

AssuredSAN 3000 Series Setup Guide

P/N 83-00005969-16-01 Revision A June 2012 Copyright © 2012 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.



Contents

Ał	pout this guide	. 11
	Intended audience	
	Prerequisites.	
	Related documentation	
	Document conventions and symbols	12
1	Components	. 15
	24-drive enclosure front panel components	15
	12-drive enclosure front panel components	
	Standard-depth model	
	Reduced-depth model	
	Controller enclosure — rear panel layout	
	3920/3930 controller module — rear panel components	
	3723/3733 controller module — rear panel components	10
	3523/3533 or 3520/3530 controller module — rear panel components	19
	3420/3430 controller module — rear panel components	20
	3320/3330 controller module — rear panel components	
	2122/3120/3130 drive enclosure rear panel components	
	2130 12-drive enclosure rear panel components	
	Component installation and replacement	
	CompactFlash	
	Super-capacitor pack	22
2	Installing the enclosures.	. 23
	Installation checklist	
	Network Equipment-Building System (NEBS) Level 3 compliance.	23
	Generic Requirements (GRs)	23
	Exceptions to GRs	
	Product documentation requirements	
	Connecting the controller enclosure and arive enclosures	
	Summary of drive enclosure cabling illustrations	25
	Testing enclosure connections.	32
	Powering on/powering off	
	AC PSU	33
	DC and AC PSUs with power switch	34
	Power Cords	35
3	Connecting hosts	. 37
Ŭ	Host system requirements.	. <i>07</i> 37
	Cabling considerations	37
	Connecting the enclosure to hosts	38
	FC host ports	38
	SAS host ports	38
	iSCSI host ports (1Gb)	38
	iSCSI host ports (10GbE)	39
	Connecting direct attach configurations	39
	Single-controller configurations	40 41
	Dual-controller configurations	41
	Connecting a management host on the network	43
	Connecting two storage systems to replicate volumes	

	Single-controller configurations	
		50
	Updating firmware	
	Obtaining IP values	57
	Setting network port IP addresses using DHCP.	
	Setting network port IP addresses using the CLI	57
٨	Basic operation	61
-	Accessing RAIDar	
	Configuring and provisioning the storage system	01
5	Troubleshooting	63
-	USB CLI port connection	63
	Fault isolation methodology	
	Basic steps	
	Options available for performing basic steps	
	Use RAIDar	
	Use the CLI	
	Monitor event notification	
	View the enclosure LEDs	
	Performing basic steps	
	Gather fault information.	
	Determine where the fault is occurring	64
	Review the event logs	
	Isolate the fault	
	If the enclosure does not initialize	
	Correcting enclosure IDs.	
	Stopping I/O.	
	Diagnostic steps	
	Is the enclosure front panel Fault/Service Required LED amber?	00 47
	Is the controller back panel FRU OK LED off?	67
	Is the controller back panel Fault/Service Required LED amber?	67
	Are both disk drive module LEDs off?	67
	Is the disk drive module Fault LED amber?	
	Is a connected host port's Host Link Status LED off?	68
	Is a connected port's Expansion Port Status LED off?	68
	Is a connected port's Network Port link status LED off?	
	Is the power supply's Input Power Source LED off?	09
	Is the Voltage/Fan Fault/Service Required LED amber?	
	Controller failure in a single-controller configuration	
	If the controller has failed or does not start, is the Cache Status LED on/blinking?	
	Transporting cache via professional services	
	Isolating a host-side connection fault	
	Host-side connection troubleshooting featuring FC or 10GbE iSCSI host ports	
	Host-side connection troubleshooting featuring SAS or iSCSI host ports	
	Isolating a controller module expansion port connection fault.	
	Isolating AssuredRemote replication faults	
	Cabling for replication	
	Replication setup and verification	
	Diagnostic steps for replication setup	
	Can you successfully use the AssuredRemote feature?	
	Can you view information about remote links?	
	Can you create a replication set?	
	Can you replicate a volume?	
	Can you view a replication image?	
	Can you view remote systems?	
	Resolving voltage and temperature warnings	
	Sensor locations	
	Power supply sensors	//

	Cooling fan sensors		78
A	LED descriptions . 24-drive enclosure front panel LEDs. 12-drive enclosure front panel LEDs. Standard-depth model . Reduced-depth model . Disk drive LEDs . Controller enclosure — rear panel layout. 3920/3930 controller module — rear panel LEDs. 3723/3733 controller module — rear panel LEDs. 3720/3730 controller module — rear panel LEDs. 3523/3533 or 3520/3530 controller module — rear panel LEDs. 3420/3430 controller module — rear panel LEDs. 3320/3330 controller module — rear panel LEDs. 320/3330 controller module — rear panel LEDs. Cache Status LED details Power supply LEDs.	· · · · · · · · · · · · · · · · · ·	79 80 81 82 84 85 86 87 88 87 88 89 90 91
	2122/3120/3130 drive enclosure rear panel LEDs		92
В	Environmental requirements and specifications. Safety requirements. Site requirements and guidelines Site wiring and AC power requirements. Site wiring and DC power requirements. Weight and placement guidelines Electrical guidelines. Ventilation requirements. Cabling requirements. Management host requirements. Physical requirements. Electrical requirements. Site wiring and power requirements. Site wiring and power requirements. Power cable requirements.	· · · · · · · · · · · · · · · ·	95 95 96 96 96 97 97 97 97
С	Electrostatic discharge		101 101 101
	USB device connection . Rear panel USB ports . USB CLI port . Emulated serial port . Supported host applications . Command-line Interface . Device driver/special operation mode . Microsoft Windows . Obtaining the software download . Linux . Setting parameters for the device driver .		103 103 104 104 104 104 104 105 105
Ind	dex	•	10/

Figures

1	CompactFlash	
2	Cabling connections between a single-controller enclosure and one drive enclosure	
3	Cabling connections between a dual-controller enclosure and one drive enclosure	
4		
5		
6	Reverse cabling between a dual-controller enclosure and four drive enclosures	
7	Reverse cabling between a dual-controller enclosure and seven drive enclosures	
8	Straight-through cabling between a dual-controller enclosure and different drive enclosure models	
9	AC PSU	
10		
11	DC and AC PSUs with power switch	
13	Connecting hosts — one server/one HBA/single path	41
	Connecting hosts — one server/one HBA/dual path	
	Connecting hosts — two servers/one HBA per server/dual path	
16	Connecting hosts — four servers/one HBA per server/dual path	
17		
18	Connecting two systems for AssuredRemote — single-controller module	
19		
20		
21	Connecting two systems for AssuredRemote — multiple servers/one switch/one location	
22	J / / /	
23		
24		
25		
26	Connecting four systems for AssuredRemote — multiple servers/switches/one location	
27	J	
28	USB device connection — CLI port	103

Tables

1	Related documents	. 12
2	Document conventions	. 12
3	Installation checklist	
4	Summary of SAS cable type requirements and related enclosure characteristics	26
5	Maximum cable lengths for 850nm Fibre Channel SFP transceivers (continued)	
6	Terminal emulator display settings	
7	Terminal emulator connection settings.	
8	Diagnostics LED status — Front panel "Fault/Service Required"	
9	Diagnostics LED status — Rear panel "FRU OK"	
10	Diagnostics LED status — Rear panel "Fault/Service Required"	67
11	Diagnostics LED status — Disk drives (LFF and SFF modules)	67
12	Diagnostics LED status — Disk drive fault status (LFF and SFF modules)	67
13	Diagnostics LED status — Rear panel "Host Link Status"	
14		
15	Diagnostics LED status — Rear panel "Network Port Link Status"	
	Diagnostics LED status — Rear panel power supply "Input Power Source"	. 09
17	Diagnostics LED status — Rear panel power supply "Voltage/Fan Fault/Service Required"	. 09
18	Diagnostics LED status — Rear panel "Cache Status"	
19	Diagnostics for replication setup — Using AssuredRemote feature	
20	Diagnostics for replication setup — Viewing information about remote links	
21	Diagnostics for replication setup — Creating a replication set	
22		
23	Diagnostics for replication setup — Viewing a replication image	
24		
	Power supply sensor descriptions	
26	Cooling fan sensor descriptions	
27	Controller module temperature sensor descriptions	. 78
28	Power supply temperature sensor descriptions	. 78
29	Voltage sensor descriptions	. 78
30	LEDs – 2U24 enclosure front panel	. 79
31	LEDs — 2U12 enclosure front panel: standard-depth	. 80
32	LEDs — 2U12 enclosure front panel: reduced-depth	
	LEDs — Disk with a dongle	
34	LEDs — Disk without a dongle	. 82
	LEDs — Disks in LFF and SFF enclosures	
	LEDs — Vdisks in LFF and SFF enclosures	
	LEDs — 3920/3930 controller module — rear panel	
	LEDs — 3723/3733 controller module — rear panel	
39	LEDs — 3720/3730 controller module — rear panel	
40	LEDs — 3523/3533 or 3520/3530 controller module — rear panel	88
41	LEDs — 3420/3430 controller module — rear panel	80
	LEDs — 3320/3330 controller module — rear panel	
	LEDs — Power supply units — rear panel	
	LEDs — 2122/31XX rear panel	
	LEDs — 2130 rear panel	
	Power requirements - AC Input.	
· —		
47		
48		
	Rackmount controller enclosure weights	
50	Rackmount compatible drive enclosure weights (ordered separately)	. 99
51	Operating environmental specifications	
	Non-operating environmental specifications	
53		104
54	USB vendor and product identification codes	104

About this guide

This guide provides information about hardware setup for the AssuredSAN™ 3000 Series products listed below:

Hybrid FC/iSCSI Controller Enclosures:

- 3920
- 3930

Fibre Channel Controller Enclosures:

- 3723
- 3733
- 3720
- 3730

Serial Attached SCSI Controller Enclosures:

- 3523
- 3533
- 3520
- 3530

Internet SCSI (10GbE) Controller Enclosures:

- 3420
- 3430

Internet SCSI (1Gb) Controller Enclosures:

- 3320
- 3330

With the exception of 3XX3 models, 3000 Series enclosures are NEBS Level 3, MIL-STD-810G (storage requirements), and European Telco compliant. The 3000 Series enclosures support either large form factor (LFF 12-disk) or small form factor (SFF 24-disk) 2U drive enclosures, using either AC or DC power supplies. See the Dot Hill web site for more information about specific models and uses: <u>http://www.dothill.com</u>.

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), Serial Attached SCSI (SAS), 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*
Installing and using optional host-based software components (CAPI Proxy, MPIO DSM, VDS Provider, VSS Provider, SES Driver)	AssuredSAN Installing Optional Software for Microsoft Windows® Server
Recommendations for using optional data-protection features (AssuredSnap, AssuredCopy, AssuredRemote)	AssuredSAN 3000 Series Using Data Protection Software
Using a rackmount bracket kit to install an enclosure into a rack	AssuredSAN Rackmount Bracket Kit Installation [*] or AssuredSAN 2-Post Rackmount Bracket Kit Installation [*]
Obtaining and installing a license to use licensed features	AssuredSAN 3000 Series Obtaining and Installing a License Certificate File
Using the web interface to configure and manage the product	AssuredSAN 3000 Series RAIDar User Guide
Using the command-line interface (CLI) to configure and manage the product	AssuredSAN 3000 Series CLI Reference Guide
Event codes and recommended actions	AssuredSAN Event Descriptions Reference Guide
Identifying and installing or replacing field-replaceable units (FRUs)	AssuredSAN 3000 Series FRU Installation and Replacement Guide

* Printed document included in product shipkit.

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

Document conventions and symbols

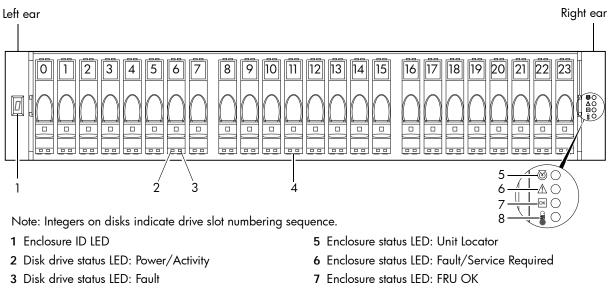
Table 2	Document conventions
---------	----------------------

Convention	Element	
Blue text	Cross-reference links and e-mail addresses	
Blue, underlined text	Web site addresses	
Bold text	 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 	
Italic text	Text emphasis	
Monospace text	 File and directory names System output Code Text typed at the command-line 	
<i>Monospace, italic text</i>	Code variablesCommand-line variables	
Monospace, bold text	Emphasis of file and directory names, system output, code, and text typed at the command-line	

- ▲ WARNING! Indicates that failure to follow directions could result in bodily harm or death.
- \triangle 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.
- 惊 TIP: Provides helpful hints and shortcuts.

1 Components

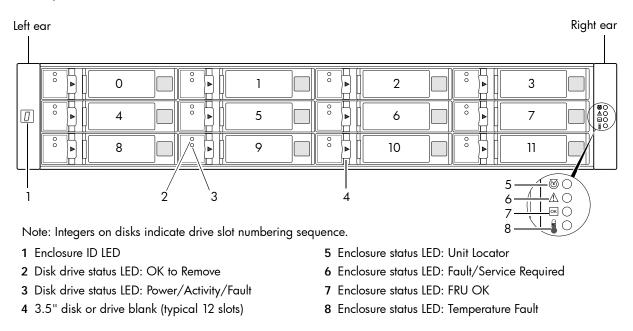
24-drive enclosure front panel components



- 4 2.5" disk or drive blank (typical 24 slots)
- 8 Enclosure status LED: Temperature Fault

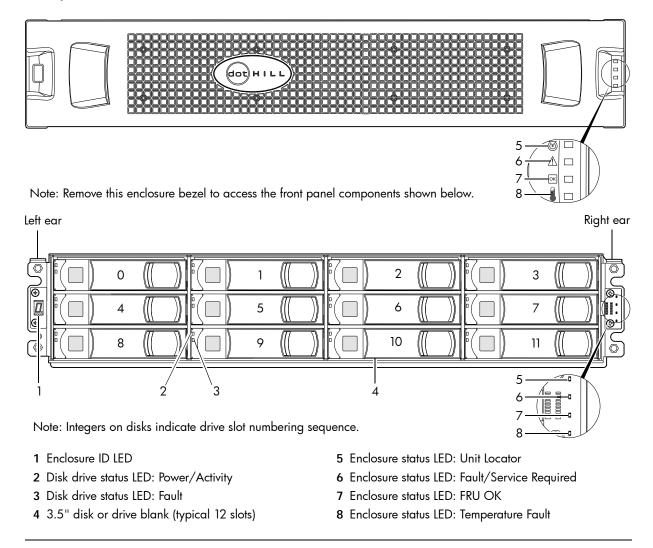
12-drive enclosure front panel components

Standard-depth model



NOTE: Front panel LEDs and rear panel LEDs for 3000 Series controller enclosures are described in LED descriptions.

Reduced-depth model



NOTE: See AssuredSAN 12-drive Enclosure Bezel Kit Installation — contained in your enclosure shipping container — for instructions on removing or installing the bezel.

The reduced-depth 12-drive enclosure includes a bezel sub-assembly that attaches to the front panel of the chassis (see the bezel illustration at the top of the page). The bezel — comprised of a vented cover attached to an EMI (Electromagnetic Interface) shield — is pre-assembled and packed within a box contained in the enclosure master shipping container. The bezel might optionally include a removable air filter that can be serviced or replaced. Hard copy instructions for attaching/removing the bezel, and for servicing or replacing the air filter, are provided in the shipping container of a new enclosure.

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

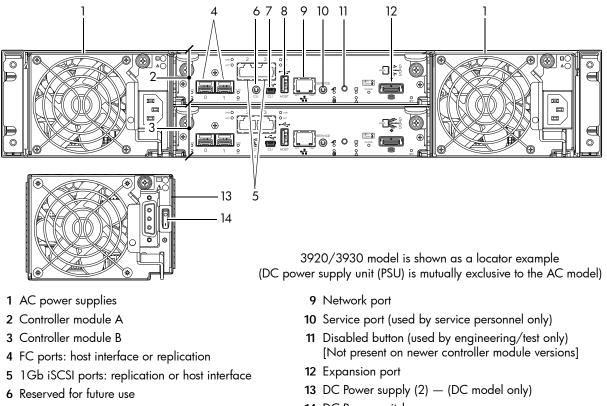
Select AssuredSAN & R/Evolution Products > 3000 Series to download the AssuredSAN 12-drive Enclosure Bezel Kit Installation document.

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

NOTE: LEDs for 3000 Series controller enclosures are described in LED descriptions.

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 3000 Series controller enclosure. The 3920/3930 is shown as a representative example of controller enclosure models included in the product series.



- 7 CLI port (USB Type B) [see Appendix D]
- 8 Host port (USB Type A; reserved for future use)
- 14 DC Power switch

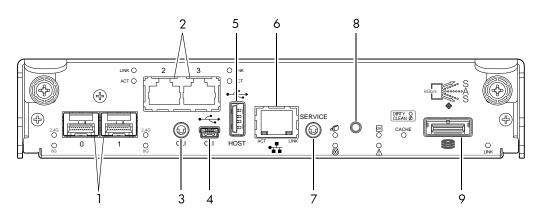
A controller enclosure accommodates two power supply FRUs of the same type — either both AC or both DC — within the two power supply slots (see two instances of callout No.1 above). The controller enclosure accommodates up to two controller module FRUs of the same type within the I/O module (IOM) slots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

IMPORTANT: In controller enclosures configured with a single controller module, the lower IOM slot is empty, and must be covered with an IOM blank 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 3000 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.

