CNC ports to iSCSI hosts, you must use the CLI (not the SMC or 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 43 for instructions).

HD mini-SAS ports used for host connection

AssuredSAN 3524/3534 models provide two 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 SAS 3.0 to support a link rate of 12 Gbit/s using the qualified connectors and cable options. See [3524/3534 SAS controller module—rear panel LEDs](#) on page 76 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), 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*
Regulatory compliance and safety and disposal information	AssuredSAN Product Regulatory Compliance and Safety*
Using a rackmount bracket kit to install an enclosure into a rack	AssuredSAN Rackmount Bracket Kit Installation* document pertaining to the specific enclosure model

Table 1 Related documents (continued)

For information about	See
Attaching or removing an enclosure bezel, and servicing the optional air filter	AssuredSAN Enclosure Bezel Kit Installation* document pertaining to the specific enclosure model
Obtaining and installing a license to use licensed features	AssuredSAN Obtaining and Installing a License Certificate File
Using the v3 and v2 web interfaces to configure and manage the product	AssuredSAN Storage Management Guide
Using the command-line interface (CLI) to configure and manage the product	AssuredSAN CLI Reference Guide
Event codes and recommended actions	AssuredSAN Event Descriptions Reference Guide
Identifying and installing or replacing field-replaceable units (FRUs)	AssuredSAN FRU Installation and Replacement Guide

* Printed document included in product shipkit.


For additional information, see Dot Hill's Customer Resource Center web site: <https://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 3004 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 J6G12 12-drive enclosure is the LFF drive enclosure used for storage expansion. The J6G24 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

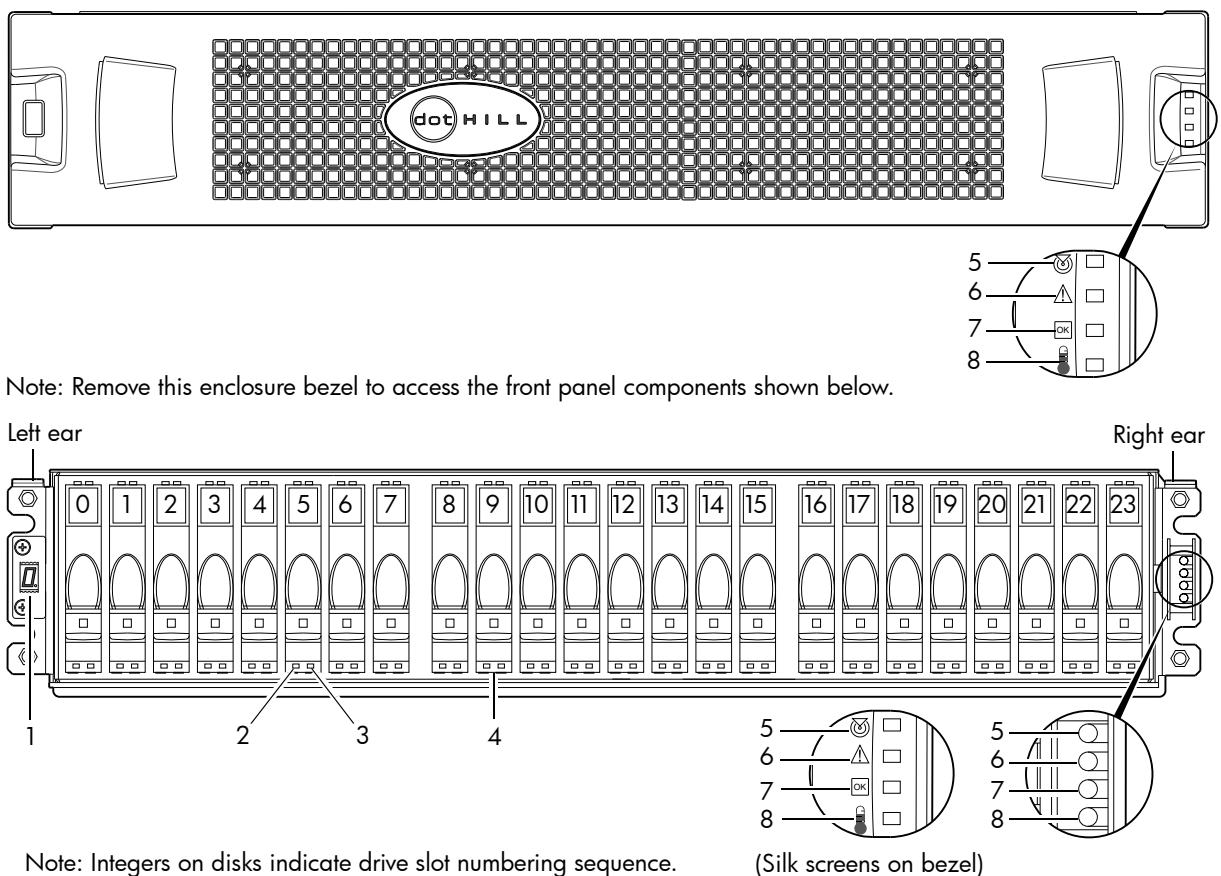
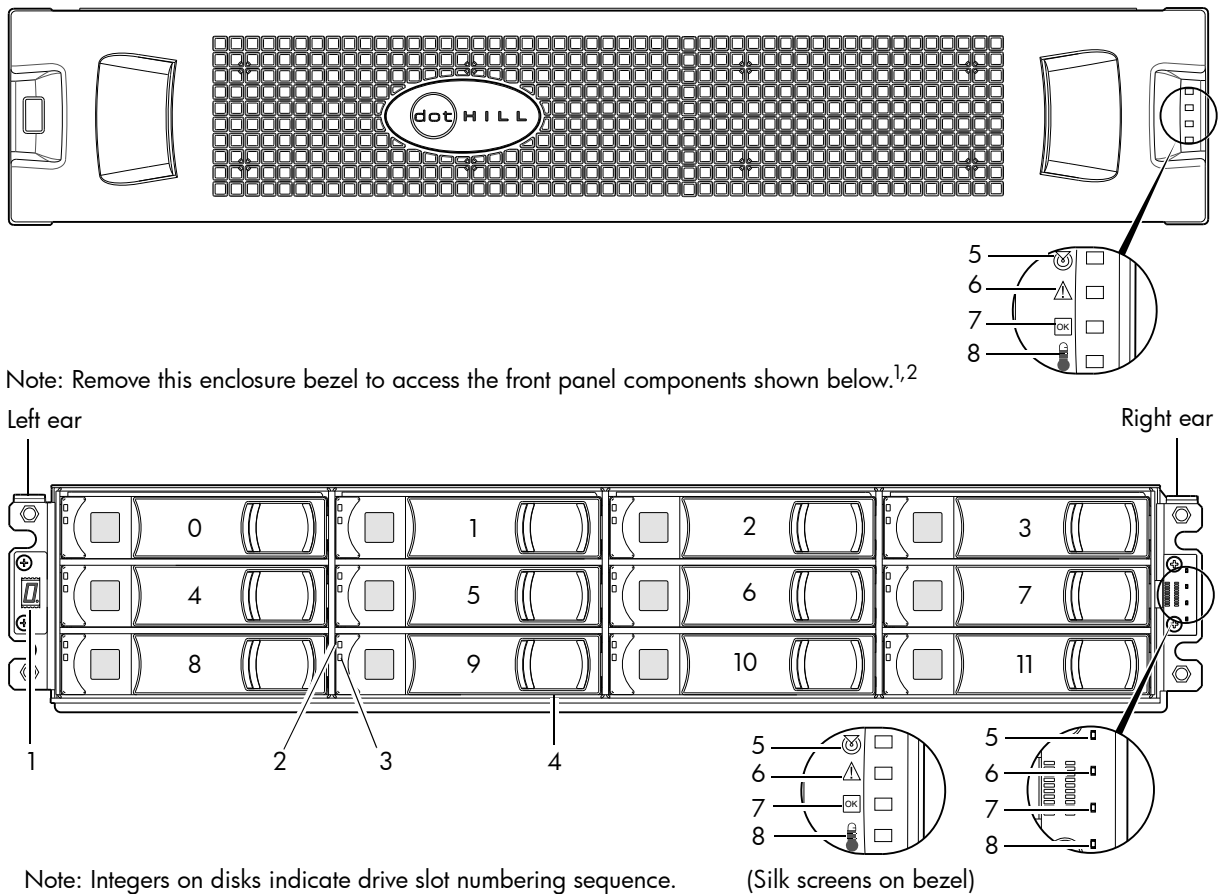


Figure 1 2U24 enclosure: front panel

TIP: See [Enclosure bezel attachment and removal](#) on page 67 and [Figure 28](#) on page 68 (2U24).

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

12-drive enclosure front panel components



1 Enclosure ID LED

2 Disk drive status LED: Fault

3 Disk drive status LED: Power/Activity

4 3.5" disk or drive blank (typical 12 slots)

5 Enclosure status LED: Unit Locator

6 Enclosure status LED: Fault/Service Required

7 Enclosure status LED: FRU OK

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 filter, 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: <https://crc.dothill.com>.

Figure 2 2U12 enclosure: front panel

TIP: See [Enclosure bezel attachment and removal](#) on page 67 and [Figure 29](#) on page 68 (2U12).

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

Disk drives used in 3004 Series enclosures

3004 Series enclosures support LFF/SFF Midline SAS and LFF/SFF Enterprise SAS disks. For information about creating disk groups and adding spares using different disk drive types, see the *AssuredSAN Storage Management 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 3004 Series controller enclosure. The 3824/3834 (FC) is shown as a representative example of controller enclosure models included in the product series. The rear panel layout applies to 2U24 and 2U12 form factors.

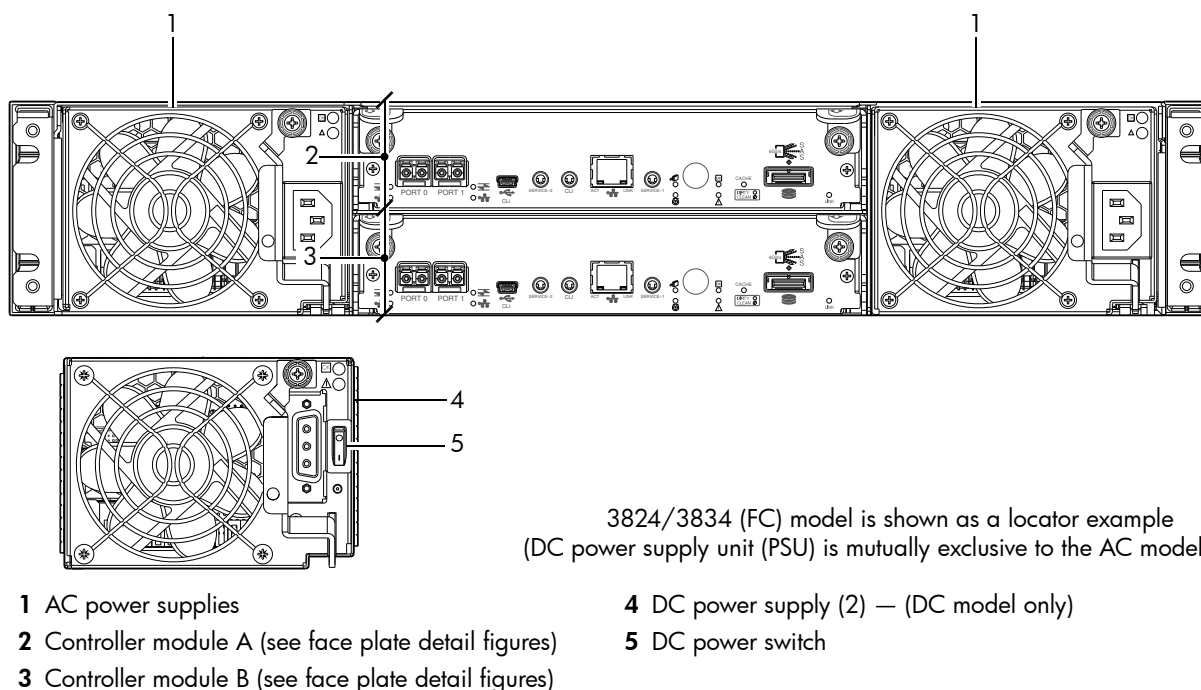


Figure 3 3004 Series controller enclosure: rear panel

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 3004 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 3004 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 3004 Series controller enclosures for expanding storage capacity.

NOTE: 3004 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.

3824/3834 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.

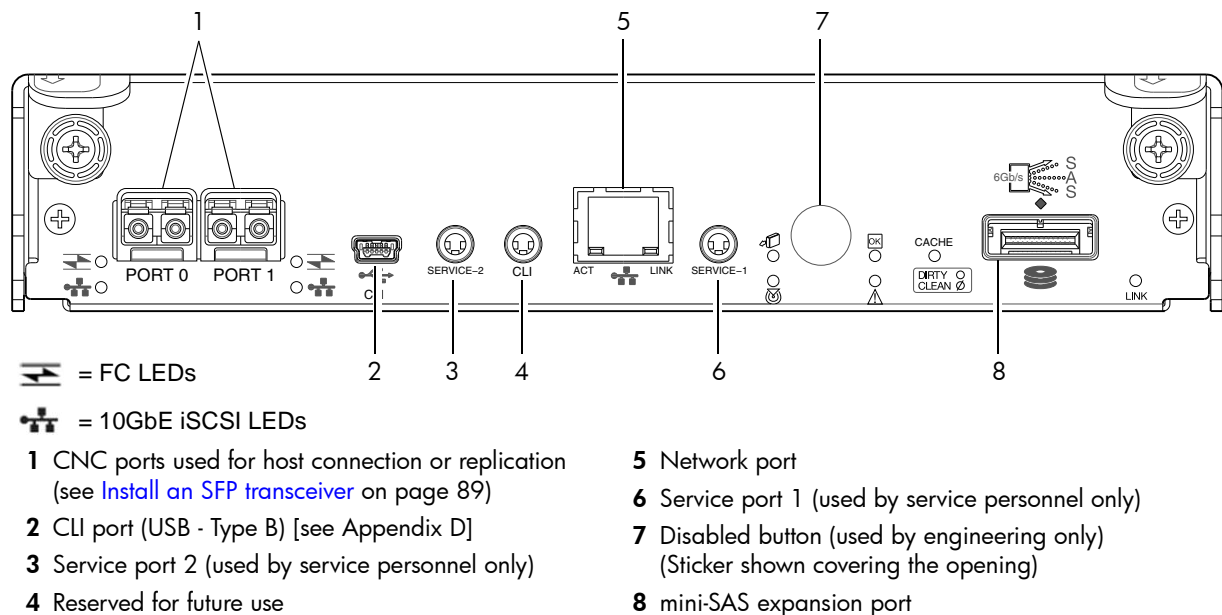


Figure 4 3824/3834 controller module face plate (FC or 10GbE iSCSI)

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

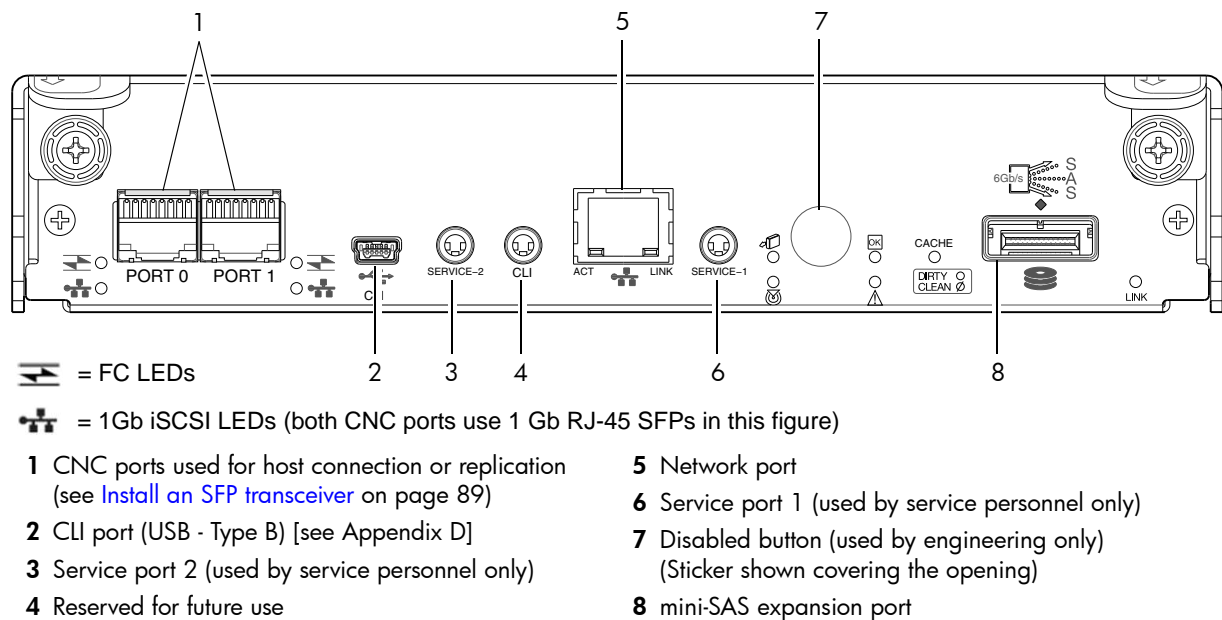
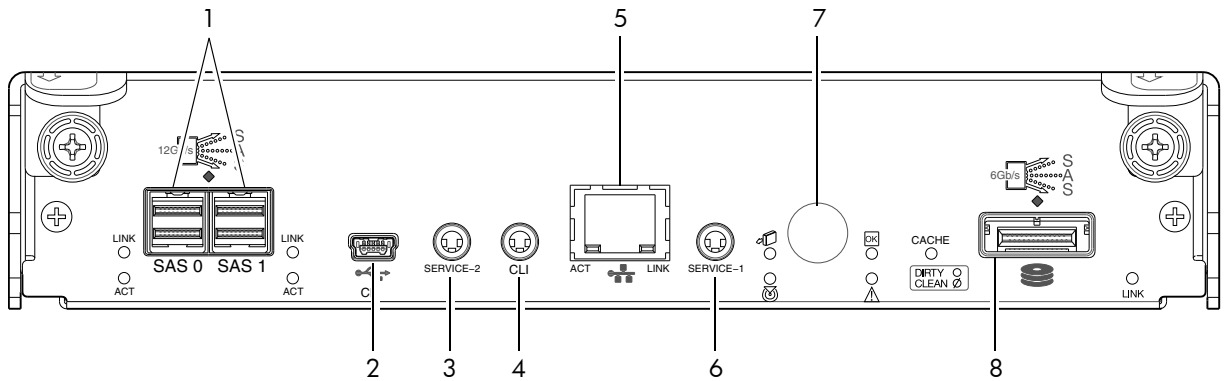


Figure 5 3824/3834 controller module face plate (1 Gb RJ-45)

NOTE: See [CNC ports used for host connection](#) on page 9 for more information about CNC technology. For CNC port configuration, see the “Configuring host ports” topic within the Storage Management Guide or online help.

