Technical Report

Introduction to NetApp E-Series E2800 arrays

Feature overview with SANtricity

Mitch Blackburn, NetApp

November 2024 | TR-4725

Abstract

The NetApp® E-Series E2800 hybrid storage system is optimal for wide-ranging storage requirements such as video surveillance, enterprise backup targets, and remote office mixed workloads. This report provides detailed system information about the multiple system configuration options of NetApp SANtricity®. It is also a great starting point to introduce E2800 system details to sales engineers, partners, service providers, and customers.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Introduction

NetApp E-Series E2800 storage systems address wide-ranging data storage requirements with balanced performance that is equally adept at handling large sequential I/O for video, analytical, and backup applications. It is also suited for handling small random I/O requirements for small and medium-sized enterprise mixed workloads. The E2800 brings together the following advantages:

- Support for hybrid drive configurations.
- Host interface flexibility (SAS, FC, and iSCSI).
- High reliability (up to 99.9999%).
- Intuitive management. Simple administration for IT generalists, detailed drill-down for storage specialists.
- Remote Storage Volumes can be used to help streamline the process for equipment upgrades and/or to provide data migration capabilities to move data from a non-E-Series device to an E-Series system.

Together, these features create an entry-level storage system with flexibility and performance capabilities to support enterprise workloads without sacrificing simplicity and efficiency. In addition, the E2800 storage system's fully redundant I/O paths, advanced protection features, and extensive diagnostic capabilities deliver a high level of availability, data integrity, and security.

E2800 primary use cases

The flexible host interface options and wide range of drive choices make E-Series E2800 storage systems an optimal storage platform for enterprises that need powerful storage systems with easy growth strategies at the lowest possible initial investment. E2800 storage systems can scale up for dedicated workloads such as:

- Business-critical backup environments for enterprises of any size
- Video applications and video surveillance environments
- Common IT applications such as Microsoft Exchange and SQL Server for small and medium enterprises
- Efficient block storage for integrated appliances

E2800 system options

As shown in Table 1, the E2800 is available in three shelf options, which support both HDDs and SSDs, to meet a wide range of performance and application requirements.

Table 1) E2800 controller shelf and drive shelf models.

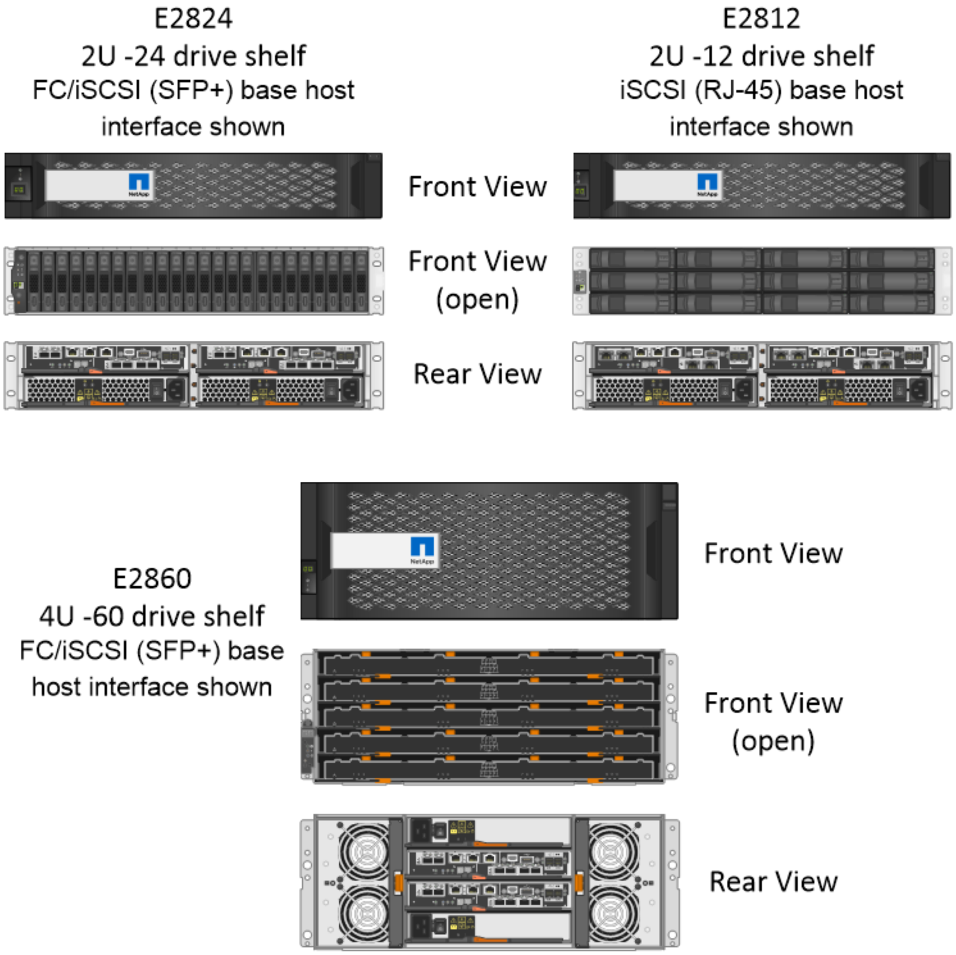
Controller shelf model	Drive shelf model	Number of drives per shelf	Type of drives
E2812	DE212C	12	3.5" NL-SAS drives 2.5" SAS SSDs
E2824	DE224C	24	2.5" SAS drives (HDDs and SSDs)
E2860	DE460C	60	3.5" NL-SAS drives 2.5" SAS drives (HDDs and SSDs)

Note: The E2812 supports a maximum of eight shelves, which includes one controller drive shelf, and up to seven expansion drive shelves. E2824 uses the same drive count, that is, 96 total drive slots (4 x 24-drive shelves). The E2860 supports up to two expansion drive shelves for a total of 180 drive slots. All shelf models can be mixed in the same storage array, but 180 total drive slots are the maximum drive slot count supported with the E2800 array family.

The E2812 and E2824 shelf options support one (simplex configuration) or two (dual configuration) controller canisters, whereas the E2860 supports only two controller canisters. All shelves support dual power supplies and dual fan units for redundancy. However, the 12- and 24-drive shelves have dual integrated power and fan canisters, whereas the 60-drive shelf (DE460C) has separate dual power supplies and fan units. The shelves are sized to hold 12 drives, 24 drives, or 60 drives, as shown in Figure 1.

Note: In a duplex configuration, both controllers must be identically configured.

Figure 1) E2800 shelf options (duplex configurations shown).



Note: The DE460C 4-rack unit (RU) 60-drive shelf requires dual ~220VAC power sources to power each shelf.

Each E2800 controller provides two Ethernet management ports for out-of-band management and has two 12Gbps (x4 lanes) wide-port SAS drive expansion ports for redundant drive expansion paths. The E2800 controllers include two built-in host ports, either two optical 16Gb FC/10Gb iSCSI or two 10Gb iSCSI Base-T ports. One of the host interface cards (HICs), listed in Table 2, can be installed in each controller.

Note: The non-base port version of the E2800 controller is no longer available.