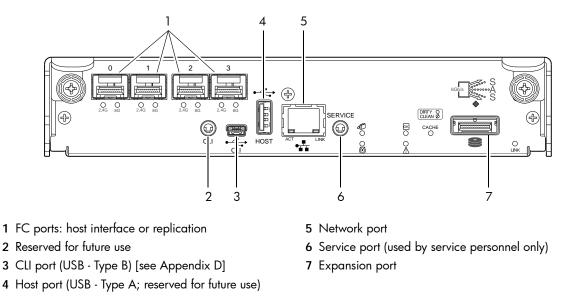
Descriptions are also provided for optional drive enclosures supported by 3000 Series controller enclosures.

3920/3930 controller module - rear panel components



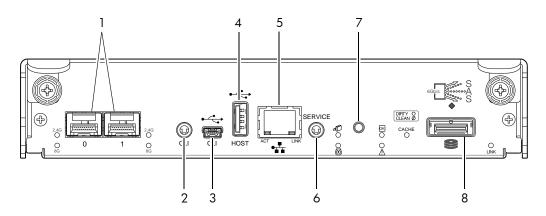
- 1 FC ports: host interface or replication
- 2 1Gb iSCSI ports: host interface or replication
- 3 Reserved for future use
- 4 CLI port (USB Type B) [see Appendix D]
- 5 Host port (USB Type A; reserved for future use)
- 6 Network port
- 7 Service port (used by service personnel only)
- 8 Disabled button (used by engineering/test only) [Not present on newer controller module versions]
- 9 Expansion port

3723/3733 controller module — rear panel components



NOTE: The 3XX3 controller modules are compatible with 3000 Series reduced-depth controller enclosure models. To realize performance improvements, the chassis must have a PCIe Gen 2 capable midplane.

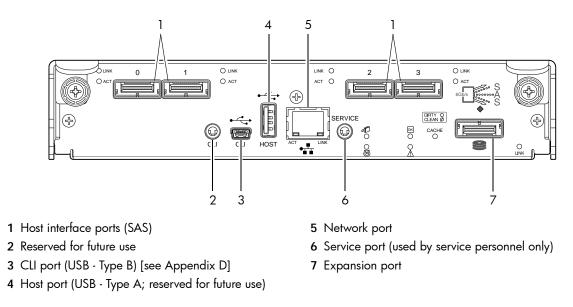
3720/3730 controller module — rear panel components



- 1 FC ports: host interface or replication
- 2 Reserved for future use
- 3 CLI port (USB Type B) [see Appendix D]
- 4 Host port (USB Type A; reserved for future use)
- 5 Network port

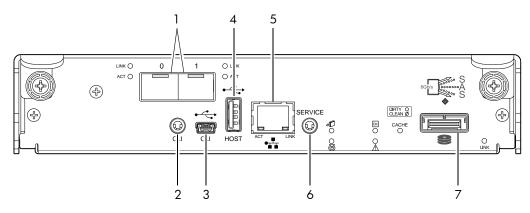
- 6 Service port (used by service personnel only)
- 7 Disabled button (used by engineering/test only) [Not present on newer controller module versions]
- 8 Expansion port

3523/3533 or 3520/3530 controller module — rear panel components



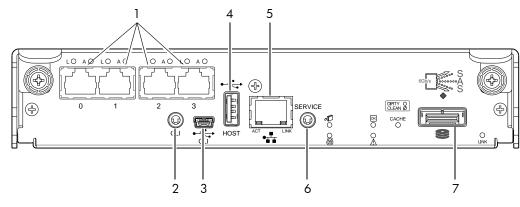
NOTE: The 3XX3 controller modules are compatible with 3000 Series reduced-depth controller enclosure models. To realize performance improvements, the chassis must have a PCIe Gen 2 capable midplane.

3420/3430 controller module — rear panel components



- 1 10GbE iSCSI ports: host interface or replication
- 2 Reserved for future use
- 3 CLI port (USB Type B) [see Appendix D]
- 4 Host port (USB Type A; reserved for future use)
- 5 Network port
- 6 Service port (used by service personnel only)
- 7 Expansion port

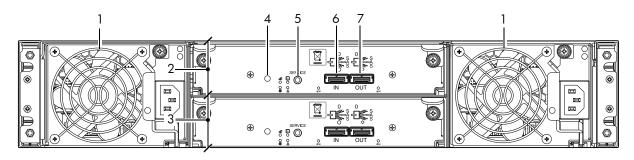
3320/3330 controller module — rear panel components



- 1 1Gb iSCSI ports: host interface or replication
- 2 Reserved for future use
- 3 CLI port (USB Type B) [see Appendix D]
- 4 Host port (USB Type A; reserved for future use)
- 5 Network port
- 6 Service port (used by service personnel only)
- 7 Expansion port

2122/3120/3130 drive enclosure rear panel components

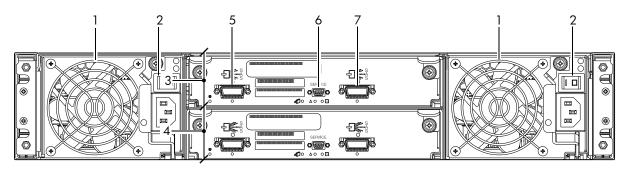
AssuredSAN 3000 Series controller enclosures support 2122, 3120 (shown below), and 3130 drive enclosures for expansion of storage capacity. The 3120 and the 3130 are available with standard-depth and reduced-depth chassis. These drive enclosures use mini-SAS (SFF-8088) connectors to facilitate backend SAS expansion. See Cable requirements for drive enclosures on page 25 for cabling information.



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

2130 12-drive enclosure rear panel components

AssuredSAN 3000 Series controller enclosures support 2130 drive enclosures for expansion of storage capacity. These drive enclosures use SAS 8470 connectors to facilitate backend SAS expansion. See Cable requirements for drive enclosures on page 25 for cabling information.



- 1 Power supplies (AC shown)
- 2 Power switches (not available on newer models)
- 3 Expansion module A
- 4 Expansion module B

- 5 SAS In port
- 6 Service port (used by service personnel only)
- 7 SAS Out port

Component installation and replacement

Installation and replacement of 3000 Series FRUs (field-replaceable units) is addressed in the *AssuredSAN* 3000 Series FRU Installation and Replacement Guide within the "Procedures" chapter.

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

- Replacing a controller or expansion module
- Replacing a disk drive module
- Replacing a power supply unit (AC and DC units with integrated cooling fans)
- Replacing ear bezels
- Replacing a Fibre Channel transceiver
- Replacing a 10GbE SFP+ transceiver
- Replacing a controller enclosure chassis

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

Select AssuredSAN & R/Evolution Products > 3000 Series to download the FRU I&R guide.

Cache

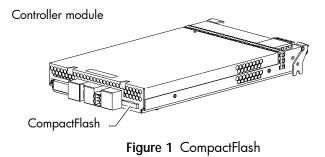
To enable faster data access from disk storage, the following types of caching are performed:

- Write-back or write-through caching. The controller writes user data into the cache memory in the
 controller module rather than directly to the disks. Later, when the storage system is either idle or aging
 — and continuing to receive new I/O data the controller writes the data to the disks.
- Read-ahead caching. The controller detects sequential data access, reads ahead into the next sequence of data — based upon settings — and stores the data in the read-ahead cache. Then, if the next read access is for cached data, the controller immediately loads the data into the system memory, avoiding the latency of a disk access.
- ☆ TIP: See the "About volume cache options" and "Changing system cache settings" topics in the RAIDar user guide for setting options.

CompactFlash

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

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



IMPORTANT: Customer removal of CompactFlash will void the product warranty. See Transporting cache via professional services on page 70 for more information.

Super-capacitor pack

To protect controller module cache in case of power failure, each controller enclosure model is equipped with super-capacitor technology, in conjunction with CompactFlash memory, built into each controller module to provide unlimited cache memory backup time. The super-capacitor 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 super-capacitor 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 ear caps or enclosure bezel. ¹	See the rack-mount bracket kit installation instructions pertaining to your enclosure. If your product uses a bezel, see its bezel kit installation instructions.
2.	Connect controller enclosure and optional drive enclosures.	See Connecting the controller enclosure and drive enclosures on page 24.
3.	Connect power cords.	See Power Cords on page 35.
4.	Test enclosure connectivity.	See Testing enclosure connections on page 32.
5.	Install required host software.	See Host system requirements on page 37.
6.	Connect hosts. ²	See Connecting the enclosure to hosts on page 38. If using the optional AssuredRemote feature, also see Connecting two storage systems to replicate volumes on page 48.
7.	Connect remote management hosts. ²	See Connecting a management host on the network, page 48.
8.	Obtain IP values and set network port IP properties on the controller enclosure.	See Obtaining IP values on page 57. For USB CLI port and cable use, see Appendix D. Also see the ship kit CD.
9.	Perform initial configuration tasks ³ :	Topics below correspond to bullets at left:
	 Sign-in to the web-based storage management application (RAIDar). 	See "Getting Started" in the web-posted <i>AssuredSAN 3000 Series RAIDar User Guide.</i>
	 Initially configure and provision the system using RAIDar.⁴ 	See "Configuring the System" and "Provisioning the System" topics in the RAIDar user guide or online help.

¹Also see AssuredSAN 3000 Series FRU Installation and Replacement Guide for illustrations showing installation of enclosure ear caps or the enclosure bezel that is provided with some models.

²For more about hosts, see the "About hosts" topic in the AssuredSAN 3000 Series RAIDar User Guide.

³RAIDar is introduced in Accessing RAIDar on page 61. See the RAIDar user guide or online help for additional information.
 ⁴If the systems are cabled for replication and licensed to use the AssuredRemote feature, you can use the Replication Setup Wizard to prepare to replicate an existing volume to another vdisk. See the RAIDar user guide 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 6Gb and 3Gb disk drives within the same enclosure.

Network Equipment-Building System (NEBS) Level 3 compliance

Generic Requirements (GRs)

Meets the NEBS requirement of GR-1089-CORE Issue 5, port types 2, 7 & 8. Meets the NEBS requirements of GR-63-CORE Issue 3, for the product's intended use. **NOTE:** Table 4 on page 26 shows NEBS-compliance for individual storage enclosures.

Exceptions to GRs

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

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

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

• None reported

Product documentation requirements

NEBS product documentation requirements applying to AssuredSAN 3000 Series controller and drive enclosures are listed beneath "NEBS (Level 3)" in the Index — under either GR-1089-CORE Issue 5 or GR-63-CORE Issue 3 — together with adjacent page locations. NEBS topics are *integrated* within the overall content of this setup guide. The requirement designators in the Index have been codified for use within index marker tags according to the following example:

NEBS generic requirement number "R1-3 [155]" appears as "R1-3.155" within the Index.

Each codified string (e.g., R1-3.155) is followed by a hyphen and brief description of the requirement. Within the Index, click on the blue page number link to navigate to the corresponding NEBS topic.

Connecting the controller enclosure and drive enclosures

AssuredSAN 3000 Series controller enclosures — available in either 24-drive (2.5") or 12-drive (3.5") chassis — support up to eight enclosures (including the controller enclosure), or a maximum of 144 disk drives. You can also configure drive enclosures of mixed model type as shown in Figure 8 on page 32. 3000 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 3000 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, Figure 5 on page 29 shows reverse cabling wherein controller OA (i.e., enclosure-ID = 0; controller-ID = Able) is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller OB is connected to the lower expansion module (B) of the last drive enclosure in

the chain, with connections moving in the opposite direction (green). Several cabling examples are provided on the following pages.

NOTE: AssuredSAN 3000 Series controller enclosures support hot-plug replacement of redundant controller modules, fans, power supplies, and I/O modules. Hot-add of drive enclosures is also supported.

Cable requirements for drive enclosures

3000 Series enclosures support 6-Gbps or 3-Gbps expansion port data rates. Observe the following guidelines when installing SAS cables (see Table 4 below):

- Use only AssuredSAN or OEM-qualified SAS cables appropriate for connecting the drive enclosure:
 - For 6-Gbps drive enclosures, use cables providing 6-Gbps data rate per lane with four lanes (4x) per SAS connector:
 - When connecting a controller enclosure to a drive enclosure, the cable length should not exceed 2.0 meters
 - When connecting drive enclosures to one another, cable lengths should not exceed 2.0 meters
 - For 3-Gbps expansion modules, use cables providing 3-Gbps data rate per lane with four lanes per SAS connector:
 - When connecting a controller enclosure to a drive enclosure, the cable length should not exceed 2.0 meters
 - When connecting drive enclosures to one another, or when connecting a drive enclosure to an HBA directly, cable lengths should not exceed 2.0 meters
 - Newer cables provide SAS connectors supporting *both* 6-Gb and 3-Gb data rates
 - Qualified cables of 0.6 meter length may be used for cabling stacked components in cascaded fashion
 - NOTE: If you connect a 3-Gbps drive enclosure to a 6-Gbps 3000 Series controller enclosure, data throughput occurs at the drive enclosure's 3-Gbps data rate.
- Refer to the Table 4 on page 26 when cabling storage system components. The following terms supplement those defined in the table footer.
 - Mini-SAS to mini-SAS cables denote SFF-8088 to SFF-8088
 - Mini-SAS to SAS cables denote SFF-8088 to 8470
 - SAS to SAS cables denote 8470 to 8470
 - ☆ TIP: SAS connector requirements for cabling 3000 Series controller enclosures and supported drive enclosures are summarized in Table 4 on page 26.

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

When using the table-matrix, note that column No.1 is model-specific and columns No.2 through No.5 each address models conforming to a group designation, allowing you to sort by column and row in determining appropriate cable/connector types. The shaded table cells indicate that cabling one controller enclosure to another controller enclosure is not allowed.

- You may need to order additional or longer cables when reverse-cabling a fault-tolerant configuration (see Figure 5 on page 29).
- Cables required, if not included, must be purchased separately.

Model	3000 Series 2U24 controller enclosure	3000 Series 2U12 controller enclosure	31XX/2122 drive enclosure (mini-SAS)	2130 drive enclosure (SAS)
3920			mini-SAS to mini-SAS	mini-SAS to SAS
3930			mini-SAS to mini-SAS	mini-SAS to SAS
3723			mini-SAS to mini-SAS	mini-SAS to SAS
3733			mini-SAS to mini-SAS	mini-SAS to SAS
3720			mini-SAS to mini-SAS	mini-SAS to SAS
3730			mini-SAS to mini-SAS	mini-SAS to SAS
3523			mini-SAS to mini-SAS	mini-SAS to SAS
3533	Not app	blicable	mini-SAS to mini-SAS	mini-SAS to SAS
3520			mini-SAS to mini-SAS	mini-SAS to SAS
3530			mini-SAS to mini-SAS	mini-SAS to SAS
3420			mini-SAS to mini-SAS	mini-SAS to SAS
3430			mini-SAS to mini-SAS	mini-SAS to SAS
3320			mini-SAS to mini-SAS	mini-SAS to SAS
3330			mini-SAS to mini-SAS	mini-SAS to SAS
3120	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to SAS
3130	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to SAS
2122	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to SAS
2130	mini-SAS to SAS	mini-SAS to SAS	mini-SAS to SAS	SAS to SAS
2130 mini-SAS to SAS mini-SAS to SAS SAS to SAS 2012 Enclosure measuring two rack units high, providing 24-drives and smaller depth dimension than 2U12. 2012: Enclosure measuring two rack units high, providing 12-drives, and larger footprint than 2U24. Praduct models (6-Gbps SAS expansion data transmission rate unless noted otherwise): 3920: 3000 Series controller enclosure (2.5" disks in 2U12 chassis) [NEBS] 3733: 3000 Series controller enclosure (3.5" disks in reduced-depth 2U24 chassis) 3723: 3000 Series controller enclosure (3.5" disks in reduced-depth 2U12 chassis) 3720: 3000 Series controller enclosure (3.5" disks in reduced-depth 2U12 chassis) 3730: 3000 Series controller enclosure (2.5" disks in reduced-depth 2U12 chassis) 3730: 3000 Series controller enclosure (3.5" disks in 2U12 chassis) [NEBS] 3730: 3000 Series controller enclosure (2.5" disks in reduced-depth 2U24 chassis) 3533: 3000 Series controller enclosure (3.5" disks in 2U12 chassis) 3533: 3000 Series controller enclosure (2.5" disks in 2U24 chassis) [NEBS] 3530: 3000 Series controller enclosure (3.5" disks in 2U12 chassis) 3530: 3000 Series controller enclosure (2.5" disks in 2U12 chassis) 3530: 3000 Series controller enclosure (2.5" disks in 2U12 chassis)				

Table 4	Summary of SAS cable type	e requirements and	related enclosure	e characteristics
---------	---------------------------	--------------------	-------------------	-------------------

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

Summary of drive enclosure cabling illustrations

The following illustrations show both *straight-through* and *reverse* cabling examples using different drive enclosure models. Illustrations show different kinds of connections: legacy enclosures use SAS connectors, and newer models use mini-SAS connectors. For optimal performance, 3000 Series controller enclosures should be cabled to 6Gb drive enclosures when adding storage. Cabling of 3Gb drive enclosures to newer 6Gb controllers is addressed for customers upgrading existing legacy systems.