3524/3534 controller module — rear panel components

Figure 5 shows host interface ports configured with 12 Gbit/s HD mini-SAS (SFF-8644) connectors.

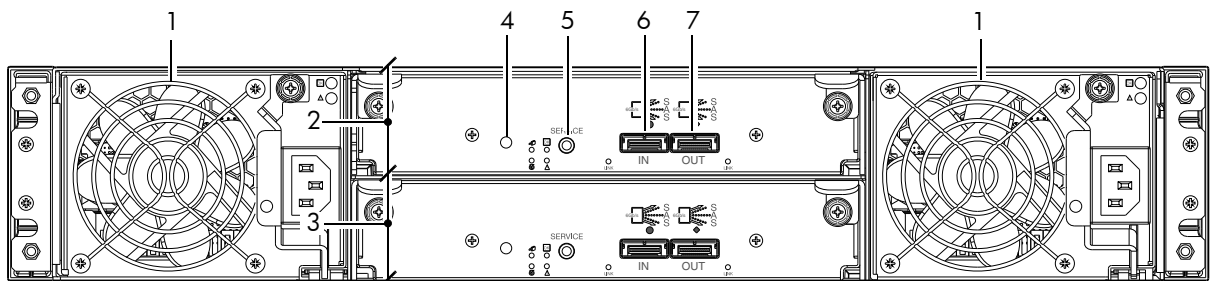


- | | |
|---|--|
| 1 HD mini-SAS ports used for host connection | 5 Network port |
| 2 CLI port (USB - Type B) [see Appendix D] | 6 Service port 1 (used by service personnel only) |
| 3 Service port 2 (used by service personnel only) | 7 Disabled button (used by engineering only)
(Sticker shown covering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

Figure 6 3524/3534 controller module face plate (HD mini-SAS)

J6G24/J6G12 drive enclosure rear panel components

AssuredSAN 3004 Series controller enclosures support SFF J6G24 24-disk and LFF J6G12 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 21 for cabling information. The rear panel view is common to both drive enclosures.



- | | |
|---|---|
| 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) | |

Figure 7 J6G24/J6G12 expansion enclosure: rear panel

Component installation and replacement

Installation and replacement of 3004 Series FRUs (field-replaceable units) is addressed in the *AssuredSAN 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 components


- 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: <https://crc.dothill.com>.

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 Storage Management Guide for more information about cache options and settings.

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. It is used for cache recovery only.

Controller module pictorial
(Midplane-facing rear view)

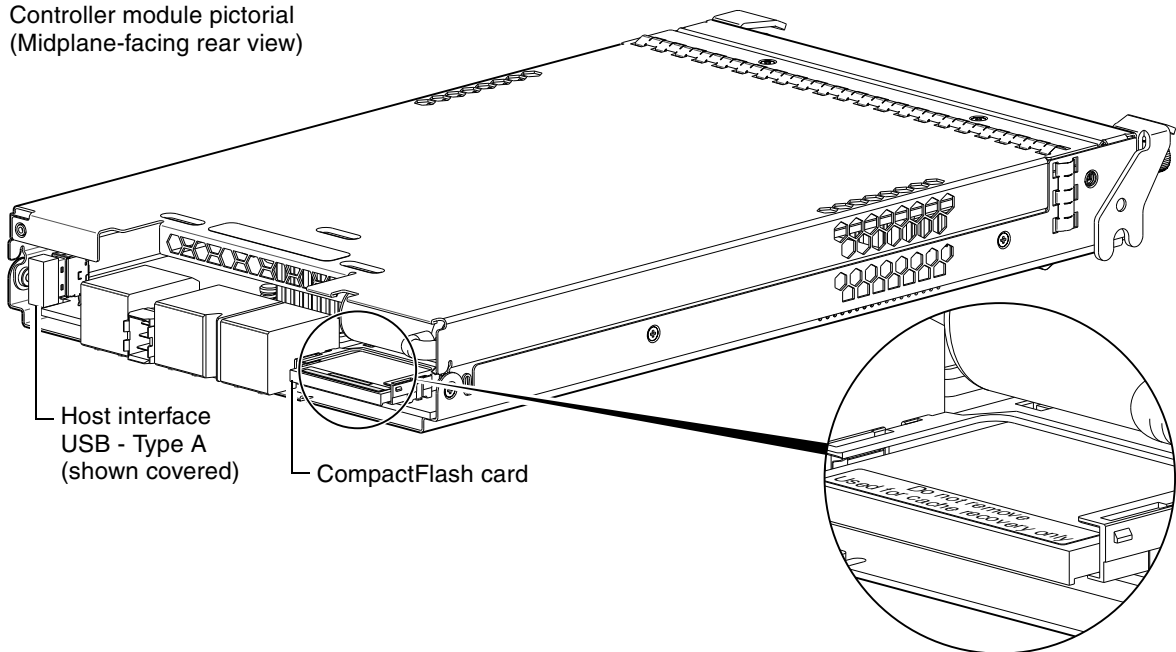


Figure 8 CompactFlash card

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 52 for more information).

△ **CAUTION:** The CompactFlash card should only be removed for transportable purposes. To preserve the existing data stored in the CompactFlash, you must transport the CompactFlash from the failed controller to the replacement controller using a procedure outlined in *AssuredSAN FRU Installation and Replacement Guide* within the procedure for replacing a controller module. Failure to use this procedure will result in the loss of data stored in the cache module. The CompactFlash must stay with the same enclosure. If the CompactFlash is used/installed in a different enclosure, data loss/data corruption will occur.

📌 **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 20.
3.	Connect power cords.	See Powering on/powering off on page 25.
4.	Test enclosure connectivity.	See Testing enclosure connections on page 24.
5.	Install required host software.	See Host system requirements on page 29.
6.	Connect hosts. ²	See Connecting the enclosure to hosts on page 29.
7.	Connect remote management hosts. ²	See Connecting a management host on the network , page 36.
8.	Obtain IP values and set network port IP properties on the controller enclosure.	See Obtaining IP values on page 40. For USB CLI port and cable use, see Appendix D.
9.	Use the CLI to set the host interface protocol.	See CNC technology on page 29. The 3824/3834 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 (v3 or v2) to access the application GUI.• Verify firmware revisions and update if necessary.• Initially configure and provision the system using the SMC (v3) or RAIDar (v2).	Topics below correspond to bullets at left: See “Getting Started” in the web-posted <i>AssuredSAN Storage Management Guide</i> . See Updating firmware . Also see the same topic in the <i>AssuredSAN Storage Management Guide</i> . See “Configuring the System” and “Provisioning the System” topics in the <i>Storage Management Guide</i> or online help.

¹ See the *AssuredSAN 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 67.

² For more about hosts, see the “About hosts” topic in the *AssuredSAN Storage Management Guide*.

³ The SMC and RAIDar are introduced in [Accessing the SMC or RAIDar](#) on page 45. See the *Storage Management 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.

Connecting the controller enclosure and drive enclosures

AssuredSAN 3004 Series controller enclosures—available in 24-drive (2.5") or 12-drive (3.5") chassis—support up to four enclosures (including the controller enclosure), or a maximum of 96 disk drives. The 3004 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 3004 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 10](#) on page 24 shows reverse cabling, wherein controller 0A (i.e., enclosure-ID = 0; controller-ID = A) 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). Cabling examples are provided on the following pages.

Connecting the 3004 Series controller to the SFF drive enclosure

The SFF J6G24 24-drive enclosure, supporting 6 Gb internal disk drive and expander link speeds, can be attached to a 3004 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 9](#) on page 23).

Connecting the 3004 Series controller to the LFF drive enclosure

The LFF J6G12 12-drive enclosure, supporting 6 Gb internal disk drive and expander link speeds, can be attached to a 3004 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 9](#) on page 23).

Connecting the 3004 Series controller to mixed model drive enclosures

The 3004 Series controllers support cabling of 6 Gb SAS link-rate SFF and LFF expansion modules—in mixed model fashion—as shown in [Figure 10](#) on page 24. The simplified rear-panel views of the J6G24 and J6G12 are identical.

Cable requirements for storage enclosures


The 3004 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 or 4 drive enclosures requires 1 m (3.28') cables.
- You may need to order additional or longer cables when reverse-cabling a fault-tolerant configuration (see [Figure 10](#) on page 24).
- 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 standard cable and fan-out cable options supporting SFF-8644 and SFF-8088 host connection (also see [HD mini-SAS host connection](#) on page 32):
 - A qualified SFF-8466 to SFF-8466 cable option is used for connecting to a 12 Gbit/s enabled host.
 - A qualified SFF-8644 to SFF-8088 cable option is used for connecting to a 6 Gbit/s enabled host.
 - A qualified bifurcated SFF-8644 to SFF-8644 fan-out cable option is used for connecting to a 12 Gbit/s enabled host.
 - A qualified bifurcated SFF-8644 to SFF-8088 fan-out cable option is used for connecting to a 6 Gbit/s enabled host.

NOTE: Using fan-out cables instead of standard cables will double the number of hosts that can be attached to a single system. Use of fan-out cables will halve the maximum bandwidth available to each host, but overall bandwidth available to all hosts is unchanged.

See [HD mini-SAS host connection](#) on page 32 and [SAS fan-out cable option](#) for more information about bifurcated SAS cables.

 **TIP:** Requirements for cabling 3004 Series controller enclosures and supported drive enclosures are summarized in [Table 4](#) on page 22.

[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) is also provided.

Table 4 Summary of cabling connections for 3004 Series enclosures

Model	Form	Host connect	SFF 24-disk drive enclosure	LFF 12-disk drive enclosure
3824 ^{1,2}	2U24	FC (8/16 Gb) SFP option	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3834 ^{1,2}	2U12	FC (8/16 Gb) SFP option	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3824 ^{1,2}	2U24	10GbE iSCSI SFP option	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3834 ^{1,2}	2U12	10GbE iSCSI SFP option	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3824 ^{1,2}	2U24	1 Gb iSCSI SFP option	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3834 ^{1,2}	2U12	1 Gb iSCSI SFP option	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3524 ^{1,3}	2U24	12 Gb HD mini-SAS	mini-SAS to mini-SAS	mini-SAS to mini-SAS
3534 ^{1,3}	2U12	12 Gb HD mini-SAS	mini-SAS to mini-SAS	mini-SAS to mini-SAS
J6G24	2U24		mini-SAS to mini-SAS	mini-SAS to mini-SAS
J6G12	2U12		mini-SAS to mini-SAS	mini-SAS to mini-SAS
<u>Enclosure chassis designators:</u> 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 81 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 29 for information about locating and installing qualified SFP options into CNC ports.

³See [HD mini-SAS host connection](#) on page 32 for information about qualified options for cabling to HD mini-SAS host-interface ports.

Summary of drive enclosure cabling illustrations

The following illustrations show both *reverse* and *straight-through* cabling examples featuring 3004 Series controller enclosures and compatible J6G24 (2U24) and J6G12 (2U12) drive enclosures. The rear-panel views of the J6G24 and J6G12 are identical. All storage enclosures use mini-SAS connectors for expansion.

NOTE: The 3004 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 15. Also see the controller module face plate illustrations that follow the rear panel layout.

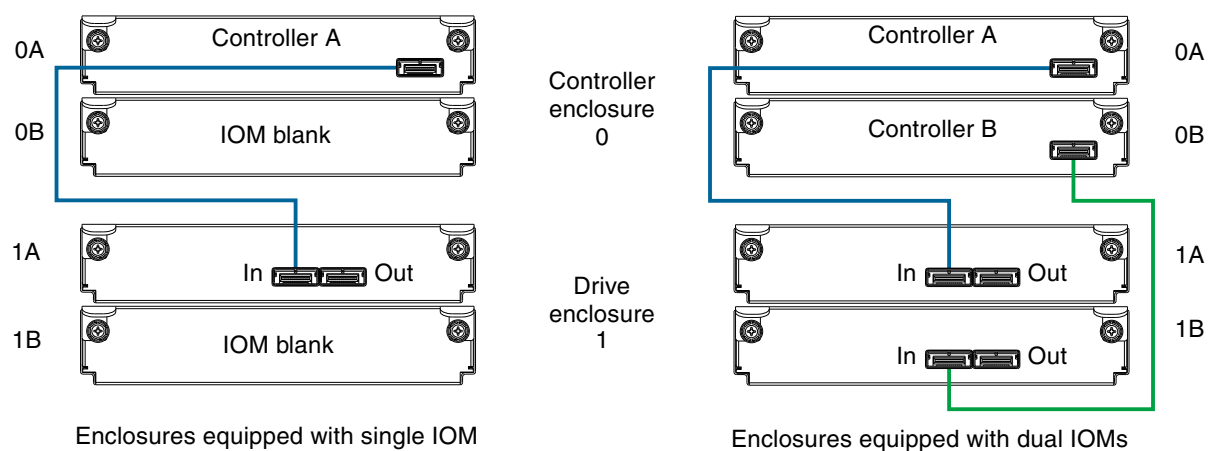


Figure 9 Cabling connections between a controller enclosure and one drive enclosure

The figure above shows examples of a 3004 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 3004 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 FRU Installation and Replacement Guide* for additional information.

NOTE: See [Figure 10](#) on page 24 for a diagram showing the maximum number of 3004 Series enclosures that can be cabled together in the rack.