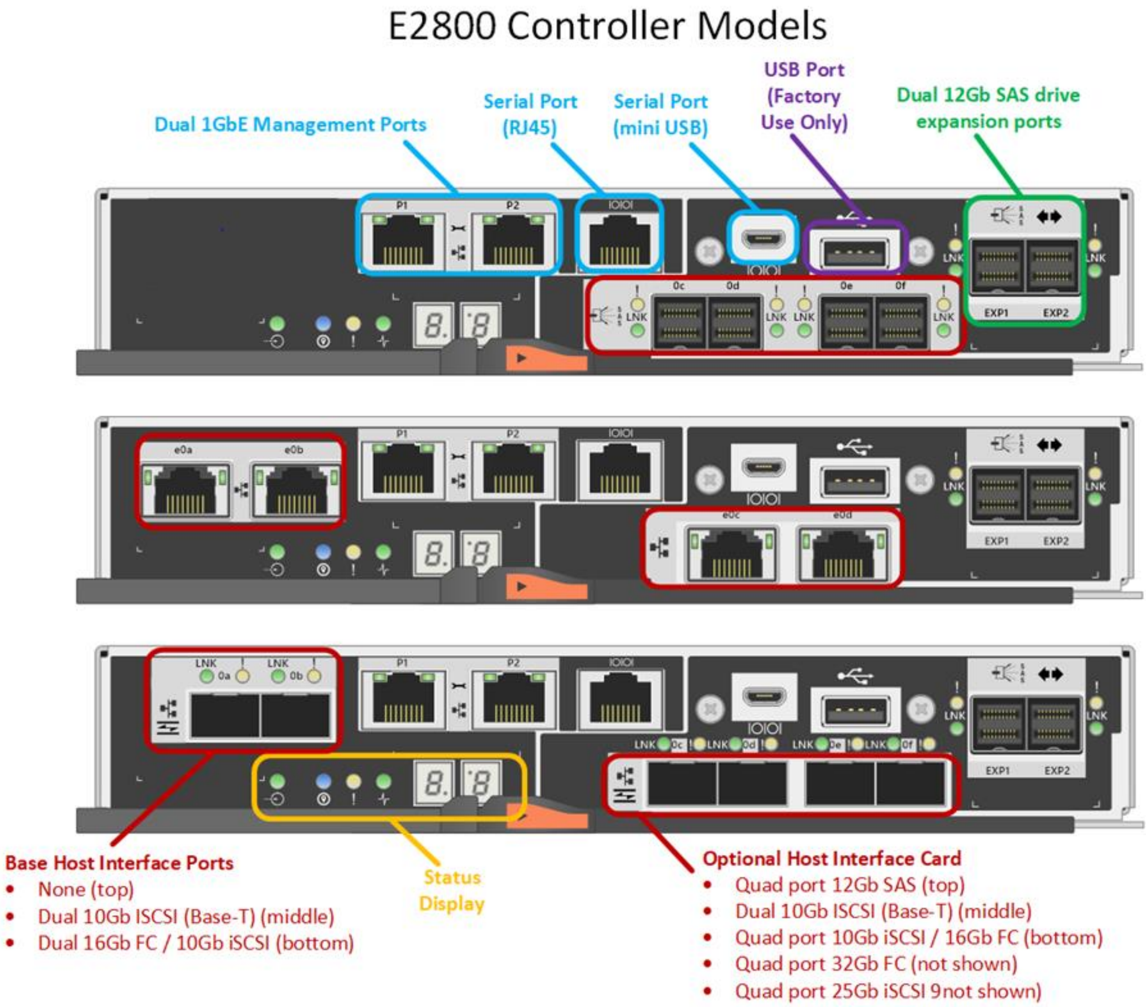
Table 2) Controller options with associated HIC options.

Controller type	2-port/ 4-port 12Gb SAS HIC	2-port/4-port 16Gb FC/10Gb iSCSI HIC	4-port 32Gb FC	4-port 25Gb iSCSI	2-port 10Gb iSCSI (Base-T)
E2800 without Baseboard Ports	Yes	Yes	Yes	Yes	Yes
E2800 w/ Base-T Baseboard Ports	Yes	No	Yes	Yes	Yes
Baseboard Ports E2800 w/ Optical	Yes	Yes	Yes	Yes	Yes

Note: A software feature pack can be applied in the field to change the host port protocol of the optical baseboard ports and the optical HIC ports from FC to iSCSI or from iSCSI to FC. Mixed protocol configurations are supported when the baseboard host ports are set for one protocol and the expansion HIC ports are set for a different protocol.

For optical connections, appropriate SFPs must be ordered for a specific implementation. All E2800 optical connections use OM4 fiber cable. Consult the Hardware Universe for a full listing of available host interface equipment. Figure 2 provides a close-up view of the E2800 onboard host interface options.

Figure 2) E2800 controller with no base ports, iSCSI Base-T ports, and optical base ports.


E2800 Controller Models
Dual 1GbE Management Ports
Serial Port (RJ45)
Serial Port (mini USB)
USB Port (Factory Use Only)
Dual 12Gb SAS drive expansion ports
P1
P2
0c
0d
0e
0f
EXP1
EXP2
e0a
e0b
e0c
e0d
0a
0b
LNK
Base Host Interface Ports
• None (top)
• Dual 10Gb ISCSI (Base-T) (middle)
• Dual 16Gb FC / 10Gb iSCSI (bottom)
Status Display
Optional Host Interface Card
• Quad port 12Gb SAS (top)
• Dual 10Gb ISCSI (Base-T) (middle)
• Quad port 10Gb iSCSI / 16Gb FC (bottom)
• Quad port 32Gb FC (not shown)
• Quad port 25Gb iSCSI 9not shown)

Note: Starting with SANtricity OS 11.80, the USB port that is for factory use only will be disabled.

Note: For 16Gb/8Gb/4Gb FC or 10Gb iSCSI, use the unified SFP (X-48895-00-R6-C), but for 1Gb iSCSI, you must use the 1Gb iSCSI SFP (X-48896-00-C).

For detailed instructions on changing the host protocol, go to the Maintain E-Series hardware -> Maintaining E2800 hardware -> Host port protocol conversion section at E-Series and SANtricity documentation resources.

SANtricity management features

NetApp E-Series and EF-Series arrays have a rock-solid reputation for reliability, availability, simplicity, and security. The new generation E-Series and EF-Series arrays running the latest SANtricity OS are common criteria certified (NDcPP v2 certification) and are listed on the Canadian Communications Security Establishment (CSE) site.

Deployment

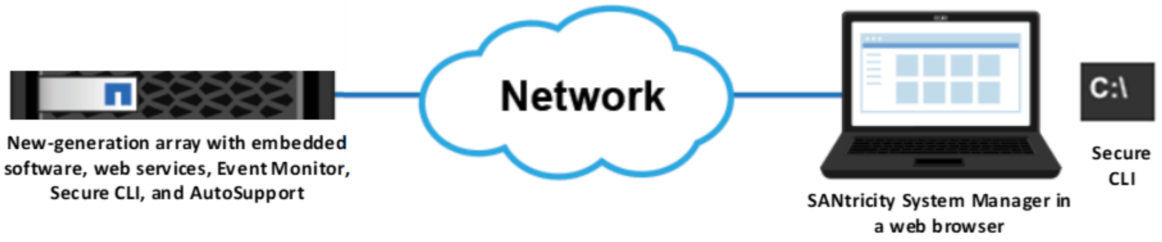
Deciding which components to install on an E2800-based storage array depends on if you want to manage single storage arrays individually or if you are managing multiple arrays.

Note: If you are using synchronous or asynchronous mirroring features, then Unified Manager is required.

Managing storage arrays individually

If you are not using synchronous or asynchronous mirroring features, then all configuration can be handled from SANtricity System Manager. Simply bookmark each array in a web browser. Figure 3 illustrates this configuration.

