Exos® Scale EX4U74 and DC4U100 Hardware Installation and Maintenance Guide

Abstract

This guide describes initial hardware setup for Exos Scale EX4U74 and DC4U100 storage enclosures. It also describes removal and installation of customer-replaceable components. The guide is intended for use by storage system administrators familiar with servers and computer networks, network administration, storage system administration and configurations, storage area network management, and relevant protocols.

Part Number: 207687200-00
Revision: A
Published: July 2026

© 2026 Seagate Technology LLC or its affiliates. All rights reserved. Seagate, Seagate Technology, and the Spiral logo are registered trademarks of Seagate Technology LLC in the United States and/or other countries. Exos is either a trademark or a registered trademark of Seagate Technology LLC or one of its affiliated companies in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. When referring to drive capacity, one gigabyte (GB) equals one billion bytes, one terabyte (TB) equals one trillion bytes, and one petabyte (PB) equals one thousand terabytes. Your computer's operating system may use a different standard of measurement and report a lower capacity. In addition, some of the listed capacity is used for formatting and other functions, and thus will not be available for data storage. All coded instruction and program statements contained herein remain copyrighted works and confidential proprietary and trade secret information of Seagate Technology LLC or its affiliates. Any use, derivation, disassembly, reverse engineering, dissemination, reproduction, or any attempt to modify, prepare derivative works, reproduce, distribute, disclose copyrighted material of Seagate Technology LLC, for any reason, in any manner, medium, or form, in whole or in part, if not expressly authorized, is strictly prohibited. Seagate reserves the right to change, without notice, product offerings or specifications.

For the latest regulatory and compliance information see www.seagate.com/support. Scroll down to the Compliance section.

Contents

1 Introduction 6
Intended audience 6
Knowledge prerequisites 6
Safety guidelines 6
Product documentation and support 6

2 System overview 7
Storage enclosure components 7
Storage enclosure chassis and drawer 7
Rear of storage enclosure modules 8
Optional components 8

3 Initial installation 9
Installation checklist 9
Complete installation prerequisites 9
Unpack and prepare the storage enclosure 11
Unpacking the enclosure without drives, manually 11
Install the rackmount kit 11
Install the rack shelves in the rack cabinet 12
Install the storage enclosure 15
Mount the storage enclosure into the rack cabinet 16
Install drives in the storage enclosure 17
Test power source for electrical earth connection 20
Route power cords and data cables 21
Route power cords from the power supply units 21
Route data cables from the IOM 21
Route enclosure management cables from the IOM 22

4 Operation 23
Apply power to the storage enclosure 23
Interpret system LEDs 24
Interpret front panel LEDs 24
Interpret drive slot LED 25
Interpret link expander module LEDs 26
Interpret IOM LED 26
Interpret fan module LED 28
Interpret PSU module LEDs 28
Storage enclosure management 29
Change password using SES 30
Change password using BMC network interface 33

Verify system health 40

5 Troubleshooting 44

Address initial start-up issues 44
Identify fault conditions 45
Isolate hardware and connectivity faults 45
Isolate system application faults 46
Take corrective action 47

6 In-service field maintenance 50

Replace a drive 51
Replace a link expansion module 53
Replace a fan module 55
Replace a PSU 56
Replace an IOM 58
Update firmware 60

Tables

Table 1 Installation checklist tasks 9
Table 2 Fault LED prioritization 24
Table 3 Methods of access to controller module 30
Table 4 Non-fault conditions 45
Table 5 Status of drive or enclosure, based on front panel Fault-Application LED 46
Table 6 Corrective action for fault conditions 49
Table 7 Time limits for FRU replacement 51

1 Introduction

The Exos Scale storage enclosure product is a high-capacity expansion enclosure designed for cloud and enterprise environments. It supports high-demand storage applications that require high data availability, high capacity and high performance. Each storage enclosure is a server-attached JBOD (Just a Bunch of Disks) that fits within 4 EIA rack space units in a 1m or 1.2m rack, depending on the product configuration. The storage enclosure is provided with a SAS-4 (Serial Attached SCSI) interface at the data transfer rate of 24Gb/s.

Intended audience

This guide is for software integration providers, storage installation professionals, and system administration personnel.

Knowledge prerequisites

Make sure you have the appropriate knowledge base prior to product installation or service.

- Server system administration
- Storage system configuration
- Serial Attached SCSI (SAS) protocol
- Ethernet protocol and TCP/IP networks
- Redfish management protocol

Safety guidelines

You must follow all safety requirements in this document. Some relate to the entire system, some to the rack, some to the storage enclosure, and others to the FRUs within it.

Product documentation and support

To obtain documentation, videos, and product information, visit www.seagate.com/support.

Content description	Document	Seagate QR codes
Enhancements, known issues, and updates	Release Notes	4U74 4U100
Overview of product shipkit contents and setup support	Getting Started (GS)*	
Installation of the rail kit and enclosure into a rack	Hardware Installation and Maintenance Guide (HIMG)	
Firmware installation and configuration	BMC CLI Reference Guide	
System Integration	System Integration Handbook (SIH)	
API methods to monitor and manage storage	Redfish API Guide	
*Printed document included in the shipkit		

2 System overview

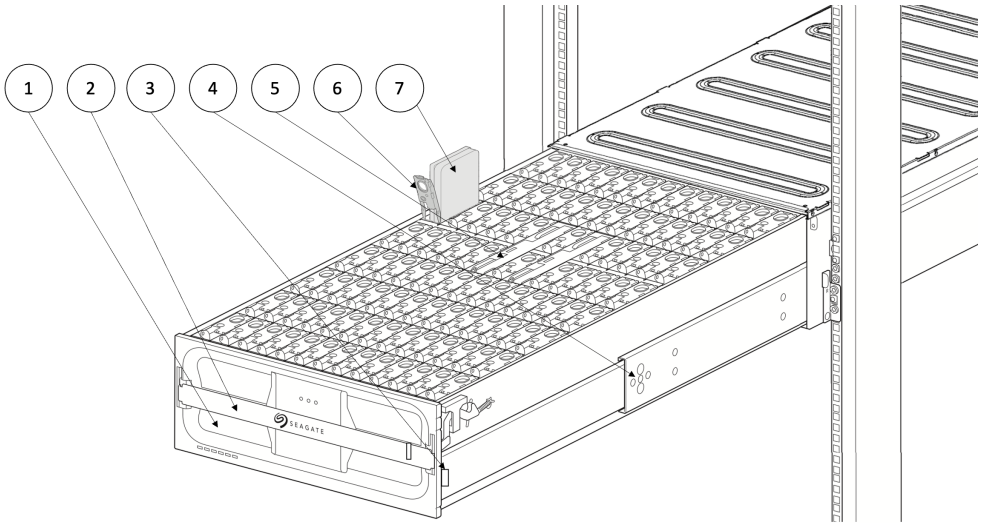
The Exos Scale storage enclosure mounts to a rack cabinet, occupying four EIA rack space units (4U) and contains up to 74 hot-swappable drives in the 1m rack variant or up to 100 hot-swappable drives in the 1.2m rack variant. The enclosure allows for the use of either spinning HDDs or a maximum of 26 SSDs. If used, SSDs must be provided with adapters and allocated to the two rows at the back of the drawer.

Storage enclosure components

- The storage enclosure chassis exterior includes the front panel, drawer, and rear plenum.
- The storage enclosure drawer contains slots for 74 drives in the 1m rack variant or 100 drives in the 1.2m rack variant. The drawer also includes 2 link expansion modules (LEMs).
- The plenum contains 2 input/output modules (IOMs), 2 CRPS (Common Redundant Power Supply) power supplies, and 4 system fan modules.
- The rackmount kit consists of 2 rack shelve assemblies and 2 rear tie-down brackets that connect the storage enclosure to the rack cabinet.

Storage enclosure chassis and drawer

The drawer and the rear panel provide access to plug-in drives and other field-replaceable units (FRUs).

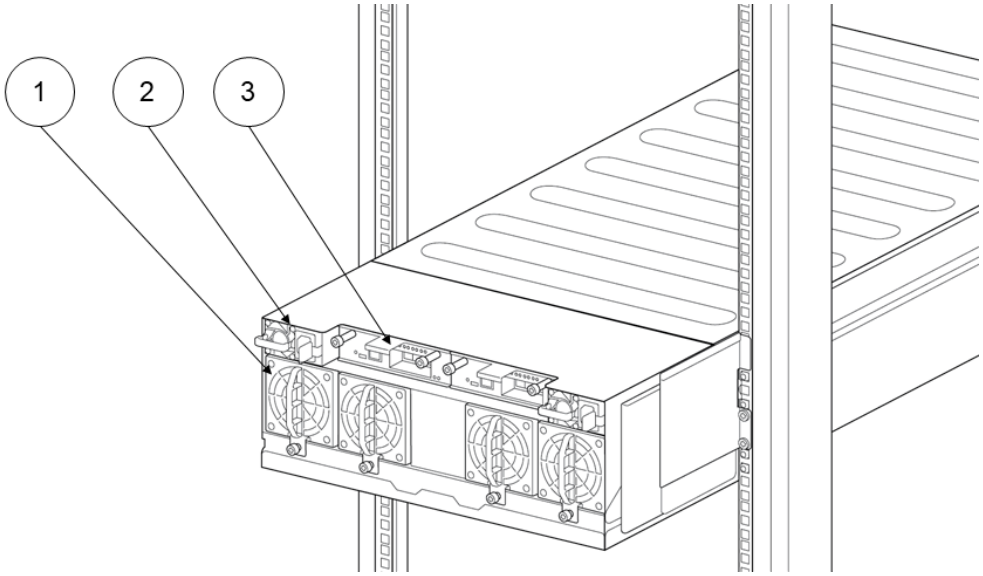


Item	Description	Function
1	Front panel	Protects the front part of the drawer
2	Handle	Allows for the drawer to be unlocked and pulled out for extension
3	Service unlock tab (2)	Unlocks drawer from service positions allowing it to move to fully out or from fully out to closed
4	Drawer rail assembly (2)	Facilitates movement, supports weight and maintains alignment of the drawer in the enclosure
5	Link expansion module (2)	Enables SAS expansion of up to 74/100 HDDs
6	HDD lifter	Lowers the HDD into the slot and extracts the HDD from the slot
7	Drive (74 or 100)	Provides data storage

Figure 1 Storage enclosure chassis and drawer

Rear of storage enclosure modules

The rear plenum of the enclosure contains the following FRUs that you can replace. Components that must be replaced by Seagate-authorized warranty and repair personnel are not identified.



Item	Description	Function
1	System fan module (4)	Provides redundant cooling for the system components
2	Power supply unit (2)	Provides redundant power to the enclosure
3	Input-output module (2)	Manages data transfer between the enclosure and the connected hosts

Figure 2 Customer-replaceable FRUs, rear view

Optional components

- **Blanks for missing FRUs**: The storage enclosure ships with an IOM blank for single controller configurations (SATA).

3 Initial installation

Each storage enclosure installation requires the same amount of preparation to successfully mount it into your industry-standard rack cabinet by qualified personnel.

WARNING! Follow all warnings and cautions on labeling and throughout this guide to reduce risk of personal injury or damage to equipment. You must adhere to all safety requirements in this document. Some relate to the entire system, some to the rack, some to the enclosure, and others to the FRUs within it.

CAUTION Use only power cords supplied in the installation kit or those that meet product specifications.

CAUTION Make sure you are not connected to power at any time during installation procedures.

IMPORTANT Only a qualified service technician should perform the installation.

Installation checklist

Use this checklist, performing each task only in the sequence presented after successful completion of the prior step.

Table 1 Installation checklist tasks

Step	Task	Reference
1	Complete all installation prerequisites	"Complete installation prerequisites" below
2	Prepare the site for installation of the enclosure into the rack cabinet	"Complete installation prerequisites" below
3	Unpack the storage enclosure	"Unpack and prepare the storage enclosure" on page 11
4	Temporarily place all drives in a ESD-protected area	"Unpack and prepare the storage enclosure" on page 11
5	Install the rackmount kit in the rack cabinet	"Install the rackmount kit" on page 11
6	Mount the enclosure into the rack cabinet	"Install the storage enclosure" on page 15
7	Install drives in the enclosure	"Install drives in the storage enclosure" on page 17
8	Test power source for electrical earth connection	"Test power source for electrical earth connection" on page 20
9	Connect all power cords and data cables	"Route power cords and data cables" on page 21
10	Apply power to the storage enclosure	"Apply power to the storage enclosure" on page 23

Complete installation prerequisites

The rackmount kit is designed to bear the maximum weight of the storage enclosure when it is properly mounted in a standard rack cabinet. Multiple storage enclosures can be installed in a single rack cabinet. For safety, heavier equipment should be installed lower in the rack to improve stability and reduce the risk of tipping.

CAUTION You must use only the supplied rackmount kit and related mounting hardware to prevent damage to the equipment and avoid invalidating the Seagate warranty.

CAUTION Do not operate enclosure outside the manufacturer's intended use.

- Storage enclosures are suitable for connection to intra-building or non-exposed wiring or cabling only.
- Storage enclosures are suitable for installation in locations where the National Electrical Code (NEC) applies but are not suitable for Outside Plant (OSP) installations.
- Customer facilities must provide for voltages with not more than ± 5% fluctuation. Customer facilities must also provide suitable surge protection.

- **Site preparation**
  1. Print out a copy of the installation checklist tasks table to properly sequence them and to cross off after completion.
  2. Clear the site for installation and secure a static-protected area.
- **Before enclosure installation**
  1. Unpack the enclosure in a clear area, using appropriate safety precautions.
  2. If drives are included in the shipment, leave them in their packaging or place them in a static-protected area until the enclosure is mounted in the rack.
  3. Review all related warnings before mounting the enclosure into the rack.

To complete installation prerequisites:

1. Prepare the host system for the installation by obtaining access to the following items:
   a. A functioning host bus adapter
   b. Known good cables for host connection that meet enclosure requirements as specified by the Compatibility Interop Matrix for your product on www.seagate.com/support
2. Familiarize yourself with system configuration requirements and the layout of enclosure modules.
3. Obtain the following:
   a. An anti-static wrist or ankle strap for handling static-sensitive components
   b. A static-protected environment for temporary storage of the enclosure and the drives
   c. A T30 driver, 6-in length
   d. A T15 driver, any length, for adjusting the rear tie-down brackets
   e. A mechanical lift with sufficient clearance and capable of safely lifting the enclosure to the desired installation height in the rack. The enclosure weighs up to 132lb (60kg) for the 4U100 model and 110lb (50kg) for the 4U74 model without drives installed.

      NOTE The enclosure does not ship with HDDs installed. The mechanical lift requirement is based on the enclosure weight without drives installed. The final installed weight varies depending on the number and type of drives installed by the customer after the enclosure is mounted.

4. Ensure the rack cabinet is suitable for use with the enclosure.
   a. A EIA-310 compatible 19in rack cabinet capable of holding 4U form factors that meets all UL and IEC safety requirements, leveled in all planes with respect to each other
   b. A minimum depth of 43.35 inches (1101mm) for the 1.2m variant and 35 inches (900mm) for the 1m variant from back of front post to maximum extremity, excluding cabling and door closure considerations

c. A rack cabinet that causes a maximum back air pressure of 5 pascals (0.5mm water gauge)
d. Weight capacity for the total number of enclosures installed, using a maximum of 300lb (136kg) for the 4U100 and 218lb (99kg) for 4U74, per enclosure

5. Secure sufficient trained personnel to assist with the installation. The following staffing is recommended for safe handling:
   a. One qualified service technician for the complete installation procedure
   b. One spotter to assist with the lift and to observe the installation from the rear of the rack cabinet
   c. At least three people to unpack the enclosure and move it onto the mechanical lift

   Additional personnel may be required depending on site safety requirements, the configured enclosure weight, and the handling equipment available.

Unpack and prepare the storage enclosure

⚠ **CAUTION** The storage enclosure ships with internal PCBAs and FRUs installed, but without drives installed. Due to the heavy weight of the enclosure, use care during handling and adhere to Seagate recommendations.

If drives are included in the shipment, leave them in their packaging or place them in a static-protected area until the storage enclosure is installed in the rack cabinet.

Unpacking the enclosure without drives, manually

To unpack the enclosure:

1. Prepare the site for the storage enclosure installation. This includes meeting all product specifications and providing a clean, clear, static-protected environment prior to unpacking the enclosure.
2. Examine packaging for damage. This includes cuts, water damage, or evidence of mishandling during shipment.
3. If there is damage, photograph and document it, but do not proceed. You must retain all original packaging for product returns.
4. Remove all external packaging:
   a. Remove pallet and plastic wrapping.
   b. Remove the cardboard lid.
   c. Remove the rackmount kit from the top tray.
   d. Remove the empty tray.
5. Open the moisture barrier bag.
6. Prepare to remove the enclosure from the container:
   a. With three persons, use the three latched lift straps and appropriate safe lifting techniques to move the enclosure to a static-protected location or lift.
   b. Remove straps.