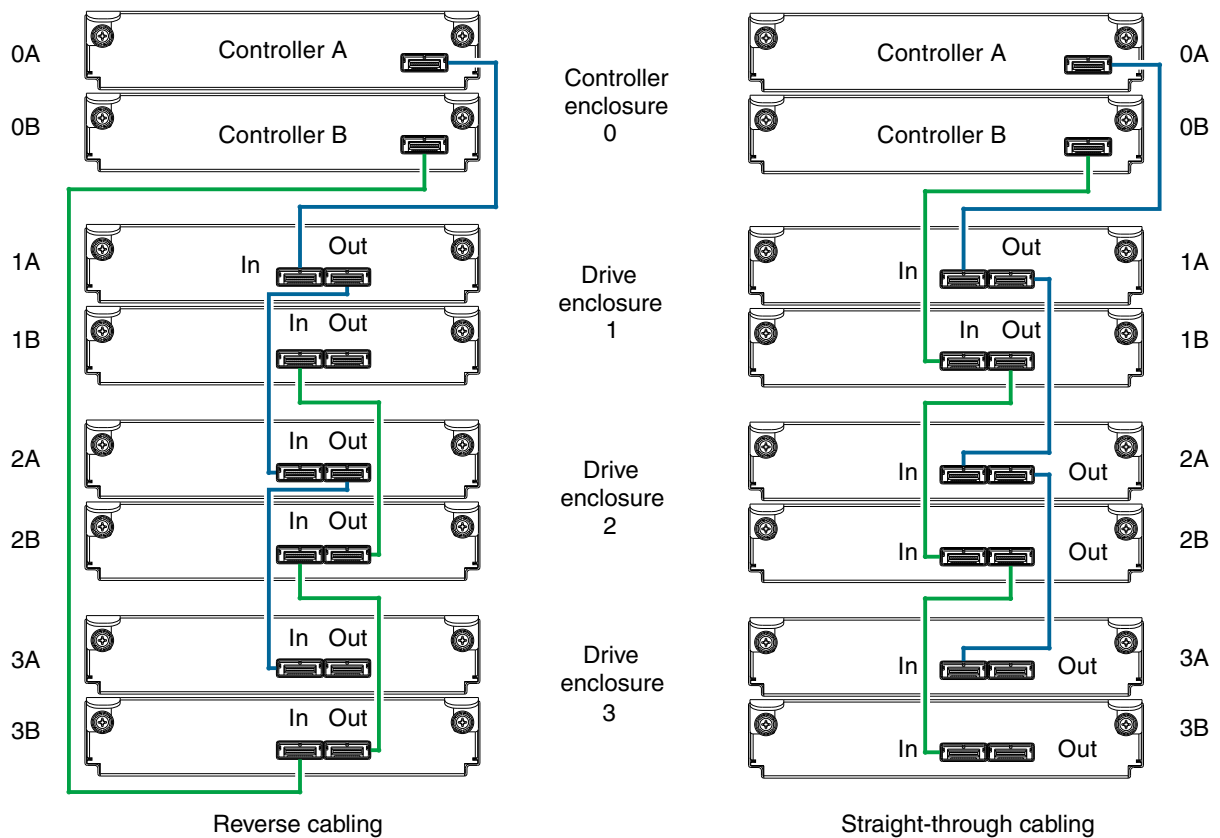


Figure 10 Fault-tolerant cabling between a dual-controller enclosure and four drive enclosures

The two diagrams in [Figure 10](#) show cabling configurations for the maximum number of 3004 Series enclosures allowed: four enclosures (including the controller enclosure).

The diagram at left (above) shows reverse cabling of a 3004 Series dual-controller enclosure and J6G24 or J6G12 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 (3B), 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 J6G24 models or all J6G12 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 3004 Series controller enclosure.

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 3004 Series controller enclosures use PSUs that have no power switch.

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 29.


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 67 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 25. 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 26.

 **IMPORTANT:** See the following PSU-specific subsections for more information about power cables supported by 3004 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.

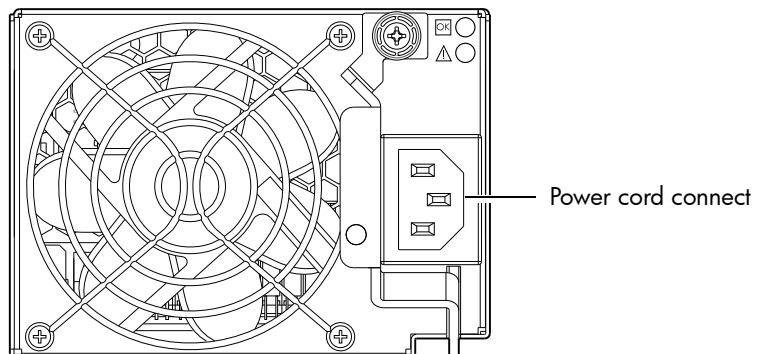


Figure 11 AC PSU

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

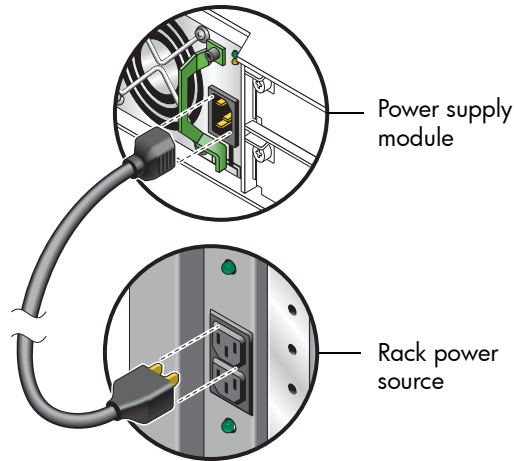


Figure 12 AC power cord

To power off the system:

1. Stop all I/O from hosts to the system (see [Stopping I/O](#) on page 49).
2. Shut down both controllers using *either* method described below:
 - Use the SMC or RAIDar to shut down both controllers, as described in the online help and *AssuredSAN Storage Management Guide*. Proceed to [step 3](#).
 - Use the command-line interface (CLI) to shut down both controllers, as described in the *AssuredSAN 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.

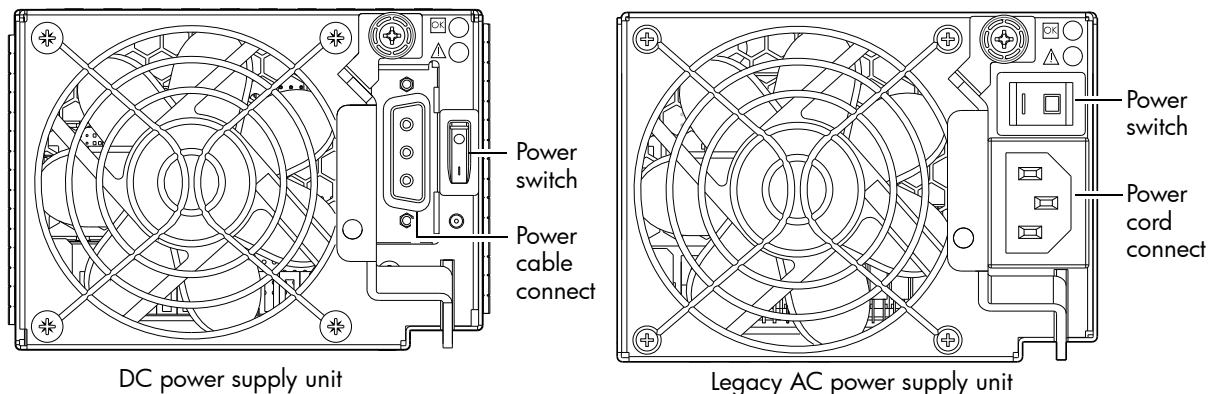


Figure 13 DC and AC PSUs with power switch

Connect power cable to DC power supply

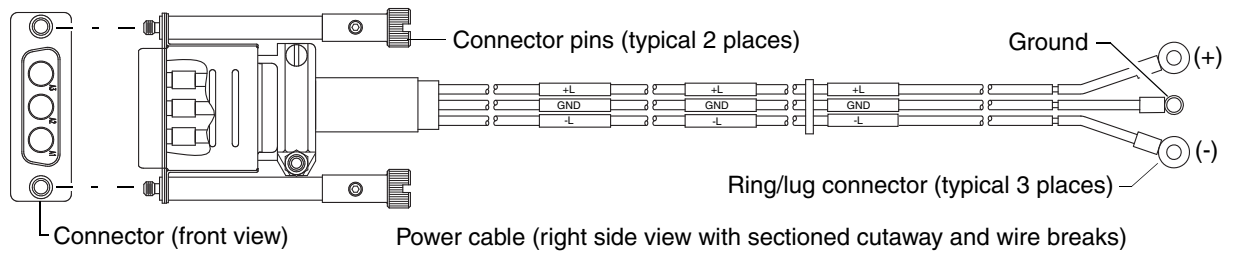
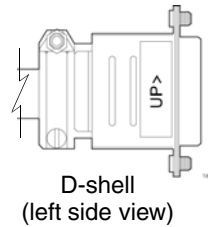


Figure 14 DC power cable featuring D-shell and lug connectors

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.

Check the three individual DC cable wire labels before connecting each cable wire lug to its power source. One cable wire is labeled *ground* (GND), and the other two are labeled *positive* (+L) and *negative* (-L), respectively (shown in [Figure 14](#) above).



△ **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 27.

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 26 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. 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 49).
2. Shut down both controllers using *either* method described below:

- Use the SMC or RAIDar to shut down both controllers, as described in the online help and *AssuredSAN Storage Management Guide*.
Proceed to [step 3](#).
 - Use the command-line interface (CLI) to shut down both controllers, as described in the *AssuredSAN 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 3004 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 2012. 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>

<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 3004 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 36. The 3824/3834 models can be licensed to support replication.

Connecting the enclosure to hosts

A *host* identifies an external port to which the storage system is attached. The external port may be a port in an I/O adapter (such as an FC HBA) in a server. Cable connections vary depending on configuration. This section describes host interface protocols supported by 3004 Series controller enclosures, while showing a few common cabling configurations.

NOTE: 3004 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 disk group ownership.

 **TIP:** See “Using the Configuration Wizard” in the *AssuredSAN Storage Management Guide* to initially configure the system or change system configuration settings (such as Configuring host ports).

CNC technology

AssuredSAN 3824/3834 models use Converged Network Controller technology, allowing you to select the desired host interface protocol 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 9 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 89.

 **IMPORTANT:** Use the `set host-port-mode` CLI command to set the host interface protocol for CNC ports using qualified SFP options. AssuredSAN 3824/3834 models ship with CNC ports configured for FC. When connecting CNC ports to iSCSI hosts, you must use the CLI (not the SMC or 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 43 for instructions).

NOTE: AssuredSAN 3824/3834 models support the optionally-licensed replication feature. Replication sets can also be created and viewed using CLI commands.

Fibre Channel protocol


AssuredSAN 3824/3834 controller enclosures support one or two controller modules using the Fibre Channel interface protocol for host connection. Each controller module provides two host ports designed for use with an FC SFP supporting data rates up to 16 Gbit/s. When configured with FC SFPs, 3824/3834 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. Point-to-point protocol can also be used for direct connection, and it is the only option supporting direct connection at 16 Gbit/s. See the `set host-parameters` command within the *AssuredSAN CLI Reference Guide* for command syntax and details about parameter settings relative 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 SMC or RAIDar Configuration Wizard to set FC port speed. Within the Storage Management Guide, see “Configuring host ports.” Use the `set host-parameters` CLI command to set FC port options, and use the `show ports` CLI command to view information about host ports.

10GbE iSCSI protocol

AssuredSAN 3824/3834 controller enclosures support one or two controller modules using the Internet SCSI interface protocol for host connection. Each controller module provides two 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 Storage Management Guide.

TIP: Use the SMC or RAIDar Configuration Wizard to set iSCSI port options. Within the Storage Management Guide, see “Configuring host ports.” Use the `set host-parameters` CLI command to set iSCSI port options, and use the `show ports` CLI command 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 3824/3834 controller enclosures support one or two controller modules using the Internet SCSI interface protocol for host port connection. Each controller module provides two 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 Storage Management Guide. Also see the admonition about CHAP preceding the “Using the Replication Setup Wizard” procedure within that guide.

TIP: Use the SMC or RAIDar Configuration Wizard to set iSCSI port options. Within the Storage Management Guide, see “Configuring host ports.” Use the `set host-parameters` CLI command to set iSCSI port options, and use the `show ports` CLI command 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 3524/3534 models use high-density mini-SAS (Serial Attached SCSI) interface protocol for host connection.

12 Gb HD mini-SAS ports

Each controller module provides two 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. Host ports can be configured via management interfaces to use standard cables (see [SAS cables with single connector at each end](#) on page 32) or fan-out cables (see [SAS cables with fan-out connectors](#) on page 32).

Connecting direct attach configurations

AssuredSAN 3004 Series controller enclosures support up to four direct-connect server connections, two 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 3824/3834 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 3824/3834 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 3824/3834 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 3524/3534 controller modules supporting HD mini-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. Management interfaces distinguish between *standard* (dual cable with a single connector at each end) and *fan-out* SAS cables. The fan-out SAS cable is comprised of a single SFF-8644 connector that branches into two cable segments, each of which is terminated by a connector. The terminating connectors attach to the host or switch, and are either both of type SFF-8644 or SFF-8088. The storage system must be cabled using either standard cables or fan-out cables: a mixture of cable types is not supported. Qualified cable options for each of these SAS cable categories are described herein.

SAS cables with single connector at each end

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').

SAS cables with fan-out connectors

Use of a bifurcated fan-out cable doubles the number of host ports that can be connected to an HD mini-SAS controller module. A qualified SFF-8644 to SFF-8644 fan-out cable option is used for attaching to a 12 Gbit/s enabled host; whereas a qualified SFF-8644 to SFF-8088 fan-out cable option is used for attaching to a 6 Gbit/s host. Qualified fan-out cable options support lengths of 1 m (3.28'), 2 m (6.56'), and 4 m (13.12').

 **IMPORTANT:** Before attaching a fan-out cable, make sure to update firmware for the SAS HBA—and switch if applicable—for devices that will be attached to the fan-out cable.

See the Storage Management Guide or CLI Reference Guide for more information about the fan-out setting and changing of host-interface settings for 3524/3534 controller modules.

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

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.

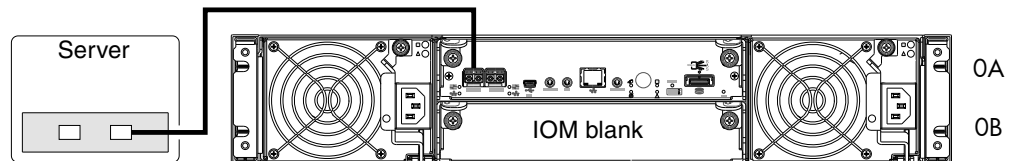
Within each cabling connection category, the HD mini-SAS model is shown beneath the CNC model.

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

3824/3834



3524/3534

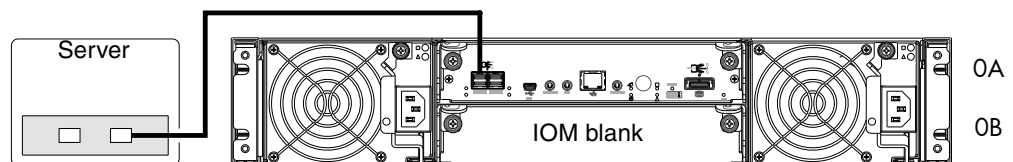


Figure 15 Connecting hosts: direct attach—one server/one HBA/single path

Figure 15 shows host connection of 3524/3534 models using standard SAS cables; whereas Figure 16 shows host connection using fan-out SAS cables.

3524/3534

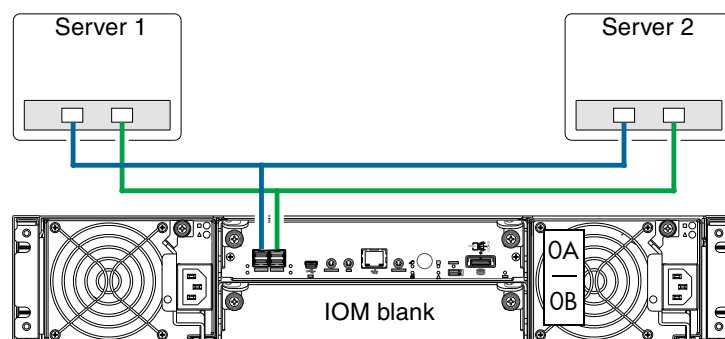


Figure 16 Connecting hosts: direct attach—two servers/two HBAs/dual path (fan-out)

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

IMPORTANT: If the 3004 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 FRU Installation and Replacement Guide* for additional information about installing IOMs.

Dual-controller configurations

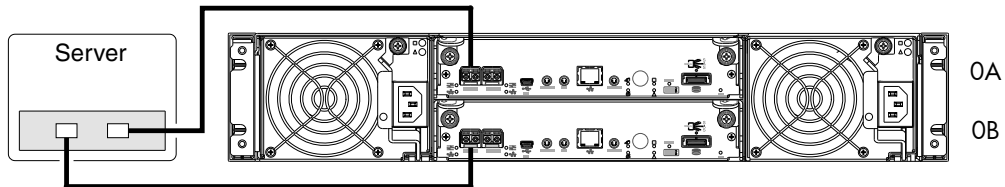
A dual-controller configuration improves application availability because in the event of a controller failure, the affected controller fails over to the partner controller with little interruption to data flow. A failed controller can be replaced without the need to shut down the storage system.

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 Storage Management Guide*).

The illustrations below show dual-controller configurations for 3004 Series controller enclosures equipped with CNC ports and HD mini-SAS ports.