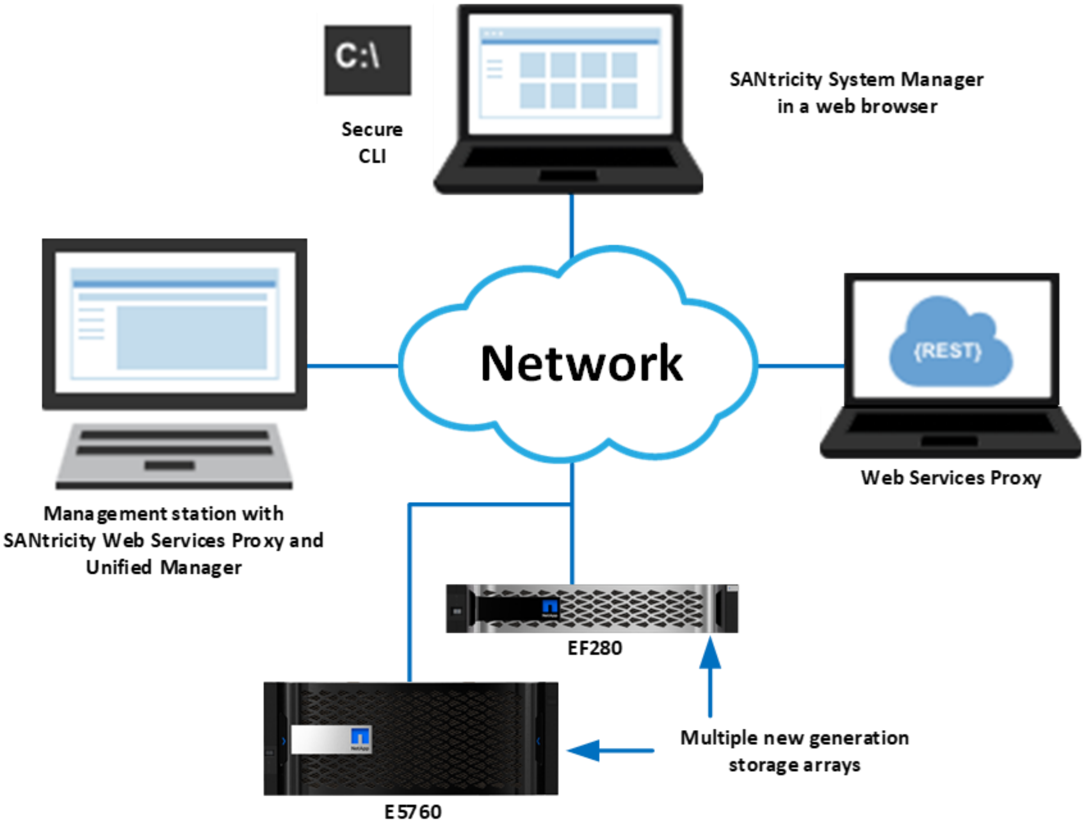
Figure 3) Managing a single E2800 with SANtricity System Manager.


New-generation array with embedded software, web services, Event Monitor, Secure CLI, and AutoSupport
Network
SANtricity System Manager in a web browser
C:\
Secure CLI

Multiple storage arrays

If you have one or more storage arrays, you can install Unified Manager to manage your overall environment while still managing all storage array-based configuration through SANtricity System Manager. To manage multiple arrays, you can launch SANtricity System Manager from Unified Manager, as shown in Figure 4.

Figure 4) Managing multiple new generation systems with SANtricity Unified Manager and SANtricity System Manager.


C:\
Secure CLI
SANtricity System Manager in a web browser
Network
{REST}
Web Services Proxy
Management station with SANtricity Web Services Proxy and Unified Manager
EF280
Multiple new generation storage arrays
E5760

SANtricity Unified Manager

SANtricity Unified Manager is a web-based central management interface that replaces the legacy SANtricity Storage Manager Enterprise Management Window (EMW) for managing new generation E-Series arrays. The Unified Manager GUI is bundled with the SANtricity Web Services Proxy starting with version 3.0 and installs on a management server with IP access to the managed arrays. Unified Manager can manage up to 500 arrays.

SANtricity Unified Manager has added the following time-saving features:

- Supports multi-factor authentication.
- Upgrade multiple arrays with the same type of controller at one time.

  Note: To upgrade to SANtricity OS 11.80.x the array must have already been upgraded to SANtricity OS 11.70.5.

- Supports Lightweight Directory Access Protocol (LDAP) and role-based access control (RBAC) just like SANtricity System Manager. Unified Manager includes a simplified certificate management workflow to manage the Unified Manager or Web Services Proxy server certificates (truststore and keystore certificates).
- Supports organizing arrays by groups that you can create, name, and arrange.
- Supports importing common settings from one array to another, saving time from duplicating setup steps for each array.
- Fully supports managing mirroring.

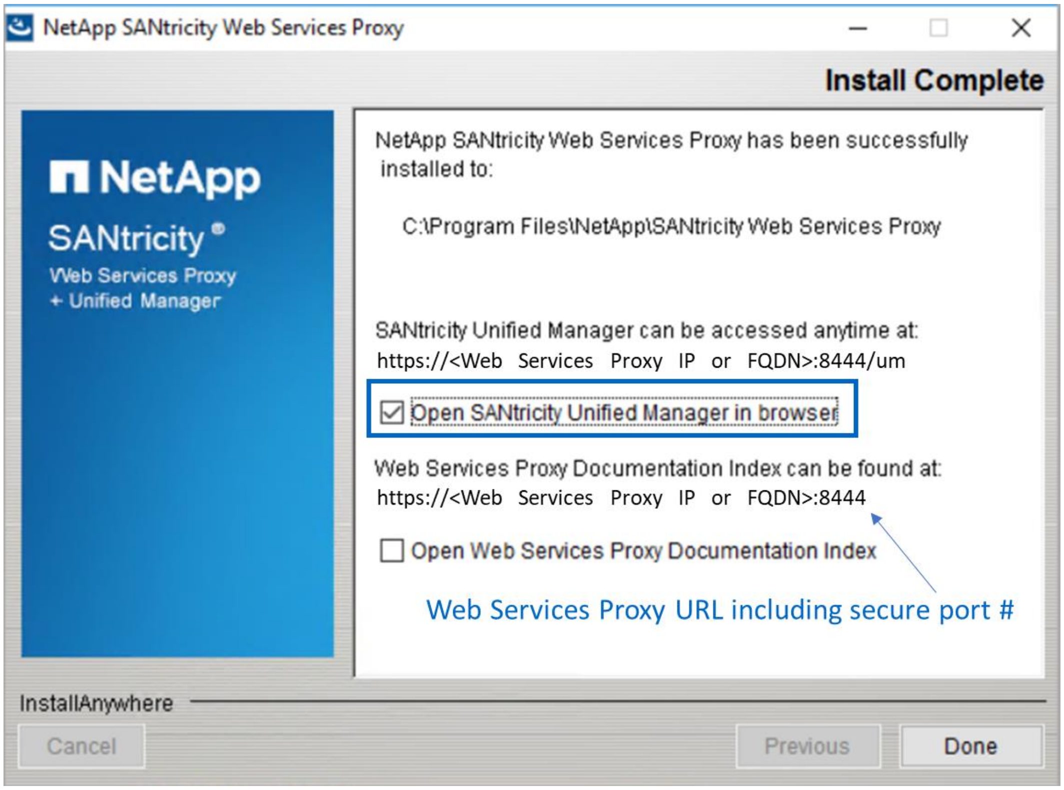
- Supports synchronous and asynchronous mirroring for all new generation arrays through the secure SSL interface. The EMW is only required if the initiator or target array is a legacy E2700, E5600/EF560, or earlier array model.

  Note: EF300 and EF600 do not support synchronous mirroring.

E-Series SANtricity Unified Manager or the E-Series SANtricity Web Services Proxy is available on the NetApp Support software download page. Either listing takes you to the combined Web Services Proxy with SANtricity Unified Manager download page.

After the installation wizard completes, you can open Unified Manager, or you can directly access the SANtricity Web Services Proxy as shown in Figure 5.

Figure 5) Final dialog box in the Web Services Proxy installation wizard.