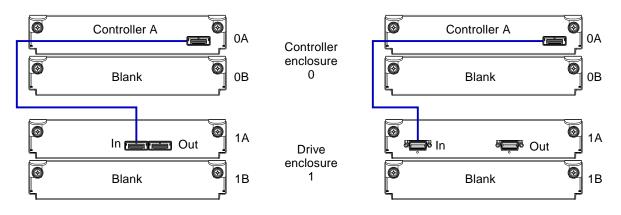


Figure 2 Cabling connections between a single-controller enclosure and one drive enclosure

The diagram at left (above) shows a single-controller enclosure connected to either a 2122, 3120, or 3130 (single expansion module); whereas the diagram at right shows the controller enclosure connected to a 2130 (single expansion module).

When cabling an enclosure containing a single controller module to an enclosure containing a single expansion module, the lower I/O module (IOM) slot in each chassis is empty, and must be covered with an IOM blank to allow optimum airflow through the enclosure during operation (see "Replacing a controller or expansion module" within the AssuredSAN 3000 Series FRU Installation and Replacement Guide for additional information).

NOTE: Some enclosures use an SFF-8088 connector interface for drive expansion, whereas other enclosures use SAS 8470. Refer to Table 4 on page 26 for SAS cable requirements.

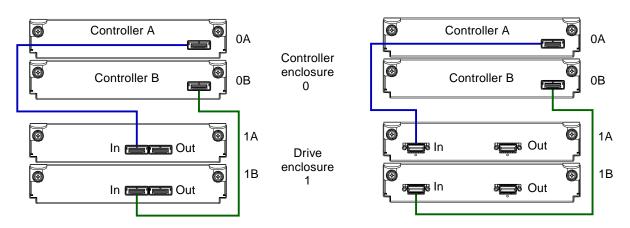


Figure 3 Cabling connections between a dual-controller enclosure and one drive enclosure

The diagram at left (above) shows a dual-controller enclosure connected to a 2122, 3120, or 3130 (two expansion modules); whereas the diagram at right shows the dual-controller enclosure connected to a 2130 (two expansion modules).

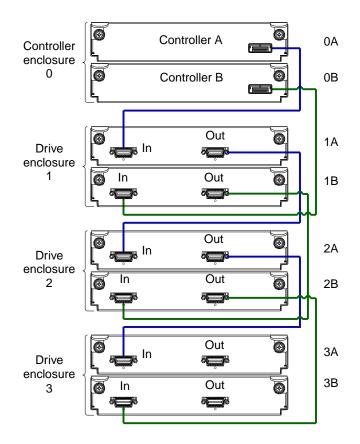


Figure 4 Straight-through cabling between a dual-controller enclosure and three drive enclosures

The diagram above shows a dual-controller enclosure cabled to 2130 drive enclosures, featuring dual-expansion modules. Controller enclosure ID number 0, featuring dual controllers, is attached to three drive enclosures in straight-through fashion.

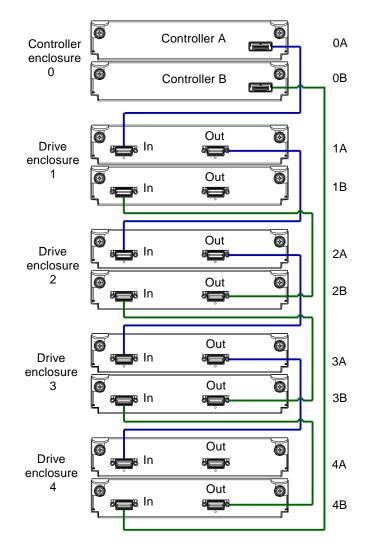


Figure 5 Reverse cabling between a dual-controller enclosure and four drive enclosures

The diagram above shows a dual-controller enclosure cabled to 2130 drive enclosures, featuring dual-expansion modules. Controller module OA is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller module OB is connected to the lower expansion module (4B) of the last drive enclosure, with connections flowing in the opposite direction (green).

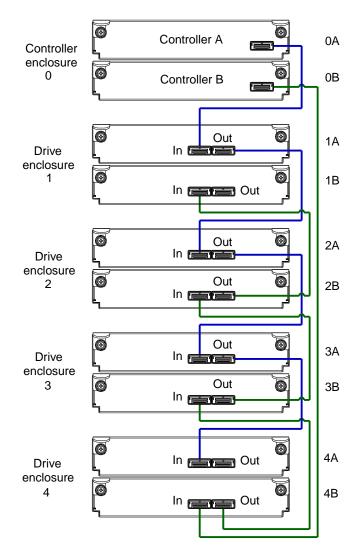
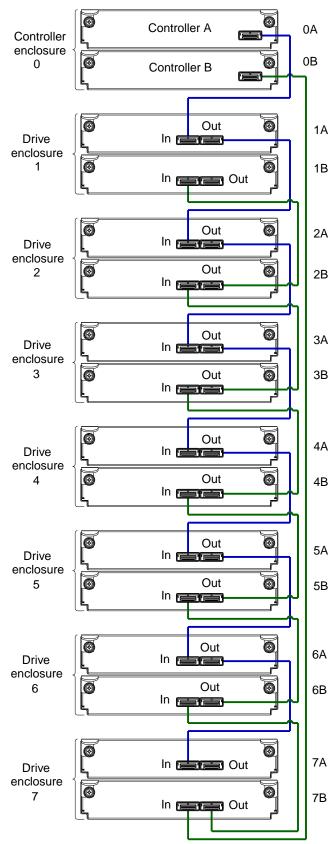


Figure 6 Reverse cabling between a dual-controller enclosure and four drive enclosures

The diagram above shows a dual-controller enclosure cabled to 2122, 3120, or 3130 drive enclosures featuring dual-expansion modules. Controller module OA is connected to expansion module 1A, with a chain of connections continuing down (blue). Controller module OB is connected to the lower expansion module (4B), of the last drive enclosure, with connections moving in the opposite direction (green).



Note:

The maximum number of supported drive enclosures (7) may require purchase of additional longer cables.

Figure 7 Reverse cabling between a dual-controller enclosure and seven drive enclosures

The diagram above shows a 3730 dual-controller enclosure cabled to 3130 drive enclosures featuring dual-expansion modules. Controller module OA is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller module OB is connected to the lower expansion module (7B), of the last drive enclosure, with connections moving in the opposite direction (green).

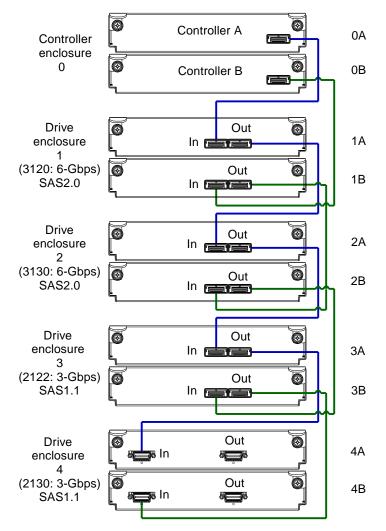


Figure 8 Straight-through cabling between a dual-controller enclosure and different drive enclosure models

The diagram above shows a dual-controller enclosure cabled to mixed 2U24 and 2U12 drive enclosures featuring dual-expansion modules. When cabling supported drive enclosures of differing model types, consider the following factors concerning drive enclosures equipped with SAS2.0 and SAS1.1:

- 3000 Series controller enclosures (2U24 or 2U12 models) support the 6-Gbps and 3-Gbps drive enclosures labeled in Figure 8 above.
- To minimize performance limitations when connecting mixed drive enclosures, cable 3-Gbps drive enclosures after 6-Gbps drive enclosures as shown in Figure 8 above.
- Performance will be limited if a 3-Gbps drive enclosure is cabled before a 6-Gbps drive enclosure and cannot be avoided – if reverse-cabled. A 6-Gbps drive enclosure will perform at 3-Gbps if cabled after a 3-Gbps drive enclosure.
- If used in a mixed-type drive environment, cable 2130 drive enclosures after other supported models, via straight-through cabling as shown in Figure 8 above.

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 other enclosures use PSUs that have no power switch.

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

The following section, Powering on/powering off, describes power cycling procedures relative to different types of 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 38.

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 power supply units (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 79 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 below. 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 with power switch on page 34.

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.

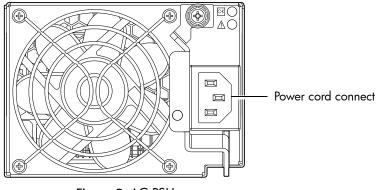


Figure 9 AC PSU

To power on the system:

 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 9 and Figure 10). Wait several seconds to allow the disks to spin up.

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

 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 9 and Figure 10).

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

Power cord facilitates power on/power off

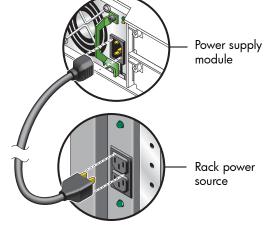


Figure 10 AC power cord

To power off the system:

- 1. Stop all I/O from hosts to the system (see Stopping I/O on page 65).
- 2. Shut down both controllers using *either* method described below:
 - Use RAIDar to shut down both controllers, as described in the online help and *AssuredSAN 3000* Series RAIDar User Guide.

Proceed to step 3.

- Use the command-line interface (CLI) to shut down both controllers, as described in the AssuredSAN 3000 Series CLI Reference Guide.
- 3. Disconnect the power cord's male plug from the power source.
- 4. Disconnect the power cord's female plug from the power cord connector on the PSU.

DC and AC PSUs with power switch

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

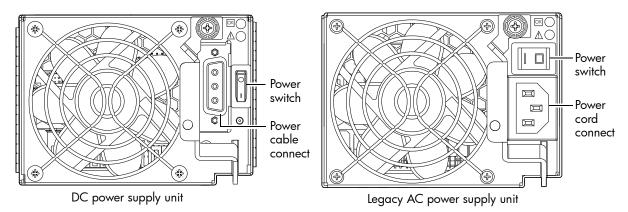


Figure 11 DC and AC PSUs with power switch

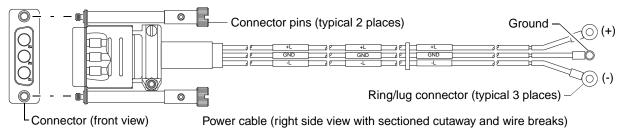
IMPORTANT: See Environmental requirements and specifications for additional information.

AC model

See Figure 10 and the illustration at right (in Figure 11) when performing the following steps:

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

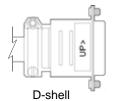
DC model





See Figure 12 and the illustration at left (in Figure 11) 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.
- 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).
- 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 (left side view) 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 12 above).

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

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.

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 65).
- 2. Shut down both controllers using *either* method described below:
 - Use RAIDar to shut down both controllers, as described in the online help and *AssuredSAN 3000* Series RAIDar User Guide.
 - Proceed to step 3.
 - Use the command-line interface (CLI) to shut down both controllers, as described in the AssuredSAN 3000 Series CLI Reference Guide.
- 3. Press the power switches at the back of the controller enclosure to the Off position.
- 4. Press the power switches at the back of each drive enclosure to the Off position.

3 Connecting hosts

Host system requirements

Hosts connected to a 3000 Series controller enclosure must meet the following requirements:

- Depending on your system configuration, host operating systems may require that multipathing is supported.
 - ☆ TIP: See the web-posted AssuredSAN Installing Optional Software for Microsoft Windows® Server to aid in planning and implementing your MPIO DSM installation.

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 R/Evolution MPIO DSM with Windows Server 2003. Download the software from <u>http://crc.dothill.com</u>.
- Use native Microsoft MPIO DSM support with Windows Server 2008. Use either the Server Manager or the command-line interface (*mpclaim* CLI tool) to perform the installation.
 See AssuredSAN Installing Optional Software for Microsoft Windows® Server and the following web sites for information about using native Microsoft MPIO DSM: http://support.microsoft.com/gp/assistsupport http://support.microsoft.com/gp/assistsupport
- To prevent Microsoft Windows 2003 hosts from displaying the Found New Hardware Wizard when the storage system is discovered, install the R/Evolution SCSI Enclosure Services driver from <u>http://crc.dothill.com</u>.
 - **NOTE:** The R/Evolution SCSI Enclosure Services driver is *required* for Windows Server 2003.

Cabling considerations

Common cabling configurations address hosts, controller enclosures, drive enclosures, and switches. 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 48 for more information.

With the exception of SAS models, host interface ports on 3000 Series controller enclosures can either connect to respective hosts via direct-attach or switch attach, or they can be used for replication. SAS host interface ports connect to SAS hosts directly, or via switches; they are *not* used for replication.

- NOTE: 3920/3930, 3723/3733, 3720/3730, 3420/3430, and 3320/3330 models support AssuredRemote replication; whereas 3523/3533 and 3520/3530 models do not.
- **IMPORTANT:** Do not connect hosts or map volumes to host ports used for replication. Attempting to do so could interfere with replication operation.

Connecting the enclosure to hosts

A *host* identifies an external port to which the storage system is attached. Cable connections vary depending on configuration. This section describes host interface protocols supported by 3000 Series controller enclosures, while showing a few common cabling configurations.

NOTE: 3000 Series controllers use Unified LUN Presentation (ULP) — a controller feature enabling a host to access mapped volumes through any controller host port.

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

☆ TIP: See "Configuring the system > Using the Configuration Wizard" in the RAIDar user guide to initially configure the system or change system configuration settings (e.g., Configuring host ports).

FC host ports

Certain 3000 Series controller enclosures use Fibre Channel (FC) interface protocol for host port connection, featuring either one or two controller modules. Each controller module provides host ports configured with a Fibre Channel small form-factor pluggable (SFP transceiver) connector, supporting data rates up to 8-Gbps.

The 3920/3930 (FC/iSCSI), 3723/3733 (FC), and 3720/3730 (FC) models support Fibre Channel Arbitrated Loop (FC-AL or "loop") or point-to-point (FC-P2P) 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. These models employ FC ports 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 Fibre Channel switch.

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

TIP: Use RAIDar's Configuration Wizard to set FC port options (within the RAIDar user guide, see "Configuring the system > Using the Configuration Wizard > Configuring host ports," and scroll to FC port options).

SAS host ports

The 3523/3533 and 3520/3530 use Serial Attached SCSI (Small Computer System Interface — SAS) interface protocol for host port connection, featuring either one or two controller modules. Each controller module provides two dual SFF-8088 mini-SAS host ports supporting data rates up to 6-Gbps per lane — and 4-lanes per SAS connector.

iSCSI host ports (1Gb)

The 3920 and 3930 FC/iSCSI models also support the Internet SCSI interface protocol in addition to FC host port connection. A 3920 or 3930 provides two iSCSI ports — each supporting data rates up to 1-Gbps — using either one-way or mutual CHAP (Challenge-Handshake Authentication Protocol).

☆ TIP: See the "Configuring CHAP" topic within the RAIDar user guide. Also see the admonition about CHAP preceding the "Using the Replication Setup Wizard" procedure within that guide. A 3920 or 3930 employs iSCSI ports in either of two capacities:

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

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

The 3320 and 3330 iSCSI models support iSCSI host interface protocol per the link rates described above; however, these models provide 4-ports per controller module. The host ports are used for attachment to iSCSI hosts directly, or through an Ethernet switch. The ports can also be used to connect storage systems through a switch for use of the licensed AssuredRemote replication feature.

TIP: Use RAIDar's Configuration Wizard to set iSCSI port options (within the RAIDar user guide, see "Configuring the system > Using the Configuration Wizard > Configuring host ports," and scroll to iSCSI port options). Also, see 3000 Series controller enclosure iSCSI considerations on page 47.

iSCSI host ports (10GbE)

The 3420 and 3430 models use the Internet SCSI interface protocol for host port connection, featuring either one or two controller modules. Each controller module provides two iSCSI host ports configured with a small form pluggable (10GbE SFP+ transceiver) connector — each supporting data rates up to 10-Gbps — using either one-way or mutual CHAP (Challenge-Handshake Authentication Protocol).

A 3420 or 3430 employs iSCSI ports 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 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.

Connecting direct attach configurations

The 3720/3730 and 3420/3430 each support up to four direct-connect server connections, two per controller module. The 3920/3930, 3723/3733, 3523/3533, 3520/3530, and 3320/3330 each support up to eight server connections, four per controller. Connect appropriate cables from the server's HBAs to the controller module's host ports as described below, and shown in the following illustrations.

To connect the 3000 Series controller enclosure to a server HBA or switch — using the controller's FC host ports — select Fibre Channel cables supporting 2/4/8 Gb data rates, that are compatible with the controller module's host port SFP connector. For applicable 3000 Series controller enclosure models, such cables are also used for connecting a local storage system to a remote storage system via a switch, to facilitate use of the optional AssuredRemote replication feature.

The table below maps SFP transceiver data rates to relative fiber optic cable characteristics (i.e., cable length, multimode fiber type (MMF), and ISO/IEC optical multimode cable performance standards). When transferring data through FC connections, cable lengths should not exceed the lengths listed for each given fiber type and performance code within the applicable data rate (2/4/8 Gb) class.