One server/multiple HBAs/dual path

3824/3834



3524/3534

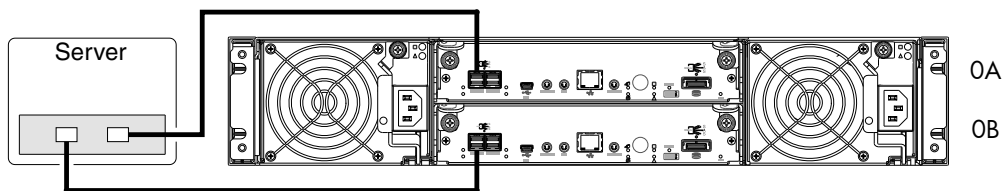
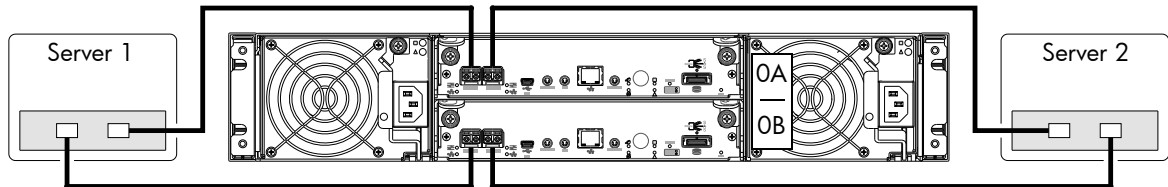


Figure 17 Connecting hosts: direct attach—one server/one HBA/dual path

Two servers/one HBA per server/dual path

3824/3834



3524/3534

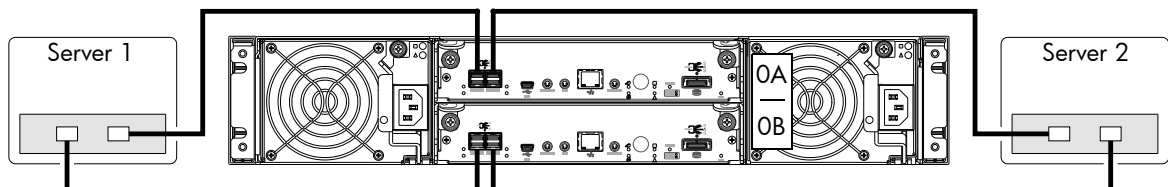


Figure 18 Connecting hosts: direct attach—two servers/one HBA per server/dual path

Figure 18 shows host connection of 3524/3534 models using standard SAS cables (bottom diagram); whereas Figure 19 shows host connection using fan-out SAS cables.

3524/3534

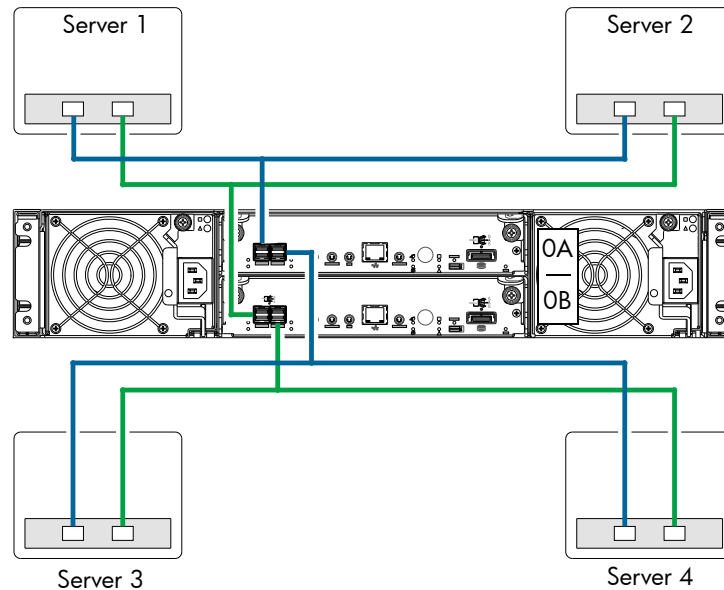


Figure 19 Connecting hosts: direct attach—four servers/one HBA per server/dual path (fan-out)

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 3004 Series controller enclosure supports 64 hosts.

Dual-controller configuration

Two servers/two switches

3824/3834

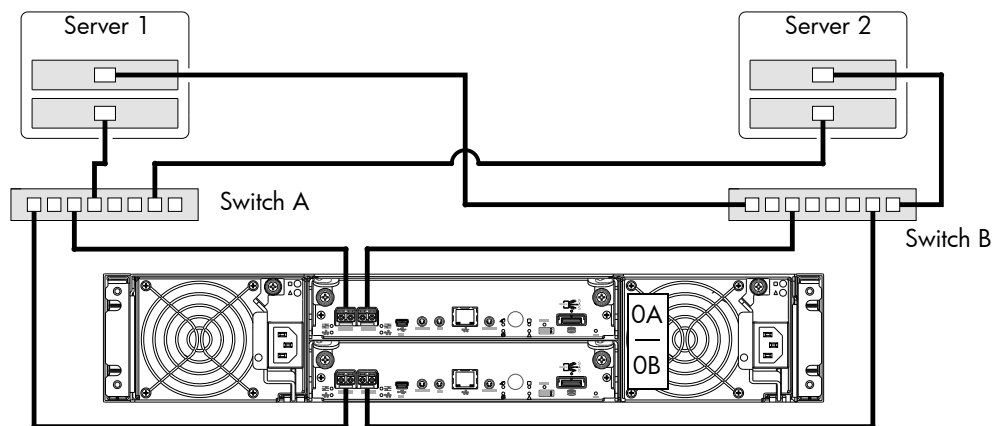


Figure 20 Connecting hosts: switch attach—two servers/two switches

3004 Series controller enclosure iSCSI considerations

When installing a 3004 Series iSCSI controller enclosure, use at least three ports per server—two for the storage LAN, and one of 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 20).

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

The 3824/3834 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 [Figure 5](#) on page 16 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

In addition to setting the port-specific options described above, you can view settings using the GUI.

- If using the SMC, in the **System** topic, select **Action > Set Up Host Ports**.
The Host Ports Settings panel opens, allowing you to access host connection settings.
- If using RAIDar, in the Configuration View panel, right-click the system and select **Configuration > System Settings > Host Interfaces**.
The Configure Host Interface panel opens, allowing you to access host connection settings.

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 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: <https://crc.dothill.com>.

Connecting two storage systems to replicate volumes

AssuredRemote™ replication is a licensed feature for disaster recovery, providing access to either of the following software product versions:

- SMC (v3) supports replication for virtual storage environments.
- RAIDar (v2) supports replication for linear storage environments.

IMPORTANT: These two replication models are mutually exclusive to one another. Choose the method that applies to your storage system. For more information, see replication topics in the Storage Management Guide.


The replication feature performs asynchronous replication of block-level data from a volume in a primary system to a volume in a secondary system by creating an internal snapshot of the primary volume, and copying the snapshot data to the secondary system via FC (linear storage only) or iSCSI links.

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 the replication feature, 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 systems on the same network, or on physically-split networks (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.
- Whereas linear storage supports FC and iSCSI host interface ports for replication, virtual storage supports iSCSI host interface ports for replication. Both linear and virtual storage support all qualified CNC options for host connection.
- If using the RAIDar (v2) user interface, be sure of the desired link type before creating the linear replication set, because you cannot change the replication link type after creating the replication set.
- 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.
- Ensure that all ports assigned for replication are able to communicate appropriately with the replication system (see the CLI Reference Guide for more information):
 - For linear replication, use the `verify remote-link` command.
 - For virtual replication, use the `query peer-connection` command.
- 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.
- 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. The cabling examples provided apply to linear replication and virtual replication.

 **IMPORTANT:** Controller module firmware must be compatible on all systems used for replication. For license information, see the Storage Management Guide.

Cabling for replication

This section shows example replication configurations for CNC-based controller enclosures. The following illustrations provide conceptual examples of cabling supporting linear replication and virtual replication. Blue cables show I/O traffic and green cables show replication traffic.

NOTE: Simplified versions of controller enclosures are used in cabling illustrations to show either FC or iSCSI host interface protocol, given that only the external connectors used in the host interface ports differ.

- Cabling for replication diagrams pertain to linear replication and virtual replication.
 - Linear replication supports FC and iSCSI host interface protocols.
 - Virtual replication supports iSCSI host interface protocol.
 - The 2U enclosure rear panel view represents 3824/3834 models.
The rear panel layouts for the two enclosures are identical.
-

Once the CNC systems are physically cabled, see the Storage Management Guide or online help for information about configuring, provisioning, and using the optional replication feature. Refer to the replication feature topic pertaining to your environment (linear replication or virtual replication).

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 host 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).

In linear storage environments [RAIDar (v2)], 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. In virtual storage environments [SMC (v3)], each CNC port can perform I/O, but replication traffic is supported by iSCSI host interface ports (either both 10GbE or both 1 Gbit/s).

Single-controller configuration

One server/single network/two switches

The diagrams below shows the rear panel of two controller enclosures with both I/O and replication occurring on the same network. Each enclosure is equipped with a single controller module.

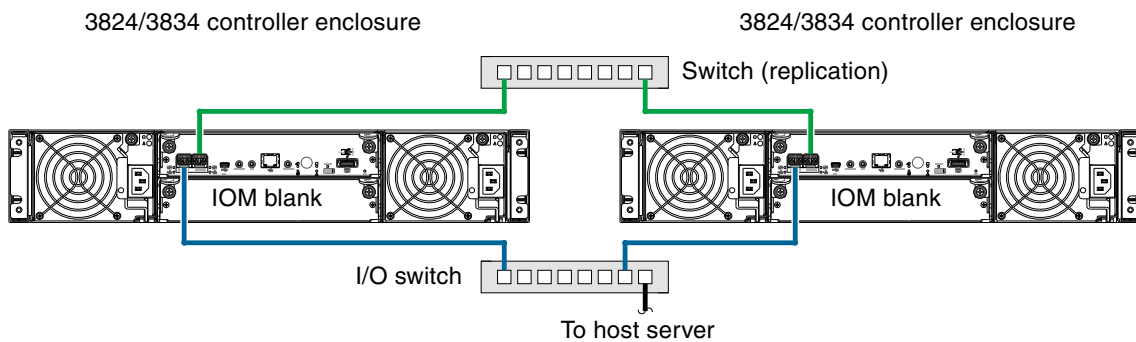


Figure 21 Connecting two storage systems for replication: one server/two switches/one location

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 3004 Series controller enclosures equipped with dual-controller modules.

IMPORTANT: Whereas linear storage supports FC and iSCSI host interface protocols for replication, virtual storage supports iSCSI host interface protocol for replication. Both linear and virtual storage support all qualified CNC options for host connection.

Multiple servers/single network

Figure 22 shows the rear panel of two 3824/3834 controller enclosures with both I/O and replication occurring on the same physical network.

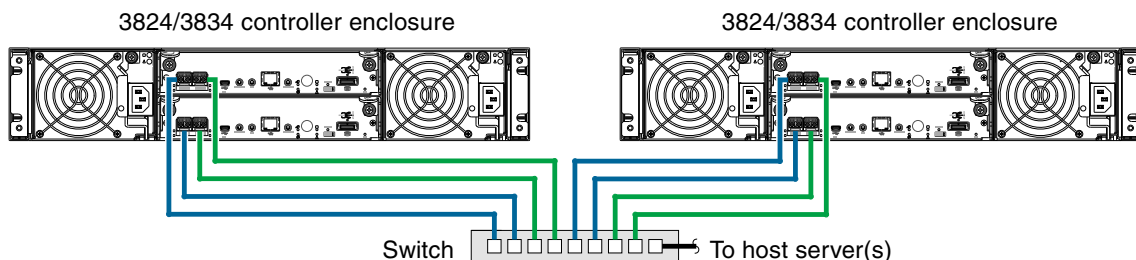


Figure 22 Connecting two storage systems for replication: multiple servers/one switch/one location

Figure 23 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 one port from each controller module to the first switch to facilitate I/O traffic, and connect one port 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.

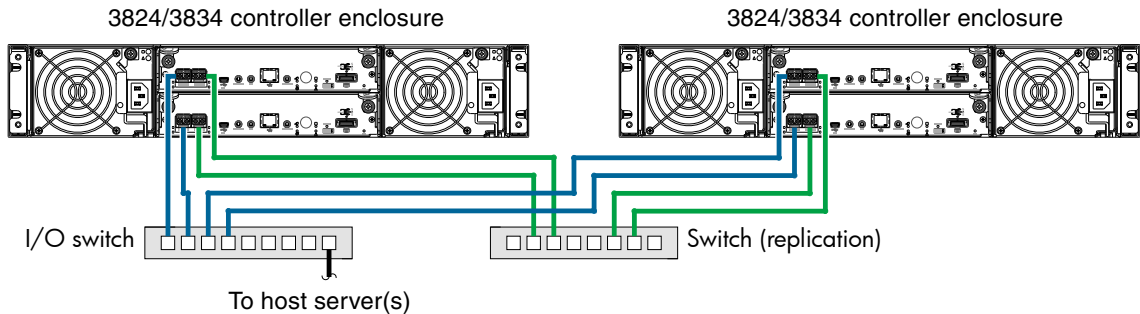


Figure 23 Connecting two storage systems for replication: multiple servers/switches/one location

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

Figure 24 shows the rear panel of two 3824/3834 controller enclosures with I/O and replication occurring on different networks.

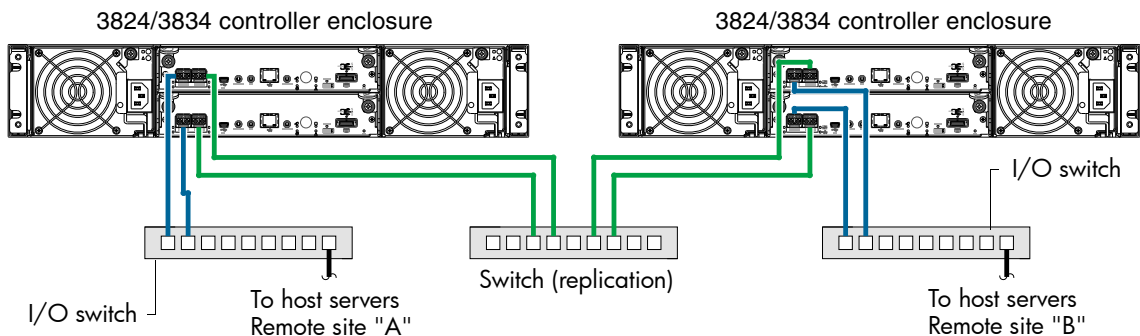


Figure 24 Connecting two storage systems for replication: multiple servers/switches/two locations

Although not shown in the preceding cabling examples, you can cable replication-enabled 3004 Series systems and compatible 4000 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.

- If using the SMC (v3), in the **System** topic, select **Action > Update Firmware**.


The Update Firmware panel opens. The Update Controller Module tab shows versions of firmware components currently installed in each controller.

NOTE: The SMC does *not* provide a check-box for enabling or disabling Partner Firmware Update for the partner controller. To enable or disable the setting, use the `set advanced-settings` command, and set the `partner-firmware-upgrade` parameter. See the CLI Reference Guide for more information about command parameter syntax.

- If using RAIDar (v2), 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 Storage Management Guide*.

 **IMPORTANT:** See the “Updating firmware” topic in the *AssuredSAN Storage Management Guide* before performing a firmware update.

Obtaining IP values

You can configure addressing parameters for each controller module’s network port. The network port supports 10 Mb/s, 100 Mb/s, or 1000 Mb/s link speed. You can set static IP values or use DHCP.

 **TIP:** See the “Configuring network ports” topic in the *AssuredSAN Storage Management 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 3004 Series systems, you must either use the CLI (Command-line Interface) to change controller IP address settings, or use the Configuration Wizard as described in the *Storage Management 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 88).

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 87.
 - Linux customers should prepare the USB port as described in [Setting parameters for the device driver](#) on page 88.
-

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 the SMC or RAIDar. Be sure to change the IP address via the SMC or RAIDar before changing the network configuration. See [Accessing the SMC or RAIDar](#) on page 45 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 the SMC, 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 25](#) on page 41 (generic 3004 Series controller module shown).

Connect USB cable to CLI
port on controller face plate

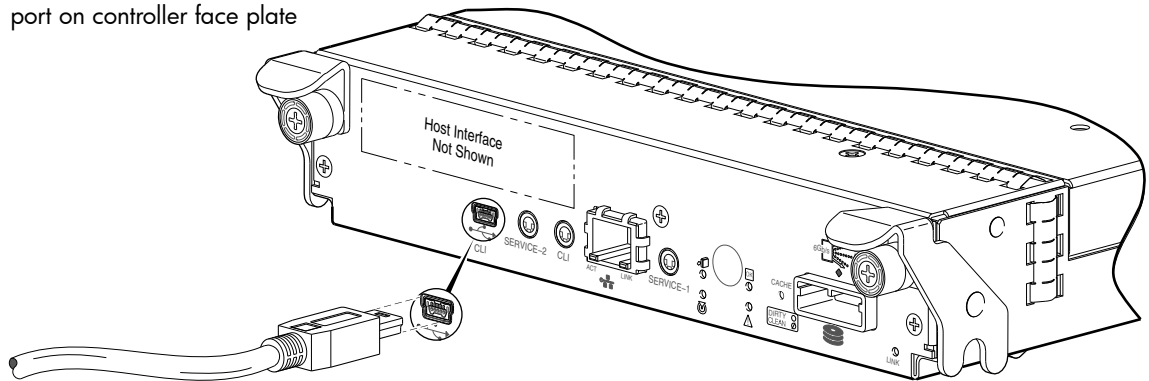


Figure 25 Connecting a USB cable to the CLI port

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 88.
 - Windows customers should locate the downloaded device driver described in [Obtaining the software download](#) on page 87, 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.