Install the rackmount kit

The storage enclosure requires rackmount hardware for installation into a standard 1m or 1.2m rack and occupies four EIA units of rack space per unit. The rackmount kit contains left and right shelf brackets, a right and left rear tie down brackets, and all necessary hardware. Product function and user safety hinge on properly installing these brackets.

NOTE Allocate and maintain a safe distance to mount or remove a storage enclosure into a rack:

- 1m rack: 1.5m (4.92 foot)
- 1.2m rack: 1.7m (5.58 foot)

CAUTION If multiple enclosures are installed in a rack, only partially or fully extend one drawer at a time.

To adhere to safety precautions when mounting an enclosure into a rack cabinet:

1. Read and observe all warning and caution labels on the enclosure.
2. Verify the rack cabinet design supports the total weight of enclosures and has stabilizing features to prevent the rack cabinet from tipping or being pushed over during installation or normal use.
3. Do not lift the enclosure without a mechanical lift. No single person should ever lift an enclosure without assistance.
4. Mount enclosures into the rack cabinet from the bottom to the top during installation.
5. Locate lighter enclosures above heavier ones to maximize stability.
6. Remove enclosures from the top of the rack cabinet to the bottom when emptying it.

Install the rack shelves in the rack cabinet

The rack shelves are attached to the left and right interior sides of the rack cabinet. The tie-down brackets are attached to the rack shelves to safely support the enclosure and prevent forward tipping when the drawer is extended. After installation, the storage enclosure must be able to slide smoothly into the rack shelves for final installation. The front mounting brackets on the chassis are provided with a 1.5-inch adjustment range (0 ± 0.75 in). The shelf kit can be adjusted for a post-to-post distance of 28 to 36 inches for 1.2 m chassis and 28 to 30 inches for 1.0 m chassis. The rear tie-down brackets are adjustable to accommodate the full adjustment range.

Slide the storage enclosure from the mechanical lift onto the rack shelves until the rear tie-down brackets fully engage with the rear chassis tie-down features and the front mounting brackets are flush with the front rack rails.

Required equipment	Qty
Rack shelf kit, includes 1 left and 1 right	2
Tie-down brackets, properly oriented	2
A retractable tape measure	1
T30 torx screwdriver, 6-in length	1
T15 screwdriver, any length	1
Panhead screw, M6x18mm length	14
Front screw plate	2
Rear screw plate	2

To install the rack shelves in the rack cabinet:

1. Remove the rack doors.
2. Adjust the post-to-post distance of the rack, measured inside to inside to 28 to 36 inches for a 1.2m chassis and 28 to 30 inches for a 1.0m chassis.
3. Identify the installation position:

a. Determine the desired 4U space in the rack.

b. Locate the bottom of the 4U space on the front rack rail.

c. Mark the position on the rack rail.

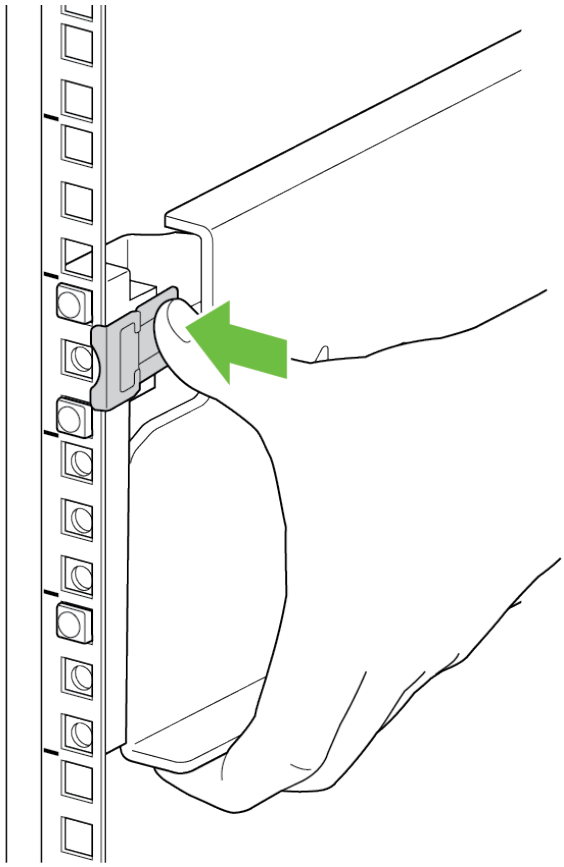


Figure 3 Installation position

4. Select the left rack shelf, orienting it so you face the embossed arrow and FRONT LEFT text.
5. Clip the rack shelf to the front post of the rack, ensuring all alignment pins are properly inserted through the post holes.

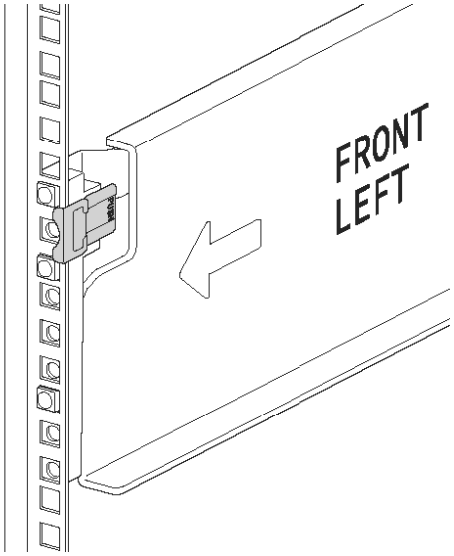


Figure 4 Rack shelf clipped to the front rack post

6. Extend the rack shelf and clip it to the rear post, ensuring all alignment pins are inserted through the post holes.
7. Insert two M6x8mm screws into the top two threaded holes of the 4 screw holes of the front rack post and tighten with a T30 torx screwdriver to a torque of 18 lbf-in (2.0 N-m). The utmost top hole is not threaded.

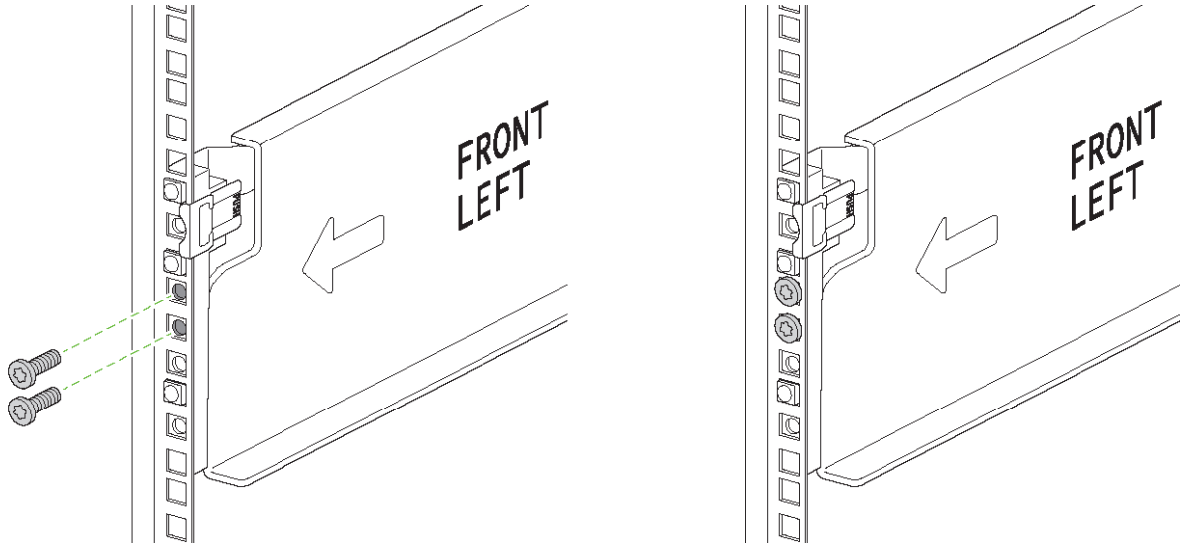


Figure 5 Rack shelf secured to the front rack post

8. Adjust the tie-down bracket slides and block as needed to align the brackets with the chassis style and rack position. Use a T15 screwdriver, then torque the screws to 10 in/lbs.

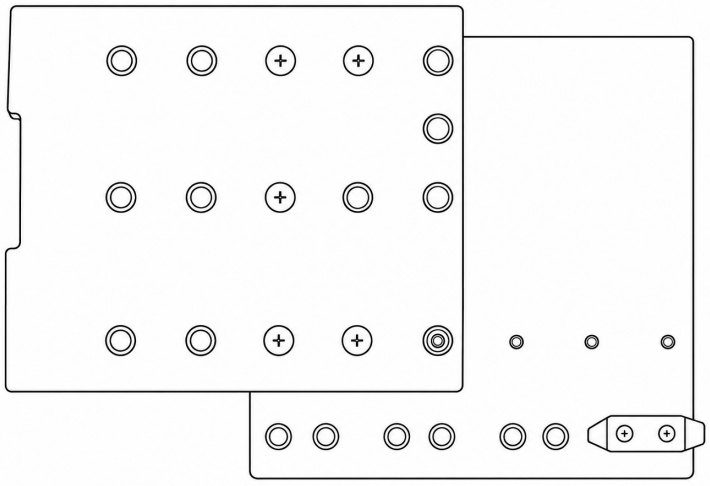


Figure 6 Tie-down bracket adjustment

9. Select the left tie-down bracket, orienting it as shown in the figure below. Position the bracket with the mounting flange on the left, the dogleg in the center, and the rectangular channel insert on the right. Ensure the bracket is placed behind the rack rails before attaching it to the rear rack post.

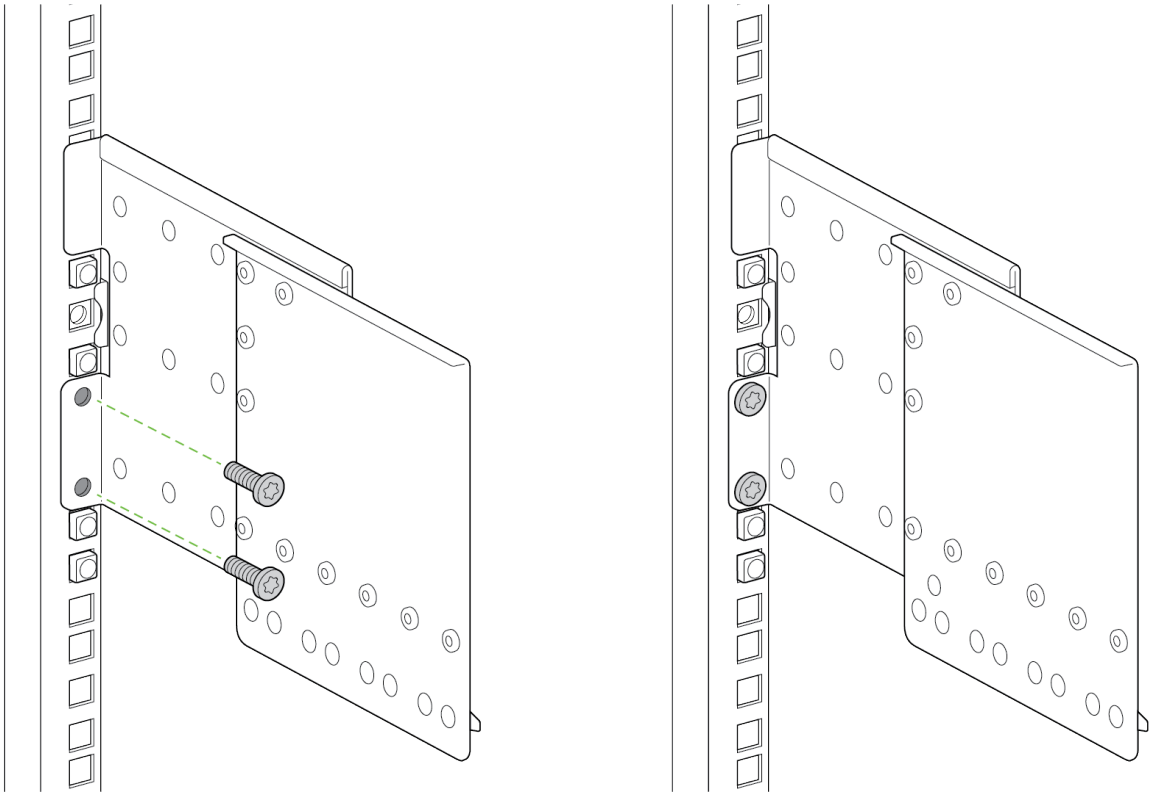


Figure 7 Tie-down bracket orientation

10. Attach the tie-down bracket to the rear rack post using 2x screw plates and M6x18mm, tightening with a T30 torx screwdriver with a minimum 12 in. bit extender to a torque of 18 lbf-in (2.0 N-m) and ensuring its vertical alignment with the rack. The bracket may angle inward slightly until the enclosure is inserted.

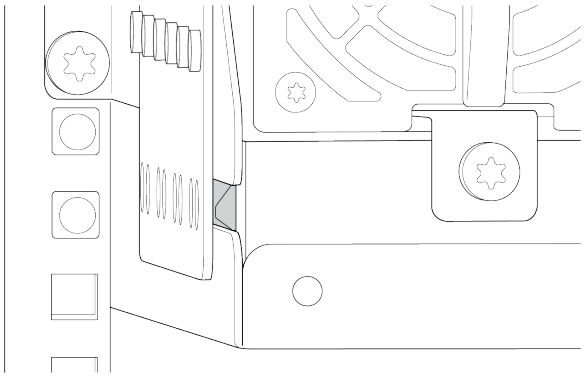


Figure 8 Tie-down bracket secured to the rear rack post

11. Repeat the adjustment process for the right rack shelf, using the proper orientation for the rack cabinet and rail.

Install the storage enclosure

After you successfully complete the installation of the rackmount kit, you can mount the storage enclosure into the rack cabinet.

CAUTION Observe all the following directives:

- Place the rack cabinet on a flat, level surface. Do not install enclosure into a rack cabinet until you verify the rack cabinet is level.
- Follow prescribed leveling procedures from the rack cabinet manufacturer.
- Only insert one enclosure into the rack cabinet, or remove one enclosure from the rack cabinet, at a time. This helps prevent the rack cabinet from tipping or falling.
- Verify the rack cabinet meets all safety requirements when configured with enclosures.
- Verify connections comply with all electrical requirements.
- Verify the system complies with all temperature and exhaust requirements.

Mount the storage enclosure into the rack cabinet

WARNING! Serious injury and mechanical failure can result if you do not adhere to rack cabinet safety precautions.

- To avoid risk of death or injury from tipping the rack, follow all rack installation guidelines, securing the rack cabinet to the floor with a concrete anchor kit.
- To avoid catastrophic failure of the rack assembly, never exceed rack cabinet weight limits.
- Entirely support the enclosure with the mechanical lift until the enclosure is in the required position.
- Follow local occupational health and safety guidelines and meet all requirements for manual material handling.

Mounting the storage enclosure into the rack cabinet is the most critical of the installation procedures and requires your full attention. Safety and hardware longevity depend on the smooth function of the rackmount kit and correct implementation of this task.

- Make sure there is sufficient clearance for the storage enclosure when fully extended in the service position and for a technician or system administrator.
- Observe rack cabinet weight limits.
- Fill the rack cabinet from the bottom to the top, with the heaviest equipment at the bottom.
- Make the approach with the mechanical lift level, straight, and parallel to the rack cabinet. Any skew, warp, or tilt prevents the storage enclosure from correctly sliding into or aligning with the rack shelves.

Required equipment	Qty
Mechanical lift	1
Storage enclosure	1
Rack cabinet with installed rack shelves and tie-down brackets	1
T30 torx screwdriver, 6-in length	1
Panhead screw, M6x18mm length	4

To mount the storage enclosure into the rack cabinet:

1. Confirm that the rack shelves are properly assembled and securely installed correctly in the rack cabinet.
2. Complete the following actions to position the lift and the storage enclosure:
   a. Using proper safety precautions, ensure the lift is stabilized and prevented from moving during the installation process, position the storage enclosure on the lift.
   b. Adjust the lift height to be as close as possible to the allocated 4U location.
3. Slide the storage enclosure onto the rack shelves until the slots engage the tabs on the rear tie-down brackets.
4. Insert two M6x18mm screws with the front screw plates into the lower two screw holes on each side of the front rack post and tighten with a T30 torx screwdriver to a torque of 18 lbf-in (2.0 N-m).