SFP data	Representative FC cable types Cable performance code		ode	
Data rate	MMF FC cable length designators OM1 OM2 C		OM3	
8-Gbps	21m with 62.5µm fiber type	Х		
	50m with 50µm fiber type X		Х	
	150m with 50μm fiber type		Х	

Table 5	Maximum cable	lengths for 850nm	Fibre Channel SFP	transceivers (continued)

SFP data	Representative FC cable types Cable performance code		ode	
Data rate	MMF FC cable length designators OM1 OM2		OM3	
4-Gbps	70m with 62.5μm fiber type	Х		
150m with 50μm fiber type			Х	
	380m with 50μm fiber type			Х
2-Gbps 150m with 62.5μm fiber type		Х		
	300m with 50µm fiber type		Х	
500m with 50μm fiber type				Х

 Table 5
 Maximum cable lengths for 850nm Fibre Channel SFP transceivers (continued)

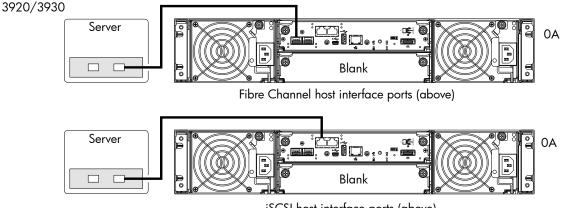
- To connect 3000 Series controller modules supporting 1Gb iSCSI host interface ports to a server HBA or switch — using the controller's iSCSI ports — select (CAT5-E minimum) Ethernet cables supporting the 1 Gb RJ-45 copper host port iSCSI connector. Minimum cable length is 0.5 meters; maximum cable length is 7 meters.
- To connect the 3523/3533 or 3520/3530 to a server HBA or switch, use AssuredSAN or OEM-qualified mini-SAS 4x cables. SAS cables connecting to host ports must support the SFF-8088 host port connector using 0.5 meter, 1 meter, 2 meter, 4 meter or 6 meter (maximum) cable lengths.
- To connect the 3420 or 3430 to a server HBA or switch using the controller's iSCSI host ports select the appropriate qualified 10GbE SFP+ option. The maximum supported cable length is 7.0 meters.

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 in environments where high availability is not required, and loss of access to data can be tolerated until failure recovery actions are completed.

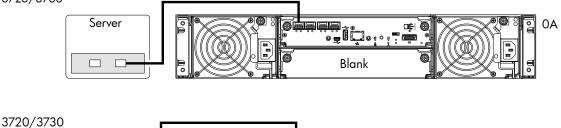
One server/one HBA/single path

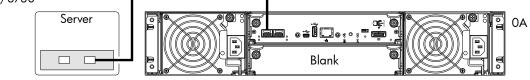
Model-specific illustrations show single-controller configurations for 3000 Series controller enclosures supporting pertinent host interface protocols.

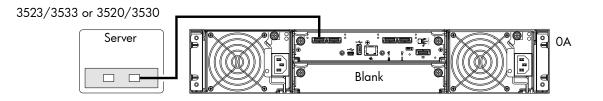


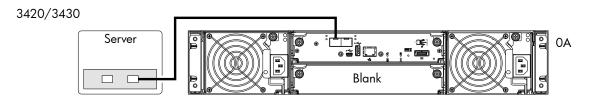
iSCSI host interface ports (above)

3723/3733









3320/3330

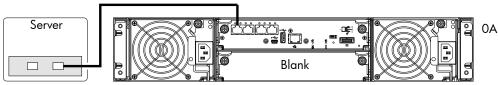


Figure 13 Connecting hosts - one server/one HBA/single path

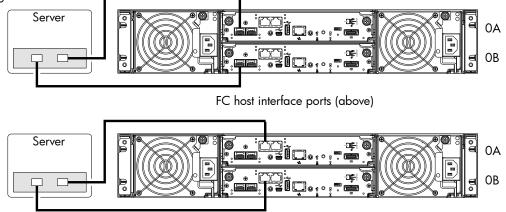
Dual-controller configurations

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 512 LUNs (0-511) for use in mapping volumes to hosts (see "ULP" in the AssuredSAN 3000 Series RAIDar User Guide).

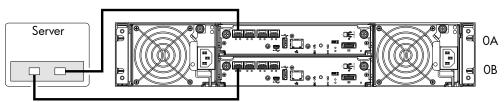
One server/one HBA/dual path

Model-specific illustrations (below) show dual-controller configurations for 3000 Series controller enclosures supporting pertinent host interface protocols.

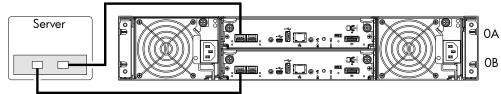


iSCSI host interface ports (above)

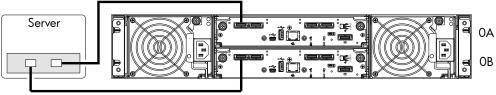
3723/3733



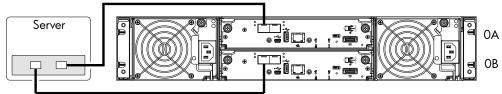
3720/3730



3523/3533 or 3520/3530



3420/3430



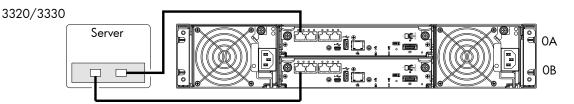
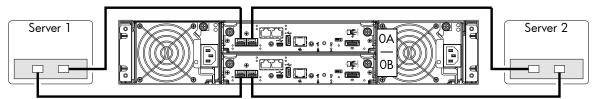


Figure 14 Connecting hosts - one server/one HBA/dual path

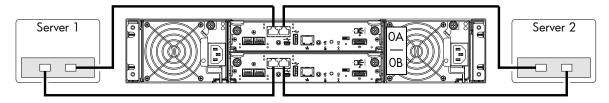
Two servers/one HBA per server/dual path

Model-specific illustrations show two-server/dual-controller configurations for 3000 Series controller enclosures supporting pertinent host interface protocols.

3920/3930

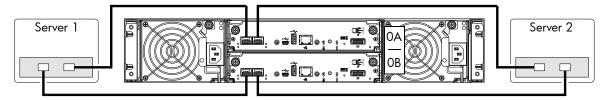


FC host interface ports (above) Note: Follow the example above when cabling the 3723/3733 to two servers

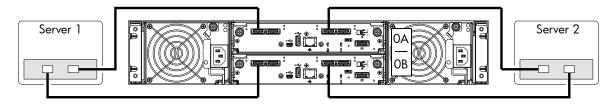


iSCSI host interface ports (above)

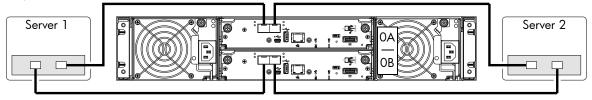
3720/3730



3523/3533 or 3520/3530



3420/3430



3320/3330

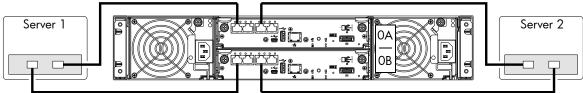
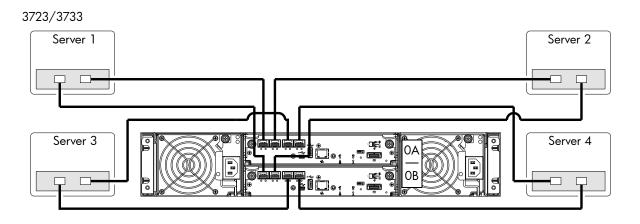


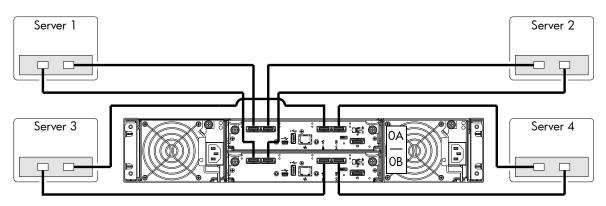
Figure 15 Connecting hosts — two servers/one HBA per server/dual path

Four servers/one HBA per server/dual path

Model-specific illustrations show four-server/dual-controller configurations for 3000 Series controller enclosures supporting pertinent host interface protocols.



3523/3533 or 3520/3530



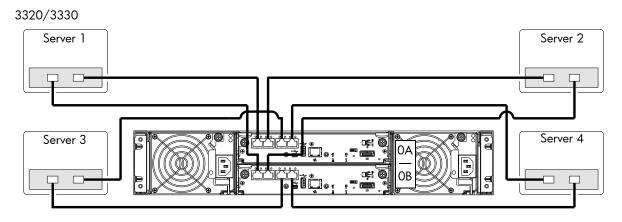


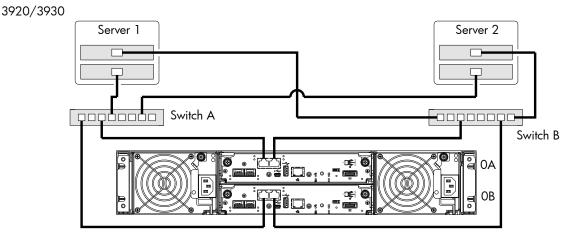
Figure 16 Connecting hosts — four servers/one HBA per server/dual path

Connecting switch attach configurations

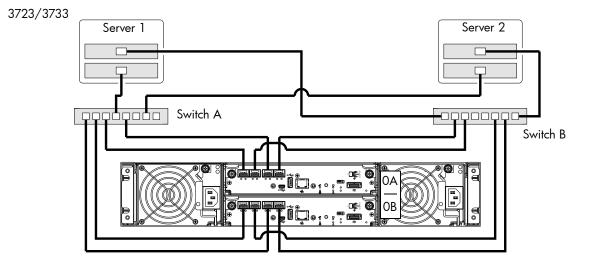
A switch attach solution — or SAN — places a switch between the servers and the controller enclosures. Using switches, a SAN shares a storage system among multiple servers, reducing the number of storage systems required for a particular environment. Using switches increases the number of servers that can be connected to the storage system. A 3000 Series controller enclosure supports 64 hosts.

Multiple servers/multiple switches

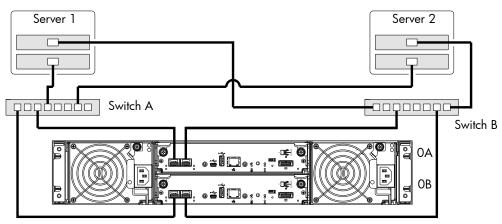
Model-specific dual-controller illustrations show switch-connect configurations for 3000 Series controller enclosures supporting pertinent host interface protocols. Connect appropriate cables from controller host ports to switch ports, and from switch ports to hosts. It is important to have a least one port connected from each switch to each controller module to provide redundancy.



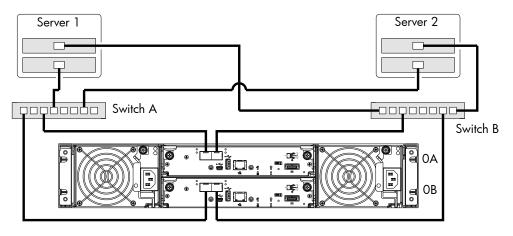
Note: FC host interface cabling is identical to that shown for 3720/3730 (below)



3720/3730



3420/3430



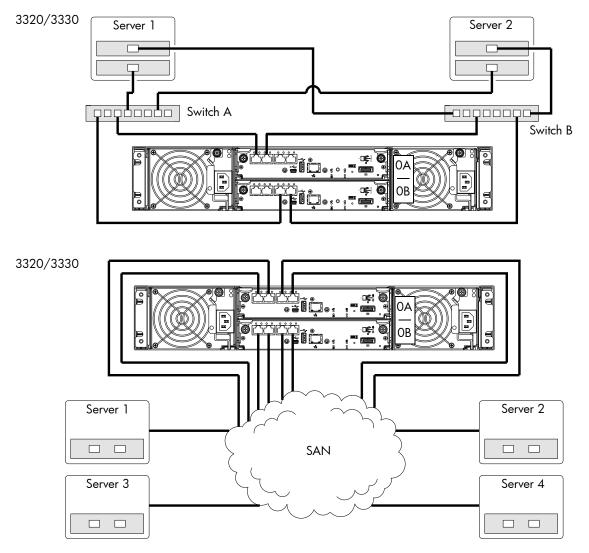


Figure 17 Connecting hosts — switch attach: multiple servers/switches

3000 Series controller enclosure iSCSI considerations

When installing a 3000 Series iSCSI controller enclosure, use at least three ports per server — two for the storage LAN, and one or more for the public LAN(s) — to ensure that the storage network is isolated from the other networks. The storage LAN is the network connecting the servers — via switch attach — to the controller enclosure (see the 3920/3930, 3420/3430, and 3320/3330 diagrams in Figure 17 on page 47).

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

The 3920/3930 uses port 2 of each controller as one failover pair, and port 3 of each controller as a second failover pair for 1Gb iSCSI traffic. Port 2 of each controller must be in the same subnet, and port 3 of each controller must be in second subnet. See 3920/3930 controller module — rear panel components on page 18 for iSCSI port numbering.

For example (with a netmask of 255.255.255.0):

- Controller A port 2: 10.10.10.100
- Controller A port 3: 10.11.10.120
- Controller B port 2: 10.10.10.110
- Controller B port 3: 10.11.10.130

The 3420/3430 (10GbE iSCSI) uses 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 3420/3430 controller module — rear panel components on page 20 for iSCSI port numbering.

For example (with a netmask of 255.255.255.0):

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

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

The 3320/3330 (1Gb iSCSI) uses a scheme that is similar to the 3420/3430 described above. See 3320/3330 controller module — rear panel components on page 20 for iSCSI port numbering.

For example (with a netmask of 255.255.255.0):

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

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

Connecting a management host on the network

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

- 1. Connect an RJ-45 Ethernet cable to the network port on each controller.
- 2. Connect the other end of each Ethernet cable to a network that your management host can access (preferably on the same subnet).
- NOTE: Connections to this device must be made with shielded cables grounded at both ends with metallic RFI/EMI connector hoods, in order to maintain compliance with NEBS and FCC Rules and Regulations. See AssuredSAN Product Regulatory Compliance and Safety (included in your product's ship kit).

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

Select AssuredSAN & R/Evolution Products > 3000 Series to download the PRC&S document.

Connecting two storage systems to replicate volumes

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

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

Replication configuration possibilities are many, and can be cabled — in switch attach fashion — to support 3000 Series controller enclosures on the same network, or on physically-split networks. As you consider the physical connections of your system — specifically connections for replication — keep several important points in mind:

- Ensure that controllers have connectivity between systems, whether local or remote.
- Assign specific ports for replication whenever possible. By specifically assigning ports available for replication, you free the controller from scanning and assigning the ports at the time replication is performed.
- For remote replication, ensure that all ports assigned for replication are able to communicate appropriately with the remote replication system (see *verify remote-link* in the CLI reference guide for more information).
- Allow at least two ports to perform replication if possible. This permits the system to load balance
 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 one port for
 replication on each controller module of a 3720/3730 or 3420/3430 system, and possibly more than
 one port per controller module on other 3000 Series models supporting replication, depending on
 anticipated replication traffic load.
- For 3920/3930 models, be sure of the desired link type before creating the replication set, because you cannot change the replication link type after creating the replication set.
- For the sake of system security, do not unnecessarily expose the controller module network port to an external network connection.

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

IMPORTANT: 3000 Series SAS controller enclosures do *not* support AssuredRemote replication.

△ CAUTION: When replacing a 3000 Series controller set supporting AssuredRemote with a 3000 Series controller set that does *not* support this licensed feature (e.g., 3520/3530), you must first delete all replication sets before swapping the controller modules. Not doing so will lead to unexpected results, and there is no way to delete replication sets after the installation. See the upgrade document supporting your product and the 3000 Series RAIDar User Guide for additional information.

IMPORTANT: AssuredRemote must be licensed on all systems configured for replication, and the controller module firmware version must be the same on all systems licensed for replication (see Updating firmware on page 56).

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

- AssuredSAN 3000 Series Using Data Protection Software
- AssuredSAN 3000 Series RAIDar User Guide

Single-controller configurations

Multiple servers/single network/two switches

The diagram below shows the rear-panel of two 3920 or 3930 controller enclosures with 2/4/8Gb FC host interface connection and 1Gb iSCSI-based replication.

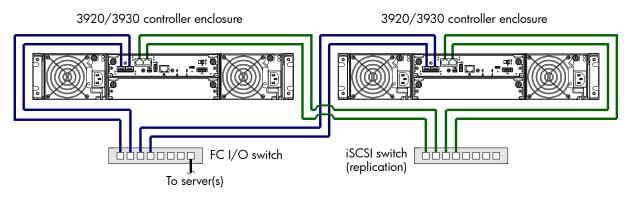


Figure 18 Connecting two systems for AssuredRemote — single-controller module

For iSCSI-based replication, the iSCSI ports should be connected to at least one iSCSI switch. For optimal protection, use two switches, with one iSCSI port from each controller connected to the first switch, and one iSCSI port from each controller connected to the second switch. Both switches should be connected to a single IP network. Using two iSCSI switches in tandem avoids the potential single point of failure inherent to using a single iSCSI switch.

Dual-controller configurations

This section shows example replication configurations for 3000 Series controller enclosures equipped with dual-controller modules. Configurations showing controller enclosures of the same model and mixed model types follow. Some of these examples show physically-split networks, while others show single-network configurations.

Multiple servers/single network

The diagram below shows 10GbE iSCSI host interface connections and 10GbE iSCSI-based replication, with both I/O and replication occurring on the same network.