NetApp SANtricity Web Services Proxy has been successfully installed to:

C:\Program Files\NetApp\SANtricity Web Services Proxy

SANtricity Unified Manager can be accessed anytime at:
https://<Web Services Proxy IP or FQDN>:8444/um

☑ Open SANtricity Unified Manager in browser

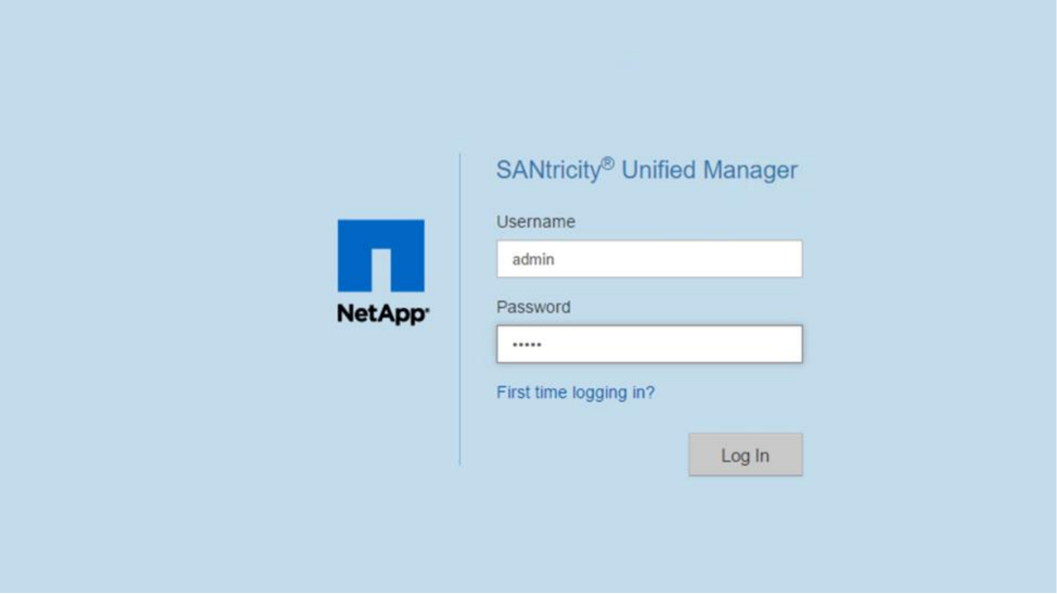
Web Services Proxy Documentation Index can be found at:
https://<Web Services Proxy IP or FQDN>:8444

□ Open Web Services Proxy Documentation Index

Web Services Proxy URL including secure port #

If you want to open the Unified Manager UI after the Web Services Proxy installation, open a browser, navigate to the server IP address and secure port number that was reserved during the Web Services Proxy software installation. For example, enter the URL in the form `https://<proxy-FQDN>:<port #>/`, and then select the link for Unified Manager. You could go directly to the Unified Manager login page (Figure 6) by adding `/um` to the URL. For example, `https://<proxy-FQDN>:<port #>/um`.

Figure 6) SANtricity Unified Manager login page.



Username: admin

Password: •••••

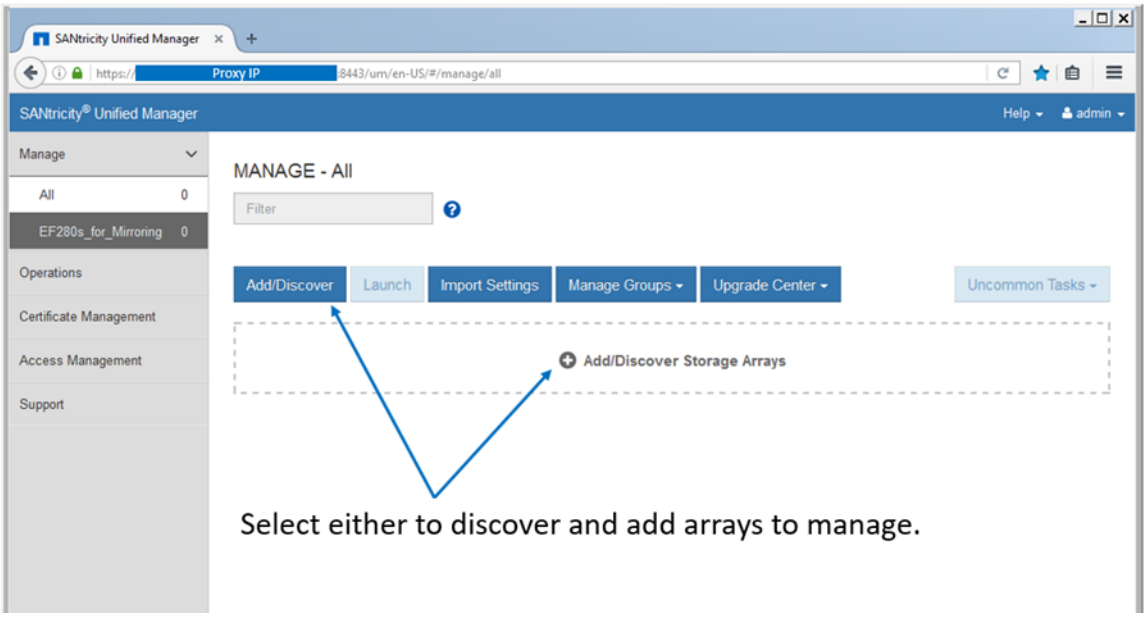
SANtricity Unified Manager navigation

The login page for SANtricity Unified Manager has a similar appearance to SANtricity System Manager and requires administrators to set the array admin password as part of the initial login. SANtricity Unified Manager has a factory default admin account: admin.

Discovering and adding storage arrays

Like the SANtricity EMW, SANtricity Unified Manager must discover arrays to manage, and, like the EMW, you can discover a single array or scan a range of IP addresses to discover multiple arrays simultaneously. Select the tab or link shown in Figure 7 to open the Add/Discover wizard. After discovering arrays, you then choose to manage them with Unified Manager.

Figure 7) SANtricity Unified Manager landing page—discover and add arrays.

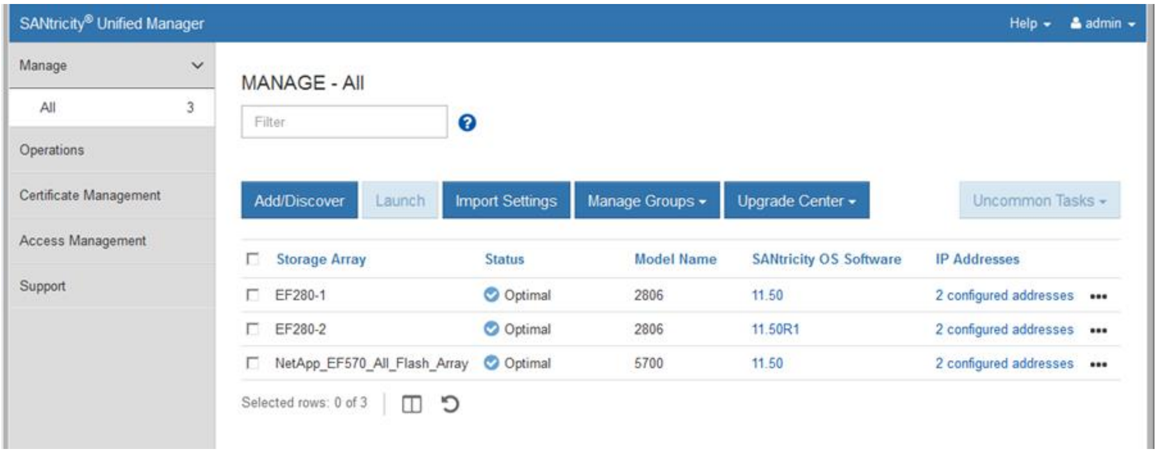


https://Proxy IP:8443/um/en-US/#/manage/all

Select either to discover and add arrays to manage.