NOTE: The following CLI commands enable you to set the management mode to v3 or v2:

- Use `set protocols` to change the default management mode.
- Use `set cli-parameters` to change the current management mode for the CLI session.

The system defaults to v3 for new customers and v2 for existing users (see the CLI Reference Guide for more information).

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, 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 43.

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 the SMC, 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 25](#) on page 41.

Change the CNC port mode

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 iSCSI.

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](#).

Configure the system

NOTE:

- After using the CLI command sequence 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 the SMC or RAIDar, and use the Configuration Wizard to initially configure the system, or change system configuration settings as described in the *AssuredSAN Storage Management Guide* and [Basic operation](#).

4 Basic operation


Verify that you have successfully completed the sequential “Installation Checklist” instructions in [Table 3](#) on page 20. 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 the SMC or RAIDar

Upon completing the hardware installation, you can access the controller module’s web-based management interface [either the SMC (v3) or RAIDar (v2)] 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 the SMC or 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 either the SMC or RAIDar, see the “Getting Started” section in the web-posted *AssuredSAN Storage Management 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 the SMC or 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 the SMC or RAIDar, you can use online help as an alternative to consulting the Storage Management Guide.

Configuring and provisioning the storage system

Once you have familiarized yourself with either the SMC or RAIDar GUI, 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 Storage Management 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 Storage Management 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 Storage Management Guide or the command topic “set-advanced-settings” in the CLI Reference Guide.

5 Troubleshooting

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

NOTE: For further troubleshooting help, after initial setup and when user data is present, contact Dot Hill support as specified at <https://crc.dothill.com>.

USB CLI port connection

AssuredSAN 3004 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 3004 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 45, use the SMC or 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 Storage Management 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 47)
- Determine where in the system the fault is occurring
(see [Determine where the fault is occurring](#) on page 47)
- Review event logs
(see [Review the event logs](#) on page 48)
- If required, isolate the fault to a data path component or configuration
(see [Isolate the fault](#) on page 48)

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 replication faults](#) on page 56 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 the SMC or 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, either the SMC or RAIDar, and the CLI provide recommended-action text online. Options for performing basic steps are listed according to frequency of use:

- Use the SMC or RAIDar

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

Use the SMC or RAIDar

The SMC and RAIDar use health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. The SMC and RAIDar enable you to monitor the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown. Use the web application'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 the SMC or 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 Recommendations 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 the SMC, RAIDar, or the CLI. Using either the SMC or 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 the SMC, 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 14](#)). 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 the SMC or RAIDar to verify any faults found while viewing the LEDs. The SMC and RAIDar are also good tools to use in determining where the fault is occurring if the LEDs cannot be viewed due to the location of the system. These web-applications provide you with a visual representation of the system and where the fault is occurring. The SMC and RAIDar 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: <https://crc.dothill.com>.

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 or disk group if a user changes channel settings without taking the storage resources assigned to it into consideration. In addition, the type of fault can help you isolate the problem to either hardware or software.

Isolate the fault

Occasionally, it might become necessary to isolate a fault. This is particularly true with data paths, due to the number of components comprising the data path. For example, if a host-side data error occurs, it could be caused by any of the components in the data path: controller module, cable, 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 the SMC, 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 the SMC (v3):

1. Verify that both controllers are operating normally.
2. Do one of the following:
 - Point to the **System** tab and select **Rescan Disk Channels**.
 - In the **System** topic, select **Action** > **Rescan Disk Channels**.
3. Click **Rescan**.


To rescan using RAIDar (v2):

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 disk groups 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 disk group 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 disk-group-statistics` command to determine if input and output has stopped. Perform these steps:

1. Using the CLI, run the `show disk-group-statistics` command.
The `Reads` and `Writes` outputs show the number of these operations that have occurred since the statistic was last reset, or since the controller was restarted. Record the numbers displayed.
2. Run the `show disk-group-statistics` command a second time.
This provides you a specific window of time (the interval between requesting the statistics) to determine if data is being written to or read from the disk group. Record the numbers displayed.
3. To determine if any reads or writes occur during this interval, subtract the set of numbers you recorded in [step 1](#) from the numbers you recorded in [step 2](#).
 - If the resulting difference is zero, then I/O has stopped.
 - If the resulting difference is not zero, a host is still reading from or writing to this disk group. Continue to stop I/O from hosts, and repeat [step 1](#) and [step 2](#) until the difference in [step 3](#) is zero.

NOTE: See *AssuredSAN 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 either the SMC or 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 the SMC, 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 LEDs (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 76).
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 the SMC or 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 53.

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 the SMC or 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 55.

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.• Verify 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.

 **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).

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 ; 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 .
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.
Yes, at a blink 1:1 rate - 1 Hz, and the controller does not boot.	See Transporting cache .
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”

NOTE: See also [Cache Status LED details](#) on page 77.

Transporting cache

To preserve the existing data stored in the CompactFlash, you must transport the CompactFlash from the failed controller to a replacement controller using the procedure outlined in the *AssuredSAN FRU Installation and Replacement Guide*. Failure to use this procedure will result in the loss of data stored in the cache module.

△ **CAUTION:** Remove the controller module only after the copy process is complete, which is indicated by the Cache Status LED being off, or blinking at 1:10 rate.

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 3004 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.

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

1. Halt all I/O to the storage system (see [Stopping I/O](#) on page 49).
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 3524/3534 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 49).
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 49).
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 replication faults

Cabling for replication

The replication feature is a licensed option for disaster-recovery, providing access to either of the following software product versions:

- SMC (v3) supports replication for virtual storage environments.
- RAIDar (v2) supports replication for linear storage environments.

IMPORTANT: These two replication models are mutually exclusive to one another. Choose the method that applies to your storage system. For more information, see replication topics in the Storage Management Guide.

Replication setup and verification

After storage systems are cabled for replication, you can use the SMC (v3) or RAIDar (v2) to prepare to use the replication feature. Alternatively, you can use telnet to access the IP address of the controller module and access the replication feature using the CLI.

NOTE: You can use the CLI to perform replication in linear or virtual storage environments.

- Set Management mode to v2 for linear replication (use Manage role).
 - Set Management mode to v3 for virtual replication (use Manage role).
-

Basic information for enabling the 3004 Series controller enclosures for replication supplements the troubleshooting procedures that follow.


- Familiarize yourself with replication by reviewing the “Getting started”, “Working in the Replications topic”, and “Using AssuredRemote to replicate volumes” chapters in the Storage Management Guide.
- For virtual replication, in order to replicate an existing volume to a pool on the peer in the primary system or secondary system, follow these steps:
 - Find the port address.
Using the CLI, run the `query peer-connection` command.
 - Create a peer connection.

To create a peer connection, use the CLI command `create peer-connection` or in the SMC **Replications** topic, select **Action > Create Peer Connection**.

- Create a virtual replication set.
To create a replication set, use the CLI command `create replication-set` or in the SMC **Replications** topic, select **Action > Create Replication Set**.
- Replicate.
To initiate replication, use the CLI command `replicate` or in the SMC **Replications** topic, select **Action > Initiate Replication**.
- For linear replication, in order to replicate an existing volume to another disk group in the primary or secondary system, follow these steps:
 - Use RAIDar’s **Wizards > Replication Setup Wizard** to prepare to replicate an existing volume to another disk group 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 Reference Guide.

NOTE: These steps are a general outline of the replication setup. Refer to the following manuals for more information about replication setup:

- See the Storage Management Guide for procedures to setup and manage replications.
 - See the CLI Reference Guide for replication commands and syntax.
 - See the Event Descriptions Reference Guide for replication event reporting.
-

 **IMPORTANT:** Controller module firmware must be compatible on all systems used for replication. For license information, see the Storage Management Guide.

Diagnostic steps for replication setup

The table cells in the following subsections show menu navigation using the SMC (v3), and using RAIDar (v2). The shorthand v3 and v2 prefixes are used to distinguish between the SMC and RAIDar, respectively.

Virtual replication using the SMC

Can you successfully use the replication feature?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The replication feature 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 Home topic in the SMC, select Action > Install License. The License Settings panel opens and displays information about each licensed feature. If the Replication feature is not enabled, obtain and install a valid license for this feature. See the Storage Management guide for license information. <hr/> <p>NOTE: Virtual replication is only supported by 3004 series iSCSI controller enclosures.</p> <hr/>
No	Compatible firmware revision supporting the replication feature is not running on each system used for replication.	<p>Perform the following actions on each system used for virtual replication:</p> <ul style="list-style-type: none"> In the System topic, select Action > Update Firmware. The Update Firmware panel opens. The Update Controller Modules tab shows firmware versions installed in each controller. If necessary, update the controller module firmware to ensure compatibility with the other systems. For more information on compatible firmware, see the topic about updating firmware in the Storage Management Guide.
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 that cabling paths between replication ports and switches are visible to one another. Verify that cable connections are securely fastened. Inspect cables for damage and replace if necessary.

Table 18 Diagnostics for replication setup: Using the replication feature (v3)

Can you view information about remote links?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Communication link is down	<ul style="list-style-type: none"> Verify controller enclosure cabling (see Table 18). Review event logs for indicators of a specific fault in a host or replication data path component. In the footer, click the events panel and select Show Event List. This will open the Event Log Viewer panel. Verify valid IP address of the network port on the remote system. Click in the Volumes topic, then click on a volume name in the volumes list. Click the Replication Sets tab to display replications and associated metadata. Alternatively, click in the Replications topic to display replications and associated metadata.

Table 19 Diagnostics for replication setup: Viewing information about remote links (v3)

Can you create a replication set?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	On controller enclosures with iSCSI host interface ports, replication set creation fails due to use of CHAP.	If using CHAP (Challenge-Handshake Authentication Protocol), see the topics about configuring CHAP and working in replications within the Storage Management Guide.
No	Unable to create the secondary volume (the destination volume in the virtual disk group to which you will replicate data from the primary volume)? ¹	<ul style="list-style-type: none"> Review event logs (in the footer, click the events panel and select Show Event List) for indicators of a specific fault in a replication data path component. Follow any Recommended Actions. Verify valid specification of the secondary volume according to either of the following criteria: <ul style="list-style-type: none"> A conflicting volume does not already exist Creation of the new volume in the disk group
No	Communication link is down.	<ul style="list-style-type: none"> See actions described in Can you view information about remote links? on page 59.
¹ After ensuring valid licensing, valid cabling connections, and network availability, create the replication set using the Replications topic, select Action > Create Replication Set .		

Table 20 Diagnostics for replication setup: Creating a replication set (v3)

Can you replicate a volume?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The replication feature is not licensed on each controller enclosure used for replication.	See actions described in Can you successfully use the replication feature? on page 58.

Table 21 Diagnostics for replication setup: Replicating a volume (v3)

Answer	Possible reasons	Actions
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 Replications topic, select Action > Create Replication Set to create one. Review event logs (in the footer, click the events panel and select Show Event List) for indicators of a specific fault in a replication data path component. Follow any Recommended Actions.
No	Network error occurred during in-progress replication.	<ul style="list-style-type: none"> Review event logs for indicators of a specific fault in a replication data path component. Follow any Recommended Actions. Click in the Volumes topic, then click on a volume name in the volumes list. Click the Replication Sets tab to display replications and associated metadata. Replications that enter the suspended state can be resumed manually.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 59.

Table 21 Diagnostics for replication setup: Replicating a volume (v3) (continued)

Has a replication set run successfully

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Last successful run shows N/A.	<ul style="list-style-type: none"> In the Volumes topic, click on the volume that is a member of the replication set. <ul style="list-style-type: none"> Select the Replication Sets table. Check the Last Successful Run information. If a replication has not run successfully, use the SMC to replicate as described in the “Working in the Replications topic” in the Storage Management Guide
No	Communication link is down.	See actions described in Can you view information about remote links? on page 59.

Table 22 Diagnostics for replication setup: Checking for a successful replication (v3)

Linear replication using RAIDar

Can you successfully use the replication feature?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The replication feature 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 the 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 this feature. <p>NOTE: Linear replication is not supported by 3004 series SAS controller enclosures.</p>
No	Compatible firmware revision supporting replication is not running on each system used for replication.	<p>Perform the following actions on each system used for virtual replication:</p> <ul style="list-style-type: none"> In the Configuration View panel in the 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 23 Diagnostics for replication setup: Using the replication feature (v2)

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 18). Review event logs (in the Configuration View panel, right-click on the system, and select View > Event Log) 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, right-click the remote system, and select Tools > Check Remote System Link. Click Check Links.

Table 24 Diagnostics for replication setup: Viewing information about remote links (v2)

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, 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, 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 Storage Management Guide 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"> Review event logs (in the Configuration View panel, right-click the system, and select View > Event Log) 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 disk group 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 disk group. Verify selection of valid remote volume on disk group. Verify valid IP address of remote system network port. Verify user name with Manage role on remote system. Verify user password on remote system. <p>NOTE: If the remote system has not been added, it cannot be selected.</p>
No	Unable to select the secondary volume (the destination volume on the disk group to which you will replicate data from the primary volume)? ¹	<ul style="list-style-type: none"> Review event logs for indicators of a specific fault in a replication data path component. Follow any Recommended Actions. Verify valid specification of the secondary volume according to either of the following criteria: <ul style="list-style-type: none"> Creation of the new volume on the disk group 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 59.
¹ After ensuring valid licensing, valid cabling connections, and network availability, create the replication set using the Wizards > Replication Setup Wizard .		

Table 25 Diagnostics for replication setup: Creating a replication set (v2)

Can you replicate a volume?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	The replication feature is not licensed on each controller enclosure used for replication.	See actions described in Can you successfully use the replication feature? on page 58.
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 Replication Setup Wizard to create one. Review event logs (in the Configuration View panel, right-click the system, and select View > Event Log) for indicators of a specific fault in a replication data path component. Follow any Recommended Actions.
No	Network error occurred during in-progress replication.	<ul style="list-style-type: none"> Review event logs for indicators of a specific fault in a replication data path component. Follow any Recommended Actions. In the Configuration View panel, 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 59.

Table 26 Diagnostics for replication setup: Replicating a volume (v2)

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, expand disk groups 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 Storage Management Guide.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 59.

Table 27 Diagnostics for replication setup: Viewing a replication image (v2)

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 59.

Table 28 Diagnostics for replication setup: Viewing a remote system (v2)

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 either the SMC or RAIDar to check enclosure health status.
 - v3: In the lower corner of the footer, overall health status of the enclosure is indicated by a health status icon. For more information, point to the **System** tab and select **View System** to see the System panel. You can select **Front**, **Rear**, and **Table** views on the System panel. If you hover over a component, its associated metadata and health status displays onscreen.
 - v2: 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 46 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.
6. Replace SFPs 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 29 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 30 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 31 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 32 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 33 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 3004 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 J6G12 12-drive enclosure is the LFF drive enclosure used for storage expansion. The J6G24 24-drive enclosure is the SFF drive enclosure used for storage expansion.

Enclosure bezels

Each AssuredSAN 3004 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 26](#)); whereas the bezel fitting the 2U12 chassis provides two debossed pockets, is equipped with an EMI (Electromagnetic Interference) shield, and may or may not be equipped with the serviceable dust filtration air filter option ([Figure 27](#)).