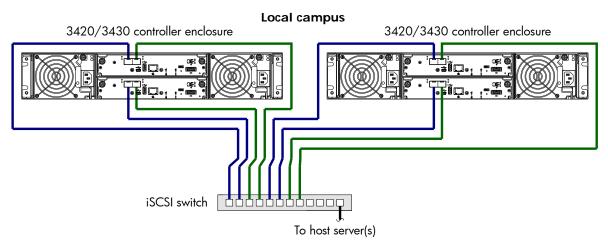


Figure 19 Connecting two systems for AssuredRemote — multiple servers/one switch/one location

The diagram below shows 1Gb iSCSI host interface connections and 1Gb iSCSI-based replication, with both I/O and replication occurring on the same network.

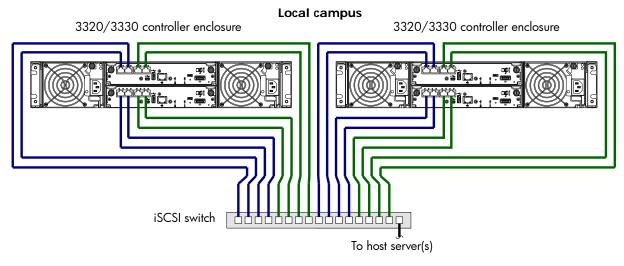
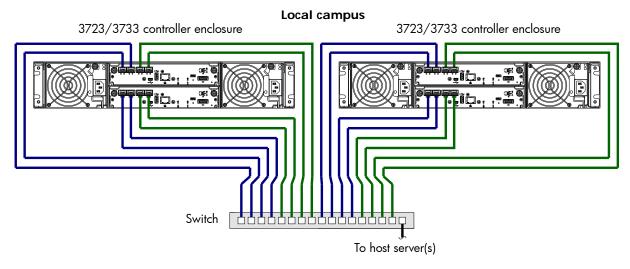
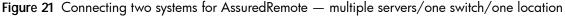


Figure 20 Connecting two systems for AssuredRemote — multiple servers/one switch/one location

With either of the replication configurations shown in the two previous figures, Virtual Local Area Network (VLAN) could be employed to provide separate networks. Whether using a single switch or multiple switches, you can create a VLAN for I/O and a VLAN for replication to isolate I/O traffic from replication traffic. Since each switch would employ both VLANs, the configuration would appear physically as a single network; while logically, the configuration would function as multiple networks.

The diagram below shows 2/4/8Gb FC host interface connections and 2/4/8Gb FC-based replication, with both I/O and replication occurring on the same network.





Note that for controller enclosures featuring 2-port FC controller modules (i.e., 3720/3730), you would cable the FC ports in similar fashion to what is shown for the 3723/3733 above, but with two fewer cables per controller module. Also see the 10GbE controller enclosures in Figure 19 on page 50 for a representative example of cabling 2-port controller modules for replication.

With the replication configuration shown in Figure 21, employ zoning to provide separate virtual networks. Whether using a single switch or multiple switches, you can create a zone for I/O and a zone for replication to isolate I/O traffic from replication traffic. Since each switch would include both zones, the configuration would appear physically as a single network, while logically, it would function as multiple networks.

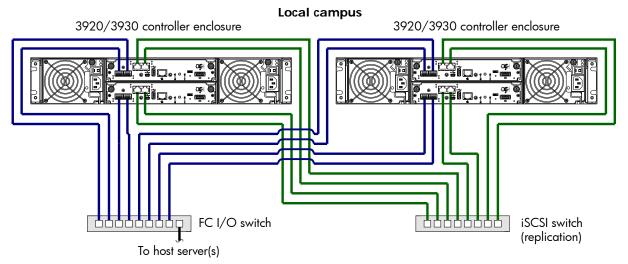


Figure 22 Connecting two systems for AssuredRemote — multiple servers/switches/one location

With the replication configuration shown in Figure 22, VLAN and zoning could 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 employ both VLANs or zones, the configuration would appear physically as a single network, while logically, it would function as multiple networks.

The preceding replication cabling diagrams show connection of controller enclosures (either single or dual-controller modules) of the same model type. The diagrams that follow provide a few examples of cabling for replication using different 3000 Series models within representative configurations.

Multiple servers/different networks/multiple switches

The diagram below shows 1Gb iSCSI and 2/4/8Gb FC host interface connections, together with 1Gb iSCSI-based replication, with I/O and replication occurring on different networks.

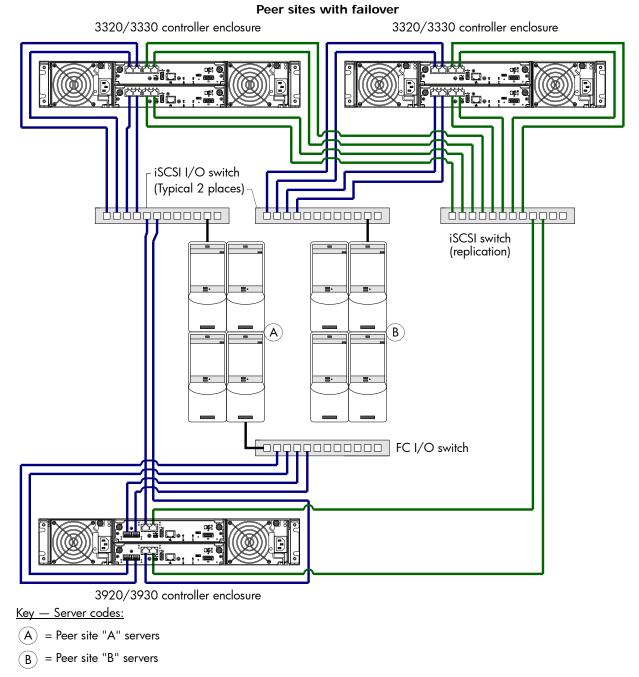
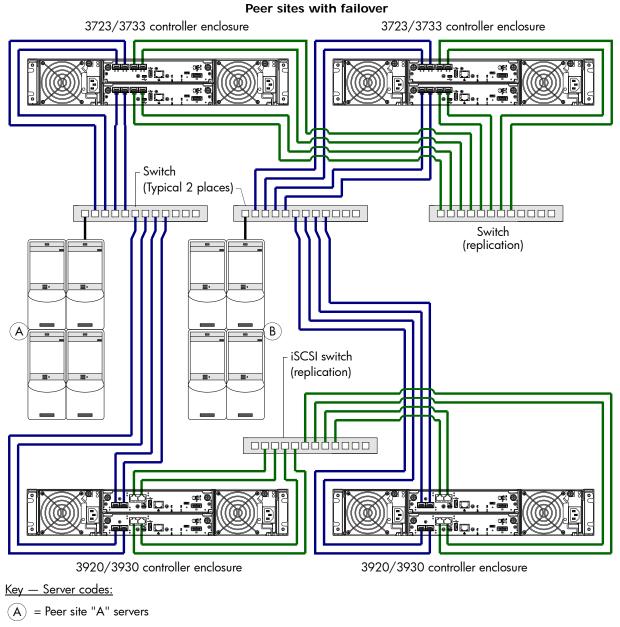


Figure 23 Connecting three systems for AssuredRemote — multiple servers/switches/two locations

The diagram below shows 1Gb iSCSI and 2/4/8Gb FC host interface connections, together with 1Gb iSCSI-based replication, with I/O and replication occurring on different networks.



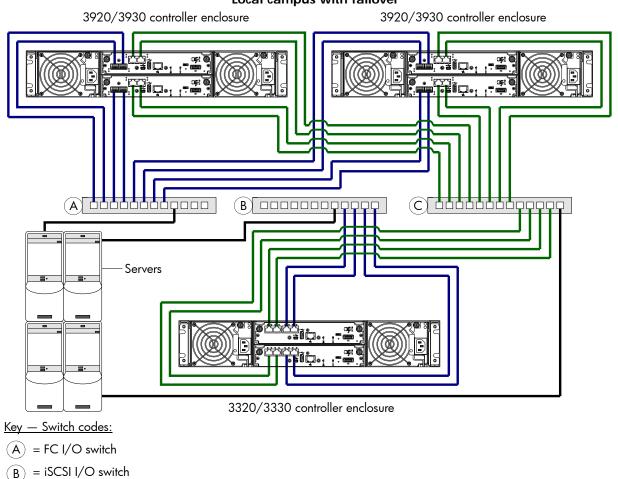
(B) = Peer site "B" servers

Figure 24 Connecting four systems for AssuredRemote — multiple servers/switches/two locations

Note that for controller enclosures featuring 2-port FC controller modules (i.e., 3720/3730), you would cable the FC ports in similar fashion to what is shown for the 3723/3733 above, but with two fewer cables per controller module.

Multiple servers/same network/multiple switches

The diagram below shows 1Gb iSCSI and 2/4/8Gb FC host interface connections, together with 1Gb iSCSI-based replication. Both I/O and replication occur on the same network with all ports assigned to factory defaults.



Local campus with failover

(C) = iSCSI replication switch

Figure 25 Connecting three systems for AssuredRemote — multiple servers/switches/one location

Multiple servers/same network/multiple switches

The diagram below shows 1Gb iSCSI, 10GbE iSCSI, and 2/4/8Gb FC host interface connections, together with 1Gb iSCSI-based and 10GbE replication. Both I/O and replication occur on the same network using a network simulator (snail).

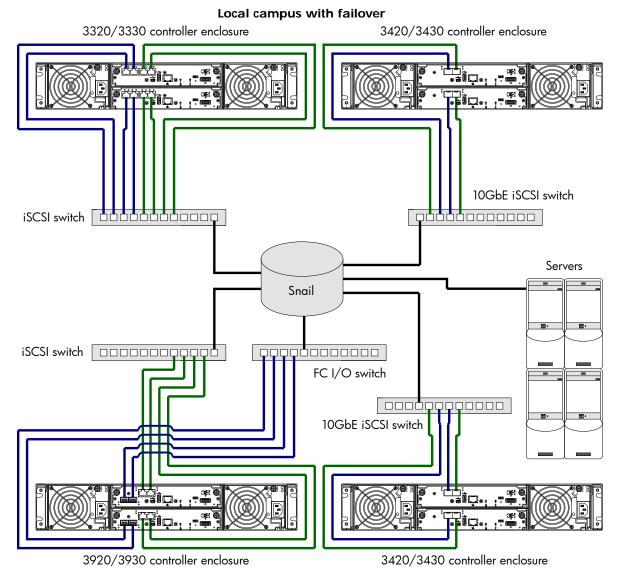


Figure 26 Connecting four systems for AssuredRemote — multiple servers/switches/one location

Updating firmware

After installing the hardware and powering on the storage system components for the first time, verify that the controller modules, expansion modules, and disk drives are using the current firmware release. Using RAIDar, right-click the system in the Configuration View panel, and select **Tools** > **Update Firmware**. The Update Firmware panel displays the currently installed firmware versions, and allows you to update them. Optionally, you can update firmware using FTP (File Transfer Protocol) as described in the AssuredSAN 3000 Series RAIDar User Guide.

When upgrading from TS100 or TS201 firmware code versions to TS230, replications in progress will temporarily halt, and report that replications have incompatible code versions. Once the partner system is successfully upgraded, the replications will resume if they have not suspended. If the replications have suspended, they can be manually resumed. See the "Suspending replication" and "Resuming replication" topics in the RAIDar user guide or online help.

Obtaining IP values

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

☆ TIP: See the "Configuring network ports" topic in the RAIDar user guide.

Setting network port IP addresses using DHCP

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one is available. If a DHCP server is unavailable, current addressing is unchanged. You must have some means of determining what addresses have been assigned, such as the list of bindings on the DHCP server.

Because DHCP is disabled by default in 3000 Series systems, you must either use the CLI (Command-line Interface) to change controller IP address settings, or use RAIDar's Configuration Wizard as described in the Using the Configuration Wizard topic in the RAIDar user guide or online help.

Setting network port IP addresses using the CLI

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.

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.

TOTE: 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 104.
- Linux customers should prepare the USB port as described in Setting parameters for the device driver on page 105.

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

Once new IP addresses are set, you can change them as needed using RAIDar. Be sure to change the IP address via RAIDar before changing the network configuration. See Accessing RAIDar on page 61 for more information concerning the web-based storage management application.

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

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

 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 27 (generic 3000 Series controller module shown). Connect USB cable to CLI port on controller face plate

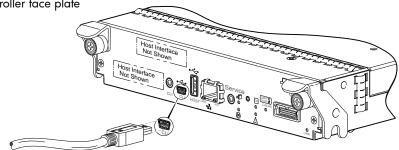


Figure 27 Connecting a USB cable to the CLI port

- 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 105.
 - Windows customers should locate the downloaded device driver described in Obtaining the software download on page 104, 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 6 and the connection settings in Table 7 (also, see the note following this procedure).

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

 Table 6
 Terminal emulator display settings

Table 7	Terminal	emulator	connection	settings

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

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

- 5. In the terminal emulator, connect to controller A.
- 6. Press Enter to display the CLI prompt (#).
 - The CLI displays the system version, MC version, and login prompt:
 - a. At the login prompt, enter the default user manage.
 - **b.** Enter the default password !manage.

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

7. At the prompt, enter the following command to set the values you obtained in step 1 for each Network port, first for controller A, and then for controller B:

set network-parameters ip *address* netmask *netmask* gateway *gateway* controller a|b where:

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

For example:

```
# set network-parameters ip 192.168.0.10 netmask 255.255.255.0 gateway
192.168.0.1 controller a
# set network-parameters ip 192.168.0.11 netmask 255.255.255.0 gateway
```

```
192.168.0.1 controller b
```

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

show network-parameters

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

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

For example:

```
# ping 192.168.0.1
Info: Pinging 192.168.0.1 with 4 packets.
Success: Command completed successfully. - The remote computer responded with 4
packets.(2011-12-19 10:20:37)
```

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

ping controller-IP-address

If you cannot access your system for at least three minutes after changing the IP address, you might need to restart the Management Controller(s) using the serial CLI.

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

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

restart mc both

- 11. When you are done using the CLI, exit the emulator.
- 12. Retain the IP addresses (recorded in step 1) for accessing and managing the controllers using either RAIDar or the CLI.

Torrest Windows host: 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 27 on page 58.

4 Basic operation

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

Accessing RAIDar

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

IMPORTANT: For detailed information on accessing and using RAIDar, see the "Getting Started" section in the web-posted AssuredSAN 3000 Series RAIDar User Guide.

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

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

Configuring and provisioning the storage system

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

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

NOTE: See the "Installing a license" topic within the RAIDar user guide for instructions about creating a temporary license, or installing a permanent license.

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

5 Troubleshooting

USB CLI port connection

AssuredSAN 3000 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 3000 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 61, use RAIDar to configure and provision the system upon completing the hardware installation. As part of this process, configure and enable event notification so the system will notify you when a problem occurs that is at or above the configured severity (see "Using the Configuration Wizard > Configuring event notification" within the RAIDar user guide). With event notification configured and enabled, you can follow the recommended actions in the notification message to resolve the problem, as further discussed in the options presented below.

Basic steps

The basic fault isolation steps are listed below:

- Gather fault information, including using system LEDs (see Gather fault information on page 64)
- Determine where in the system the fault is occurring (see Determine where the fault is occurring on page 64)
- Review event logs (see Review the event logs on page 64)
- If required, isolate the fault to a data path component or configuration (see Isolate the fault on page 65)

Cabling systems to enable use of the licensed AssuredRemote feature — to replicate volumes — is another important fault isolation consideration pertaining to initial system installation. See Isolating AssuredRemote replication faults on page 73 for more information about troubleshooting during initial setup.

Options available for performing basic steps

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

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

Use RAIDar

RAIDar uses health icons to show OK, Degraded, Fault, or Unknown status for the system and its components. RAIDar enables you to monitor the health of the system and its components. If any component has a problem, the system health will be Degraded, Fault, or Unknown. Use RAIDar's GUI to drill down to

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

Use the CLI

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

Monitor event notification

With event notification configured and enabled, you can view event logs to monitor the health of the system and its components. If a message tells you to check whether an event has been logged, or to view information about an event in the log, you can do so using either RAIDar or the CLI. Using RAIDar, you would view the event log and then click on the event message to see detail about that event. Using the CLI, you would run the show events detail command (with additional parameters to filter the output) to see the detail for an event.

View the enclosure LEDs

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

Performing basic steps

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

Gather fault information

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

Begin by reviewing the reported fault:

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

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

Determine where the fault is occurring

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

When a fault occurs, the Fault ID status LED on an enclosure's right ear illuminates (see the diagram pertaining to your product's front panel components on page 15). Check the LEDs on the back of the enclosure to narrow the fault to a FRU, connection, or both. The LEDs also help you identify the location of a FRU reporting a fault.

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

Review the event logs

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

• Critical. A failure occurred that may cause a controller to shut down. Correct the problem *immediately*.

- Error. A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
- Warning. A problem occurred that may affect system stability, but not data integrity. Evaluate the problem and correct it if necessary.
- Informational. A configuration or state change occurred, or a problem occurred that the system corrected. No immediate action is required.

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

See Dot Hill's Customer Resource Center web site for additional information: <u>http://crc.dothill.com</u>. Select AssuredSAN & R/Evolution Products > 3000 Series to download the Event Descriptions guide.