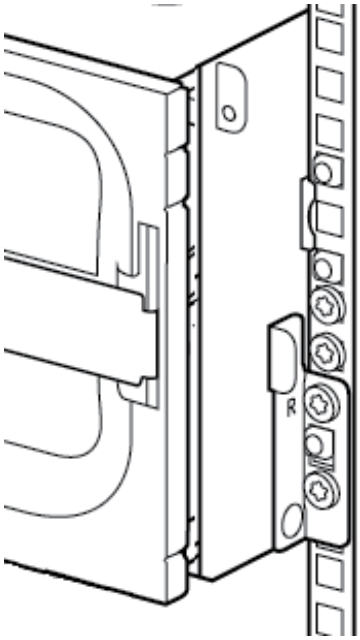


Figure 9 Storage enclosure attached to rack

Install drives in the storage enclosure

3.5" HDDs can be installed without any carrier/adapter. An adapter is required and available for 2.5" SSD drives. Contact Seagate sales for details.

IMPORTANT Do not intermix drive types. Use only SATA drives or only SAS drives within a single storage enclosure. Some slots may remain empty.

IMPORTANT If you partially populate the storage enclosure with drives, you must populate from back to front. The drawer edges have labels that show the slot numbers in each row.

To install drives in the storage enclosure:

1. Facing the front of the enclosure, lift up the pull handle and steadily pull the drawer out on its rails until it locks in the first service position.

⚠ **WARNING!** To avoid risk of injury from pinching your fingers, lift the front handle by holding it from underneath.

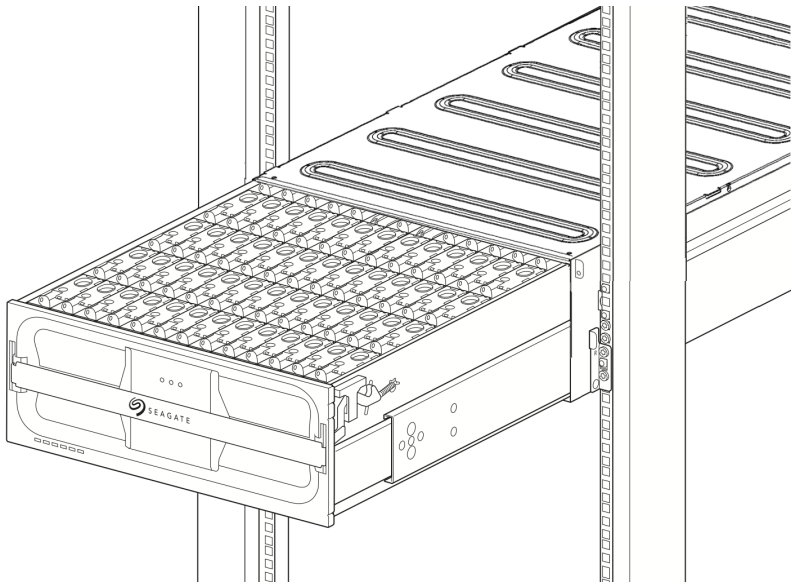


Figure 10 Drawer in service position

2. While pushing the drawer slightly in, pull the service unlock tabs towards you, to unlock the second service position and pull the drawer out on its rails until it locks in the fully extended position.

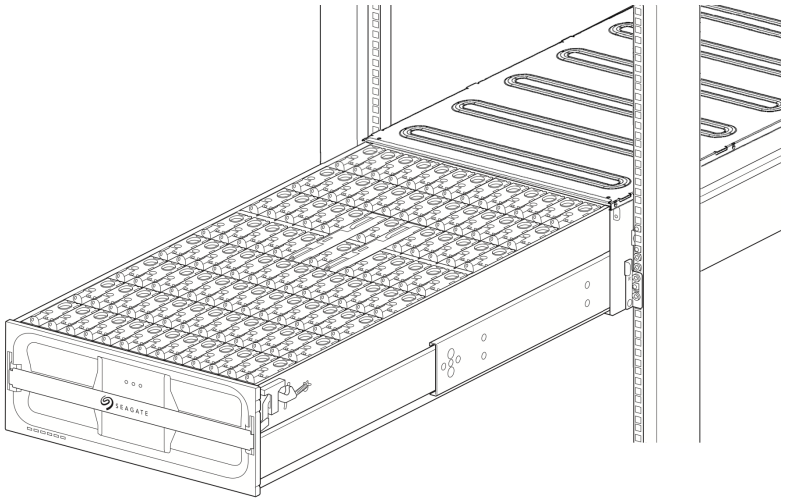


Figure 11 Drawer in extended position

3. Start loading drives with slot 73 or 99 depending on the enclosure. The minimum configuration is 10 drives.

⚠ **IMPORTANT** SSDs must be installed exclusively in the last two rows of the drawer. Intermix of SSDs and HDDs is permissible in the last 2 rows. Leaving slots empty is permissible and no blank fillers are required.

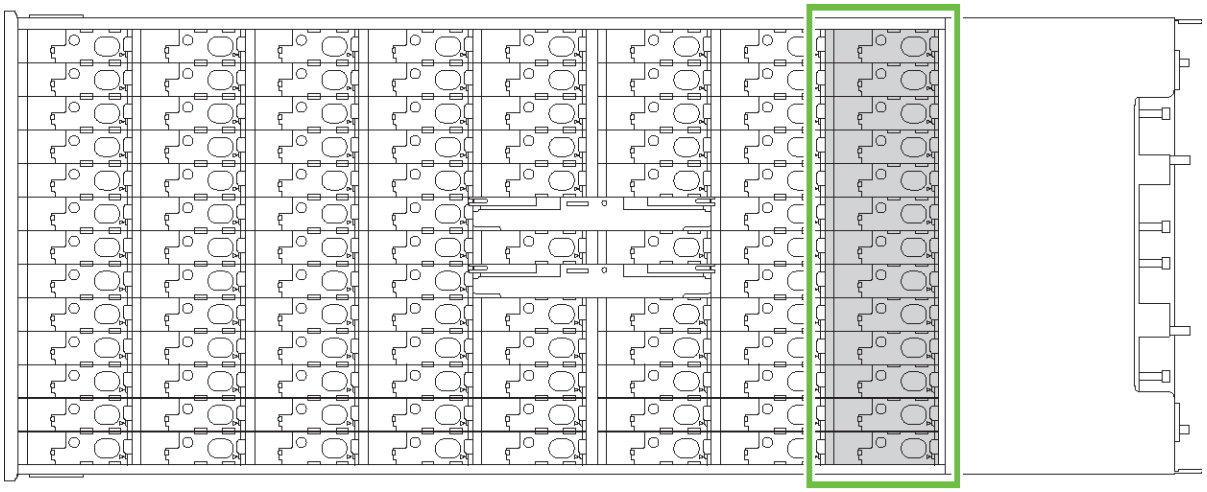


Figure 12 Minimal drive loading configuration (at least 10 of the 13 slots must be populated)

4. Complete the following actions to insert disk drives into the enclosure:

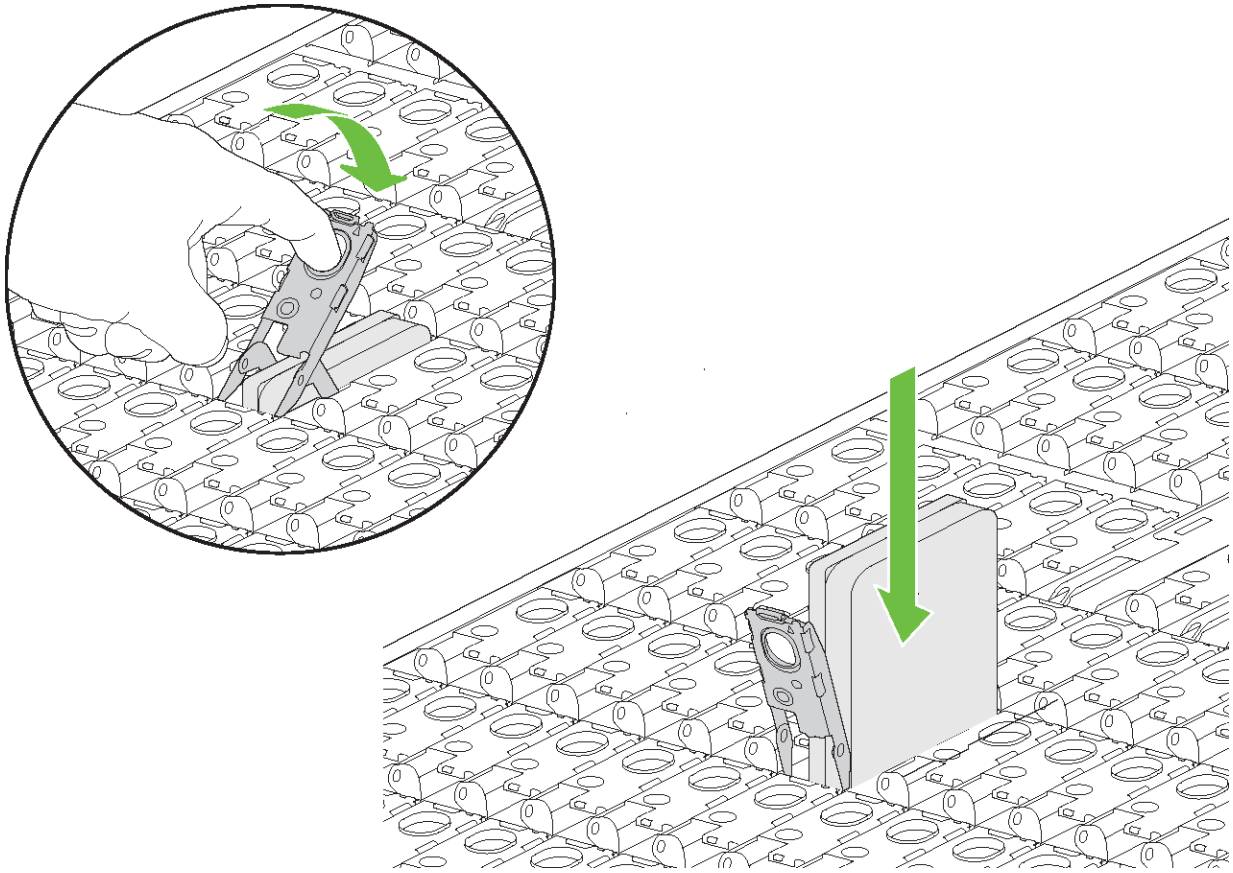


Figure 13 Insert drives

a. Insert a finger into the ringed hole of the first drive slot cover and slide it toward you until the latch is released.

b. Rotate the drive cover toward the front of the chassis.

c. Repeat this step for each drive slot cover.

d. Insert a disk drive into each open slot with the connector facing down and the label facing right.

e. Rotate the HDD lifter to lower the HDD into the slot and onto the HDD SAS connector.

f. Gently press down on the lifter cover until the green latch locks into place.

NOTE Replacement HDD cover/lifters are available if damage occurs. Contact Seagate sales for more on this.

CAUTION Before closing the drawer please ensure all drive covers are closed to prevent damage to drive covers.

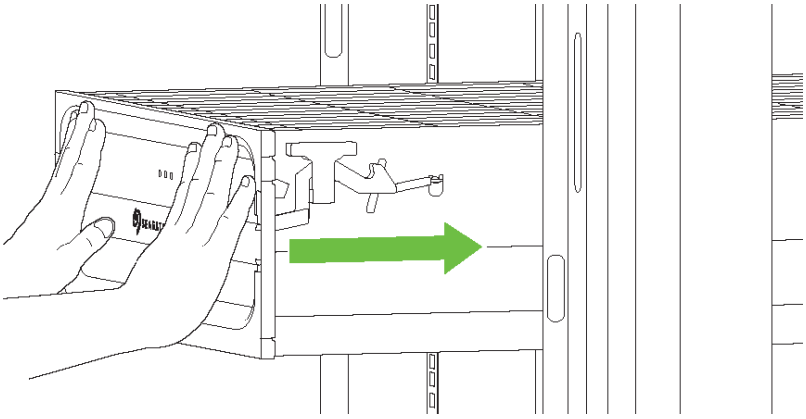
g. Repeat the above steps for all drive slot covers in the same row.

5. Repeat for all rows of the enclosure.

IMPORTANT SSDs must be installed exclusively in the rear two rows of the drawer. Leaving slots empty is permissible and no blank fillers are required.

6. Pull the service unlock tabs on both sides of the drawer towards you and press the drawer forward until fully closed.

WARNING! To avoid risk of injury from pinching your fingers, remove your fingers from the service unlock tabs after you start pressing the drawer forward. Once the locks are disengaged, place your hands on the handle to fully close the drawer.



Test power source for electrical earth connection

After completion of all installation procedures, the enclosure is ready for connection to power. The enclosure must only be connected to a power source that has a safety electrical earth connection. Have a qualified electrical engineer confirm the earth connection meets the product specifications.

CAUTION If multiple enclosures are installed in a rack cabinet, the importance of the earth connection increases, since each enclosure increases earth leakage current.

IMPORTANT Only a qualified electrical engineer who meets local and national standards should perform the inspection.

Route power cords and data cables

Power cords and data cables enable efficient operation of the storage enclosure. They must properly routed to facilitate in-rack service of enclosure modules.

CAUTION The enclosure ground is established through the PSU connection. Install the equipment close to the tested socket outlets and make sure the outlets are easily accessible because the plug on the power supply cord is the primary disconnect device.

To adhere to electrical safety precautions:

1. Confirm the power supply input voltage range is high line 200V to 240V AC at 50Hz to 60Hz before operating the enclosure.
2. You must provide a suitable power source with electrical overload protection to meet technical specification requirements.
3. You must use a provided power cord that has a tested, safe electrical earth connection for each enclosure power supply.
4. Do not operate an enclosure with less than the provided two PSUs, four system fans, and at least one input/output module, other than to provide in-service maintenance in the required time allotment.

Route power cords from the power supply units

This basic task connects the supplied power cords to the redundant power supply units.

CAUTION Use only power cords supplied in the installation kit or those that meet product specifications.

CAUTION Adhere to the following electrical safety guidelines:

- During installation, never connect a power cord to a power supply unit (PSU) before installing it in the appropriate enclosure slot.
- Only connect the power cord to power that complies with the product specifications within a range of 200 to 240VAC, per the hazardous voltage warning label on the PSU.
- During service, always remove the PSU from power by disconnecting the power connector before removal of the PSU.

To route power cords from the power supply units:

1. Select both power cords from the packaging and connect a power cord connector to each PSU.
2. Route each cable to the PDU such that it doesn't block any future maintenance on the fan FRU or IOM FRU.

Route data cables from the IOM

The storage enclosure requires mini-SAS data cables and an Ethernet cable with a RJ45 connector connected to the IOM module.

To connect and route mini-SAS data cables from the IOM modules:

1. If required, label the data cables you selected for this installation.
2. Attach the Ethernet cable to the RJ45 port.
3. Attach the mini-SAS cables to the SAS ports. You can attach up to 4 cables per IOM.

IMPORTANT When installing the cables, make sure that the bend radius of each cable adheres to the manufacturer's guidelines to avoid damage.

4. Route the cable to facilitate in-rack service of enclosure modules.

Route enclosure management cables from the IOM

The storage enclosure requires enclosure management cables connected to the input/output module.

To connect and route enclosure management cables from the IOMs:

1. Sequentially label two Ethernet cables you selected for this installation with RJ45 connectors.
2. Attach each cable to the corresponding network port of the module.

4 Operation

Once the storage enclosure has been installed in the rack, drives inserted into the enclosure, and data cables properly routed the enclosure is ready to be powered on and checked out for proper operation.

The following steps will help ensure the enclosure is ready for proper operation.

1. Power on the enclosure.
2. Interpret system LEDs.
3. Connect to the BMC Management CLI.
4. Verify the system health.

CAUTION Only operate the storage enclosure in a dust-free environment to meet temperature control and airflow requirements.

Apply power to the storage enclosure

The storage enclosure relies on main power provided through separate, independent Power Distribution Units (PDUs). If power is lost to both PDUs for any reason, the storage enclosure automatically restarts after power restoration.

CAUTION Adhere to the following electrical safety guidelines:

- During installation, never connect a power cord to a power supply unit (PSU) before installing it in the appropriate enclosure slot.
- Only connect the power cord to power that complies with the product specifications within a range of 200 to 240VAC, per the hazardous voltage warning label on the PSU.
- During service, always remove the PSU from power by disconnecting the power connector before removal of the PSU.