After the arrays are discovered and added, they are displayed on the landing page of Unified Manager (Figure 8).

Figure 8) SANtricity Unified Manager landing page.

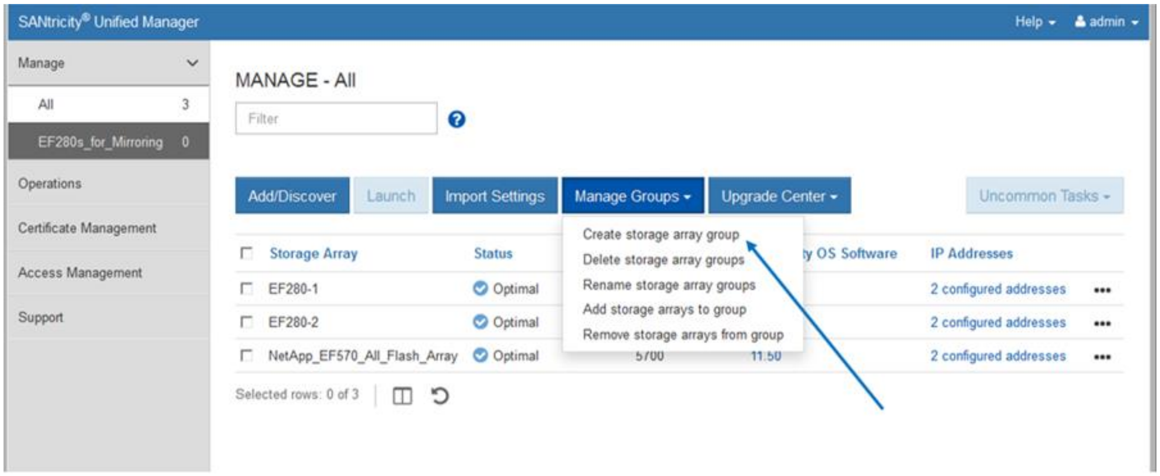


□	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses	
□	EF280-1	✓ Optimal	2806	11.50	2 configured addresses	•••
□	EF280-2	✓ Optimal	2806	11.50R1	2 configured addresses	•••
□	NetApp_EF570_All_Flash_Array	✓ Optimal	5700	11.50	2 configured addresses	•••

Organizing arrays by group

After you add arrays to Unified Manager, you can group them to organize your array management environment. Figure 9 shows EF280 arrays added to a group. This capability is available for all new generation E-Series and EF-Series arrays.

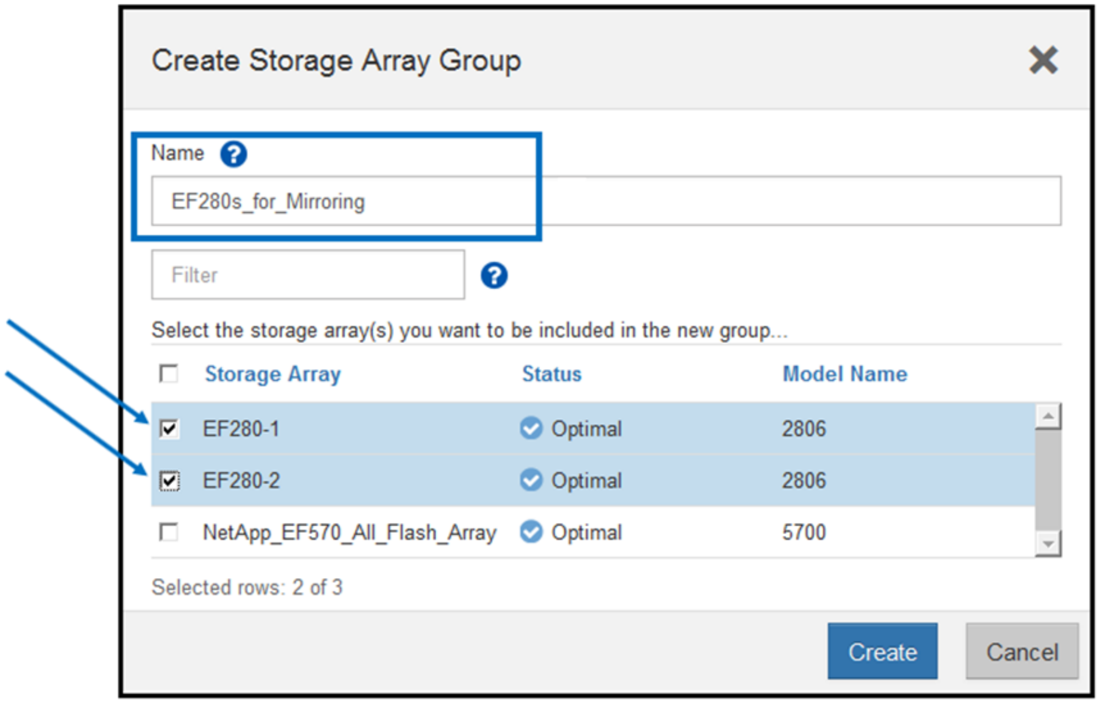
Figure 9) Creating a group to organize arrays in SANtricity Unified Manager.



□	Storage Array	Status		ty OS Software	IP Addresses	
□	EF280-1	✓ Optimal			2 configured addresses	•••
□	EF280-2	✓ Optimal			2 configured addresses	•••
□	NetApp_EF570_All_Flash_Array	✓ Optimal	5700	11.50	2 configured addresses	•••

The built-in wizard makes adding arrays to groups quick and easy, as shown in Figure 10.

Figure 10) Creating a group in Unified Manager.



Create Storage Array Group

Name: EF280s_for_Mirroring

Filter

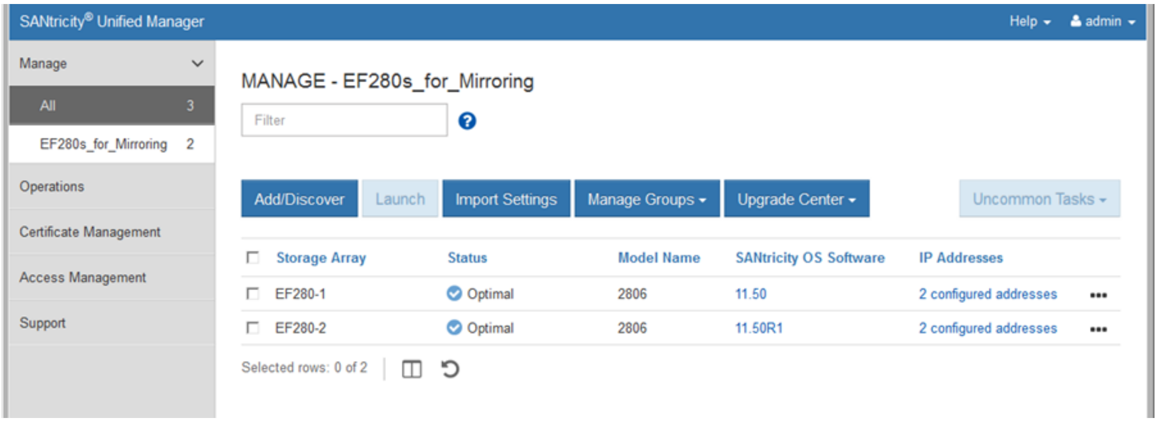
Select the storage array(s) you want to be included in the new group...

□	Storage Array	Status	Model Name
☑	EF280-1	Optimal	2806
☑	EF280-2	Optimal	2806
□	NetApp_EF570_All_Flash_Array	Optimal	5700

Selected rows: 2 of 3

SANtricity Unified Manager enables you to see just the subset of arrays in the new group, as shown in Figure 11.