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

Isolate the fault

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

If the enclosure does not initialize

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

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

Correcting enclosure IDs

When installing a system with drive enclosures attached, the enclosure IDs might not agree with the physical cabling order. This is because the controller might have been previously attached to enclosures in a different configuration, and it attempts to preserve the previous enclosure IDs if possible. To correct this condition, make sure that both controllers are up, and perform a rescan using RAIDar or the CLI. This will reorder the enclosures, but can take up to two minutes for the enclosure IDs to be corrected.

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

rescan

- To rescan using RAIDar:
- 1. Verify that controllers are operating normally
- 2. In the Configuration View panel, right-click the system and select Tools > Rescan Disk Channels
- 3. Click Rescan
- NOTE: The reordering enclosure IDs action only applies to Dual Controller mode. If only one controller is available, due to either Single Controller configuration or controller failure, a manual rescan will not reorder the drive enclosure IDs.

Stopping I/O

When troubleshooting drive and connectivity faults, ensure you have a current full backup. As an additional data protection precaution, stop all I/O to the affected vdisks.

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

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

1. Using the CLI, run the show vdisk-statistics command.

The Number of Reads and Number of Writes outputs show the number of these operations that have occurred since the statistic was last requested.

2. Run the show vdisk-statistics command a second time.

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

3. If any reads or writes occur during this interval, a host is still reading from or writing to this vdisk. Continue to stop IOPS from hosts, and repeat step 1 until the Number of Reads and Number of Writes statistics are zero.

Torrection Water Click See Assured SAN 3000 Series CLI Reference Guide for additional information.

Diagnostic steps

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

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

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

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

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	A fault condition exists.	 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.
Yes	A fault occurred. If installing an I/O module FRU, the module has gone online and likely failed its self-test.	 Check the event log for specific information regarding the fault. Isolate the fault. If installing an I/O module FRU, try removing and reinstalling the new I/O module, and check the event log for errors. Replace if necessary. Contact an authorized service provider for assistance.

Table 8 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.	 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 9
 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: • Hardware-controlled power-up error • Cache flush error • Cache self-refresh error	 Restart this controller from the other controller using RAIDar or the CLI. Remove the controller and reinsert it. Contact an authorized service provider for assistance. Replace the controller.

 Table 10
 Diagnostics LED status
 Rear panel "Fault/Service Required"

Are both disk drive module LEDs off?

Answer	Possible reasons	Actions
Yes	There is no powerThe drive is offlineThe drive is not configured	Check that the drive is fully inserted and latched in place, and that the enclosure is powered on.

 Table 11
 Diagnostics LED status
 Disk drives (LFF and SFF modules)

Is the disk drive module Fault LED amber?

Answer	Possible reasons	Actions
Yes, and the online/activity LED is off .	The drive is offline. An event message may have been received for this device.	 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 drive is active, but an event message may have been received for this device.	 Check the event log for specific information regarding the fault. Isolate the fault. Contact an authorized service provider for assistance.

 Table 12
 Diagnostics LED status
 Disk drive fault status (LFF and SFF modules)

Is a connected host port's Host Link Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required (see Link LED note: page 91).
Yes	The link is down.	 Check cable connections and reseat if necessary. Inspect cable for damage. Swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. Verify that the switch, if any, is operating properly. If possible, test with another port. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational. In RAIDar, review event logs for indicators of a specific fault in a host data path component. Contact an authorized service provider for assistance. See Isolating a host-side connection fault on page 70.

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

Is a connected port's Expansion Port Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	 Check cable connections and reseat if necessary. Inspect cable for damage. Swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. In RAIDar, review the event logs for indicators of a specific fault in a host data path component. Contact an authorized service provider for assistance. See Isolating a controller module expansion port connection fault on page 72.

 Table 14 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 15
 Diagnostics LED status — Rear panel "Network Port Link Status"

Is the power supply's 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.	 Verify that the power cord is properly connected, and check the power source to which it connects. Check that the power supply FRU is firmly locked into position. Check the event log for specific information regarding the fault. Isolate the fault. Contact an authorized service provider for assistance.

 Table 16
 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.	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.
		 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 17
 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 event 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 super-capacitor. This process typically takes 60 seconds per 1 Gbyte of cache. After the cache is copied to CompactFlash, the remaining power left in the super-capacitor is used to refresh the cache memory. While the cache is being maintained by the super-capacitor, the Cache Status LED flashes at a rate of 1/10 second off and 9/10 second on.

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

Answer	Actions
No, the Cache LED status is off, and the controller does not boot.	If valid data is thought to be in Flash, see Transporting cache via professional services on page 70; otherwise, replace the controller.
No, the Cache Status LED is off, and the controller boots.	The system is flushing data to disks. If the problem persists, replace the controller.
Yes, at a strobe 1:10 rate - 1 Hz, and the controller does not boot.	See Transporting cache via professional services.
Yes, at a strobe 1:10 rate - 1 Hz, and the controller boots.	The system is flushing data to disks. If the problem persists, replace the controller.

 Table 18
 Diagnostics LED status – Rear panel "Cache Status" (continued)

Answer	Actions
Yes, at a blink 1:1 rate - 1 Hz, and the controller does not boot.	See Transporting cache via professional services.
Yes, at a blink 1:1 rate - 1 Hz, and the controller boots.	The system is flushing data to disks. If the problem persists, replace the controller.

 Table 18 Diagnostics LED status — Rear panel "Cache Status" (continued)

Transporting cache via professional services

IMPORTANT: Transportable cache only applies to single-controller configurations. In dual-controller configurations, there is no need to transport a failed controller's cache to a replacement controller because the cache is duplicated between the partner controllers.

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

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

Isolating a host-side connection fault

During normal operation, when a controller module host port is connected to a data host, the port's host link status LED and host link activity LED are 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 FC or 10GbE iSCSI host ports

The procedure below pertains to AssuredSAN 3000 Series controller enclosures employing small form factor pluggable (SFP) transceiver connectors in either 2/4/8Gb Fibre Channel or 10GbE iSCSI host interface ports. In the following procedure, *SFP* and *host cable* are used to refer to either an SFP with FC cable or a qualified 10GbE SFP+ option.

- 1. Halt all I/O to the storage system (see Stopping I/O on page 65).
- 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's cached data is flushed to the disk drives.
 - Blinking Data is still being written to disk.
 - Off Cache is clean (no unwritten data).
- 4. Inspect the cable for damage.
- 5. Reseat the SFP and host cable.
 - 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.

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 LED on?

- Yes You now know that the SFP, host cable, and host-side devices are functioning properly. Return the SFP and 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 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 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 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 LED on?

- No The controller module's 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 SFPs, damaged cables, and HBAs.

Host-side connection troubleshooting featuring SAS or iSCSI host ports

The procedure below applies to AssuredSAN 3000 Series controller enclosures configured with either 6Gb SFF miniSAS or 1Gb iSCSI host interface ports.

- 1. Halt all I/O to the storage system (see Stopping I/O on page 65).
- 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's cached data is flushed to the disk drives.
 - Blinking Data is still being written to disk.
 - Off Cache is clean (no unwritten data).
- 4. Inspect the cable for damage.
- 5. Reseat the cable.

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.
- 6. Move the 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's port. Replace the controller module.
- No Proceed to the next step.
- 7. Verify that the switch, if any, is operating properly. If possible, test with another port.
- 8. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
- 9. 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.
- 10. Move the cable back to its original port.

Is the host link status LED on?

- No The controller module's 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 65).
 - **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's cached data is flushed to the disk drives.
 - Blinking Data is still being written to disk.
 - Off Cache is clean (no unwritten data).
- 4. Reseat the expansion cable, and inspect it for damage.

Is the expansion port status LED on?

- Yes Monitor the status to ensure there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
- No Proceed to the next step.
- 5. Move the expansion cable to a port on the controller enclosure with a known good link status. This step isolates the problem to the expansion cable or to the controller module's expansion port. Is the expansion port status LED on?
 - Yes You now know that the expansion cable is good. Return the cable to the original port. If the expansion port status LED remains off, you have isolated the fault to the controller module's expansion port. Replace the controller module.
 - No Proceed to the next step.
- 6. Move the expansion cable back to the original port on the controller enclosure.
- 7. Move the expansion cable on the drive enclosure to a known good expansion port on the drive enclosure.

Is the expansion port status LED on?

- Yes You have isolated the problem to the drive enclosure's port. Replace the expansion module.
- No Proceed to the next step.

8. Replace the cable with a known good cable, ensuring the cable is attached to the original ports used by the previous cable.

Is the host link status LED on?

- Yes Replace the original cable. The fault has been isolated.
- No It is likely that the controller module must be replaced.

Isolating AssuredRemote replication faults

Cabling for replication

AssuredRemote replication is a disaster-recovery feature that performs batch replication of block-level data from a primary volume in one 3000 Series controller enclosure to a secondary volume in the same system, or in a second, independent 3000 Series controller enclosure. The second system can be located at the same site as the first system, or at a different site. See Connecting two storage systems to replicate volumes on page 48 for host connection information concerning AssuredRemote.

NOTE: See the AssuredRemote topic within the RAIDar guide or online help for additional information. 3920/3930, 3723/3733, 3720/3730, 3420/3430, and 3320/3330 models support AssuredRemote replication; whereas 3523/3533 and 3520/3530 models do not.

△ CAUTION: When replacing a 3000 Series controller set supporting AssuredRemote with a 3000 Series controller set that does not support this licensed feature (e.g., 3520/3530), you must first delete all replication sets before swapping the controller modules. Not doing so will lead to unexpected results, and there is no way to delete replication sets after the installation. See the upgrade document supporting your product and the 3000 Series RAIDar User Guide for additional information.

Replication setup and verification

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

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

- See AssuredSAN 3000 Series Using Data Protection Software for best practices.
- See AssuredSAN 3000 Series RAIDar User Guide for procedures to setup and manage replications.
- See AssuredSAN 3000 Series CLI Reference Guide for replication commands and syntax.
- See AssuredSAN 3000 Series Event Descriptions Reference Guide for replication event reporting.

Basic information for enabling the 3000 Series controller enclosures for replication supplements the troubleshooting procedures that follow.

- Familiarize yourself with AssuredRemote by reviewing the "Getting started" and "Using AssuredRemote to replicate volumes" chapters in the RAIDar User Guide.
- For best practices concerning replication-related tasks, see Using Data Protection Software.
- Use RAIDar's Wizards > Replication Setup Wizard to prepare to replicate an existing volume to another vdisk in the primary system or secondary system.

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

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

Diagnostic steps for replication setup

Answer	Possible reasons	Actions	
Yes	System functioning properly.	No action required.	
No	AssuredRemote is not licensed on each controller enclosure used for replication.	 Verify licensing of the optional feature per system: In RAIDar's Configuration View panel, 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. MOTE: AssuredRemote is not supported by 3000 Series SAS controller enclosures. 	
No	Proper firmware revision supporting AssuredRemote is not running on each system used for replication.	 Perform the following actions on each system used for replication: In RAIDar's Configuration View panel, 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.)	 Verify controller enclosure cabling: 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. 	

Can you successfully use the AssuredRemote feature?

 Table 19
 Diagnostics for replication setup — Using AssuredRemote feature

Can you view information about remote links?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Communication link is down	 Check cable connections and reseat if necessary. Inspect cable for damage. Swap cables to determine if fault is caused by a defective cable; replace cable if necessary. In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. In RAIDar's Configuration View panel, right-click the remote system, and select Tools > Check Remote System Link. Click Check Links.

 Table 20
 Diagnostics for replication setup — Viewing information about remote links

enclosures with iSCSI ports, replication set due to use of CHAP. ect the primary volume the data to replicate? ect the replication	 No action required. If using CHAP (Challenge-Handshake Authentication Protocol), configure it as described in the RAIDar topics "Using the Replication Setup Wizard" or "Replicating a volume." In RAIDar's Configuration View panel, expand vdisk entries to show secondary volumes. In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. 	
e ports, replication set due to use of CHAP. ect the primary volume the data to replicate?	 configure it as described in the RAIDar topics "Using the Replication Setup Wizard" or "Replicating a volume." In RAIDar's Configuration View panel, expand vdisk entries to show secondary volumes. In RAIDar, review event logs for indicators of a specific fault 	
the data to replicate?	to show secondary volumes.In RAIDar, review event logs for indicators of a specific fault	
ect the replication		
	 In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. In RAIDar's Configuration View panel, right-click a subordinate volume, and select View > Overview to view links. Local Replication mode replicates to a secondary volume residing in the local storage system. Verify selection of a valid local volume on vdisk. Remote Replication mode replicates to a secondary volume residing in an independent storage system: Verify selection of a valid remote volume on vdisk. Verify selection of valid remote volume on vdisk. Verify valid IP address of remote system's network port. Verify user name with Manage role on remote system. Verify user's password on remote system. 	
ect the secondary lestination volume on vhich you will replicate primary volume)? ¹	 In RAIDar, review event logs for indicators of a specific fault in a replication data path component. Verify valid specification of the secondary volume according to either of the following criteria: Creation of the new volume on vdisk Selection of replication-prepared volume In RAIDar's Configuration View panel, right-click the secondary volume, and select View > Overview to display the Replication Volume Overview table. Verify the type and numbering of ports used for the inter-system link. Verify that the vdisk volume has sufficient space to accommodate replicated data. 	
on link is down.	 See actions described in Can you view information about remote links? on page 74. 	
•	on link is down.	

Table 21Diagnostics for replication setupCreating a replication set

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	AssuredRemote is not licensed on each controller enclosure used for replication.	See actions described in Can you successfully use the AssuredRemote feature? on page 74.
No	Nonexistent replication set.	 Determine existence of primary or secondary volumes. If a replication set has not been successfully created, use RAIDar's Replication Setup Wizard to create one. In RAIDar, review event logs for indicators of a specific fault in a replication data path component.
No	Network error occurred during in-progress replication.	 In RAIDar, review event logs for indicators of a specific fault in a replication data path component. In RAIDar's Configuration View panel, right-click the secondary volume, and select View > Overview to display the Replication Volume Overview table: 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 74.

 Table 22
 Diagnostics for replication setup — Replicating a volume

Can you view a replication image?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Nonexistent replication image.	 In RAIDar's Configuration View panel, expand vdisks and subordinate volumes to reveal the existence of a replication image. If a replication image has not been successfully created, use RAIDar to create one as described in the "Using AssuredRemote to replicate volumes" topic within the RAIDar User Guide.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 74.

Table 23Diagnostics for replication setup — Viewing a replication image

Can you view remote systems?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Non-existent replication set.	See actions described in Can you replicate a volume? on page 76.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 74.

 Table 24
 Diagnostics for replication setup — Viewing a remote system

Resolving voltage and temperature warnings

 Check that all of the fans are working by making sure the Voltage/Fan Fault/Service Required LED on each power supply module is off, or by using RAIDar to check enclosure health status. In the Configuration View panel, right click the enclosure and click View > Overview to view the health status of the enclosure and its components.

See Options available for performing basic steps on page 63 for a description of health status icons and alternatives for monitoring enclosure health.

- 2. Make sure that all modules are fully seated in their slots and that their latches are locked.
- 3. Make sure that no slots are left open for more than two minutes.

If you need to replace a module, leave the old module in place until you have the replacement or use a blank module to fill the slot. Leaving a slot open negatively affects the airflow and can cause the enclosure to overheat.

- 4. Try replacing each power supply one at a time.
- 5. Replace the controller modules one at a time.

Sensor locations

The storage system monitors conditions at different points within each enclosure to alert you to problems. Power, cooling fan, temperature, and voltage sensors are located at key points in the enclosure. In each controller module and expansion module, the enclosure management processor (EMP) monitors the status of these sensors to perform SCSI enclosure services (SES) functions.

The following sections describe each element and its sensors.

Power supply sensors

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

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

 Table 25
 Power supply sensor descriptions

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's 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.

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

 Table 26
 Cooling fan sensor descriptions

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.

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

 Table 27
 Controller module temperature sensor descriptions

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 28	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

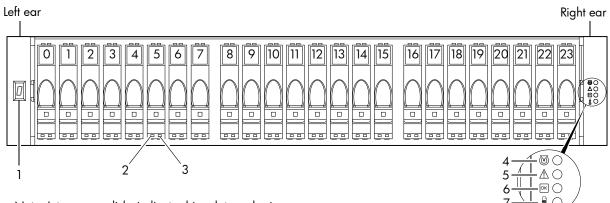
Power supply voltage sensors ensure that an enclosure's power supply voltage is within normal ranges. There are three voltage sensors per power supply.

 Table 29
 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

24-drive enclosure front panel LEDs



Note: Integers on disks indicate drive slot numbering sequence.

Table 30 LEDs - 2U24 enclosure front panel

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 82.
3	Disk drive — Right LED	See Disk drive LEDs on page 82.
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.

12-drive enclosure front panel LEDs

Standard-depth model

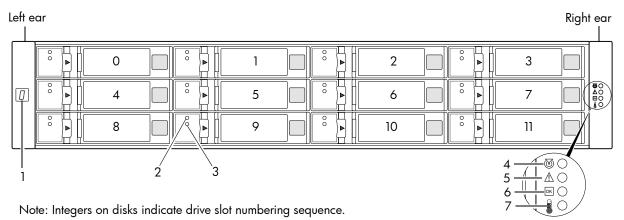
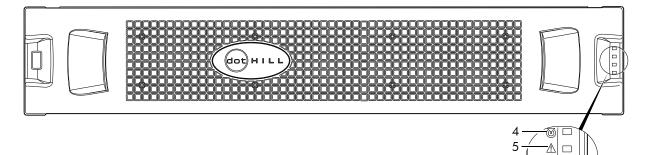


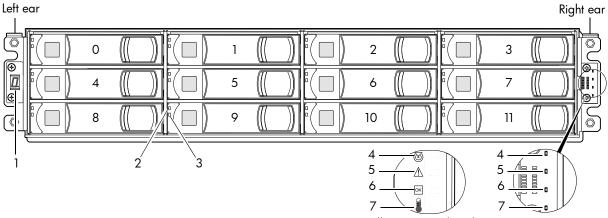
Table 31 LEDs -2U12 enclosure front panel: standard-depth

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 82.
3	Disk drive — Lower LED	See Disk drive LEDs on page 82.
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.