Before you power on the storage enclosure, do the following:

- Verify that all drives are in their correct slots and that you properly engaged them by pressing down firmly until each one locks into place on its baseplane.
- Confirm that airflow paths at the front and rear of the enclosure are clear and remain clear.
- Proceed to the power-on task.

To apply power to the storage enclosure:

1. Facing the rear of the rack cabinet, connect the plug for each of the PSUs to an independent power distribution unit (PDU).

   IMPORTANT The storage enclosure design requires two redundant power supply units (PSUs). It is recommended that each PSU power cord is plugged into an independent PDU that connects to an uninterruptible power system.

2. Facing the front, observe the LEDs on the front panel as described in "Interpret front panel LEDs" on the next page and confirm the *System power* LED is in a steady green state.
3. When you are ready to power down the storage enclosure, disconnect the power connector from both PSUs.

Interpret system LEDs

Use LEDs throughout the storage enclosure to determine if there is a critical fault.

The storage enclosure registers the following states using the identified LED colors.

1. **Green or unlit LED**: Indicates a module is functioning normally
2. **Flashing green or amber LED**: Indicates a non-critical condition
3. **Amber LED**: Indicates a critical fault
4. **Blue LED**: Indicates system component identification, so is not a fault or critical condition

Since the LEDs use fast or slow flashes to cover multiple conditions, here is the priority for simultaneous indications:

Table 2 Fault LED prioritization

Priority	Flash rate	Indication	Description
Top priority	Fast flash (1s on, 1s off)	Identify	Locate the enclosure or module
Priority 2	Amber On	Fault	Fault condition detected
Priority 3	Slow flash (3s on, 1s off)	Enclosure condition	Logical fault or non-critical notification
Lowest priority	Green On or LED Off	No condition	System functioning normally

Interpret front panel LEDs

The storage enclosure front panel contains a series of LEDs to reflect system status. You can monitor the front panel LEDs to determine system status in combination with the user interface content.

In the case of a system fault condition, identified in the state column in bold and with an asterisk (*), troubleshoot the fault.

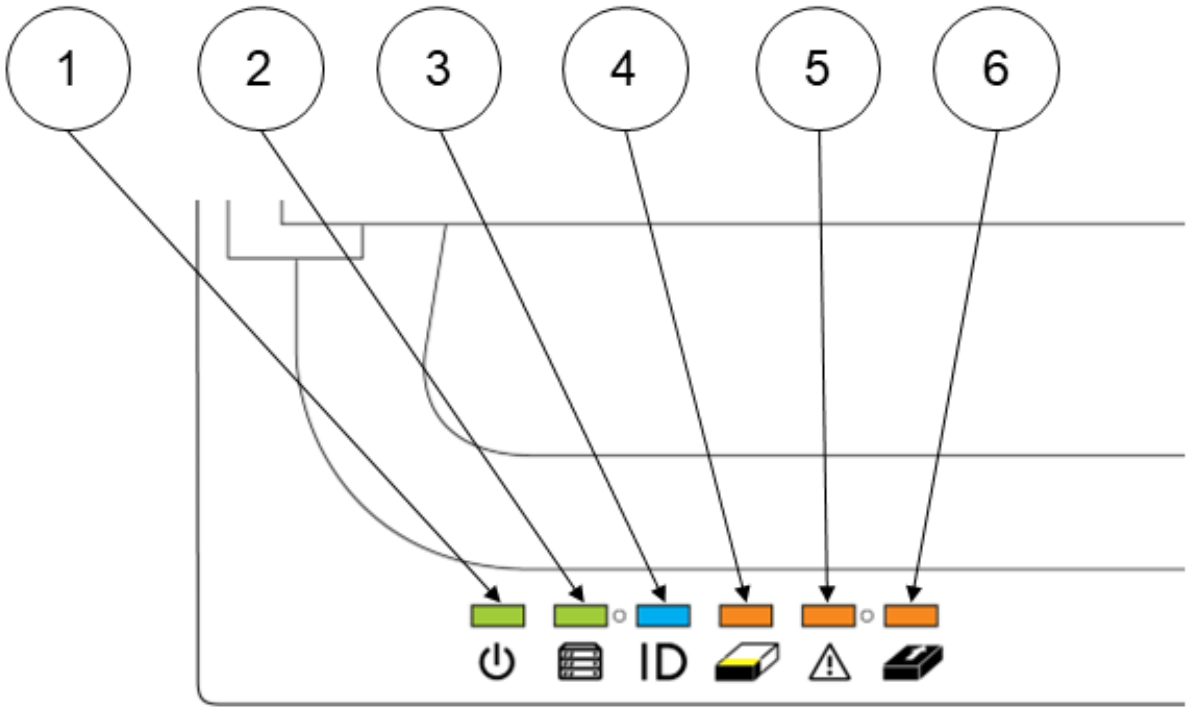


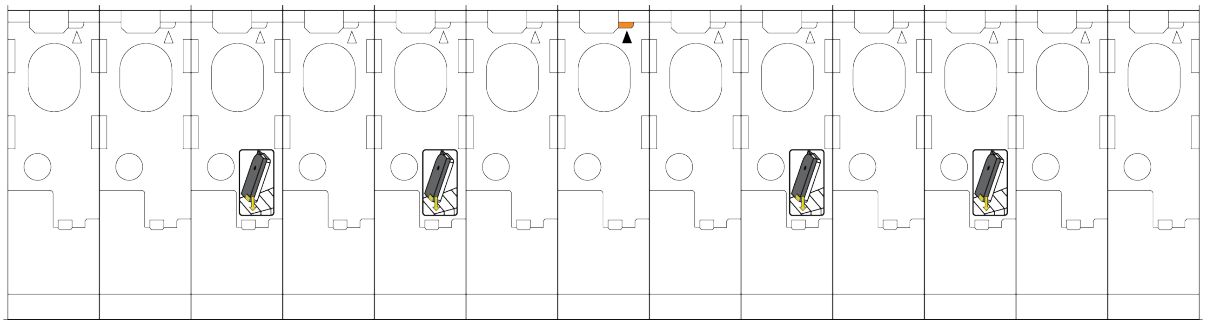
Figure 14 Front panel LEDs

LED	LED number: Name	Color	State	Status
	1: System power	Green	On	System powered on
			Off	System powered off
	2: Host connectivity	Green	On	Host successfully linked to the IOM
			Off	No connection to the IOM
	3: System ID	Blue	Flashing	System unit identification (UID) active
			Off	Normal state, no query for UID active
	4: Fault-drawer	Amber	**On***	System hardware fault in the slot
			Off	System hardware in the slot is functioning normally
	5: Fault-Application	Amber	**On***	System application logic fault, initiated by the IOM
			Off	System application logic initiated by the IOM is functioning normally
	6: Fault-Rear panel	Amber	**On***	System hardware fault in the rear panel area
			Flashing*	
			Off	System hardware in the rear panel area is functioning normally

Figure 15 Interpretation of front panel LEDs

Interpret drive slot LED

The storage enclosure drive slot contains a single fault LED to reflect the operating condition of the drive. The drive slot LEDs are visible when the drive drawer is opened. Drive slots include an orientation label indicating the correct direction for inserting the drive.

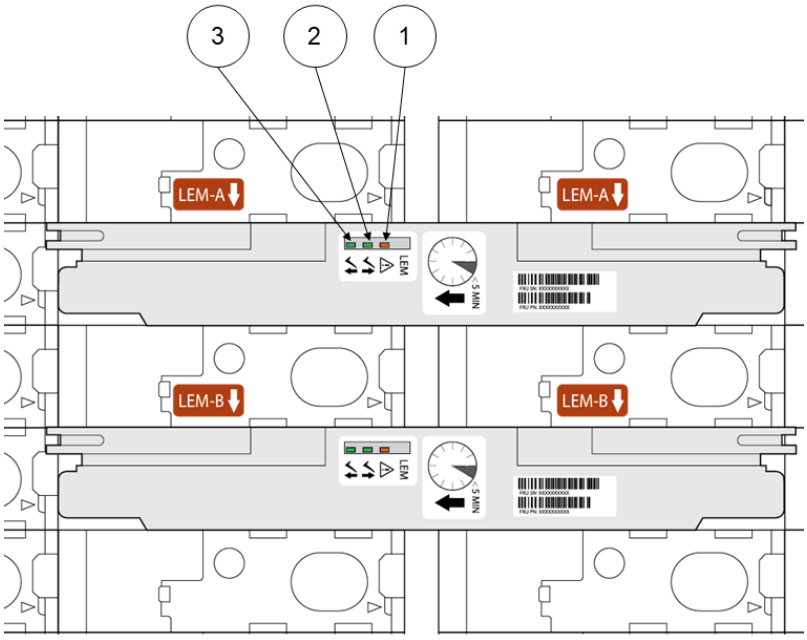


LED	Color	State	Status
Fault LED	Amber	On	A physical fault has been detected on the drive slot or the user/host software has indicated that a fault is present on the drive through SES, Redfish or the CLI.
		Flashing 1s On, 1s Off	The user has requested the enclosure to identify the drive slot
		Flashing 3s On, 1s Off	The host I/O stack has requested the enclosure display an array condition indication on the drive slot, such as an enclosure rebuild.
		Solid Off	No drive fault or enclosure condition exists

Figure 16 Drive slot LEDs and the orientation labels

Interpret link expander module LEDs

The storage enclosure expander module contains three LEDs to reflect the expander system status. Each expander module is labeled for identification.



Pos	LED	Color	State	Status
1	Fault LED	Amber	On	A physical fault has been detected on the expander module or the user/host software has indicated that a fault is present on the expander module through SES, Redfish or the CLI.
			Flashing 1s On, 1s Off	The user has requested the enclosure to identify the expander module
			Off	No I/O module fault or identify condition exists
2	Expander 0 status	Green	On	The expander is powered and has booted.
			Flashing 0.25s On, 0.25s Off	The expander is powered and is booting.
			Off	The expander is not powered.
3	Expander 1 status	Green	On	The expander is powered and has booted.
			Flashing 0.25s On, 0.25s Off	The expander is powered and is booting.
			Off	The expander is not powered.

Figure 17 Interpretation of expander module LED

Interpret IOM LED

Each IOM contains a series of LEDs to reflect the system status. You can monitor the front panel LEDs to determine system status in combination with the user interface content.

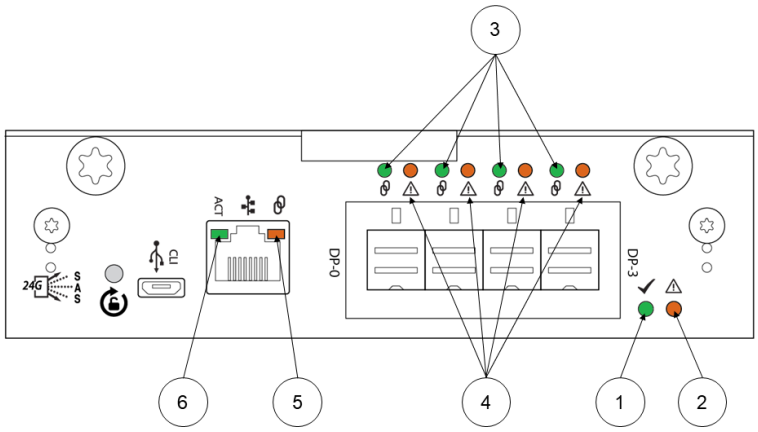


Figure 18 IOM LEDs

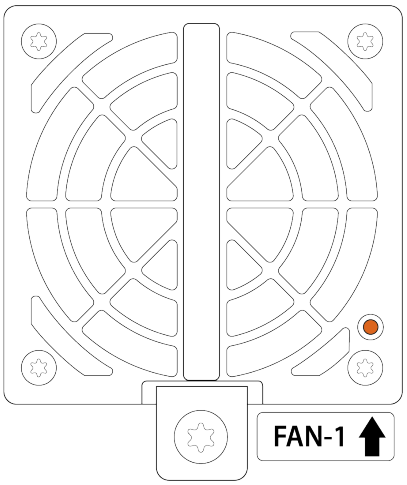
Pos	LED	Color	State	Status
1	Power/status LED	Green	On	The I/O module's BMC is powered and functional
			Flashing 0.25s On, 0.25s Off	The I/O module's BMC is powered and booting
			Off	The I/O module is unpowered, or the BMC is not able to boot
2	Fault LED	Amber	On	A fault within the IOM has been detected or the user has requested the enclosure to report a fault on the IOM via SES, Redfish or the CLI
			Flashing 1s On, 1s Off	The enclosure has been requested to identify the IOM by the user/host application using SES, Redfish, or the CLI
			Off	There is no fault or identify condition on the IOM
3	Mini-SAS-HD Port Activity	Green	On	One of more phys on the port have linked up
			Flashing Off	One of more phys on the port have detected SAS activity
			Off	All phys on the port have linked down
4	Mini-SAS-HD Port Fault	Amber	On	A fault with the attached cable or the port hardware has been detected.
			Flashing 1s On, 1s Off	The enclosure has been requested to identify the mini-SAS HD port by the user/host application using SES, Redfish, or the CLI
			Off	There is no fault or identify condition on the port/cable
5	Ethernet network port speed	Amber	on	1000base -T negotiated rate
			off	10/100base-T negotiated rate
6	Ethernet network port activity	Green	on	Ethernet link is up
			off	Ethernet link is down

Figure 19 Interpretation of IOM LEDs

The RJ45 Ethernet port LEDs are driven by the Ethernet PHY hardware and implement a multi-purpose indication scheme using its amber and green LEDs.

Interpret fan module LED

The storage enclosure fan module contains single LED to reflect fan module status. Each fan module is labeled for identification.



LED	Color	State	Status
Fault LED	Amber	On	A physical fault has been detected on the fan module or the user/host software has indicated that a fault is present on the fan module through SES, Redfish or the CLI.
		Flashing 1s On, 1s Off	The user has requested the enclosure to identify the fan module
		Off	No fan module fault or enclosure condition exists

Figure 20 Interpretation of fan module LED

Interpret PSU module LEDs

The storage enclosure PSU module contains a single LED to reflect PSU module status. Each PSU module is labeled for identification.

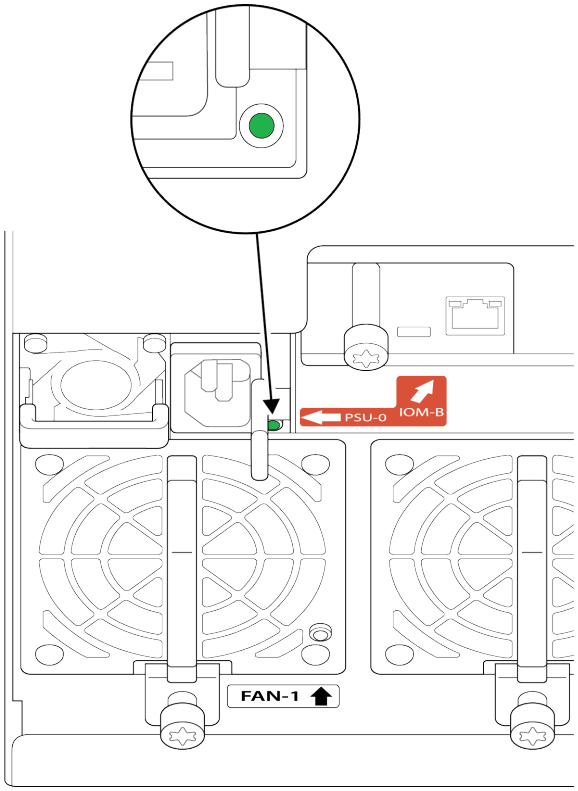


Figure 21 PSU LEDs

LED	Color	State	Status
PSU status LED	Green/Amber	Solid Green	Output on and PSU OK
		Solid Off	No AC on all PSUs
		Flashing 1 Hz Green	PSU Standby or Cold Standby with AC present
		Solid Amber	No AC on PSU with other PSU powered or a PSU failure event has been detected
		Flashing 1 Hz Amber	A PSU warning event has been detected
		Flashing 2 Hz Green	A PSU firmware update is in progress

Figure 22 Interpretation of PSU module LED

Storage enclosure management

Enclosure Management for configuring, monitoring, and managing the enclosure is controlled by an embedded Baseboard Management Controller (BMC) on each IOM. Enclosure Management is accessed using either the in-band SAS interface or the out-of-band Ethernet interface. It uses the BMC and associated monitoring and control logic, such as the SCSI Enclosure Services (SES) service, to identify, assess, and diagnose storage enclosure system.