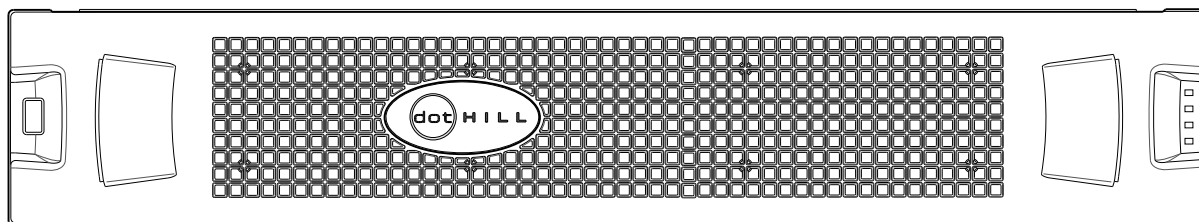


Figure 26 Front panel enclosure bezel: 24-drive enclosure (2U24)

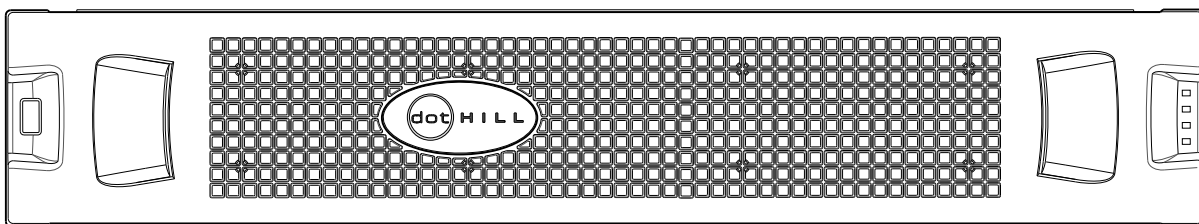


Figure 27 Front panel enclosure bezel: 12-drive enclosure (2U12)

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 26](#)
- Front view of 12-drive enclosure (2U12): [Figure 27](#)
- Bezel alignment for 24-drive enclosure (2U24): [Figure 28](#) on page 68
- Bezel alignment for 12-drive enclosure (2U12): [Figure 29](#) on page 68

Enclosure bezel attachment

Orient the enclosure bezel to align its back side with the front face of the enclosure as shown in [Figure 28](#) on page 68 and [Figure 29](#) on page 68. 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.

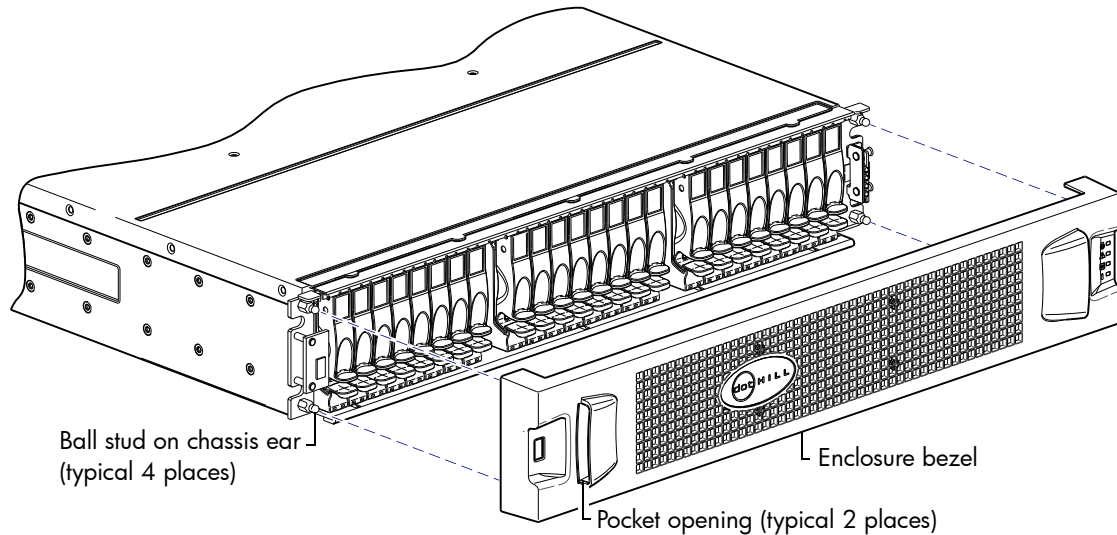


Figure 28 Partial assembly showing bezel alignment with 2U24 chassis

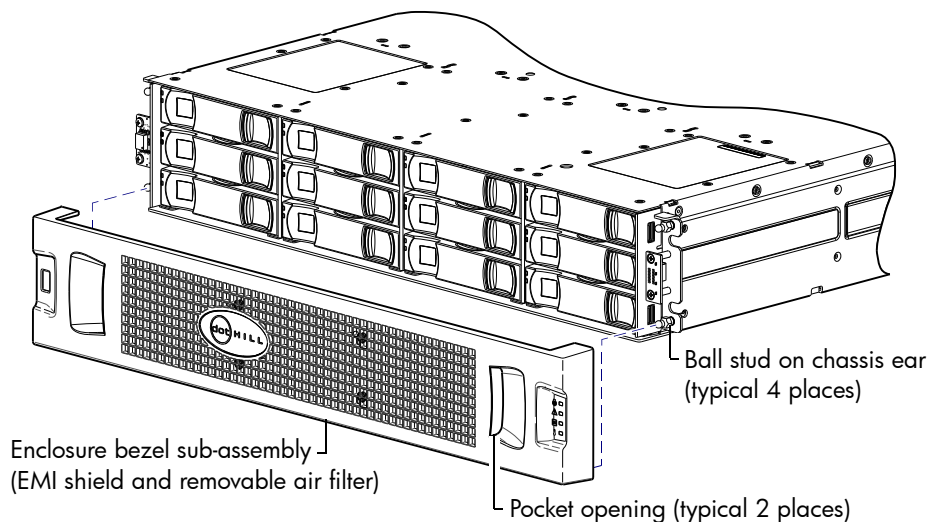


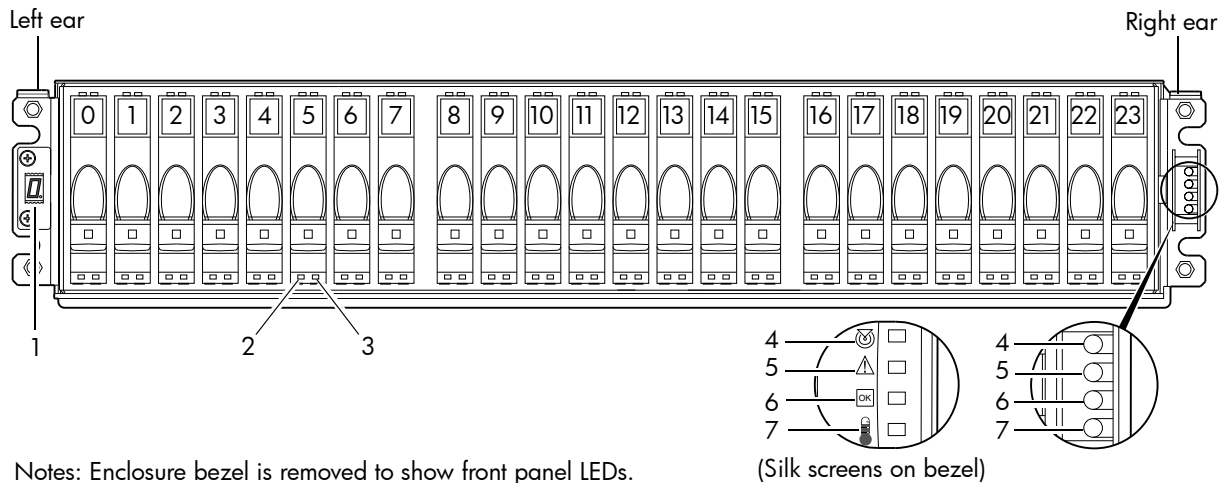
Figure 29 Partial assembly showing bezel alignment with 2U12 chassis

NOTE: For more information about servicing or replacing the removable air filter option for this particular bezel ([Figure 29](#)), 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.



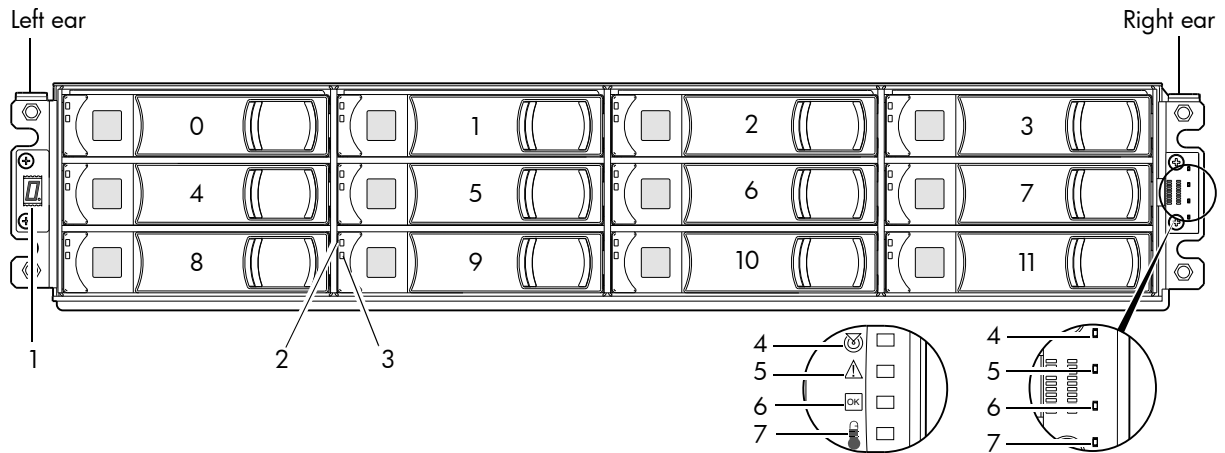
Notes: Enclosure bezel is removed to show front panel LEDs.
Integers on disks indicate drive slot numbering sequence.

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 71.
3	Disk drive — Right LED	See Disk drive LEDs on page 71.
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 30 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 71.
3	Disk drive — Lower LED	See Disk drive LEDs on page 71.
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.

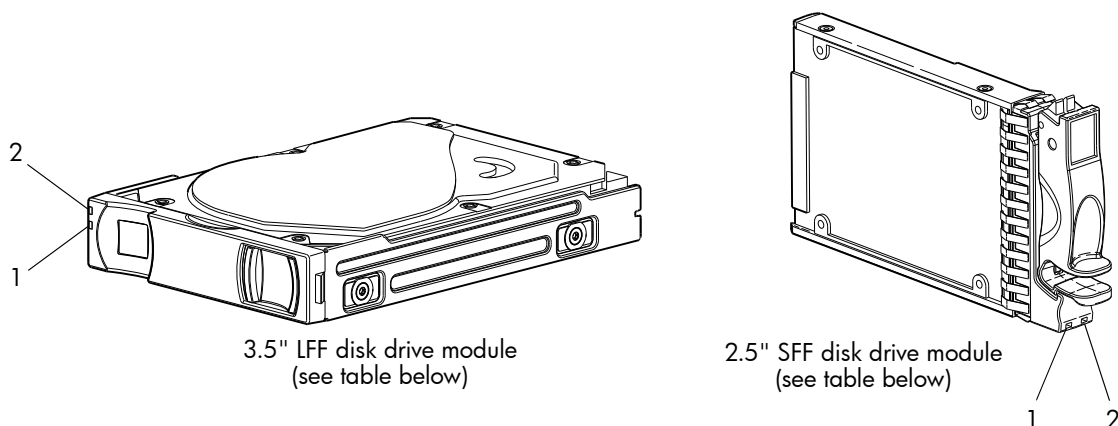
Figure 31 LEDs: 2U12 enclosure front panel

The enclosure bezel for this model provides the EMI protection from the product. The bezel should be securely attached to the enclosure during operation (see [Enclosure bezel attachment](#) on page 67 and [Figure 29](#) on page 68).

△ **CAUTION:** Whether configured with or without an air filter, to ensure adequate EMI protection from the product, 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 disk group 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 disk group 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 disk group is located (alternates blinking amber).

Figure 32 LEDs: Disk drive modules

For information about disk drive types supported in 3004 Series LFF and SFF disk drive modules, see [Disk drives used in 3004 Series enclosures](#) on page 14.

For information about replacing a disk drive module in a 3004 Series controller enclosure or J6G24/J6G12 drive enclosure, refer to the “Replacing a disk drive module” topic in the *AssuredSAN FRU Installation and Replacement Guide*. Instructions are provided for replacing LFF and SFF disk drive modules therein.

For information about creating a disk group, or a vdisk with volumes, and mapping the volumes to hosts, see the “Provisioning the system” topic within the *AssuredSAN Storage Management Guide*.

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

Table 34 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.

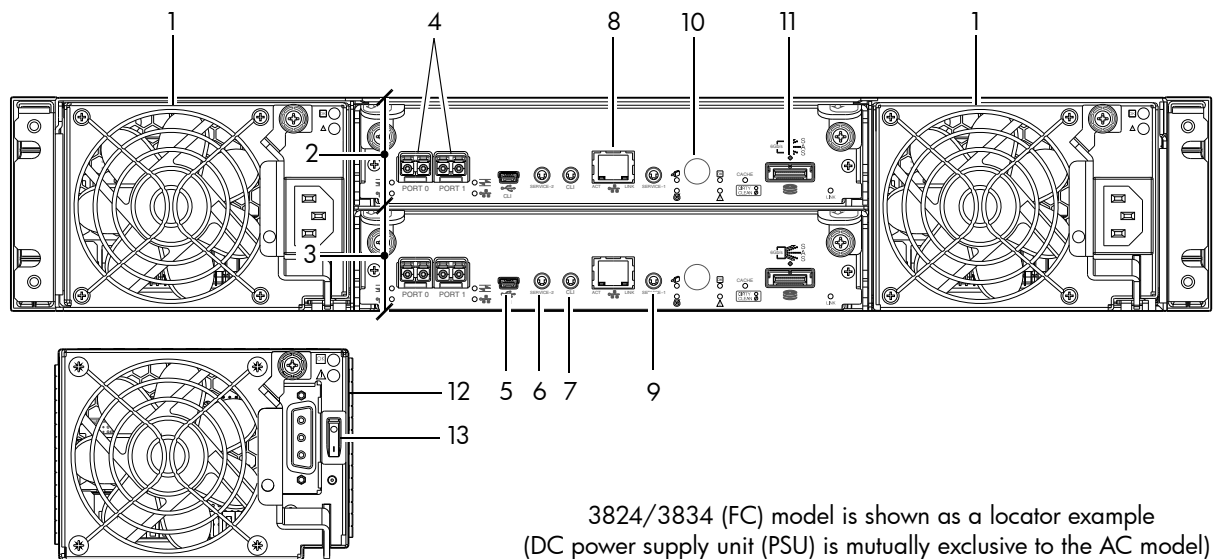
Table 35 LEDs: Disk groups in SFF and LFF enclosures

Disk group LED behavior		LFF/SFF disks	
Description	State	Color	Action
FTOL	On (operating normally)	Green	On
Disk group activity	Disk group is reconstructing	Green	Blink
	Disk group is initializing	Green	Blink
Disk group degraded	Disk group 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 3004 Series controller enclosure. In [Figure 33](#) below, a 3824/3834 (FC) 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 33 3004 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).

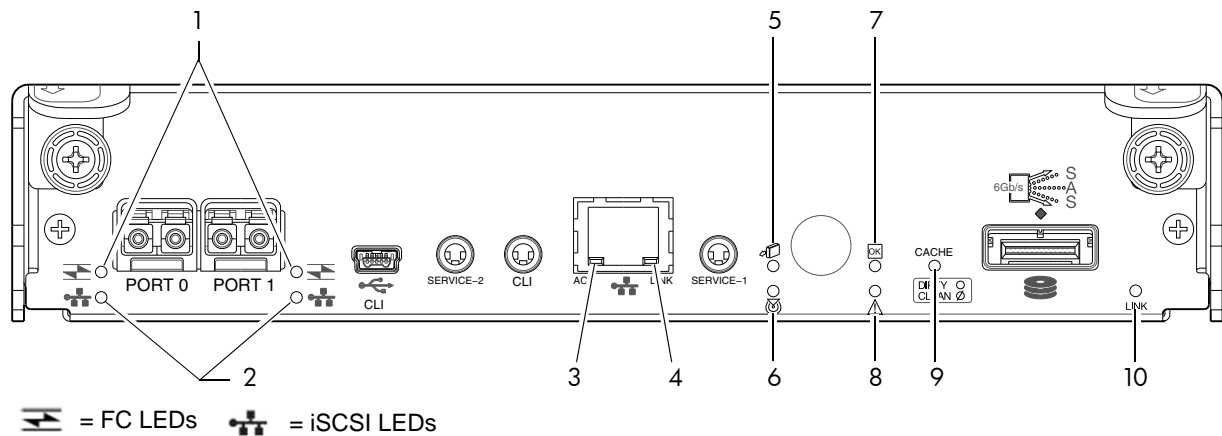
IMPORTANT: If the 3004 Series controller enclosure is configured with a single controller module, the controller module must be installed in the upper slot (see callout No.2 above) and the I/O module blank must be installed in the lower slot (see callout No.3 above). This configuration is required to allow sufficient air flow through the enclosure during operation (also see [Figure 9](#) on page 23).

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 3004 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 3004 Series controller enclosures.

For information about replacing 3004 Series controller enclosure FRUs, refer to the appropriate FRU replacement procedure in the *AssuredSAN FRU Installation and Replacement Guide*.

3824/3834 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 ⁴	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 ⁴	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 77.
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.