Reduced-depth model



Note: Remove this enclosure bezel to access the front panel components shown below. Left ear



(Silk screens on bezel)

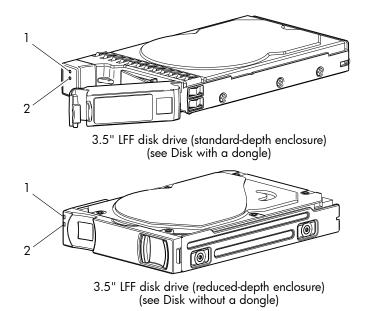
6

7

Note: Bezel is removed to show front panel LEDs. Integers on disks indicate drive slot numbering sequence. **Table 32** LEDs — 2U12 enclosure front panel: reduced-depth

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 82.
3	Disk drive — Lower LED	See Disk drive LEDs on page 82.
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.

Disk drive LEDs



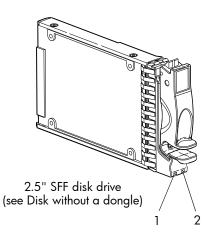


Table 33	LEDs —	Disk	with	a	dongle
----------	--------	------	------	---	--------

LED No./Description	Color	State	Definition
1 — OK to Remove	Blue	On	The disk has been removed from any active vdisk, spun down, and prepared for removal.
		Off	The disk drive module is not prepared for removal.
2— Power/Activity/Fault	Green	On	The disk drive module is operating normally.
		Blink	The disk drive module is initializing; active and processing I/O; performing a media scan; or the vdisk is initializing or reconstructing.
		Off	If not green or amber, the disk is not powered on.
	Amber	On	The disk has failed; experienced a fault; is a leftover; or the vdisk that it is associated with is down or critical.
		Blink	Physically identifies the disk drive module.
		Off	If not green or amber, the disk is not powered on.

Table 34	LEDs — Disk without a don	gle

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

Table 35	LEDs —	Disks	in LFF	and	SFF	enclosures
----------	--------	-------	--------	-----	-----	------------

Disk drive module L	ED behavior	LFF — 1	2-drive ¹	SFF — 24-drive		
Description	State	Color	Action	Color	Action	
Disk drive OK, FTOL	Off	None	None	None	None	
	On (operating normally)	Green	On	Green	On	
	OK to remove	Green	Blink	Green	On	
		Blue	On	Blue	On	
	Identifying self — offline/online	Amber	Blink	Green ²	On	
				Amber	Blink	
Disk drive I/O	Initializing	Green	Blink	Green	Blink	
	Active and processing I/O	Green	Blink	Green	Blink	
	Performing a media scan	Green	Blink	Green	Blink	
Disk drive leftover	Disk drive is a leftover	Amber	On	Amber	On	
	Identifying a leftover	Amber ³	Blink	Amber	Blink	
		Blue ²	On	Blue ²	Blink	
Disk drive failed	Fault or failure	Amber	On	Green ²	On	
				Amber	On	
	Fault and remove disk drive	Amber	On	Green	On	
		Blue	On	Amber	On	
	Fault and identify disk drive	Amber	Blink	Green	On	
				Amber	On	
	Fault, identify, and remove disk drive	Amber	Blink	Green	On	
		Blue	On	Amber	Blink	
				Blue	On	

¹The LFF disks used in LFF 12-drive reduced-depth enclosures follow SFF 24-drive disk LED behavior. ²This color may or may not illuminate.

³Bitonal LED blinks amber/green.

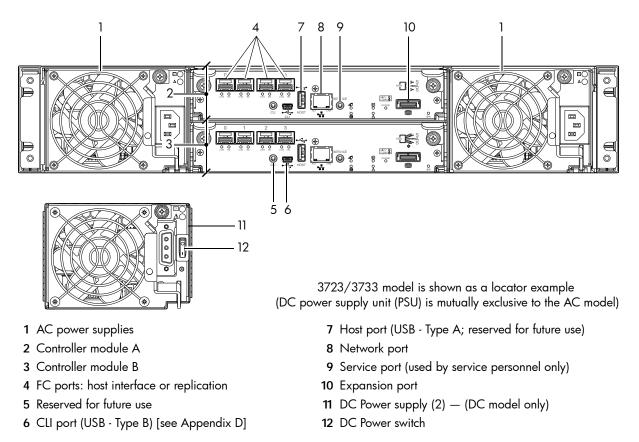
 Table 36
 LEDs — Vdisks in LFF and SFF enclosures

Vdisk LED behavior	LFF — 1	2-drive ¹	SFF — 24-drive		
Description	State	Color	Action	Color	Action
FTOL	On (operating normally)	Green	Blink	Green	On
Vdisk activity	Vdisk is reconstructing	Green	Blink	Green	Blink
	Vdisk is initializing	Green	Blink	Green	Blink
Vdisk degraded	Vdisk is critical/down See note 1 below See no		See note	e 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 3000 Series controller enclosure. The 3723/3733 is shown as a representative example of controller enclosure models included in the product series.



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: In controller enclosures configured with a single controller module, the lower IOM slot is empty, and must be covered with an IOM blank 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 3000 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 3000 Series controller enclosures.

3920/3930 controller module — rear panel LEDs

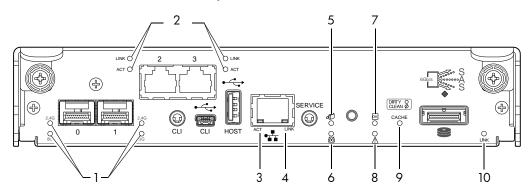


 Table 37
 LEDs - 3920/3930 controller module - rear panel

LED No./Description	Color	State	Definition
1 — Host 2/4/8Gb FC Link Status/ Link Activity	Green	On	Port is connected and the link is up. 2,4G LED illuminates — link speed is 2 or 4-Gbps 8G LED illuminates — link speed is 8-Gbps
		Off	Both LEDs off — link speed is 1-Gbps ¹
		Blink	1Hz — no link detected
2 — Host 1Gb iSCSI	Green	On	The port is connected and the link is up.
Link Status		Off	The port is empty or the link is down.
Link Activity	Green	Blink	Link has I/O activity.
		Off	Link is idle.
3 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
4 — Network Port Link Status	Green	On	The Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
5 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
6 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
7 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
8 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
9 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 91)
10 — Expansion Port Status	Green	On	Port is connected and the link is up.
		Off	Port is empty or link is down.

¹The 8Gb SFP modules do not support 1Gb link speeds.

3723/3733 controller module — rear panel LEDs

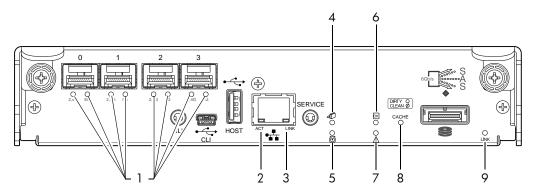


Table 38	LEDs - 3723/3733	controller module — rear panel
	1203 072070700	connoner medele real panel

LED No./Description	Color	State	Definition
1 — Host 2/4/8Gb FC Link Status/ Link Activity	Green	On	Port is connected and the link is up. 2,4G LED illuminates — link speed is 2 or 4-Gbps 8G LED illuminates — link speed is 8-Gbps
		Off	Both LEDs off — link speed is 1-Gbps ¹
		Blink	1Hz — no link detected
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	The Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 91)
9 — Expansion Port Status	Green	On	Port is connected and the link is up.
		Off	Port is empty or link is down.

¹The 8Gb SFP modules do not support 1Gb link speeds.

NOTE: The 3XX3 controller modules are compatible with 3000 Series reduced-depth controller enclosure models. To realize performance improvements, the chassis must have a PCIe Gen 2 capable midplane.

3720/3730 controller module — rear panel LEDs

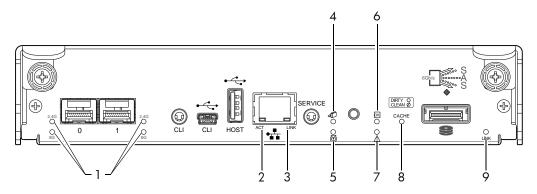


Table 39 LEDs - 3720/3730 controller module - rear panel

LED No./Description	Color	State	Definition
1 — Host 2/4/8Gb FC Link Status/ Link Activity	Green	On	Port is connected and the link is up. 2,4G LED illuminates — link speed is 2 or 4-Gbps 8G LED illuminates — link speed is 8-Gbps
		Off	Both LEDs off — link speed is 1-Gbps ¹
		Blink	1Hz — no link detected
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	The Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 91)
9 — Expansion Port Status	Green	On	Port is connected and the link is up.
		Off	Port is empty or link is down.

¹The 8Gb SFP modules do not support 1Gb link speeds.

3523/3533 or 3520/3530 controller module — rear panel LEDs

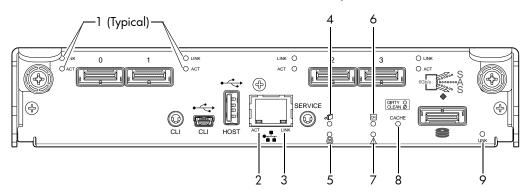


Table 40 LEDs - 3523/3533 or 3520/3530 controller module - rear panel

LED No./Description	Color	State	Definition
1 — 6Gb SAS Link Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.
6Gb SAS Link Activity	Green	Blink	Link has I/O activity.
		Off	Link is idle.
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 91)
9 — Expansion Port Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.

NOTE: The 3XX3 controller modules are compatible with 3000 Series reduced-depth controller enclosure models. To realize performance improvements, the chassis must have a PCIe Gen 2 capable midplane.

3420/3430 controller module — rear panel LEDs

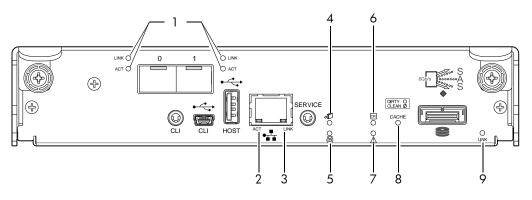


Table 41 LEDs — 3420/3430 controller module — rear panel	Table 41	LEDs — 3420/3430 contr	roller module — rear panel
--	----------	------------------------	----------------------------

LED No./Description	Color	State	Definition
1 — 10GbE iSCSI Link Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.
10GbE iSCSI Link Activity	Green	Blink	Link has I/O activity.
		Off	Link is idle.
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 91)
9 — Expansion Port Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.

3320/3330 controller module — rear panel LEDs

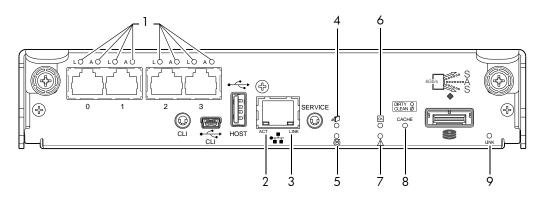


Table 42	LEDs — 3320/3330 controller module — rear panel
----------	---

LED No./Description	Color	State	Definition
1 — 1Gb iSCSI Link Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.
1Gb iSCSI Link Activity	Green	Blink	Link has I/O activity.
		Off	Link is idle.
2 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.
3 — Network Port Link Status	Green	On	Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Cache Status	Green	On	Cache is dirty and operation is normal.
		Off	Cache is clean (contains no unwritten data).
		Blink	CompactFlash flush or cache self-refresh is in progress, indicating cache activity. (See Cache Status LED details on page 91)
9 — Expansion Port Status	Green	On	The port is connected and the link is up.
		Off	The port is empty or the link is down.

IMPORTANT: Early versions of 3000 Series controller modules show network port LEDs in reversed position: LINK is shown on the left and ACT is shown on the right. On such units, the LED labeled LINK reports ACT behavior and the LED labeled ACT reports LINK behavior.

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

When a controller is shut down or otherwise rendered inactive — its Link Status LED remains illuminated — falsely indicating that the controller can communicate with the host. Though a link exists between the host and the chip on the controller, the controller is not communicating with the chip. To reset the LED, the controller must be power-cycled (see Powering on/powering off on page 33).

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 super-capacitor 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.

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 (the newer model shown below has no power switch). Whether a power supply has a power switch is significant to powering on/off.

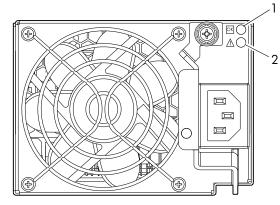
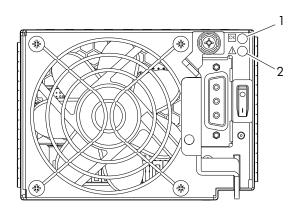


 Table 43
 LEDs — Power supply units — rear panel

AC model



DC model

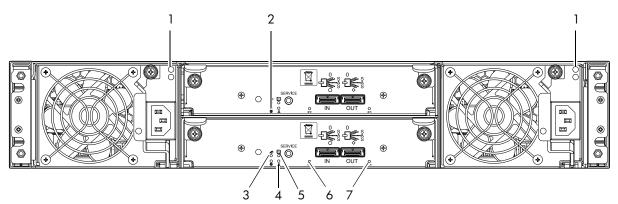
LED No./Description	Color	State	Definition
1 — Input Source Power Good	Green	On	Power is on and input voltage is normal.
		Off	Power is off, or input voltage is below the minimum threshold.
2 — Voltage/Fan Fault/Service Required	Amber	On	Output voltage is out of range, or a fan is operating below the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

NOTE: See Powering on/powering off on page 33 for information on power-cycling enclosures.

2122/3120/3130 drive enclosure rear panel LEDs

The rear panel layouts of the 2122, 3120, and 3130 drive enclosures are nearly identical. Using mini-SAS (SFF-8088) external connectors, the 2122 supports a 3-Gbps data rate for backend SAS expansion; whereas the 31XX models support 6-Gbps. Accordingly, the 31XX expansion modules feature a "6 Gb/s" label above each SAS (ingress/egress) expansion port, whereas the 2122 does not.

Newer models of these drive enclosures feature AC power supplies without power switches, as per the system shown below. See Powering on/powering off on page 33 for more information.



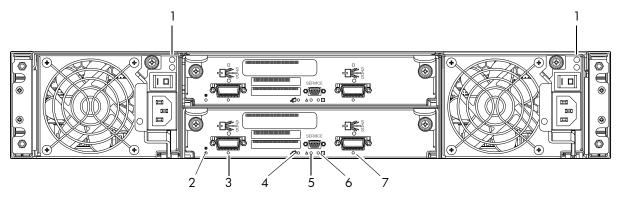
Note: Callouts do not tag multiple instances of an identified LED.

Table 44	LEDs —	- 2122/31XX	rear	panel
----------	--------	-------------	------	-------

LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 91.
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.

2130 12-drive enclosure rear panel LEDs

The rear panel layout of the 2130 drive enclosure is shown below. Using SAS (8470) external connectors, this model supports 3-Gbps data rate for backend SAS expansion. Although power switches are shown on AC power supplies in the diagram below, newer models of this drive enclosure feature AC power supplies without power switches. See Powering on/powering off on page 33 for more information.



Note: Callouts do not tag multiple instances of an identified LED.

LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 91.
2 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the expansion module.
3 — SAS In Port Status	Green	On	Port is connected and link is up.
		Off	Port is empty or link is down.
4 — OK to Remove	Blue	Off	Not implemented.
5 — Fault/Service Required	Amber	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up.
6 — FRU OK	Green	On	Expansion module is operating normally.
		Off	Expansion module is not OK.
		Blink	System is booting.
7 — SAS Out Port Status	Green	On	Port is connected and link is up.
		Off	Port is empty or link is down.

Table 45 LEDs — 2130 rear panel

B Environmental requirements and specifications

Safety requirements

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

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

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

Select AssuredSAN & R/Evolution Products > 3000 Series to download the PRC&S document.

Site requirements and guidelines

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

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

Site wiring and AC power requirements

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

Measurement	Rating
Input power requirements	100-240VAC, 50/60Hz
Maximum input power	436W maximum continuous
Heat dissipation	1,488 BTUs/hour

Table 46 Power requirements - AC Input

- 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 47	Power re	quirements -	DC Input
----------	----------	--------------	----------

Measurement	Rating
Input power requirements	-40 to -72VDC, -48/-60V nominal
Maximum input power	436W maximum continuous
Heat dissipation	1,488 BTUs/hour

The 3000 Series system is suitable for installation as part of the Common Bonding Network (CBN). The system's Battery Return (BR) Input Terminals are considered to be an Isolated DC Return (DC-I).