The Storage enclosure has secure built in enclosure management software that is used to configure and manage the enclosure. The software interface running in the enclosure is called the BMC Management CLI and is password protected. It comes from the factory with the following default admin user credentials:

- Username: admin
- Password: admin123

When you access the CLI the first time the system will require you to change the password.

Methods to access the BMC Management CLI described in the table below.

Table 3 Methods of access to controller module

Type	Description
In-band SES	In-band through the SAS ports using an SES utility such as Seagate's fwdownloader utility.
SSH	Each IOM has a RJ45 1G Ethernet management port that can be connected to a user network that has access to a management host running a terminal program such as PuTTY.
USB serial (disabled by default)	Each IOM has a USB port that presents as a serial (COM) port device when a USB A/C to Micro USB B cable is connected between a terminal machine and the enclosure IOM.

Change password using SES

The SES CLI provides a mechanism for issuing CLI commands to the Exos-E BMC in-band using vendor-unique SES pages 84h and 85h. The interface works by writing the command line to the enclosure and collecting the resulting command output. Full details of the SES CLI protocol can be found in the GEM ANSI SES Specification. The SES CLI is non-interactive and requires a host utility such as Seagate's fwdownloader.

Factory default credentials

The factory-default admin credentials are:

- Username: admin
- Password: admin123

Procedure

The following steps are used to update the credentials on both IOMs:

1. Retrieve the SES targets for both IOMs.
2. Set the new password on IOM A.
3. Set the new password on IOM B.
4. Verify that the password has been successfully changed.

The default admin credentials must be changed on both IOMs.

Retrieving SES targets

Use the fwdownloader-ses command to get the SES target device for each IOM:

```
root@deserve05:/home/stxeng# fwdownloader-ses
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
-----------
SES Device 0 Addr='/dev/sg1'
Found SES Page 1 for Device 0 (/dev/sg1) size 308 (0x134)
```

```
WWN: 500c0ff0ff2d753c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6041 S/N: SWB0D005S5
----------
----------
SES Device 1 Addr='/dev/sg4'
Found SES Page 1 for Device 1 (/dev/sg4) size 308 (0x134)
WWN: 500c0ff0ff2d753c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6041 S/N: SWB0D005S5
----------
```

In this example, one SES target was found for each IOM, Device 0 (`/dev/sg1`) and Device 1 (`/dev/sg4`)

Changing password using SES

IOM A

Use `fwdownloader` to change the password for the admin user on IOM A. Use lower case for `cli` and replace `x` with the SES target device number:

```
fwdownloader-d x-cli ‘set password password<new_password> admin’ -U admin -P admin123
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 1 -CLI 'set password passwordTestit123! admin' -U admin -P admin123
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
Found SES Page 1 for Device 1 (/dev/sg4) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
You must update your password before using this account
Changes being made to current user
Password updated successfully for admin
Changes will take effect on next log in. Please log out
Role updated for user admin
Interface list updated for user admin
Command Completed. ("set password passwordTestit123! admin -U admin -P admin123")
```

IOM B

Use `fwdownloader` to change the password for the admin user on IOM B. Use lower case for `cli` and replace `x` with the SES target device number:

```
fwdownloader-d x-cli ‘set password password<new_password> admin’ -U admin -P admin123
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 1 -CLI 'set password passwordTestit123! admin' -U admin -P admin123
```

```
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
Found SES Page 1 for Device 1 (/dev/sg4) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
You must update your password before using this account
Changes being made to current user
Password updated successfully for admin
Changes will take effect on next log in. Please log out
Role updated for user admin
Interface list updated for user admin
Command Completed. ("set password passwordTestit123! admin -U admin -P admin123")
```

Verifying password changes using SES

IOM A

Verifying the `admin` password has changed is accomplished by running valid BMC CLI commands. In this case, we chose the `show network` command as this command will also return the BMC IP address for use later on. Run this command as follows, replacing `<new password>` with the desired new password:

```
fwdownloader –d 0 –cli "show network" –U admin –P <new password>
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 0 -cli 'show network' -U admin -P Testit123!
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
Found SES Page 1 for Device 0 (/dev/sg1) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
MAC Address: 00:c0:ff:ff:5b:9e
ORIGIN ADDRESS DEFAULT GATEWAY
DHCP 192.168.20.189/24 192.168.20.1
Command Completed. ("show network -U admin -P Testit123!")
```

In this example output, `Testit123!` is the new password, which has worked as the `show network` command accepted the new password and returned the BMC IP.

IOM B

Verifying the `admin` password has changed is accomplished by running valid BMC CLI commands. In this case, we chose the `show network` command as this command will also return the BMC IP address for use later on. Run this command as follows, replacing `<new password>` with the desired new password:

```
fwdownloader –d 1 –cli "show network" –U admin –P <new password>
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 1 -CLI 'show network' -U admin -P Testit123!
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
Found SES Page 1 for Device 1 (/dev/sg4) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
MAC Address: 00:c0:ff:ff:5b:9e
ORIGIN ADDRESS DEFAULT GATEWAY
DHCP 192.168.20.207/24 192.168.20.1
Command Completed. ("show network -U admin -P Testit123!")
```

In this example output, `Testit123!` is the new password, which has worked as the `show network` command accepted the new password and returned the BMC IP.

Change password using BMC network interface

To use the BMC Network Interface, you need to obtain the BMC IP Address for both IOMs. Each IOM has its own BMC Network Interface IP Address. By default, the storage enclosure management ports are set to DHCP. The IP Address for each IOM can be obtained using 3 different methods:

1. From the network DHCP server by looking at the network DHCP server for assigned IP Addresses
2. Directly from the storage enclosure BMC using in-band SES Show Network command
3. Directly from the storage enclosure SES Page 7

Methods 2 and 3 require obtaining the SES Target Device (example: `fwdownloader-ses`).

Getting BMC IP Address using `fwdownloader`

IOM A

Use the `show network` command with lower case `cli`:

```
fwdownloader -d 0 -cli "show network"
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 0 -cli 'show network'
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
Found SES Page 1 for Device 0 (/dev/sg1) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
MAC Address: 00:c0:ff:ff:5b:9e
ORIGIN ADDRESS DEFAULT GATEWAY
DHCP 192.168.20.189/24 192.168.20.1
Command Completed. ("show network")
```

In this example, 192.168.20.189/24 is the IP address.

IOM B

Use the show network command with upper case CLI:

```
fwdownloader –d 1 –CLI "show network"
```

```
The command will provide the following output:

root@deserve05:/home/stxeng# fwdownloader-d 1 -CLI 'show network'

Seagate fwdownloaderv4.23

Scanning SES devices...Please Wait...2 SES devices found.

Found SES Page 1 for Device 1 (/dev/sg4) size 308 (0x134)

WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF

Product Revision: 6039 S/N: SWB0D005RN

MAC Address: 00:c0:ff:ff:5b:9e

ORIGIN ADDRESS DEFAULT GATEWAY

DHCP 192.168.20.207/24 192.168.20.1

Command Completed. ("show network")
```

In this example, 192.168.20.207/24 is the IP address.

Getting BMC IP address using SES page 7

Use SES Page 7to get IP addresses for both IOMs using the following command:

```
sg_ses–p 7 <SES Target Device> | grep IP
```

The command will provide the following output:

```
root@SMC-1:/home/stxeng/Voyager-Juno/tools_r5.86# sg_ses-p 7 /dev/sg0 | grep IPElement 0 descriptor:
TP=D9;SN=XXXXXXXXXXXXXXX;F1=6046;BL=;VR=0100;VC=D228F9BA;CR=;FR=01;FC=9751A830;PN=XXXXXXXXXX;FF1=06000046;PC=06860000;PD=;USM=6.0-r2025.33.0-rel-527;SB=0;IP=10.235.194.162 ;IPM=DHCP;MAC=00:C0:FF:63:10:15;NK=255.255.252.0;Element 1 descriptor:
TP=D9;SN=XXXXXXXXXXXXXXX;F1=6046;BL=;VR=0100;VC=D228F9BA;CR=;FR=01;FC=9751A830;PN=XXXXXXXXXX;FF1=06000046;PC=06860000;PD=;USM=6.0-r2025.33.0-rel-527;SB=0;IP=10.235.194.191 ;IPM=DHCP;MAC=00:C0:FF:63:10:24;NK=255.255.252.0;root@SMC-1:/home/stxeng/Voyager-Juno/tools_r5.86#
```

In this example output, 10.235.194.162 is the BMC IP address for IOM A and 10.235.194.191 is the BMC IP address for IOM B.

Change password using SSH

IOM A

1. Connect to the BMC via SSH by running the following command, replacing <IOM A IP Address> with the IP address of IOM A:

   ```
   ssh admin@<IOM A IP Address>
   ```

   The command will provide the following output:

   ```
   root@SMC-1:/home/stxeng/Voyager-Juno/tools_r5.86# ssh admin@10.235.194.162The authenticity of host '10.235.194.162 (10.235.194.162)' can't be established.RSA key fingerprint is SHA256:yl71qjGeve3mKrhVIZgzFFKjbjCJfTwzS1C0NEOrjsg.Are you sure
   ```

```
you want to continue connecting (yes/no/[fingerprint])? yesWarning: Permanently added '10.235.194.162' (RSA) to the list of known hosts.BMC VERSION:6.0-r2025.33.0-rel-527SERIAL NUMBER:SLB0V63188
```

```
admin@10.235.194.162's password:You must update your password before using this account
```

```
exos-e-ast2600-runbmc-a>
```

2. Enter the default password `admin123` when prompted.
3. Change the password by running the following command:

```
set password
```

The command will provide the following output:

```
Changing current logged-in user admin
```

```
Enter current password for user admin
```

```
:Enter new password for user admin:
```

```
Confirm new password for user admin
```

```
:Password updated successfully for admin
```

```
Changes will take effect on next log in. Please log out
```

```
Role updated for user admi
```

```
nInterface list updated for user admin
```

```
exos-e-ast2600-runbmc-a
```

4. Verify the password change:
   1. Log out of the current SSH session.
   2. SSH back into the BMC using the new password.
   3. Confirm access by running a command, for example `show help`.

IOM B

1. Connect to the BMC via SSH by running the following command, replacing `<IOM B IP Address>` with the IP address of IOM B:

```
ssh admin@<IOM B IP Address>
```

The command will provide the following output:

```
root@SMC-1:/home/stxeng/Voyager-Juno/tools_r5.86# ssh admin@10.235.194.191The authenticity of host '10.235.194.191 (10.235.194.191)' can't be established.RSA key fingerprint is SHA256:yl71qjGeve3mKrhVIZgzFFKjbjCJfTwzS1C0NEOrjsg.Are you sure you want to continue connecting (yes/no/[fingerprint])? yesWarning: Permanently added '10.235.194.191' (RSA) to the list of known hosts.BMC VERSION:6.0-r2025.33.0-rel-527SERIAL NUMBER:SLB0V63188
```

```
admin@10.235.194.191's password:You must update your password before using this account
```

```
exos-e-ast2600-runbmc-b>
```

2. Enter the default password `admin123` when prompted.
3. Change the password by running the following command:

```
set password
```

The command will provide the following output:

```
Changing current logged-in user admin
Enter current password for user admin
:Enter new password for user admin:
Confirm new password for user admin:
Password updated successfully for admin
Changes will take effect on next log in. Please log out
Role updated for user admin
Interface list updated for user admin
exos-e-ast2600-runbmc-b>
```

4. Verify the password change:
    1. Log out of the current SSH session.
    2. SSH back into the BMC using the new password.
    3. Confirm access by running a command, for example `show help`.

Change password using Redfish

Each IOM on the storage enclosure has a Redfish service running on the BMC. Redfish commands are sent from the attached host using HTTP Requests. Popular HTTP Request tools such as cURL exist in many operating systems. The following steps use the cURL tool to send Redfish commands to change the `admin` credentials.

Procedure

1. Establish a Redfish session with the BMC on IOM A
2. Set the new password on IOM A
3. Establish a Redfish session with the BMC on IOM B
4. Set the new password on IOM B

NOTE Take care when cutting and pasting the following command examples between Windows and Linux. Windows uses a different character encoding than Linux for characters such as double quotes " and single quotes '. This may require manually re-entering the command examples in Linux.

Establishing a Redfish session
IOM A

1. Use a POST request to the Redfish Session Service endpoint to authenticate and create a session:

```
root@SMC-1:/home/stxeng# curl -k -D --X POST 'https://10.235.194.162/redfish/v1/SessionService/Sessions' -H "Content-Type: application/json" -d '{ "UserName": "admin", "Password": “admin123" }’
```

In this command:

- -X POST specifies the request method
- -H "Content-TYpe: application/json" sets the request header
- -d provides the credential payload
- -k allows SSL connections without certificate validation
- -D outputs the response headers to the console

2. If authentication is successful, the BMC returns an `HTTP 201 Created` response, such as:

```
HTTP/1.1 201 Created
Allow: GET, HEAD, POST
OData-Version: 4.0
X-Auth-Token: 9iUNAKRFYKnyx0ii64eV
Location: /redfish/v1/SessionService/Sessions/TYa4qQMLXc
Strict-Transport-Security: max-age=31536000; includeSubdomains
Pragma: no-cache
Cache-Control: no-store, max-age=0
X-Content-Type-Options: nosniff
Content-Type: application/json
Date: Wed, 28 Feb 2024 01:00:09 GMT
Content-Length: 267
{
"@odata.id": "/redfish/v1/SessionService/Sessions/TYa4qQMLXc",
"@odata.type": "#Session.v1_5_0.Session",
"ClientOriginIPAddress": "10.235.192.78",
"Description": "Manager User Session",
"Id": "TYa4qQMLXc",
"Name": "User Session",
"UserName": "admin"
```

3. In the response headers, locate:

```
X-Auth-Token: 9iUNAKRFYKnyx0ii64eV
Location: /redfish/v1/SessionService/Sessions/TYa4qQMLXc
```

- `X-Auth-Token` is the session token
- `Location` identifies the created session resource

4. Include the `X-Auth-Token` header in all Redfish API requests made during the active session. The token remains valid until the session expires or is explicitly deleted.

IOM B

1. Use a POST request to the Redfish Session Service endpoint to authenticate and create a session:

   ```
   'root@SMC-1:/home/stxeng# curl -k -D --X POST 'https://10.235.194.191/redfish/v1/SessionService/Sessions' -H "Content-Type: application/json" -d '{ "UserName": "admin", "Password": “admin123" }'
   ```

   In this command:

   - -X POST specifies the request method
   - -H "Content-TYpe: application/json" sets the request header
   - -d provides the credential payload
   - -k allows SSL connections without certificate validation
   - -D outputs the response headers to the console

2. If authentication is successful, the BMC returns an `HTTP 201 Created` response, such as:

   ```
   HTTP/1.1 201 Created
   Allow: GET, HEAD, POST
   OData-Version: 4.0
   X-Auth-Token: HgJs04Tmzh6GZBxpIX8k
   Location: /redfish/v1/SessionService/Sessions/TYa4qQMLXc
   Strict-Transport-Security: max-age=31536000; includeSubdomains
   Pragma: no-cache
   Cache-Control: no-store, max-age=0
   X-Content-Type-Options: nosniff
   Content-Type: application/json
   Date: Wed, 28 Feb 2024 01:00:09 GMT
   Content-Length: 267
   {
   "@odata.id": "/redfish/v1/SessionService/Sessions/TYa4qQMLXc",
   "@odata.type": "#Session.v1_5_0.Session",
   "ClientOriginIPAddress": "10.235.192.78",
   "Description": "Manager User Session",
   "Id": "TYa4qQMLXc",
   "Name": "User Session",
   "UserName": "admin"
   ```

3. In the response headers, locate:

```
X-Auth-Token: HgJs04Tmzh6GZBxpIX8k
```

```
Location: /redfish/v1/SessionService/Sessions/TYa4qQMLXc
```

   - `X-Auth-Token` is the session token
   - `Location` identifies the created session resource
4. Include the `X-Auth-Token` header in all Redfish API requests made during the active session. The token remains valid until the session expires or is explicitly deleted.

Changing the password using Redfish

IOM A

1. Use a PATCH request to the Redfish Account Service to update the admin password:

```
curl -k -H 'X-Auth-Token: 9iUNAKRFYKnyx0ii64eV' -X PATCH 'https://10.235.194.162/redfish/v1/AccountService/Accounts/admin' -H "Content-Type: application/json" -d '{ "Password": "Seagate123" }'
```

   In this command:

   - -X PATCH updates an existing resource
   - X-Auth-Token authenticates the request using the active session
   - The request body contains the new password for the admin account
   - -k allows SSL connections without certificate validation
2. If the request is successful, the BMC returns a confirmation message similar to the following:

```
"@Message.ExtendedInfo": [
{
"@odata.type": "#Message.v1_1_1.Message",
"Message": "The request completed successfully.",
"MessageArgs": [],
"MessageId": "Base.1.16.0.Success",
"MessageSeverity": "OK",
"Resolution": "None"
}
]
}
```

   This confirms that the admin password has been updated successfully.