Figure 11) SANtricity Unified Manager showing a newly created group.



MANAGE - EF280s_for_Mirroring

Filter

□	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses	
□	EF280-1	Optimal	2806	11.50	2 configured addresses	•••
□	EF280-2	Optimal	2806	11.50R1	2 configured addresses	•••

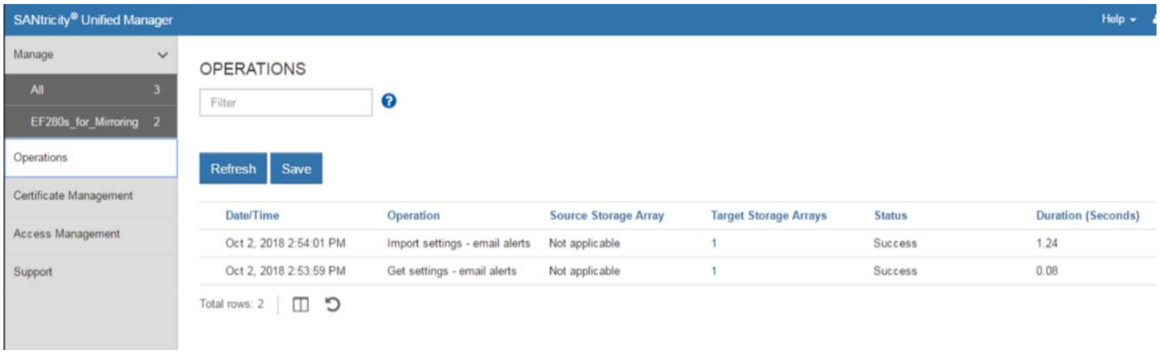
Selected rows: 0 of 2

Importing settings and viewing operations

Other features in SANtricity Unified Manager require the ability to view operations that take some time to complete. One example is importing settings from one storage array to another. This feature is especially helpful and time saving when you install a new array in an environment that already contains E-Series or EF-Series arrays running SANtricity 11.50 or later. For example, if you want the same alerting and NetApp AutoSupport® settings on all systems, use the Import Settings wizard to select the setting category, the array to copy from, and the array to import to and click Finish. The operation to copy the settings is displayed in the Operations view, as shown in Figure 12.

Note: Be careful when importing settings from another storage array, especially if you have different alerting requirements and unique storage configurations. The storage configuration option is successful only when the source and destination arrays have identical hardware configurations. The import feature does not show details about the pending import and does not prompt for confirmation. When you click Finish, you cannot stop the copy/import process.

Figure 12) SANtricity Unified Manager Operations view.



OPERATIONS

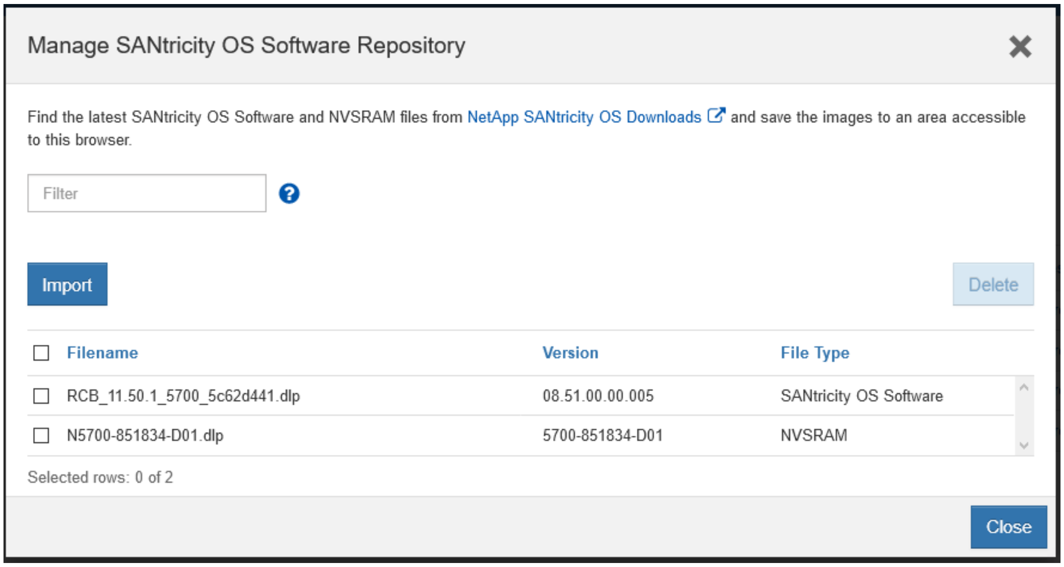
Date/Time	Operation	Source Storage Array	Target Storage Arrays	Status	Duration (Seconds)
Oct 2, 2018 2:54:01 PM	Import settings - email alerts	Not applicable	1	Success	1.24
Oct 2, 2018 2:53:59 PM	Get settings - email alerts	Not applicable	1	Success	0.08

Total rows: 2

Updating SANtricity OS through Unified Manager

To upgrade the array's firmware, complete the following steps:

1. Import the SANtricity OS software into the Unified Manager's SANtricity OS Software Repository using the Manage SANtricity OS Software Repository dialog box under Upgrade Center on the landing page.



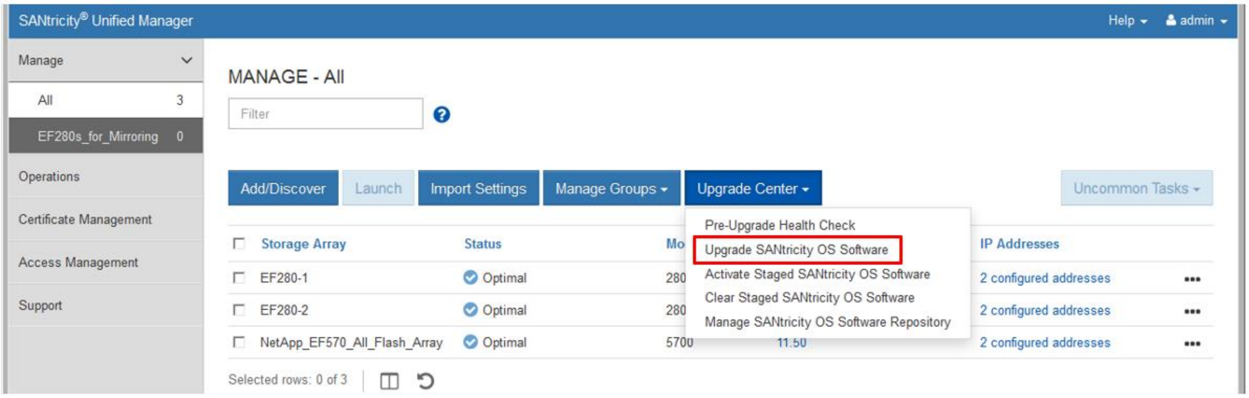
Manage SANtricity OS Software Repository

Find the latest SANtricity OS Software and NVSRAM files from NetApp SANtricity OS Downloads and save the images to an area accessible to this browser.