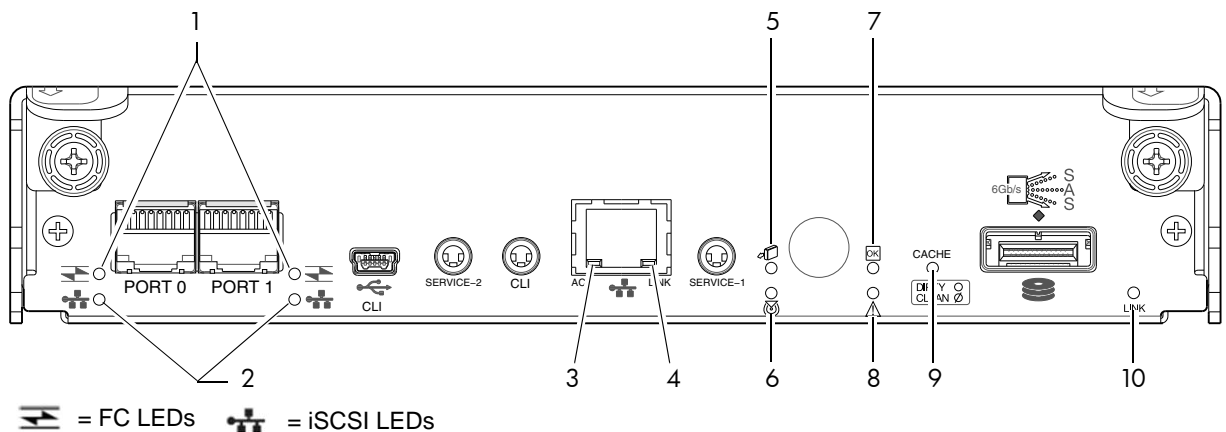
²When in 10GbE iSCSI mode, the SFPs must be a qualified 10GbE iSCSI optic option.

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

⁴When port is down, both LEDs are off.

Figure 34 LEDs: 3824/3834 CNC controller module (FC and 10GbE SFPs)

NOTE: For information about supported host interface protocols in CNC ports, see [CNC ports used for host connection](#) on page 9 and the “Configuring host ports topic” in the Storage Management Guide.



LED	Description	Definition
1	Not used in example ¹	The FC SFP is not shown in this example (see Figure 34 on page 74).
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 ⁴	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 ⁴	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 77.
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.

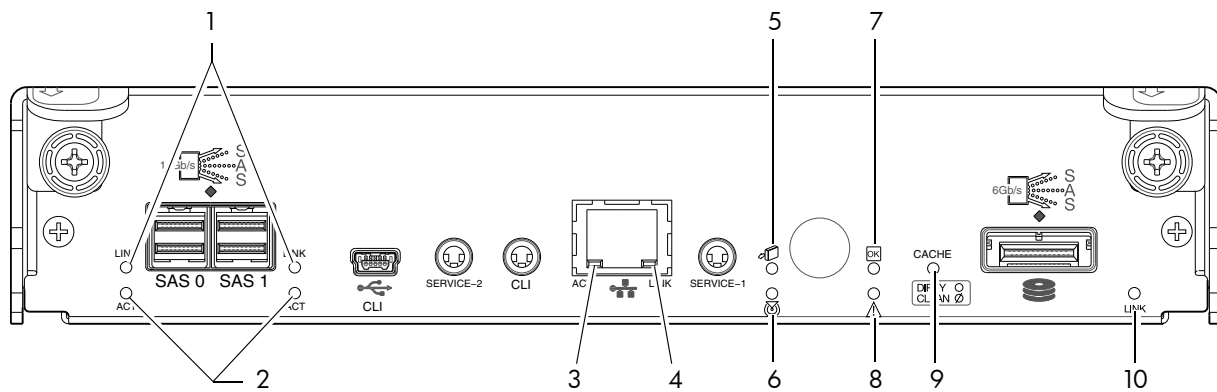
²When in 1 GbE iSCSI mode, the SFPs must be a qualified 1 GbE iSCSI optic option.

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

⁴When port is down, both LEDs are off.

Figure 35 LEDs: 3824/3834 CNC controller module (1 Gb RJ-45 SFPs)

3524/3534 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 ⁴	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 ⁴	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 77.
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 3524/3534 controller to a 12 Gb SAS HBA.

³Use a qualified SFF-8644 to SFF-8088 cable option when connecting the 3524/3534 controller to a 6 Gb SAS HBA.

⁴When port is down, both LEDs are off.

Figure 36 LEDs: 3524/3534 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 the SMC, 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 25).

Cache Status LED details

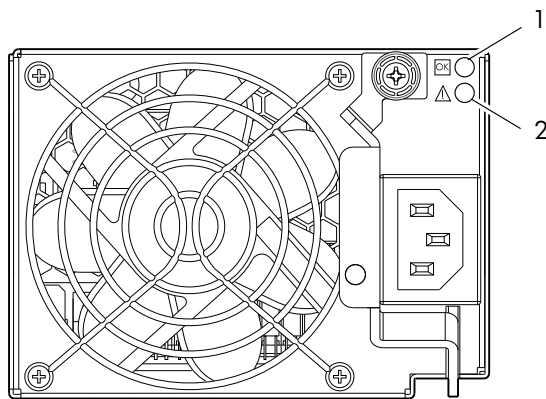
If the LED is blinking evenly, a cache flush is in progress. When a controller module loses power and write cache is dirty (contains data that has not been written to disk), the supercapacitor pack provides backup power to flush (copy) data from write cache to CompactFlash memory. When cache flush is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

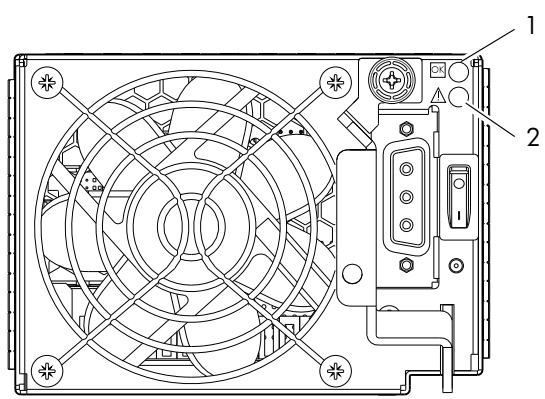
△ **CAUTION:** If the Cache Status LED illuminates solid green—and you wish to shut-down the controller—do so from the user interface, so unwritten data can be flushed to CompactFlash.

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.



AC model



DC model

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.

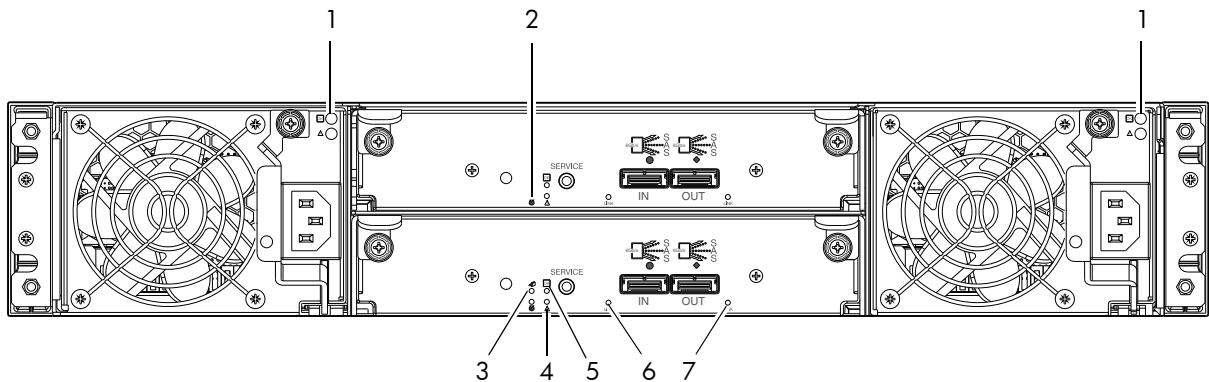
Figure 37 LEDs: Power supply units — rear panel

NOTE: See [Powering on/powering off](#) on page 25 for information on power-cycling enclosures.

J6G24/J6G12 drive enclosure rear panel LEDs

The rear panel layout of the J6G24 (2U24)/J6G12 (2U12) 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 25 for more information.



LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 77.
2 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the expansion module.
3 — OK to Remove	Blue	Off	Not implemented.
4 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up.
5 — FRU OK	Green	On	Expansion module is operating normally.
		Off	Expansion module is not OK.
		Blink	System is booting.
6 — SAS In Port Status	Green	On	Port is connected and the link is up.
		Off	Port is empty or link is down.
7 — SAS Out Port Status	Green	On	Port is connected and the link is up.
		Off	Port is empty or link is down.

Figure 38 LEDs: J6G24/J6G12 drive enclosure — rear panel

B Specifications and requirements

Safety requirements

Install the system in accordance with the local safety codes and regulations at the facility site. Follow all cautions and instructions marked on the equipment.

 **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: <https://crc.dothill.com>.

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 36 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 37 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 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 81 for detailed size and weight specifications.

- Refer to the rackmount bracket kit installation sheet pertaining to your product for guidelines about installing enclosures into the rack.
- 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 83 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.

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.

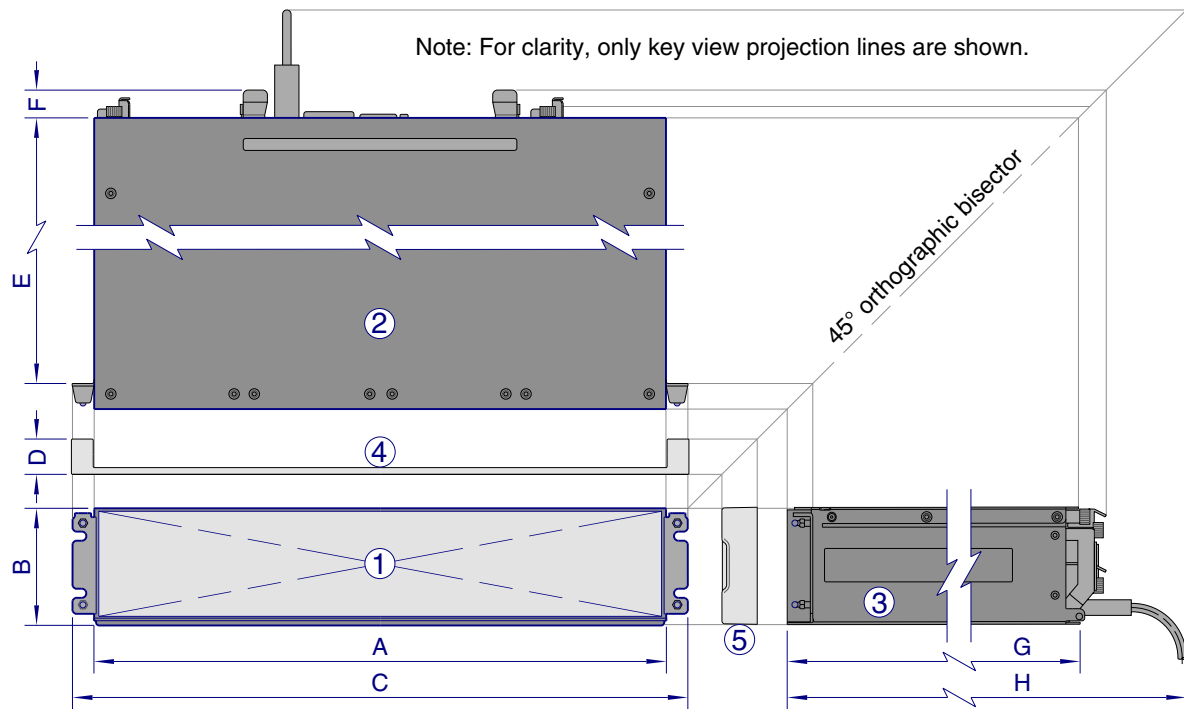
NOTE: Connections to this device must be made with shielded cables – grounded at both ends – with metallic RFI/EMI connector hoods, in order to maintain compliance with FCC Rules and Regulations.

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.

[Figure 39](#) and [Table 38](#) on page 82 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 22):
 - “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 22):
 - “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)

	A		B		C		D		E		F		G		H	
Form	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 39 Rackmount enclosure dimensions

Table 38 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 and air management modules installed.

NOTE: The table below provides information about the optional drive enclosures that are compatible with the 3004 Series controller enclosure.

Table 39 Rackmount compatible drive enclosure weights (ordered separately)

Specifications	Rackmount
J6G24 (SFF 2.5" 24-drive enclosure)	8.6 kg (19.0 lb) [chassis]
• Chassis with FRUs (no disks) ¹⁻³	16.2 kg (35.8 lb)
• Chassis with FRUs (including disks) ¹⁻⁴	22.2 kg (49.0 lb)
J6G12 (LFF 3.5" 12-drive enclosure)	8.5 kg (18.8 lb) [chassis]
• Chassis with FRUs (no disks) ¹⁻³	16.1 kg (35.6 lb)
• Chassis with FRUs (including disks) ¹⁻⁴	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 and air management modules installed.

Environmental requirements

Table 40 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 41 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)

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 100–240 VAC with an input frequency of 50–60 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 uses two power cables designed for use with the enclosure power supply module. 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 3004 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 8](#) on page 18), 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 40](#)).

USB CLI port

Connect USB cable to CLI
port on controller face plate

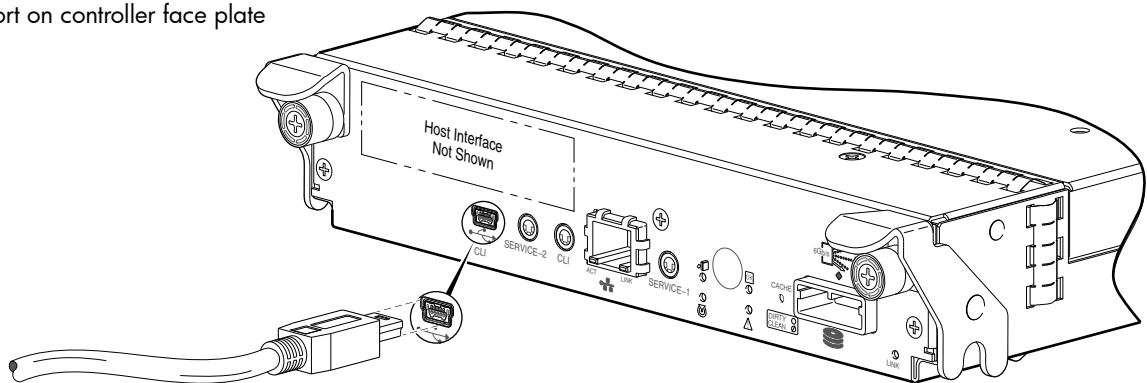


Figure 40 USB device connection — CLI port

AssuredSAN 3004 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 88). For Windows computers a special device driver file, `gserial.inf`, must be downloaded from a web site, and installed on the computer that will be cabled directly to the controller's CLI port (see [Microsoft Windows](#) on page 87).

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 3004 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

3004 Series controllers support the following applications to facilitate connection.

Table 42 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 43 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 3004 Series controller enclosures. Dot Hill provides a device driver for use in the Windows environment. The USB device driver and installation instructions are available via a download.

Obtaining the software download

1. Verify that the management computer has Internet access.
2. See Dot Hill's customer resource center (CRC) web site <https://crc.dothill.com>.
 - a. Select the color-filled **Download Firmware/Software** button on the home page.
Peruse the list of downloads for an entry pertaining to "USB driver."
 - b. Select the color-filled **Download** button on the shaded "USB driver" box.
The File Download dialog displays.
 - c. From the File Download dialog, save the zip file locally to the management computer.
 - d. Follow the instructions accompanying the device driver—within the zip file—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 3004 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 (COMn)” —where *n* is your system’s COM port number.

3. Set network port IP addresses using the CLI (see procedure on [page 40](#)).

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 COMn port assigned to the Disk Array Port.
 - b. Right-click on the hung **Disk Array USB Port (COMn)**, and select **Disable**.
 - c. Wait for the port to disable.
2. Right-click on the previously hung—now disabled—**Disk Array USB Port (COMn)**, 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 40](#)).

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.