IOM B

1. Use a PATCH request to the Redfish Account Service to update the admin password:

```
curl -k -H 'X-Auth-Token: HgJs04Tmzh6GZBxpIX8k' -X PATCH 'https://10.235.194.162/redfish/v1/AccountService/Accounts/admin' -H "Content-Type: application/json" -d '{ "Password": "Seagate123" }'
```

In this command:

- -X PATCH updates an existing resource
- X-Auth-Token authenticates the request using the active session
- The request body contains the new password for the admin account
- -k allows SSL connections without certificate validation

2. If the request is successful, the BMC returns a confirmation message similar to the following:

```
"@Message.ExtendedInfo": [
{
"@odata.type": "#Message.v1_1_1.Message",
"Message": "The request completed successfully.",
"MessageArgs": [],
"MessageId": "Base.1.16.0.Success",
"MessageSeverity": "OK",
"Resolution": "None"
}
]
}
```

This confirms that the admin password has been updated successfully.

Verify system health

The final step of the initial setup is to validate that the storage enclosure is in a healthy operational state. This validation consists of two checks:

- Drive status - confirm that all drives are detected and enabled
- System health - confirm that the system reports no faults

You can perform these checks using either SES or SSH, depending on your access method. Both approaches provide the same information.

Verifying system status using SES

1. Confirm that all drives are present and enabled by running the following command, replacing <new password> with your new admin password:

```
fwdownloader -d 0 -cli “show drive-status" -U admin -P <new password>
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 0 -cli 'show drive-status' -U admin -P Testit123!
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
```

```
Found SES Page 1 for Device 0 (/dev/sg1) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
Drive Vendor Model Revision Serial number Capacity State
----------------------------------------------------------------------------------------------------------------
Drive0 SEAGATE ST24000NM007H EE05 ZYD5XSDA 24.0TB Enabled
Drive1 SEAGATE ST24000NM007H EE05 ZYD75VTF 24.0TB Enabled
.
.
.
Drive98 SEAGATE ST24000NM007H EE05 ZYD4HCJB 24.0TB Enabled
Drive99 SEAGATE ST24000NM007H EE05 ZYD67KNT 24.0TB Enabled
```

This output indicates that all drives are listed and each drive reports its state as enabled.

2. Check the overall health of the storage enclosure by running the following command, replacing `<new password>` with your new admin password:

```
fwdownloader -d 0 -cli “show system-health" -U admin -P <new password>
```

The command will provide the following output:

```
root@deserve05:/home/stxeng# fwdownloader-d 0 -cli 'show system-health' -U admin -P Testit123!
Seagate fwdownloaderv4.23
Scanning SES devices...Please Wait...2 SES devices found.
Found SES Page 1 for Device 0 (/dev/sg1) size 308 (0x134)
WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
Product Revision: 6039 S/N: SWB0D005RN
System Information
---------------------------------------
System Name : 4U74
Midplane Serial Number : SWB0D005RN
Vendor Name : SEAGATE
Product ID : 1110346-05
Health : OK
PFU Activation Status : Inactive
```

```
BMC Status : BMC ready
```

```
Command Completed. ("show system-health -U admin -P Testit123!")
```

In this output, the `Health:` and `MBC Status:` fields indicate that the enclosure is in a healthy operational state.

Verifying system status using SSH

1. Log in to the IOM using the following command, replacing `<IOM_BMC_IP>` with the IP address of the IOM:

   ```
   ssh admin@<IOM_BMC_IP>
   ```

   For example:

   ```
   root@SMC-1:/home/stxeng#sshadmin@10.235.194.162
   ```

2. Confirm that all drives are detected and enabled by running the following command:

   ```
   show drive-status
   ```

   The command will provide the follwoing output:

   ```
   root@deserve05:/home/stxeng# fwdownloader-d 0 -cli 'show drive-status' -U admin -P Testit123!
   ```

   ```
   Seagate fwdownloaderv4.23
   ```

   ```
   Scanning SES devices...Please Wait...2 SES devices found.
   ```

   ```
   Found SES Page 1 for Device 0 (/dev/sg1) size 308 (0x134)
   ```

   ```
   WWN: 500c0ff0ff2d593c Vendor ID: SEAGATE Product ID: ST4C0-E24VFF
   ```

   ```
   Product Revision: 6039 S/N: SWB0D005RN
   ```

   ```
   Drive Vendor Model Revision Serial number Capacity State
   ```

   ```
   ----------------------------------------------------------------------------------------------------------
   ```

   ```
   Drive0 SEAGATE ST24000NM007H EE05 ZYD5XSDA 24.0TB Enabled
   ```

   ```
   Drive1 SEAGATE ST24000NM007H EE05 ZYD75VTF 24.0TB Enabled
   ```

   ```
   .
   ```

   ```
   .
   ```

   ```
   .
   ```

   ```
   Drive98 SEAGATE ST24000NM007H EE05 ZYD4HCJB 24.0TB Enabled
   ```

   ```
   Drive99 SEAGATE ST24000NM007H EE05 ZYD67KNT 24.0TB Enabled
   ```

   In this output, all drives are shown as listed and the drive state is enabled.

3. Check the overall system health by running the following command:

   ```
   show system-health
   ```

   The command will provide the follwoing output:

   ```
   exos-swb0e003fs-a> show system-health
   ```

```
System Information
------------------------------------------
System Name : 4U74
Midplane Serial Number : SWB0D005RN
Vendor Name : SEAGATE
Product ID : 1110346-05
Health : OK
PFU Activation Status : Inactive
BMC Status : BMC ready
```

In this output, the `Health:` and `MBC Status:` fields indicate that the enclosure is in a healthy operational state.

5 Troubleshooting

The storage enclosure management interface allows for provisioning, monitoring, and managing the storage enclosure. It uses the storage enclosure processor (SEP) and associated monitoring and control logic, such as the SCSI Enclosure Services (SES) service, to identify, assess, and diagnose power, drive, and cooling systems. Temperature sensors throughout the enclosure and its components monitor the thermal health of the storage system. If a critical sensor value exceeds a threshold limit, you receive a system notification that requires your attention.

If you encounter any issues during installation or initial configuration, sequentially use the topics in this section to assist you in fault isolation and correction.

IMPORTANT Do not use this section for configured systems already interacting with production data. For the kind of assistance you need in such cases, contact Seagate for technical support.

Address initial start-up issues

You must successfully complete the installation tasks in the identified sequence. You must use the power cords provided with the system and install interface cables that meet system requirements.

To address initial start-up issues:

1. Complete the following actions to eliminate power cord issues during installation:
   a. Request a replacement for damaged or missing power cords.
   b. Request a replacement for cords with plugs that do not match your outlets or voltage requirements
   c. Request a replacement for power cords that are too short to reach a power distribution unit.
2. Use LEDs throughout the storage enclosure as a means to determine if there is a critical fault. See "Interpret system LEDs" on page 24.
3. Complete the following actions to verify your installation if the host system does not recognize the storage enclosure:
   a. Verify the interface cables connected from the storage enclosure to each host bus adapter are not damaged, loose, or wired improperly.
   b. Look for any SAS Linkup indicators on both controller modules.
   c. Look for SAS target visibility by using the OS' device scan capability, or in the HBA BIOS.
   d. Verify that the host bus adapter drivers for the operating system are correctly installed.
4. Complete the following actions if the storage enclosure does not report as much capacity as expected:
   a. Verify that all drives are correctly installed and latched to the baseplane connectors.
   b. Verify all installed drives display green LEDs, rather than an LED with a fault status. Follow the replacement procedure for drives displaying a fault status. See "Interpret drive slot LED" on page 25.
5. Complete the following actions:
   a. Verify each power cord is properly and securely connected on both ends.
   b. Reconfirm that the power source used to power the storage enclosure is viable and meets the installation criteria.
   c. Power cycle the storage enclosure by removing both power cord connectors from both PSUs.
   d. Examine the IOM log for errors.
6. If the issue persists, contact Seagate support at www.seagate.com.

Identify fault conditions

Fault conditions do not necessarily cause the storage enclosure to cease functioning. Fault conditions do require a system administrator to take an appropriate action to clear the fault condition.

The IOMs allow you to choose from multiple fault isolation methods. This section provides the basic methodology used to locate faults within a storage system, then identify the affected FRUs.

When performing fault isolation and troubleshooting steps, select the option or options that best suit your site environment. Use of any one of the following options is not mutually exclusive to the use of another option. The order for the options is based on frequency of use.

1. Monitor event and alert notifications through your host system interface.
   a. **Alert notifications**: An alert reports a system fault, registers the type and severity, then tracks its resolution.
2. Alerts fall into three categories, listed in order of severity. Resolve them, from most severe to least severe.
   a. **Critical alerts**: Such alerts require immediate resolution, since they may cause an IOM to shut down or place data at risk.
   b. **Warnings**: Such alerts require immediate attention so you can evaluate the problem and correct it.
   c. **Informational alerts**: Such alerts neither require immediate attention nor immediate action.
3. Visually inspect the front panel fault LEDs, then locate the component fault LEDs, based on general location identified through the front panel. If a hardware issue prevents access to CLI, this is the only option available.

Table 4 Non-fault conditions

Symptom	Cause	Recommended action
Front panel LEDs, no fault conditions		
System power, system ID, and host connectivity LEDs with no fault condition LEDs	System functioning properly	No action required
HDD LED lightpipe, no fault conditions		
Amber LED on	Drive fault detected by enclosure	No action required
Amber flashing LED: 1s on, 1s off	Drive locate	No action required
Amber flashing LED: 3s on, 1s off	Drive reconstruction or drive in critical condition	No action required
PSU LEDs, no fault conditions		
Green LED on	AC power is present, PSU functioning normally	No action required
Input/output module LEDs, no fault conditions		
LEDs other than Hardware fault LED	System likely functioning properly	Often, no action required. See "Interpret IOM LED" on page 26 or "Isolate system application faults" on the next page.

Isolate hardware and connectivity faults

You may occasionally have to isolate a fault related to the storage enclosure hardware or related to data connections associated with the storage enclosure. This is particularly true with data paths because of the number of components involved along the data path and the complexity of the interactions. For example, if a host-side data error occurs, it could be caused by any of the involved hardware components: it could be a faulty host bus adapter (HBA) or a faulty IOM, cable, connector, or switch. It also could be a failure involving more than one of these components.

Use this section to gather common installation hardware fault information and isolate the fault.

△ **CAUTION** When you suspect a disk drive or connection is the fault, halt all input and output operations to the drive group or groups from all hosts as a data protection precaution. Make sure your regularly scheduled backup is good and that you conduct another backup at the time of failure as an additional data protection precaution.

To isolate hardware and connectivity faults associated with the storage enclosure:

1. Complete the following actions to gather fault information:
   a. Examine host application or operating system logs for fault identification.
   b. Examine system logs from both controller modules for errors, such as log and status output for fault identification.
   c. Use system alerts to help narrow the fault to an area of the storage enclosure.
   d. Visually inspect the front panel LEDs. A fault LED indicates there is a hardware issue and provides a general location: the front drawer and rear panel.
   e. Access the identified location, then look for an amber fault LED to help identify a faulty module. The SAS expander module fault LED faces the sidewall, so look carefully along the sidewall for faults in the slot.
   f. If you cannot find a fault in any of the listed areas, the fault most likely lies outside the storage enclosure.
2. Isolate the fault to one of the components in the storage enclosure. There can be a significant number of components interacting to create a viable data path, each potentially creating an issue. For example, if a host-side data error occurs, it could be hardware, such as the controller module or a faulty cable, or it could be the data host.
3. Proceed to the next section and take the recommended corrective action. This may mean obtaining a replacement FRU of the same type before replacing the faulty module.

Isolate system application faults

System application faults generally fall into two categories: drive and enclosure faults or input/output module (IOM) faults.

To troubleshoot system application errors:

1. If a drive or enclosure is at fault, determine the cause and take the related recommended action.

Table 5 Status of drive or enclosure, based on front panel *Fault-Application* LED

	Cause	**Recommended action**
Off	System application logic initiated by IOM functioning normally	None.
On	Application stack or enclosure fault	If the application fault LED is on, the fault has been detected by the application stack. Consult the help for their specific application software. If the module fault is illuminated, a fault has been detected by the enclosure itself and the enclosure's CLI, SES and Redfish status will report additional information. The application I/O stack may also relay this information via any additional interfaces it provides.

2. Determine the cause of a SAS port host-side or IOM-side connection fault.

a. Inspect the storage enclosure status through the application stack UI and follow any guidance provided.
b. If no guidance is available from the application stack, read the fault status from the enclosure CLI, SES, or Redfish interface.
c. For application-related faults, follow the instructions provided through the application stack UI.
d. For physical drive faults, follow the drive replacement procedure.
e. For IOM or LEM faults, quiesce inputs/outputs on the faulty IOM path if required by the application stack.
f. Ensure there is no unwritten data.
g. Inspect the host cable and connectors for any visible damage, then reseat the host cable.
h. If the fault condition persists after reconnection, move the host cable to a port with a confirmed good link status to isolate the issue.
i. If the fault persists after reseating the host cable, replace it with a known good cable.
j. Ensure the Host Bus Adapter (HBA) is fully seated in the PCI slot and confirm the slot is powered on and functioning.
k. If the fault condition persists, replace the IOM.
l. If the fault condition persists, reseat the HBA.
m. If the SAS host port activity LED still flashes amber, replace the HBA and reconnect the cable.
n. If replacing or reseating the IOM or LEM does not resolve the problem, consider that the fault might be related to a passive component in the data path, such as the midplane, rear baseplane, or internal cable harness.
o. If these steps do not resolve the fault, contact Seagate support for further assistance.

Take corrective action

After you follow the process above and isolate the fault to an area of the storage enclosure or to a particular module, use the following chart to determine the type of corrective action you should take. For the latest regulatory and compliance information see www.seagate.com/support.

Table 6 Corrective action for fault conditions

Symptom	Cause	Recommended action
Front panel fault LEDs for system application faults		
Fault-Application LED is on	A fault condition related to the system application logic	1. Scan the enclosure event log for specific information for the fault. 2. For system application faults, see "Isolate system application faults" on the previous page. 3. If the above actions do not resolve the fault, isolate the fault to the failing component identified in the rear panel area and follow the instructions below.
Front panel fault LEDs for slots		

Table 6 Corrective action for fault conditions (continued)

Symptom	Cause	Recommended action
Fault slot LED is on and a disk drive or LEM fault LED is on	A fault condition related to the hardware in the slot	1. Inspect LEMs for a fault amber LED that is on. If so, replace the LEM as soon as you have a replacement. 2. Inspect the LEDs on the slot drives for these conditions: • Drive fault LED is off. 3. Select one of the following actions: • If the drive LED is off, verify that the drive is fully inserted, the latch is fully engaged, and the storage enclosure is powered on. • If the fault LED is on, narrow the fault to the drive, a connection, or both. 4. Scan the enclosure event log for specific fault information and follow recommended actions. 5. If the above actions do not resolve the fault, replace the faulty drive or cable and connector as soon as you have a replacement.
Front panel fault LEDs for rear panel area		
Fault-Rear panel LED is on	A fault condition related to the hardware in the rear panel area	1. Inspect the FRUs in the rear panel for fault condition LEDs: the controller modules (IOMs), the system fan modules, and the power supply units (PSUs). 2. Scan the enclosure event log for specific fault information and follow recommended actions. 3. Narrow the fault to a FRU, a connection, or both, then follow the recommended actions for the related FRU.
Fault-Rear panel LED is on and a system fan fault LED is on	A fault condition related to the system fan	1. Select one of the following actions: • If only one system fan is failing, remove the system fan, wait 1 minute, then reseat the system fan. 2. If the system fan is still failing, replace it within the period specified in "In-service field maintenance" on page 50.
Fault-Rear panel LED is on and a PSU fault LED is on	A fault condition related to the PSU, such as a power fault condition	1. Verify AC mains connections to the PSU are live. 2. Confirm the redundant PSU is properly functioning. 3. Select one of the following actions: • If both are failing, follow shut down instructions and power off the system enclosure by removing power to both PSUs. Do not power on until after you successfully replace them both. • If only one PSU is failing, remove the power cord, wait 1 minute, then reseat the power cord. • Do not remove the PSU if it is being programmed. This will manifest with programming LED blink pattern shown in the prior section. If the PSU is stuck in programming mode, then the problematic PSU may be reseated and programming restarted. 4. If the PSU is still failing, remove it, wait 1 minute, then reseat it. 5. If the PSU is still failing, replace it within the period specified in "In-service field maintenance" on page 50. 6. If the power fault condition persists, contact Seagate for support.