□	Filename	Version	File Type
□	RCB_11.50.1_5700_5c62d441.dlp	08.51.00.00.005	SANtricity OS Software
□	N5700-851834-D01.dlp	5700-851834-D01	NVSRAM

Selected rows: 0 of 2

2. On the Unified Manager landing page, click Upgrade Center and then click Upgrade SANtricity OS Software.



SANtricity® Unified Manager — Help ▾ — admin ▾

Manage
- All 3
- EF280s_for_Mirroring 0
- Operations
- Certificate Management
- Access Management
- Support

MANAGE - All

Filter

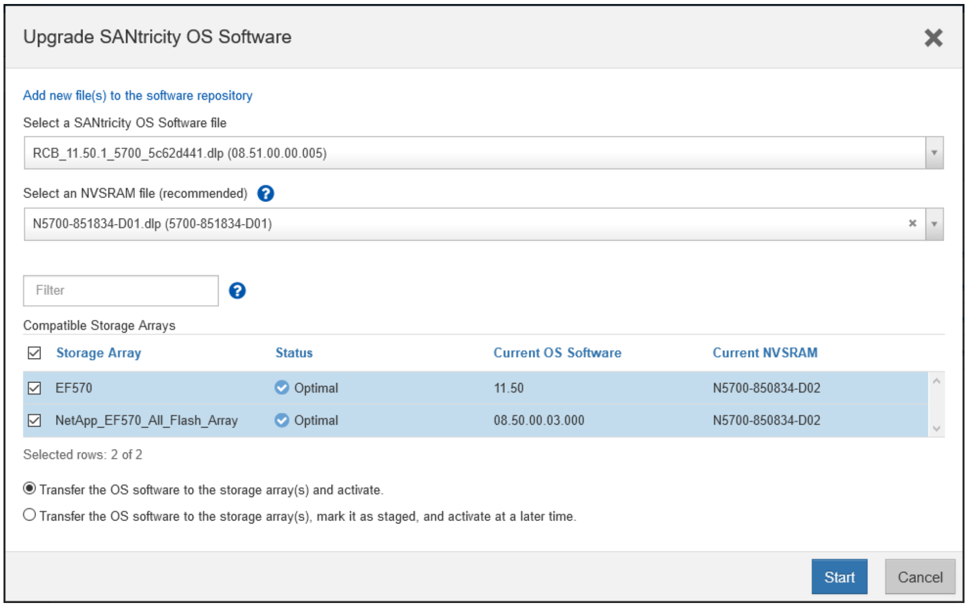
Add/Discover | Launch | Import Settings | Manage Groups ▾ | Upgrade Center ▾ | Uncommon Tasks ▾

Upgrade Center menu:
- Pre-Upgrade Health Check
- Upgrade SANtricity OS Software
- Activate Staged SANtricity OS Software
- Clear Staged SANtricity OS Software
- Manage SANtricity OS Software Repository

□	Storage Array	Status	Mo		IP Addresses	
□	EF280-1	Optimal	280		2 configured addresses	•••
□	EF280-2	Optimal	280		2 configured addresses	•••
□	NetApp_EF570_All_Flash_Array	Optimal	5700	11.50	2 configured addresses	•••

Selected rows: 0 of 3

3. On the Upgrade SANtricity OS Software page, select the following items:
   - The desired SANtricity OS and/or NVSRAM files
   - The arrays to be upgraded that are appropriate to the selected SANtricity OS files
   - Whether to transfer and activate the OS files immediately or later
4. Click Start to continue.



Upgrade SANtricity OS Software

Add new file(s) to the software repository

Select a SANtricity OS Software file: RCB_11.50.1_5700_5c62d441.dlp (08.51.00.00.005)

Select an NVSRAM file (recommended): N5700-851834-D01.dlp (5700-851834-D01)

Filter

Compatible Storage Arrays

☑	Storage Array	Status	Current OS Software	Current NVSRAM
☑	EF570	Optimal	11.50	N5700-850834-D02
☑	NetApp_EF570_All_Flash_Array	Optimal	08.50.00.03.000	N5700-850834-D02

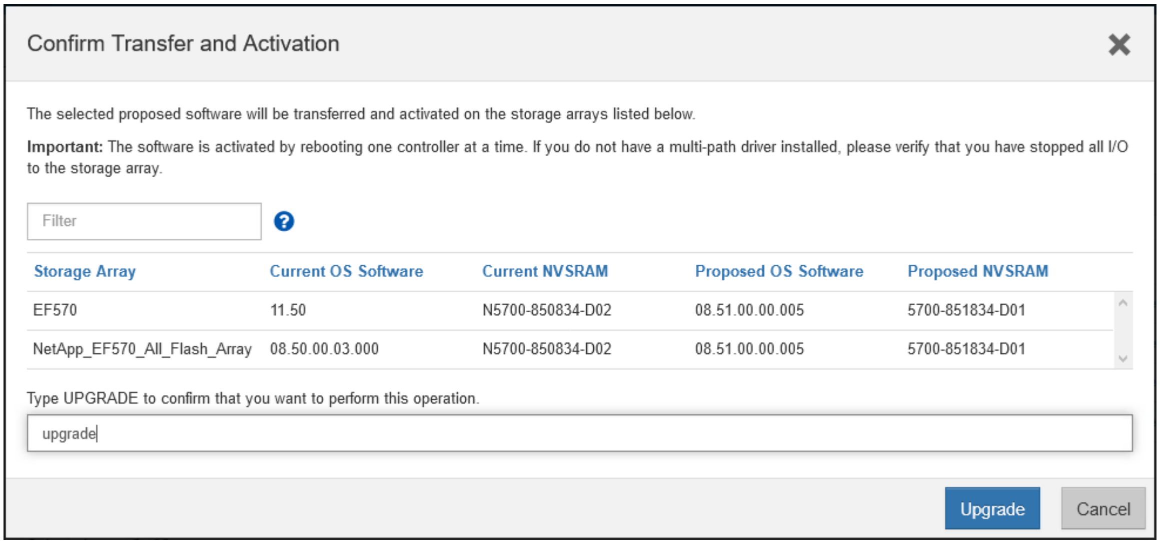
Selected rows: 2 of 2

● Transfer the OS software to the storage array(s) and activate.

○ Transfer the OS software to the storage array(s), mark it as staged, and activate at a later time.

Start | Cancel

5. On the Confirm Transfer and Activation page, enter Upgrade and then click Upgrade to begin the SANtricity OS files transfer.


Confirm Transfer and Activation

The selected proposed software will be transferred and activated on the storage arrays listed below.

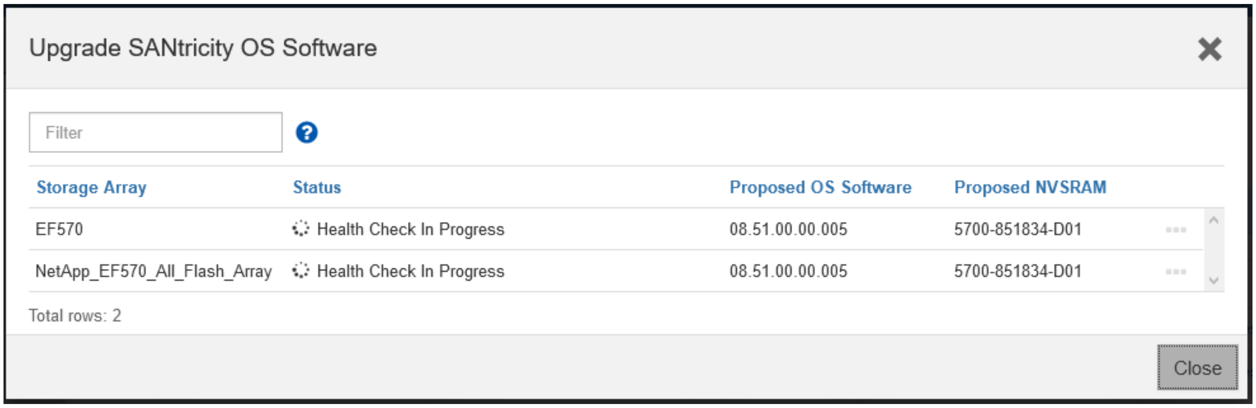
Important: The software is activated by rebooting one controller at a time. If you do not have a multi-path driver installed, please verify that you have stopped all I/O to the storage array.