The following criteria are required for all installations:

- All DC mains and supply conductors to power distribution boxes for the rack-mounted system must comply with local, national, or other applicable government codes and regulations.
- Ensure that the voltage of your power source matches the voltage inscribed on the equipment's electrical label.
- To ensure redundancy, provide two separate power sources for the enclosures. These power sources must be independent of each other, and each must be controlled by a separate circuit breaker at the power distribution point.
- The system requires voltages within minimum fluctuation. The customer-supplied facilities' voltage must maintain a voltage within the range specified on the equipment's electrical rating label. The customer facilities must also provide suitable surge protection.
- Site wiring must include an earth ground connection to the DC power source. Grounding must comply with local, national, or other applicable government codes and regulations.
- Power circuits and associated circuit breakers must provide sufficient power and overload protection.

Weight and placement guidelines

Refer to Physical requirements on page 97 for detailed size and weight specifications.

- The weight of an enclosure depends on the number and type of modules installed.
- Ideally, use two people to lift an enclosure. However, one person can safely lift an enclosure if its weight is reduced by removing the power supply modules and disk drive modules.
- Do not place enclosures in a vertical position. Always install and operate the enclosures in a horizontal 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 99 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.
- 3000 Series controller and drive enclosures are suitable for connection to intra-building or non-exposed wiring or cabling only.
- 3000 Series controller and drive enclosures are suitable for installation in Network Telecommunication Facilities and locations where the NEC applies. 3000 Series enclosures are not suitable for Outside Plant (OSP) installations.

Management host requirements

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

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

Physical requirements

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

The chassis of a 3000 Series controller or drive enclosure is comprised of sheet steel that is bonded together using rivets, welding, and other forced contact methods. The metal surfaces are free from non-conductive coatings and paint.

Table 48 and Table 49 on page 98 show enclosure dimensions and weights. Enclosure designators are described below. Enclosure weights assume the following configuration characteristics:

- 2U12 enclosure (LFF also see Table 4 on page 26):
 - "2U12" denotes the 3.5" 12-drive enclosure (with controller or expansion modules)
 - The 2U12 chassis is equipped with a disk in each disk drive slot
 - LFF is further delineated by standard-depth and the new reduced-depth (short) chassis
- 2U24 enclosure (SFF– also see Table 4 on page 26):
 - "2U24" denotes the 2.5" 24-drive enclosure (with controller or expansion modules)
 - The 2U24 chassis is equipped with a disk in each disk drive slot

- SFF is further delineated by standard-depth and the new reduced-depth (short) chassis
- Two controller modules or two expansion modules per enclosure
- Two power supply modules per enclosure

Table 48 Rackmount enclosure dimensions

Specifications	Rackmount
2U Height (y-axis):	8.9 cm (3.5 inches)
Width (x-axis):	
Chassis-onlyChassis with ear caps or enclosure bezel	44.7 cm (17.6 inches) 47.9 cm (18.9 inches)
Depth (z-axis): SFF standard-depth enclosure (2U24):	
Back of chassis ear to controller latchFront of chassis ear to back of cable bend	53.8 cm (21.2 inches) 59.9 cm (23.6 inches)
SFF reduced-depth enclosure (2U24):	
Back of chassis ear to controller latchFront of chassis ear to back of cable bend	51.8 cm (20.4 inches) 57.9 cm (22.8 inches)
LFF standard-depth enclosure (2U12):	
Back of chassis ear to controller latchFront of chassis ear to back of cable bend	59.7 cm (23.5 inches) 67.1 cm (26.4 inches)
LFF reduced-depth enclosure (2U12):	
Back of chassis ear to controller latchFront of chassis ear to back of cable bend	54.9 cm (21.6 inches) 59.9 cm (23.6 inches)

Table 49	Rackmount	controller	enclosure	weights
----------	-----------	------------	-----------	---------

Specifications	Rackmount
SFF standard-depth controller enclosure (2U24):	9.1 kg (20.0 lb) [chassis]
 Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	17.9 kg (39.4 lb) 23.9 kg (52.6 lb)
SFF reduced-depth controller enclosure (2U24):	8.6 kg (19.0 lb) [chassis]
 Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	17.4 kg (38.4 lb) 23.4 kg (51.6 lb)
 LFF standard-depth controller enclosure (2U12) Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	9.3 kg (20.6 lb) [chassis] 18.1 kg (40.0 lb) 27.7 kg (61.0 lb)
 LFF reduced-depth controller enclosure (2U12) Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	8.5 kg (18.8 lb) [chassis] 17.3 kg (38.2 lb) 26.9 kg (59.2 lb)

¹Weights shown are nominal, and subject to variances.

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

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

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

NOTE: The table below provides information about optional drive enclosures that are compatible with 3000 Series controller enclosures.

 Table 50
 Rackmount compatible drive enclosure weights (ordered separately)

Specifications	Rackmount
3120 (SFF 2.5" 24-drive standard-depth enclosure)	9.1 kg (20.0 lb) [chassis]
 Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	16.7 kg (36.8 lb) 22.7 kg (50.0 lb)
3120 (SFF 2.5" 24-drive reduced-depth enclosure)	8.6 kg (19.0 lb) [chassis]
 Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	16.2 kg (35.8 lb) 22.2 kg (49.0 lb)
3130 (LFF 3.5" 12-drive standard-depth enclosure)	9.3 kg (20.6 lb) [chassis]
 Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	17.0 kg (37.4 lb) 26.5 kg (58.4 lb)
3130 (LFF 3.5" 12-drive reduced-depth enclosure)	8.5 kg (18.8 lb) [chassis]
 Chassis with FRUs (no disks)¹⁻³ Chassis with FRUs (including disks)¹⁻⁴ 	16.1 kg (35.6 lb) 25.6 kg (56.6 lb)
2122 (SFF 2.5" 24-drive enclosure: 2002 Series)	See data sheet on web site ⁵
2130 (LFF 3.5" 12-drive enclosure: 2002 Series)	See data sheet on web site ⁵

¹Weights shown are nominal, and subject to variances.

 $^2\mathrm{Rail}$ kits add between 2.8 kg (6.2 lb) and 3.4 kg (7.4 lb) to the aggregate enclosure weight.

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

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

⁵See AssuredSAN 2002 Series on the Dot Hill web site for the 3Gb drive enclosure data sheet.

NOTE: For information/specifications concerning AssuredSAN 3000 Series-compatible 2122 and 2130 3Gb drive enclosures, see the Dot Hill web site: <u>http://www.dothill.com</u>.

Environmental requirements

 Table 51
 Operating environmental specifications

Specification	Range
Altitude	To 3,000 meters (10,000 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	5.0 g, 11 ms, ½ sine pulses, X, Y, Z
Vibration	(Shaped-spectrum) 5 Hz to 500 Hz, 0.114 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 52 Non-operating environmental specifications (continued)

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

Table 52 Non-operating environmental specifications (continued)

Specification	Range
Shock	15.0 g, 11 ms, ½ sine pulses, X, Y, Z
Vibration	(Shaped-spectrum) 2.8 Hz to 365.4 Hz, 0.852 G _{rms} total (horizontal) 2.8 Hz to 365.4 Hz, 1.222 G _{rms} total (vertical)

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

Electrical requirements

Site wiring and power requirements

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

Power cable requirements

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

C Electrostatic discharge

Preventing electrostatic discharge

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

To prevent electrostatic damage:

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

Grounding methods to prevent electrostatic discharge

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

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

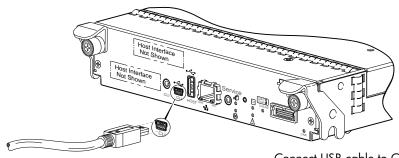
If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part. For more information about static electricity or assistance with product installation, contact an authorized reseller.

D USB device connection

Rear panel USB ports

AssuredSAN 3000 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), and each interface is accessed via its port on the controller module face plate. The port labeled Host (USB Type A) is reserved for future use, 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 28 for USB port locations).

USB CLI port



Connect USB cable to CLI port on controller face plate

Figure 28 USB device connection - CLI port

AssuredSAN 3000 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 new 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 105). For Windows computers a special device driver file, gserial.inf, must be downloaded from a CD or web site, and installed on the computer that will be cabled directly to the controller's CLI port (see Microsoft Windows on page 104).

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 3000 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

3000 Series controllers support the following applications to facilitate connection.

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

 Table 53
 Supported terminal emulator applications

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 54 USB vendor and product identification codes

USB Identification code type	Code
Dot Hill Systems, Inc. vendor ID code	0x210C
AssuredSAN 3000 Series product ID code	0xa4a7

Microsoft Windows

Microsoft Windows operating systems provide a USB serial port driver. However, the USB driver requires details for connecting to AssuredSAN 3000 Series controller enclosures. Dot Hill provides a device driver for use in the Windows environment. The USB device driver and installation instructions are provided on the ship kit CD. Alternatively, you can download this data.

Obtaining the software download

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

Linux

Although Linux operating systems do not require installation of a device driver, certain parameters must be provided during driver loading to enable recognition of the AssuredSAN 3000 Series controller enclosures.

Setting parameters for the device driver

- Enter the following command: modprobe usbserial vendor=0x210c product=0xa4a7 use_acm=1
 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.

Index

Numerics

2U12 3.5" 12-drive enclosure 98 2U24 2.5" 24-drive enclosure 98

A

accessing RAIDar (web-based management GUI) 61 AssuredRemote licensed replication feature 48 audience 11

В

bezel enclosure 16

С

cables FCC compliance statement 48, 97 shielded 48, 97 cabling cable routing requirements 97 connecting controller and drive enclosures 24 connecting storage systems for replication 48 considerations 37 direct attach configurations 39 switch attach configurations 45 cache post-write 22 read-ahead 22 clearance requirements service 97 ventilation 97 command-line interface using to set controller IP addresses 57 CompactFlash transporting 70 components 12-drive enclosure front panel 15 2122/3120/3130 rear panel 20 2130 rear panel 21 24-drive enclosure front panel 15 3000 Series controller enclosure rear panel 17 3320/3330 rear panel 1Gb iSCSI ports (host interface or replication) 20 CLI port (USB) 20 expansion port 20 network port 20 service port 20 USB Type A (reserved for future use) 20 3420/3430 rear panel 10GbE iSCSI ports (host interface or replication) 20

CLI port (USB) 20 expansion port 20 network port 20 service port 20 USB Type A (reserved for future use) 20 3523/3533 or 3520/3530 rear panel CLI port (USB) 19 expansion port 19 network port 19 SAS host interface ports 19 service port 19 USB Type A (reserved for future use) 19 3720/3730 rear panel CLI port (USB) 19 E/T button (disabled) 19 expansion port 19 FC ports (host interface or replication) 19 network port 19 service port 19 USB Type A (reserved for future use) 19 3723/3733 rear panel CLI port (USB) 18 expansion port 18 FC ports (host interface or replication) 18 network port 18 service port 18 USB Type A (reserved for future use) 18 3920/3930 rear panel 1Gb iSCSI ports (host interface or replication) 18 CLI port (USB) 18 E/T button (disabled) 18 expansion port 18 FC ports (host interface or replication) 18 network port 18 service port 18 USB Type A (reserved for future use) 18 Power Supply Unit (PSU) AC 17 DC 17 connecting controller enclosures to hosts 37, 38, 40 to remote management hosts 48 connections test 33 verify 32 console requirement 97 controller enclosures connecting to hosts 37, 38, 40 connecting to remote management hosts 48 conventions document 12

D

DHCP obtaining IP addresses 57 server 57 direct attach configurations 37, 38, 40 disk drive LEDs general 82 specific states 83 document conventions 12 prerequisite knowledge 11 related documentation 12

E

electrostatic discharge grounding methods 101 precautions 101 enclosure cabling 24 dimensions 98 IDs, correcting 65 initial configuration 23 input frequency requirement 100 input voltage requirement 100 installation checklist 23 site requirements 97 troubleshooting 65 weight 98, 99 Ethernet cables requirements 40, 48

F

faults isolating a host-side connection 70 expansion port connection fault 72 methodology 63

Η

host ports FC 38 loop topology 38 point-to-point topology 38 iSCSI (10GbE) 39 iSCSI (1Gb) 38 SAS 38 hosts defined 38 optional software 37 stopping I/O 66 system requirements 37 humidity non-operating range 99 humidity operating range 99

I

IDs, correcting for enclosure 65 Installing a license permanent 61 temporary 61 IP addresses setting using DHCP 57 setting using the CLI 57

L

LEDs 2122/31XX face plate Fault/Service Required 92 FRU OK 92 OK to Remove 92 SAS In Port Status 92 SAS Out Port Status 92 Unit Locator 92 2130 face plate Fault/Service Required 93 FRU OK 93 OK to Remove 93 SAS In Port Status 93 SAS Out Port Status 93 Unit Locator 93 2U12 front panel Disk drive 80, 81 Enclosure ID 80, 81 FRU OK 80, 81 Temperature Fault 80, 81 Unit Locator 80, 81 2U24 front panel Disk drive 79 Enclosure ID 79 Fault/Service Required 79 FRU OK 79 Temperature Fault 79 Unit Locator 79 3000 Series controller enclosure rear panel 84 3320/3330 face plate Cache Status 90 Expansion Port Status 90 Fault/Service Required 90 FRU OK 90 Link Activity 90 Link Status 90 Network Port Activity 90 Network Port Link Status 90 OK to Remove 90 Unit Locator 90 3420/3430 face plate Cache Status 89 Expansion Port Status 89 Fault/Service Required 89 FRU OK 89 Link Activity 89 Link Status 89 Network Port Activity 89 Network Port Link Status 89 OK to Remove 89 Unit Locator 89 3520/3530 face plate

Cache Status 88 Expansion Port Status 88 Fault/Service Required 88 FRU OK 88 Link Activity 88 Link Status 88 Network Port Activity 88 Network Port Link Status 88 OK to Remove 88 Unit Locator 88 3720/3730 face plate Cache Status 87 Expansion Port Status 87 Fault/Service Required 87 FRU OK 87 Link Activity 87 Link Status 87 Network Port Activity 87 Network Port Link Status 87 OK to Remove 87 Unit Locator 87 3723/3733 face plate Cache Status 86 Expansion Port Status 86 Fault/Service Required 86 FRU OK 86 Link Activity 86 Link Status 86 Network Port Activity 86 Network Port Link Status 86 OK to Remove 86 Unit Locator 86 3920/3930 face plate Cache Status 85 Expansion Port Status 85 Fault/Service Required 85 FC Link Activity 85 FC Link Status 85 FRU OK 85 iSCSI Link Activity 85 iSCSI Link Status 85 Network Port Activity 85 Network Port Link Status 85 OK to Remove 85 Unit Locator 85 Disk with dongle OK to Remove 82 Power/Activity/Fault 82 Disk without dongle Fault 82 Power/Activity 82 Power Supply Unit (PSU) AC 91 DC 91 using to diagnose fault conditions 66 local management host requirement 97

Μ

MPIO DSM

Dot Hill MPIO DSM installation 37 native Microsoft installation 37 see related documentation 37

Ν

NEBS (Level 3) Exceptions to GR-63-CORE 24 Airborne Contaminants 24 Equipment - Fan Filters 24 Heat Dissipation 24 Spatial Requirements 24 GR-1089-CORE Issue 5 23 R1-3.155 - hard copy Cautions and Warnings 95 R2-5.5 - documented ESD sensitivity 101 R2-6.6 - operating environmental specs 95, 96, 99 R2-7.7 - grounding to prevent ESD 101 R3-1.159 - emission and immunity criteria 48 R4-16.171 - suitable for intra-building cabling 97 R4-89.210 - surge protective device 95, 96 R9-10.79 - electrical continuity 97 R9-16.151 - BR input terminals are DC-I 96 R9-3.76 - suitable for installing as part of CBN 96 R9-6.213 - suitable installation sites 97 GR-63-CORE Issue 3 23 R4-17.157 - fans and cooling units 21 NEBS (Network Equipment-Building System) 23 non-operating ranges, environmental 99

0

operating ranges, environmental 99 optional software 37

Ρ

physical requirements 97 power cord requirements 100 power cycle power off 36 power on 34, 35 power supply AC power requirements 95 DC power requirements 96 site wiring requirements 95 prerequisite knowledge 11

R

RAIDar web-based storage management interface 61 regulatory compliance notices shielded cables 48, 97 see related document 95 related documentation 12 remote management 48 requirements cabling 97 clearance 97 Ethernet cables 48 host system 37 physical 97 ventilation 97 RFI/EMI connector hoods 48, 97 rugged chassis European Telco compliant 11 MIL-STD-810G (storage requirements) compliant 11 NEBS Level 3 compliant 11

S

safety precautions 95 SCSI Enclosure Services (SES) driver 37 sensors locating 77 power supply 77 temperature 78 voltage 78 shock non-operating range 99 shock operating range 99 site planning local management host requirement 97 physical requirements 97 safety precautions 95 storage system setup configuring 61 getting started 61 provisioning 61 replicating 61 super-capacitor pack 22 switch attach configurations 45

Т

temperature non-operating range 99 temperature operating range 99 troubleshooting 63 controller failure, single controller configuration 69 correcting enclosure IDs 65 enclosure does not initialize 65 expansion port connection fault 72 host-side connection fault 70 using system LEDs 66

U

Unified LUN Presentation 38 USB device connection command line interface (CLI) 104 device driver 104 emulated serial port 103 rear panel USB ports 103 supported host applications 104 vendor and product ID codes 104

V

ventilation requirements 97 vibration non-operating range 99 vibration operating range 99

W

warnings

temperature 77 voltage 77 web site Dot Hill Systems Customer Resource Center 12, 21, 65