Table 6 Corrective action for fault conditions (continued)

Symptom	Cause	Recommended action
Fault-Rear panel LED is on and an amber IOM fault LED is on	A fault condition related to the IOM	1. Restart the IOM with a CLI or Redfish command. 2. Confirm the redundant IOM is properly functioning. 3. Select one of the following actions: • Contact Seagate Support to verify that the action will not adversely affect the data paths. • If both IOMs are failing, follow shut down instructions and power off the system enclosure by removing power to both PSUs. Do not power on until after you successfully replace them both. • If only one IOM is failing, without shutting down the enclosure, remove the power cord, wait 1 minute, then reset the IOM. 4. If the IOM is still failing, and the failure is related to a IOM host port, follow the steps associated with system application faults below. 5. If the IOM is still failing, remove the power cord, wait 1 minute, then reseat the IOM. 6. If the IOM is still failing, replace it within the period specified in "In-service field maintenance" on page 50. 7. If installing a new IOM that is still failing, remove it, inspect connections for bent pins, reinstall it, then check the event log for errors.
Thermal monitoring and control		
Fault-Rear panel LED is on and the amber fault LEDs on all FRUs are on	Internal temperature exceeds the present threshold for the storage enclosure	1. Consult CLI, SES or Redfish to confirm the root cause of the failure. 2. Confirm you have met ambient temperature requirements identified in the Environmental Requirements section and that the air flow moves from the front to the rear of the storage enclosure. 3. Determine if one of the fans failed or is in the process of failing. Verify all fans are running at a similar RPM. If the impellers of a fan turn more than 2K RPM slower than the other fans, replace the fan. 4. Follow instructions related to increases in fan speed, identified below. 5. Shut down the storage enclosure and investigate before continuing.
Increased fan speed is consistently greater than 6K RPM when the ambient temperature is below 23°C (73.4°F).	Increases in fan speed are associated with reaching a thermal threshold as the first stage of the thermal control process. If you encounter fan speeds consistently greater than 12K RPM when the ambient temperature is below 23°C (73.4°F), the likely cause is reduced airflow through the system.	1. Look for airflow restrictions at the front and rear of the storage enclosure. **Recommendation**: If a rack door blocks airflow by more than 60%, make sure it has a front minimum gap of 75mm (3 in) and a rear minimum gap of 152mm (6 in). 2. Confirm there are no restrictions based on contaminates, such as dust. **Recommendation**: Improve removal of contaminates and keep area clean. 3. Look for excessive re-circulation of heated air from the rear to the front of the storage enclosure. **Recommendation**: Avoid mounting in rack cabinets that are fully enclosed. 4. Verify temperature is within product specifications. See Standards and regulations. **Recommendation**: Reduce the ambient temperature in the room.

6 In-service field maintenance

You may service the identified storage enclosure FRUs and update firmware while still maintaining continuous operation during the replacement, but with two very important qualifiers:

- You must determine whether your system allows for continuous operation during service replacement of the storage enclosure drives without interrupting access to enclosure file systems.
- You must complete the replacement in the allotted time, replacing only one FRU at a time. The storage enclosure design provides for redundancy, so the loss of a single FRU does not impact functionality for a limited time.

The tasks identified in this chapter cover all FRUs. It is absolutely essential you adhere to all safety precautions when servicing storage enclosure FRUs.

- "Replace a drive" on the facing page
- "Replace a link expansion module" on page 53
- "Replace a fan module" on page 55
- "Replace a PSU" on page 56
- "Replace an IOM" on page 58

△ **CAUTION** If you remove any FRU while the storage enclosure is powered up, you must replace it with a tested good spare within the allotted time for that FRU. If you do not replace the FRU and, when applicable, close the related cover within the identified time limit, you void the product warranty and the storage enclosure might overheat, causing equipment failure and possible data loss.

△ **CAUTION** When performing maintenance on the enclosure or its components:

- Observe the caution label affixed to each drive or FRU prior to handling or replacing it.
- Do not remove a defective FRU until you have its functional replacement ready for insertion.

To adhere to safety precautions when replacing a FRU in a storage enclosure:

1. Replace any defective FRU with a fully operational one as soon as possible.
2. Replace any defective FRU within the identified replacement time to minimize air loss and maintain optimum cooling within the storage enclosure.

Table 7 Time limits for FRU replacement

Defective FRU	Replacement time limit
Main slot	
Drives, LFF or SFF	5 minutes
Link expansion module (LEM)	5 minutes
Rear panel area	
System fan module	5 minutes
Power supply unit	5 minutes
Input/output module (IOM)	5 minutes

Table 7 Time limits for FRU replacement (continued)

Defective FRU	Replacement time limit
Attachments	
Rackmount shelf kit	N/A
Cable kits: Standard HD mini-SAS to HD mini-SAS (SF-8644)	N/A

3. Prevent electrostatic discharge from damaging the storage enclosure or its components.
   a. Keep a static-protected work surface clear of clutter, including plastic, vinyl, and foam.
   b. Transport and store FRUs in static-safe containers.
   c. Keep FRUs in their containers until reaching a clear, static-protected work surface.
   d. Always wear a grounded ESD wrist strap that meets a minimum 1 megohm (± 10%) resistance standard and that is snug against your skin.
   e. Use heel straps, toe straps, or boot straps on both feet to ground to your conductive floor or dissipating floor mat or use a portable field service kit with a grounded, static-dissipating work mat.
   f. Use conductive field service tools.
   g. When removing a FRU, immediately place it in anti-static packaging.
   h. Avoid touching pins, leads, or circuitry.

Replace a drive

Drives store and provide access to system data. Each drive slot can hold a single low-profile 3.5-in or 2.5-in form factor drive. The 2.5-in drives require an adapter.

There is a LED lightpipe adjacent to the drives. The LEDs use an amber fault LED to identify various states. Those items in the state column with an asterisk (*) indicate a fault condition.

Color	State	Status
None	Off	No AC power is present or the disk drive is functioning normally.
Amber	**On***	The drive has a hardware fault. Replace as soon as possible.
	Fast flash*(1s)	AC power is present and unit identification (UID) bit is set. Not a fault.
	Slow flash*(3s)	See the system log for identified fault conditions.

Figure 23 Interpretation of drive fault LED on top panel

An important feature of the storage enclosure design is redundancy. You can still maintain continuous operation during the replacement of a single drive for up to 5 minutes.

△ **CAUTION** If you remove any FRU while the storage enclosure is powered up, you must replace it with a tested good spare within the allotted time for that FRU. If you do not replace the FRU and, when applicable, close the related cover within the identified time limit, you void the product warranty and the storage enclosure might overheat, causing equipment failure and possible data loss.

△ **CAUTION** If you suspect a disk drive or disk drive connection is faulty, halt all input and output operations to the drives from all hosts as a data protection precaution. Make sure your regularly scheduled backup is good and that you conduct another backup at the time of failure as an additional data protection precaution.

To remove and replace a drive:

1. If you plan on removing all drives, properly shut down the storage enclosure.
2. Retrieve the new drive in its static-protected container, ready to access and use it upon removal of the faulty one.
3. (Optional) As an extra safety measure while installing drives, support the storage enclosure with a mechanical lift to avoid any potential issues caused by downward forces.
4. Facing the front of the enclosure, lift the pull handle and steadily pull the drawer out on its rails until it locks in the first service position. If the drive is in a rear row and cannot be accessed from the first service position, pull the service unlock tabs on both sides of the drawer toward you, and then pull the drawer out until it locks in the final service position.

> ⚠ **WARNING!** To avoid risk of injury from pinching your fingers, lift the front handle by holding it from underneath.

5. Locate the drive you need to replace. The fault LED for each drive is a steady or blinking amber for a fault condition. Otherwise, it is off.

> △ **CAUTION** You must replace the faulty drive with a drive of the same type with a capacity equal to or greater than the one due for replacement. Otherwise, the storage enclosure cannot use the new drive to reconstruct the disk group.

6. Insert a finger into the ringed hole of the required drive slot cover and slide it toward you until the latch is released.
7. Lift the cover upward toward yourself.
8. Remove the drive.

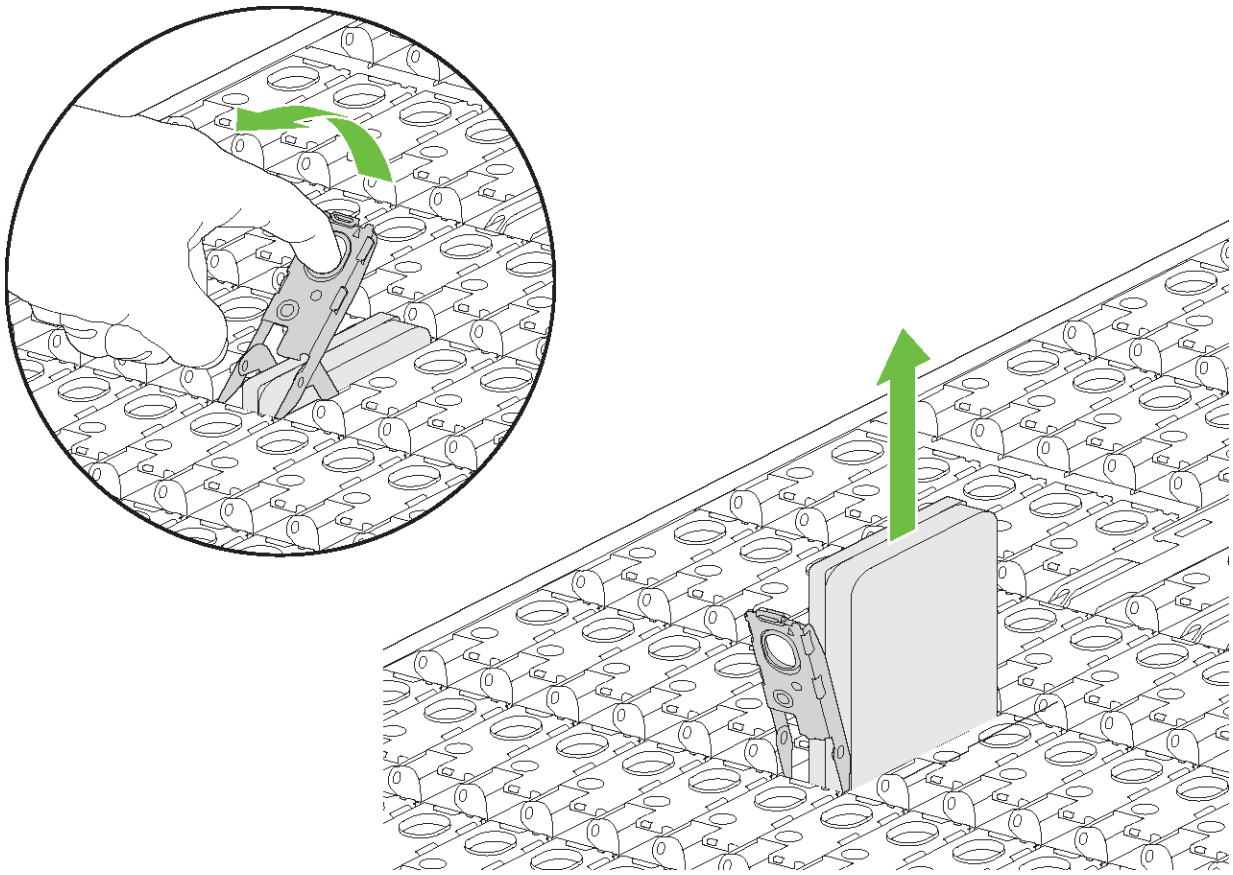


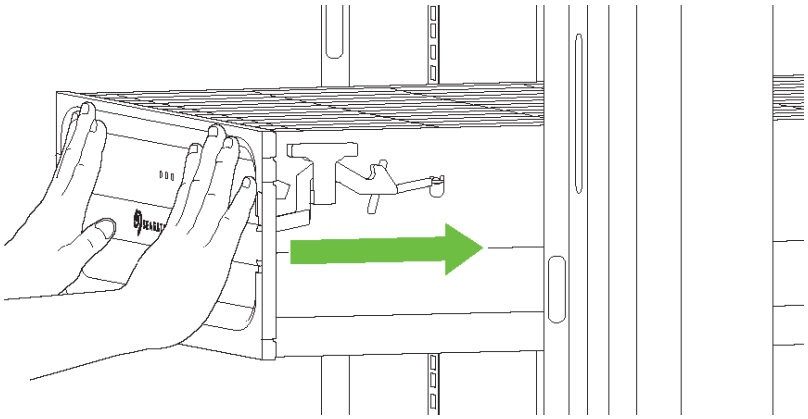
Figure 24 Drive removal

9. While maintaining proper static protection, remove the new drive from its static-protected container.
10. Insert the disk drive into the open slot with the connector facing down and the label facing right.
11. Gently press the cover of the open slot forward and down to seat the drive in the slot.

> ⚠ **CAUTION** Before closing the drawer please ensure all drive covers are closed to prevent damage to drive covers.

12. If you are replacing all drives, repeat the entire process for each of them.
13. Verify the drive fault LED is off.
14. Close the drawer by pulling on the green service tabs on either side of the drawer towards you and press the drawer forward until fully closed.

> ⚠ **WARNING!** To avoid risk of injury from pinching your fingers, remove your fingers from the service unlock tabs after you start pressing the drawer forward. Once the locks are disengaged, place your hands on the handle to fully close the drawer.



15. (Optional) Lower and remove the mechanical lift.

Replace a link expansion module

Link Expansion Modules (LEMs) facilitate internal expansion of storage capacity in the enclosure.

> ⚠ **CAUTION** If you remove any FRU while the storage enclosure is powered up, you must replace it with a tested good spare within the allotted time for that FRU. If you do not replace the FRU and, when applicable, close the related cover within the identified time limit, you void the product warranty and the storage enclosure might overheat, causing equipment failure and possible data loss.

To remove and replace a LEM:

1. Consider the implications of the replacement, reviewing all solution service documentation for pre- and post-replacement procedures to minimize system disruption.
2. (Optional) If you plan on removing all LEMs, properly shut down the storage enclosure.
3. Retrieve the new LEM in its static-protected container, ready to access and use it upon removal of the faulty one.
4. Facing the front of the enclosure, lift up the pull handle and steadily pull the drawer out on its rails until it locks in the service position.

⚠ **WARNING!** To avoid risk of injury from pinching your fingers, lift the front handle by holding it from underneath.

5. Pull the service unlock tabs on both sides of the drawer towards you and pull the drawer out on its rails until it locks in the extended position.
6. Locate the LEM you need to replace. The fault LED for each LEM is a steady or blinking amber for a fault condition. Otherwise, it is off.
7. Pull up on both cam handles. They will rotate upward and disconnect from the embedded connectors.
8. Carefully remove the LEM by sliding upward on the internal guides until it clears the drawer.