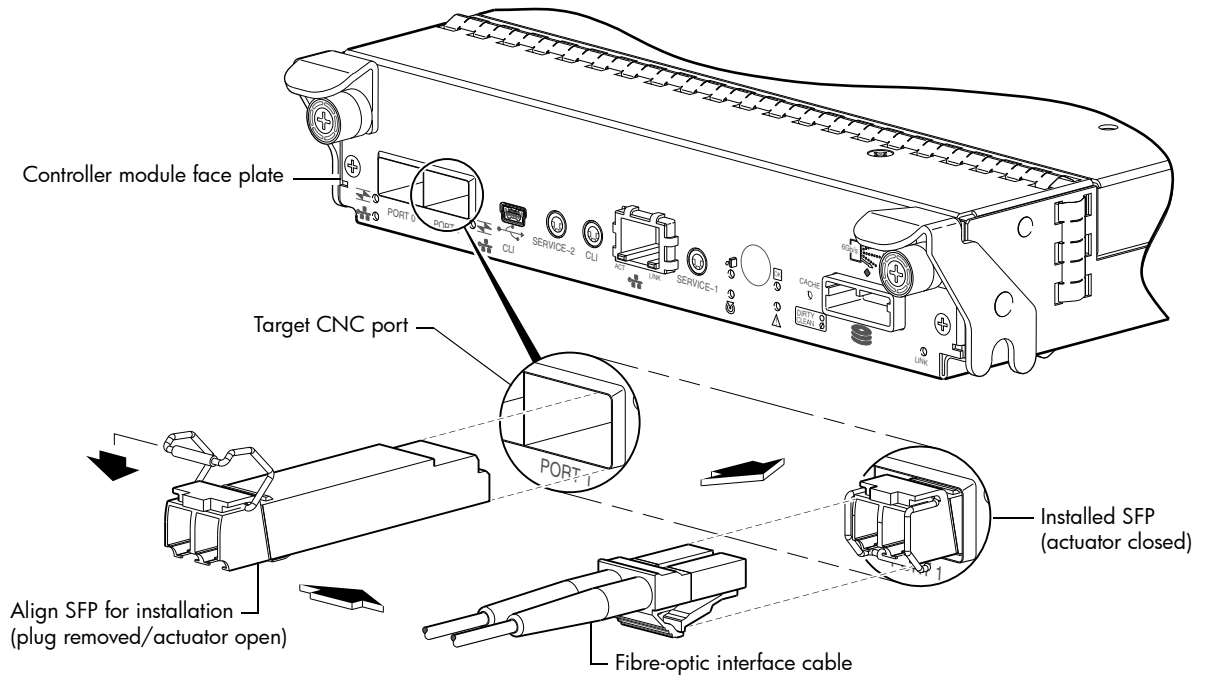


Figure 41 Install a qualified SFP option

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).

F SAS fan-out cable option

Locate the SAS fan-out cable

Locate the appropriate qualified SAS fan-out cable option for your 2-port SAS controller module. Qualified fan-out cable options are described within [Cable requirements for storage enclosures](#) on page 21 and [HD mini-SAS host connection](#) on page 32. Cabling examples showing use of SAS fan-out cables are provided:

- See [Figure 16](#) on page 33: direct attach featuring one server/two HBAs/dual path (single-IOM)
- See [Figure 19](#) on page 35: direct attach featuring four servers/four HBAs/dual path (dual-IOMs)

Install the SAS fan-out cable

Orient the cable for connection to the controller module and host as shown in [Figure 42](#) and [Figure 43](#) on page 91. For each fan-out cable type, the pull-tab is facing upwards when aligned for insertion into the host interface port of the 3524/3534 controller module. The port closer to the pull-tab is the first of the two ports, and the port located away from the pull tab is the second of the two ports.

NOTE: Using qualified fan-out cable options, connect hosts to the same ports on both controllers to align with the usage shown in the SMC or RAIDar.

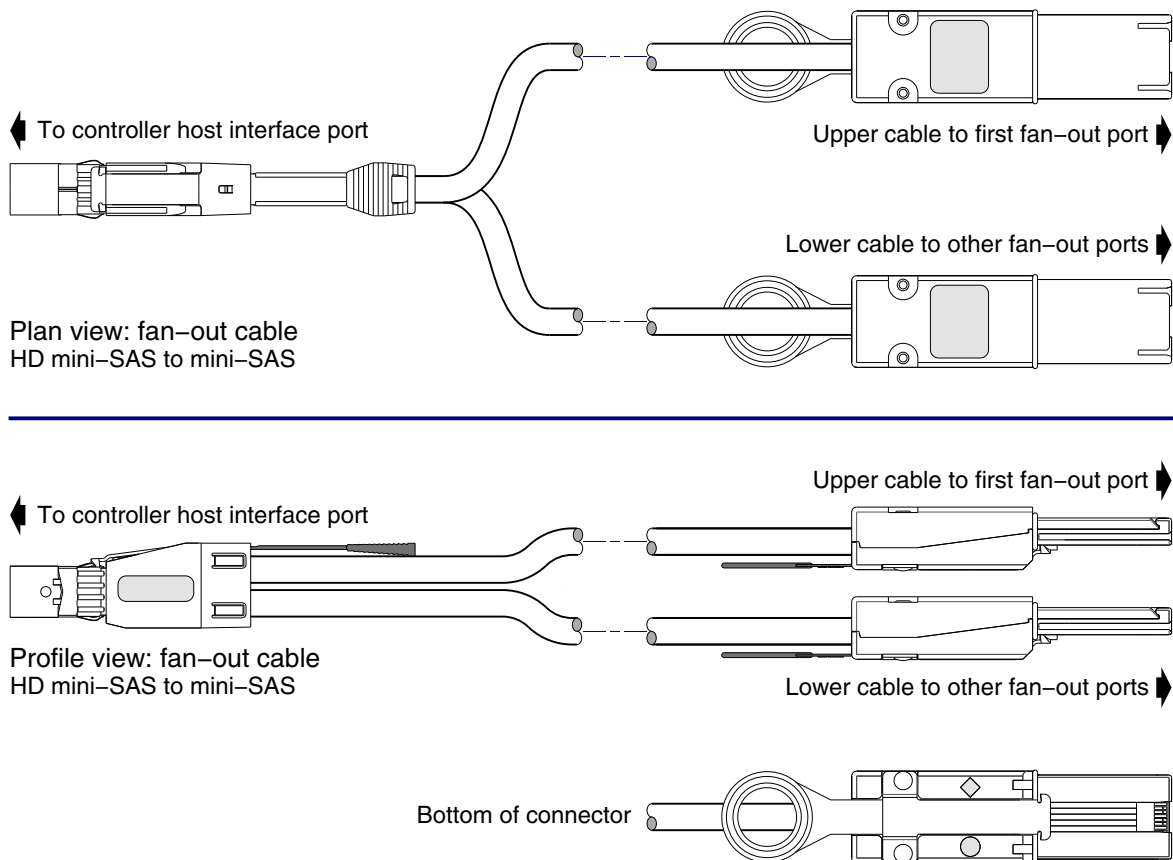


Figure 42 HD mini-SAS to mini-SAS fan-out cable

Simplified plan and profile views of the bifurcated HD mini-SAS to mini-SAS cable show orientation for connection to the controller module (on left) and the host (on right).

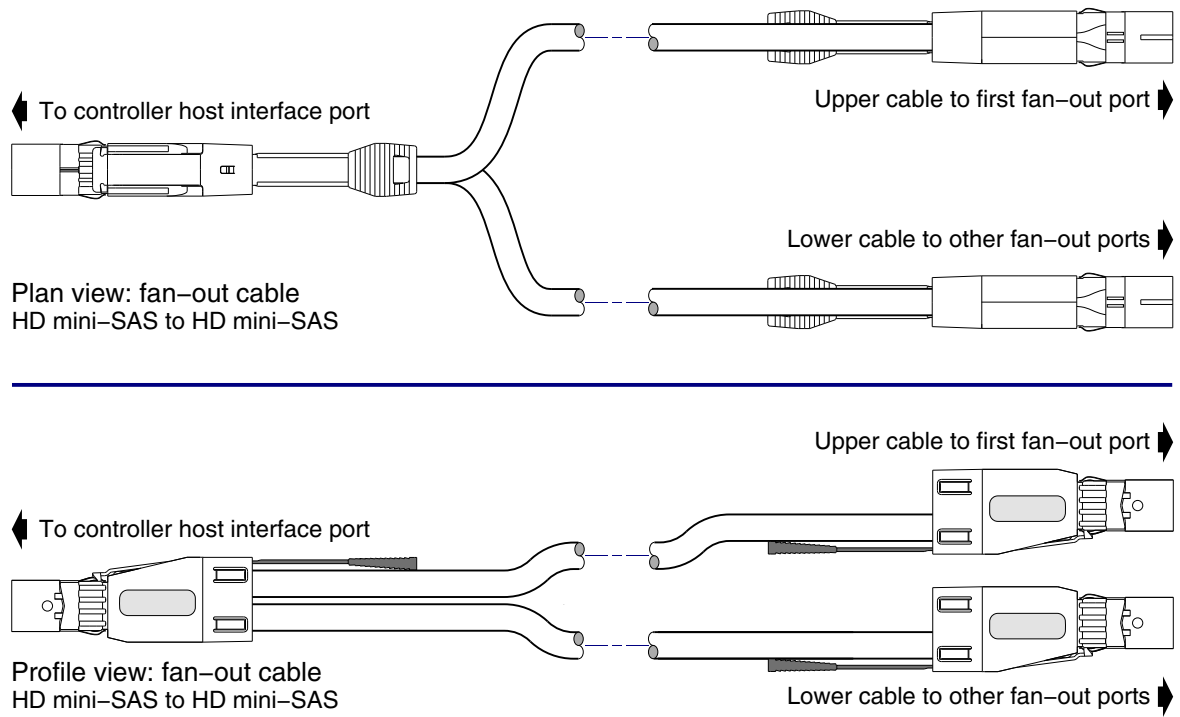


Figure 43 HD mini-SAS to HD mini-SAS fan-out cable

Simplified plan and profile views of the bifurcated HD mini-SAS to mini-SAS cable show orientation for connection to the controller module (on left) and the host (on right).

Index

Numerics

2U12

3.5" 12-drive enclosure 81

2U24

2.5" 24-drive enclosure 81

A

accessing

CLI (Command-line Interface) 41

RAIDar (web-based management GUI) 45

SMC (web-based management GUI) 45

AssuredRemote

licensed replication feature 36

audience 10

B

bezel

2U12 enclosure 67

2U24 enclosure 67

C

cables

FCC compliance statement 36, 81

shielded 36, 81

cabling

cable routing requirements 81

connecting controller and drive enclosures 20

considerations 29

direct attach configurations 31

switch attach configurations 35

cache

post-write 18

read-ahead 18

clearance requirements

service 81

ventilation 81

CNC ports

change port mode 43

locate and install SFPs 89, 90

SFP transceivers 29

Command-line Interface

using to set controller IP addresses 40

CompactFlash

card location 18

transporting 53

components

12-drive enclosure front panel 14

3524/3534 rear panel

12 Gb SAS ports 17

CLI (reserved for future use) 17

CLI port (USB) 17

expansion port 17

network port 17

service port 1 17

service port 2 17

3824/3834 rear panel

CLI (reserved for future use) 16

CLI port (USB) 16

CNC ports (1 Gb iSCSI) 16

CNC ports (FC/10GbE) 16

expansion port 16

network port 16

service port 1 16

service port 2 16

J6G24/J6G12 rear panel 17

Power Supply Unit (PSU)

AC 15

DC 15

connecting

controller enclosures to hosts 29

to remote management hosts 36

connections

test 25

verify 24

console requirement 81

controller enclosures

connecting to hosts 29

connecting to remote management hosts 36

controller modules

2-port 1 Gb iSCSI (CNC) 9

2-port 10GbE iSCSI (CNC) 9

2-port 12 Gb HD mini-SAS 9

2-port 8/16 Gb FC (CNC) 9

conventions

document 11

D

DHCP

obtaining IP addresses 40

server 40

direct attach configurations 29

disk drive

LEDs

general 71

specific states 72

document

conventions 11

prerequisite knowledge 10

related documentation 10

E

electrostatic discharge

grounding methods 85

precautions 85

enclosure

cabling 21

- IDs, correcting [48](#)
- initial configuration [20](#)
- input frequency requirement [83](#)
- input voltage requirement [83](#)
- installation checklist [20](#)
- site requirements [81](#)
- troubleshooting [48](#)
- weight [82](#), [83](#)
- Ethernet cables
 - requirements [36](#)

F

- faults
 - isolating
 - a host-side connection [53](#)
 - expansion port connection fault [55](#)
 - methodology [46](#)

H

- host interface ports
 - FC (8/16 Gb) [30](#)
 - FC host interface protocol
 - loop topology [30](#)
 - point-to-point protocol [30](#)
 - iSCSI (10GbE) [30](#)
 - iSCSI (1Gb) [31](#)
 - iSCSI host interface protocol
 - mutual CHAP [30](#), [31](#)
 - SAS (12 Gb) [31](#)
 - SAS host interface protocol [31](#)
- hosts
 - defined [29](#)
 - optional software [29](#)
 - stopping I/O [49](#)
 - system requirements [29](#)
- humidity non-operating range [83](#)
- humidity operating range [83](#)

I

- IDs, correcting for enclosure [48](#)
- Installing a license
 - permanent [45](#)
 - temporary [45](#)
- IP addresses
 - setting using DHCP [40](#)
 - setting using the CLI [40](#)

L

- LEDs
 - 2U12 front panel
 - Disk drive [70](#)
 - Enclosure ID [70](#)
 - Fault/Service Required [70](#)
 - FRU OK [70](#)
 - Temperature Fault [70](#)
 - Unit Locator [70](#)
 - 2U24 front panel
 - Disk drive [69](#)

- Enclosure ID [69](#)
- Fault/Service Required [69](#)
- FRU OK [69](#)
- Temperature Fault [69](#)
- Unit Locator [69](#)
- Disk
 - Fault [71](#)
 - Power/Activity [71](#)
- enclosure rear panel
 - 3524/3534
 - 12 Gb Host Link Activity [76](#)
 - 12 Gb Host Link Status [76](#)
 - Cache Status [76](#)
 - Expansion Port Status [76](#)
 - Fault/Service Required [76](#)
 - FRU OK [76](#)
 - Network Port Link Active [76](#)
 - Network Port Link Speed [76](#)
 - OK to Remove [76](#)
 - Unit Locator [76](#)
 - 3824/3834
 - 10GbE iSCSI Host Link Status/Link Activity [74](#)
 - 1Gb iSCSI Host Link Status/Link Activity [75](#)
 - Cache Status [74](#), [75](#)
 - Expansion Port Status [74](#), [75](#)
 - Fault/Service Required [74](#), [75](#)
 - FC Host Link Status/Link Activity [74](#)
 - FRU OK [74](#), [75](#)
 - Network Port Link Active [74](#), [75](#)
 - Network Port Link Speed [74](#), [75](#)
 - OK to Remove [74](#), [75](#)
 - Unit Locator [74](#), [75](#)
 - J6G24/J6G12 face plate
 - Fault/Service Required [78](#)
 - FRU OK [78](#)
 - OK to Remove [78](#)
 - SAS In Port Status [78](#)
 - SAS Out Port Status [78](#)
 - Unit Locator [78](#)
- Power Supply Unit (PSU)
 - AC [78](#)
 - DC [78](#)
 - using to diagnose fault conditions [49](#)
- local management host requirement [81](#)

M

- MPIO DSM
 - native Microsoft installation [29](#)
 - see related documentation [29](#)

N

- non-operating ranges, environmental [83](#)

O

- operating ranges, environmental [83](#)
- optional software [29](#)

P

- physical requirements 81
- power cord requirements 84
- power cycle
 - power off 27
 - power on 26
- power supply
 - AC power requirements 79
 - DC power requirements 80
 - site wiring requirements 79
- prerequisite knowledge 10

R

- RAIDar
 - web-based storage management interface 45
- regulatory compliance
 - notices
 - shielded cables 36, 81
 - see related document 79
- related documentation 10
- remote management 36
- requirements
 - cabling 81
 - clearance 81
 - Ethernet cables 36
 - host system 29
 - physical 81
 - ventilation 81
- RFI/EMI connector hoods 36, 81

S

- safety precautions 79
- sensors
 - locating 64
 - power supply 64
 - temperature 65
 - voltage 66
- SFP transceivers
 - installing 89
 - locating 89, 90
 - supported options 29
 - verifying operation 89
- shock non-operating range 83
- shock operating range 83
- site planning
 - local management host requirement 81
 - physical requirements 81
 - safety precautions 79
- SMC
 - web-based storage management interface 45
- storage system setup
 - configuring 45
 - getting started 45
 - provisioning 45
 - replicating 45
- supercapacitor pack 19
- switch attach configurations 35

T

- temperature non-operating range 83
- temperature operating range 83
- troubleshooting 46
 - controller failure, single controller configuration 52
 - correcting enclosure IDs 48
 - enclosure does not initialize 48
 - expansion port connection fault 55
 - host-side connection fault 53
 - using event notification 47
 - using RAIDar 47
 - using system LEDs 47, 49
 - using the CLI 47

U

- Unified LUN Presentation 29
- USB device connection
 - Command-line Interface (CLI) 87
 - device driver 87
 - emulated serial port 86
 - rear panel USB ports 86
 - supported host applications 87
 - vendor and product ID codes 87

V

- ventilation requirements 81
- vibration non-operating range 83
- vibration operating range 83

W

- warnings
 - temperature 64
 - voltage 64
- web site
 - Dot Hill Systems Customer Resource Center 11