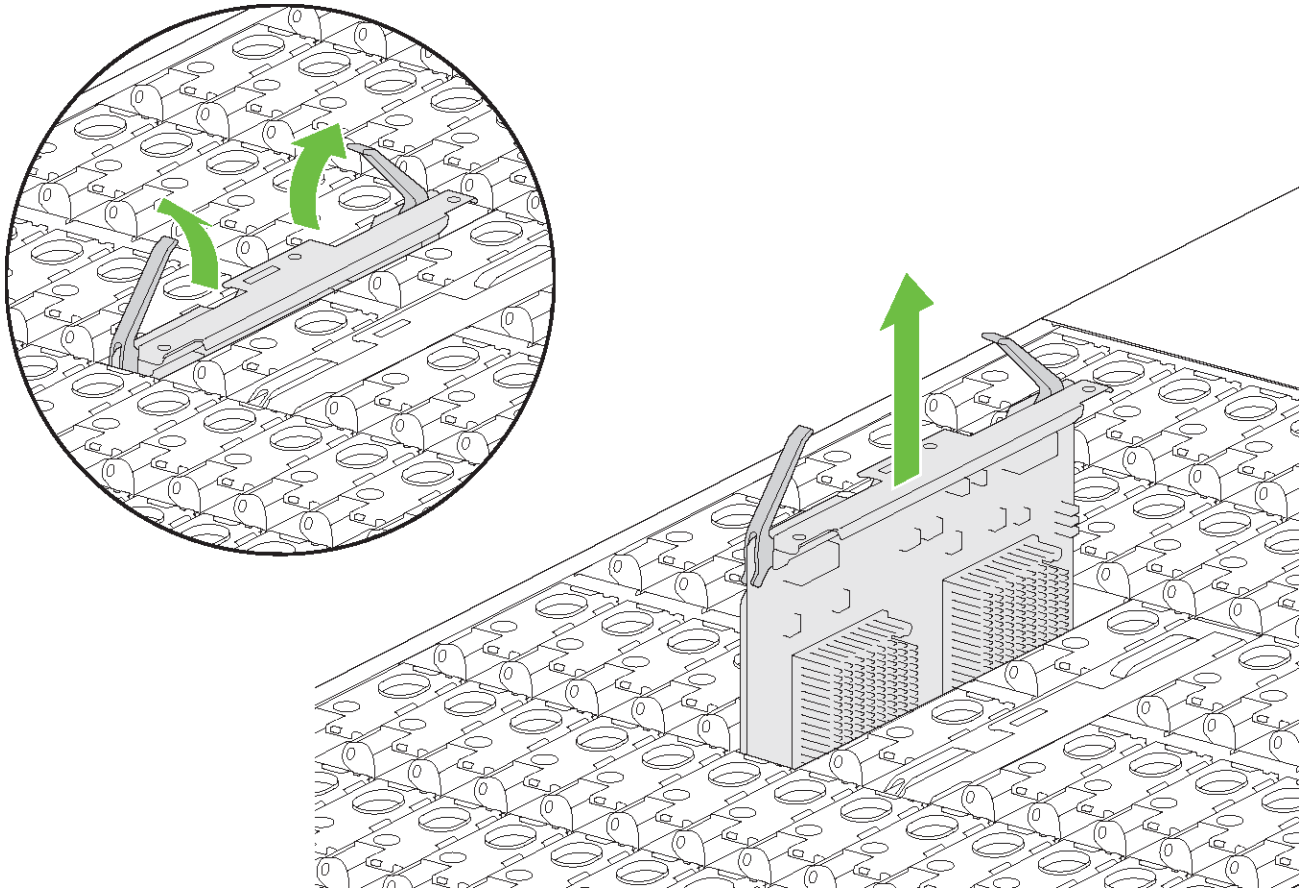
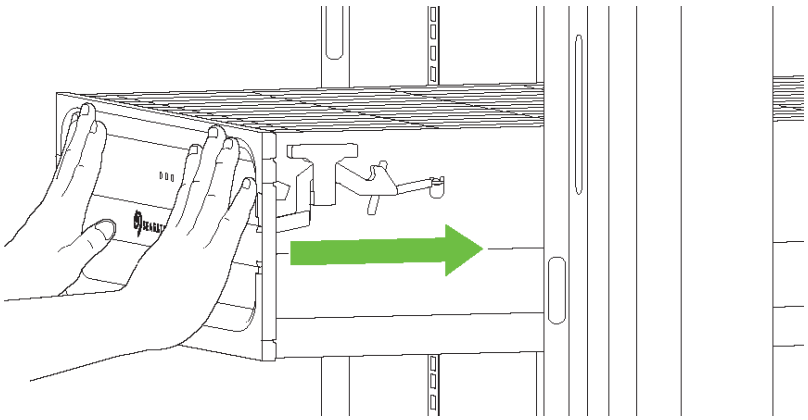


Figure 25 LEM removal

9. While maintaining proper static protection, remove the new LEM from its static-protected container.
10. Carefully insert the LEM in to the vacant slot by engaging the PCB into the guides on either side.
11. When near the end of travel, rotate the cam levers up until they engage the slots on either side of the slot.
12. With the cam levers engaged in the respective slots, rotate and press down until the levers are both horizontal. Gently push down on the cam levers to ensure they LEM is fully connected.
13. Pull the service unlock tabs on both sides of the drawer towards you and press the drawer forward until fully closed.
14. Verify that the front and rear expander status LEDs are green.

⚠ **WARNING!** To avoid risk of injury from pinching your fingers, remove your fingers from the service unlock tabs after you start pressing the drawer forward. Once the locks are disengaged, place your hands on the handle to fully close the drawer.

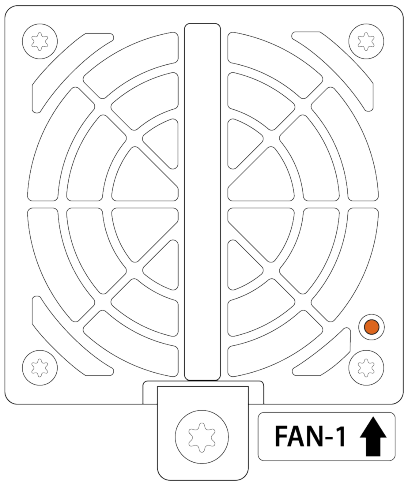


15. (Optional) Lower and remove the mechanical lift.

Replace a fan module

The 4 system fan modules provide cooling to the main slot of the storage enclosure.

Each system fan module has an amber fault LED. The asterisk (*) indicates a fault condition.



Color	State	Status
None	Off	No AC power is present or the system fan module is functioning normally. Fan activity indicates AC power is present.
Amber	**On***	The system fan module has a hardware fault.
	Flashing	AC power is present and the system fan module is undergoing system identification.

Figure 26 Interpretation of system fan module fault LED

An important feature of the storage enclosure design is redundancy. The storage enclosure can maintain continuous operation during the replacement of a single system fan module, as long as it is within the time limit of 5 minutes, since removal of a system fan module significantly reduces airflow in the slot.

△ **CAUTION** If you remove any FRU while the storage enclosure is powered up, you must replace it with a tested good spare within the allotted time for that FRU. If you do not replace the FRU and, when applicable, close the related cover within the identified time limit, you void the product warranty and the storage enclosure might overheat, causing equipment failure and possible data loss.

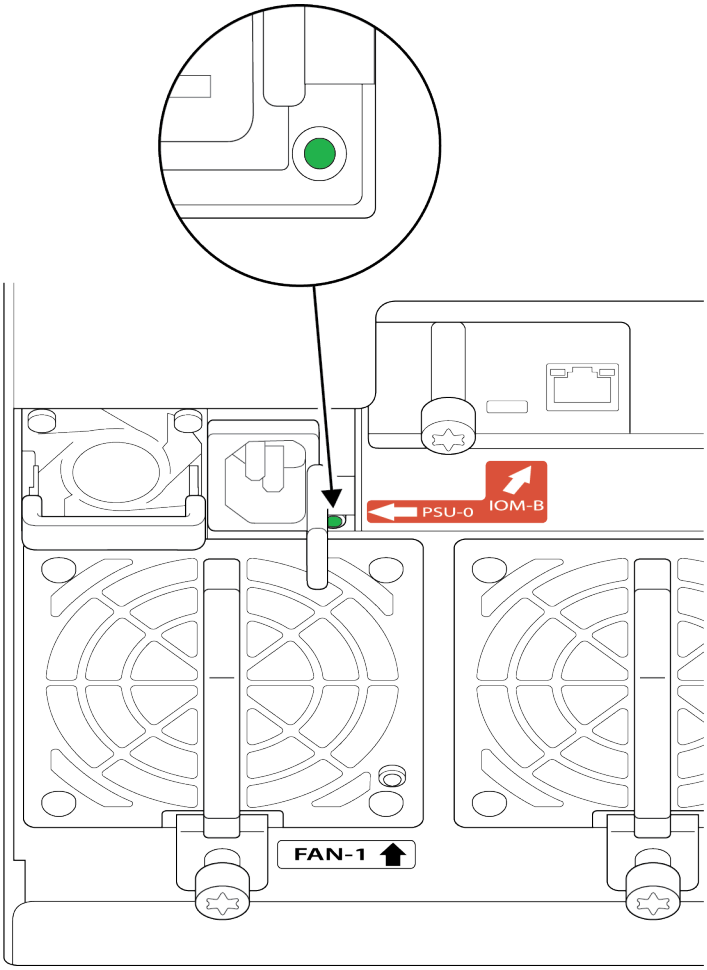
To remove and replace a system fan module:

1. If you plan on removing all system fan modules, properly shut down the storage enclosure.
2. Retrieve the new system fan module in its static-protected container, ready to access and use it upon removal of the faulty one.
3. Completely loosen thumb screw using your fingers, T15, or flathead screw driver.
4. Using the handle, gently remove the system fan module using a steady pressure to pull it from the storage enclosure while supporting it with your other hand and set it aside.
5. While maintaining proper static protection, remove the new system fan module from its static-protected container.
6. Inspect the system fan module carefully to make sure it is not damaged or bent in any way.
7. Properly orient the system fan module so you can grasp the handle, then orient it to its empty slot.
8. Slide the system fan module into its empty slot until it connects to the power midplane and stops.
9. Tighten the thumb screw using hand or a T-15 Torx or flathead driver to 3 in-lbs.
10. If you are replacing all system fan modules, repeat the entire process for each of them.
11. Verify the system fan module fault LED is steady amber when the cooling fans began spinning, then goes out when the cooling fans reach their optimal rotational speed.
12. Return to the front panel of the storage enclosure and verify that the *Fault-Rear panel* LED is not steady amber.

Replace a PSU

Both power supply units (PSUs) provides power to the storage enclosure within the following specifications: 200V to 240V AC at 50Hz to 60Hz.

The storage enclosure PSU module contains a single LED to reflect PSU module status.



LED	Color	State	Status
PSU status LED	Green/Amber	Solid Green	Output on and PSU OK
		Solid Off	No AC on all PSUs
		Blink 1 Hz Green	PSU Standby or Cold Standby with AC present
		Solid Amber	No AC on PSU with other PSU powered or a PSU failure event has been detected
		Blink 1 Hz Amber	A PSU warning event has been detected
		Blink 2 Hz Green	A PSU firmware update is in progress

Figure 27 Interpretation of PSU module LED

An important feature of the storage enclosure design is redundancy. You can still maintain continuous operation during the replacement of a single PSU, as long as it is within the time limit of 5 minutes.

CAUTION If you remove any FRU while the storage enclosure is powered up, you must replace it with a tested good spare within the allotted time for that FRU. If you do not replace the FRU and, when applicable, close the related cover within the identified time limit, you void the product warranty and the storage enclosure might overheat, causing equipment failure and possible data loss.

CAUTION Do not remove covers from any FRU. There is a danger of electric shock inside. Return the FRU to your supplier for repair.

To remove and replace a power supply unit:

1. If you plan on removing both PSUs, properly shut down the storage enclosure.
2. Retrieve the new PSU in its static-protected container, ready to access and use it upon removal of the faulty one.
3. Facing the rear of the enclosure, disconnect the provided power connector from the faulty PSU or both PSUs for complete removal of power from the power distribution unit (PDU).
4. Depress the latch and pull the PSU out of the hole.
5. Gently pull the PSU out of the enclosure.
6. While maintaining proper static protection, remove the new PSU from its static-protected container.
7. Inspect the PSU carefully to make sure it is not damaged or bent in any way, paying particular attention to connector pins.
8. Push the PSU in until the latch clicks.
9. If you are replacing both PSUs, repeat the entire process for the second PSU.
10. Re-connect the power cord to the newly repalced PSU.
11. Verify the PSU status LED is steady green and the cooling fans are spinning.
12. Return to the front panel of the storage enclosure and verify that the *Fault-Rear panel* LED is not steady amber.

Replace an IOM

Both input/output modules (IOM) manage the flow of data to and from the storage enclosure. Each IOM provides a very specialized, solutions-specific interaction that depends on your system configuration and software implementation, including SAS zoning, failover and failback procedures, and multipath procedures.

The IOM has a number of ports, each with independent status LEDs. Those items in the state column with an asterisk (*) indicate a fault condition.

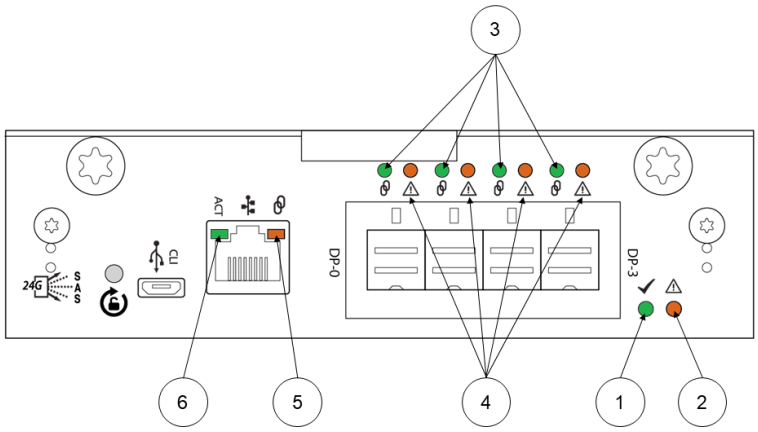


Figure 28 IOM LEDs

Pos	LED	Color	State	Status
1	Power/status LED	Green	On	The I/O module's BMC is powered and functional
			Flashing 0.25s On, 0.25s Off	The I/O module's BMC is powered and booting
			Off	The I/O module is unpowered, or the BMC is not able to boot
2	Fault LED	Amber	On	A fault within the IOM has been detected or the user has requested the enclosure to report a fault on the IOM via SES, Redfish or the CLI
			Flashing 1s On, 1s Off	The enclosure has been requested to identify the IOM by the user/host application using SES, Redfish, or the CLI
			Off	There is no fault or identify condition on the IOM
3	Mini-SAS-HD Port Activity	Green	On	One of more phys on the port have linked up
			Flashing Off	One of more phys on the port have detected SAS activity
			Off	All phys on the port have linked down
4	Mini-SAS-HD Port Fault	Amber	On	A fault with the attached cable or the port hardware has been detected.
			Flashing 1s On, 1s Off	The enclosure has been requested to identify the mini-SAS HD port by the user/host application using SES, Redfish, or the CLI
			Off	There is no fault or identify condition on the port/cable
5	Ethernet network port speed	Amber	on	1000base -T negotiated rate
			off	10/100base-T negotiated rate
6	Ethernet network port activity	Green	on	Ethernet link is up
			off	Ethernet link is down

Figure 29 Interpretation of IOM LEDs

The RJ45 Ethernet port LEDs are driven by the Ethernet PHY hardware and implement a multi-purpose indication scheme using its amber and green LEDs.

Consult your solution service documentation for details on how to minimize system disruption during service replacement of a controller module. Fault conditions include the following:

- Logs or events indicate a fault condition for the IOM.
- The *Fault*LED on the storage enclosure front panel is steady amber.
- Troubleshooting indicates a problem with the IOM. When you are isolating connectivity or drive fault conditions, stop the data flow to the affected disk groups from all hosts as a data protection precaution and back up your data.

△ **CAUTION** If you remove any FRU while the storage enclosure is powered up, you must replace it with a tested good spare within the allotted time for that FRU. If you do not replace the FRU and, when applicable, close the related cover within the identified time limit, you void the product warranty and the storage enclosure might overheat, causing equipment failure and possible data loss.

To remove and replace an IOM:

1. Consider the implications of the replacement, reviewing all solution service documentation for pre- and post-replacement procedures to minimize system disruption.
2. If you plan on removing all IOMs, properly shut down the storage enclosure.
3. Retrieve the new IOM in its static-protected container, ready to access and use it upon removal of the faulty one.
4. Facing the rear of the rack cabinet, locate the faulty IOM.
5. Completely loosen both thumbscrews using your hand or a T-15 Torx or flathead driver.
6. Pull outward using metal tab provided until it disconnects with connector.
7. Gently pull the IOM away and keeping it level with both hands during removal, then set aside.
8. While maintaining proper static protection, remove the new IOM from its static-protected container.
9. Inspect the IOM to make sure it is not damaged or bent in any way, paying particular attention to connector pins.
10. Properly orient the IOM so you can grasp the handle, then orient it to its empty slot.
11. Slide the IOM into its empty slot until you feel it fully connect to the midplane.
12. After pressing against it once more to make sure it is fully seated.
13. Tighten each thumb screw on the IOM to approximately 3 in-lbs using a T15 torx or flat-head screw driver.
14. Reconnect each of the cables to its labeled location, again making sure all are fully seated.
15. If you are replacing both IOMs, repeat the entire process for each of them.
16. Verify each IOM fault LED is off.
17. Return to the front panel of the storage enclosure and verify that the *Fault-Rear panel* LED is not steady amber.

Update firmware

All modules within the storage and expansion enclosure system, such as drives, controllers, power supply units, and fans, must be compatible and must run on firmware revisions from the same Universal Storage Module™ (USM) firmware release. After installing the storage enclosure and applying power for the first time, verify that all modules and drives within the storage and expansion enclosures have the most current USM firmware.

Additionally, confirm the system configuration (including SAS zoning) is correct per solution requirements.