Storage Array	Current OS Software	Current NVSRAM	Proposed OS Software	Proposed NVSRAM
EF570	11.50	N5700-850834-D02	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	08.50.00.03.000	N5700-850834-D02	08.51.00.00.005	5700-851834-D01

Type UPGRADE to confirm that you want to perform this operation.

upgrade

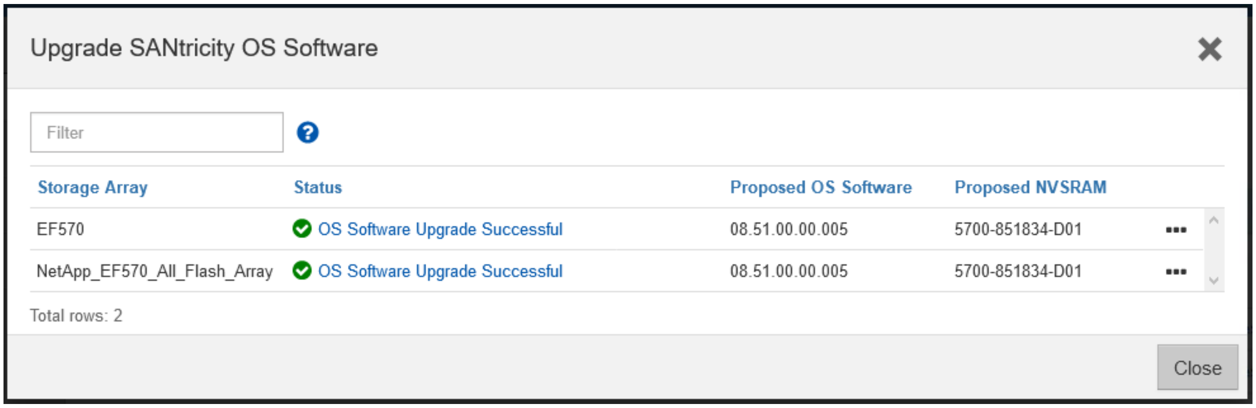
After transfer starts, the Upgrade SANtricity OS Software window is displayed. The status of the selected arrays is updated throughout the upgrade process. The first status is Health Check in Progress, followed by File Transfer in Progress, and finally Reboot in Progress.


Upgrade SANtricity OS Software

Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF570	Health Check In Progress	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	Health Check In Progress	08.51.00.00.005	5700-851834-D01

Total rows: 2

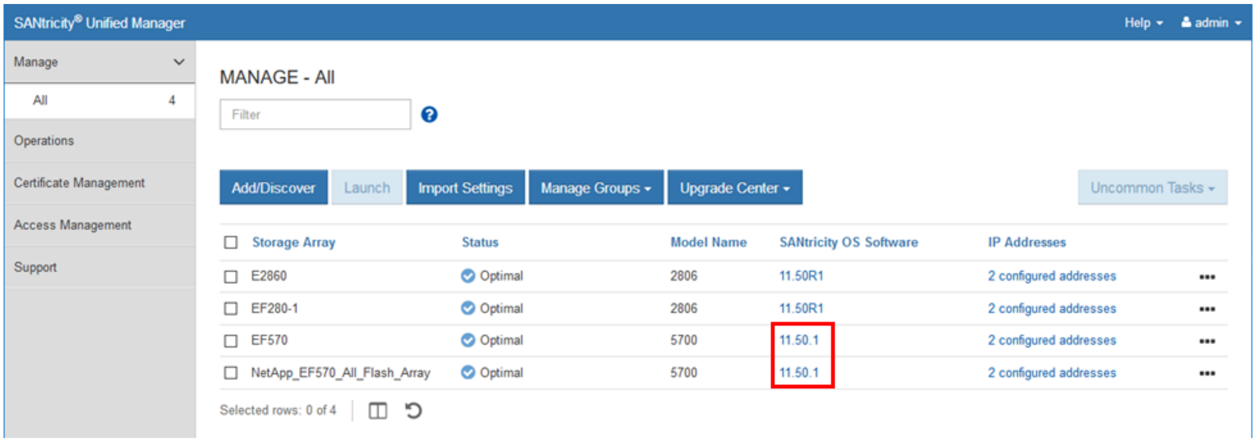
After the files have been transferred and the controllers have completed rebooting, the status changes to OS Software Upgrade Successful.


Upgrade SANtricity OS Software

Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF570	✓ OS Software Upgrade Successful	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	✓ OS Software Upgrade Successful	08.51.00.00.005	5700-851834-D01

Total rows: 2

Back on the Unified Manager landing page, the SANtricity OS Software version reflects the newly installed SANtricity OS version.



☐	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses	
☐	E2860	Optimal	2806	11.50R1	2 configured addresses	•••
☐	EF280-1	Optimal	2806	11.50R1	2 configured addresses	•••
☐	EF570	Optimal	5700	11.50.1	2 configured addresses	•••
☐	NetApp_EF570_All_Flash_Array	Optimal	5700	11.50.1	2 configured addresses	•••

SANtricity Unified Manager security

SANtricity Unified Manager supports the same secure management features as SANtricity System Manager, including LDAP, RBAC, and SSL certificates. For complete details and workflow examples, see TR-4712: NetApp SANtricity Management Security Feature Details and Configuration Guide.

Remote mirroring with SANtricity Unified Manager

With Unified Manager, you can set up remote mirroring between two new generation arrays. Starting with SANtricity 11.62, Unified Manager is used to create mirror relationships. See SANtricity Synchronous and Asynchronous Mirroring (11.62 and above) in the E-Series and SANtricity 11 Documentation Center or the Online Help in SANtricity Unified Manager for a complete description. SANtricity Unified Manager must be version 4.2 or later and SANtricity System Manager must be OS version 11.62 or later.

Note: Asynchronous mirroring is only supported on EF300 and EF600 for SANtricity OS version 11.80 or later.

Note: Drives types should be the same on source and destination. Either both NVMe drives or both non-NVMe drives. NVMe 4Kn volumes mirror only to another NVMe 4Kn volume, and 512e to 512e.

Note: EF300 and EF600 do not support synchronous mirroring.

Before SANtricity 11.62, for a description of mirroring between two new generation E-Series arrays or between a new generation E-Series array and a legacy E-Series array, see SANtricity Synchronous and Asynchronous Mirroring (11.61 and earlier).

SANtricity System Manager

Overview

SANtricity System Manager provides embedded management software, web services, event monitoring, secure CLI, and AutoSupport for E2800 arrays. Previous arrays that use the E2700 and E5600 controllers do not have this embedded functionality, or the security features introduced in SANtricity System Manager 11.40 and later versions.

E2800 storage systems are shipped preloaded with SANtricity OS, which includes SANtricity System Manager 11.60 or later. To discover E2800 storage systems running SANtricity OS from a central view, download the latest version of the Web Services Proxy, which includes the latest version of SANtricity Unified Manager.

Following are reasons to download and install the latest version of the SANtricity Web Services Proxy and Unified Manager:

- You have multiple new generation E-Series or EF-Series arrays and want the enterprise view from SANtricity Unified Manager.
- You plan to use synchronous or asynchronous remote mirroring with only new generation arrays.
- You want to use the new management features to set up and organize arrays in a more user-friendly UI.
- You want a more secure enterprise view that supports the same user and session security as SANtricity System Manager.

If you do not want to use SANtricity Unified Manager to discover and manage your E-Series arrays, you do not need to download and install the Web Services Proxy software. When customers implement E-Series with Windows and Linux operating systems, they can use the settings in the Host Utilities to properly configure each host, according to the latest Interoperability Matrix Tool (IMT) guidance. See the appropriate OS Express Guide for host setup requirements, instructions, and references. The guides are available on the E-Series and SANtricity documentation resources page.

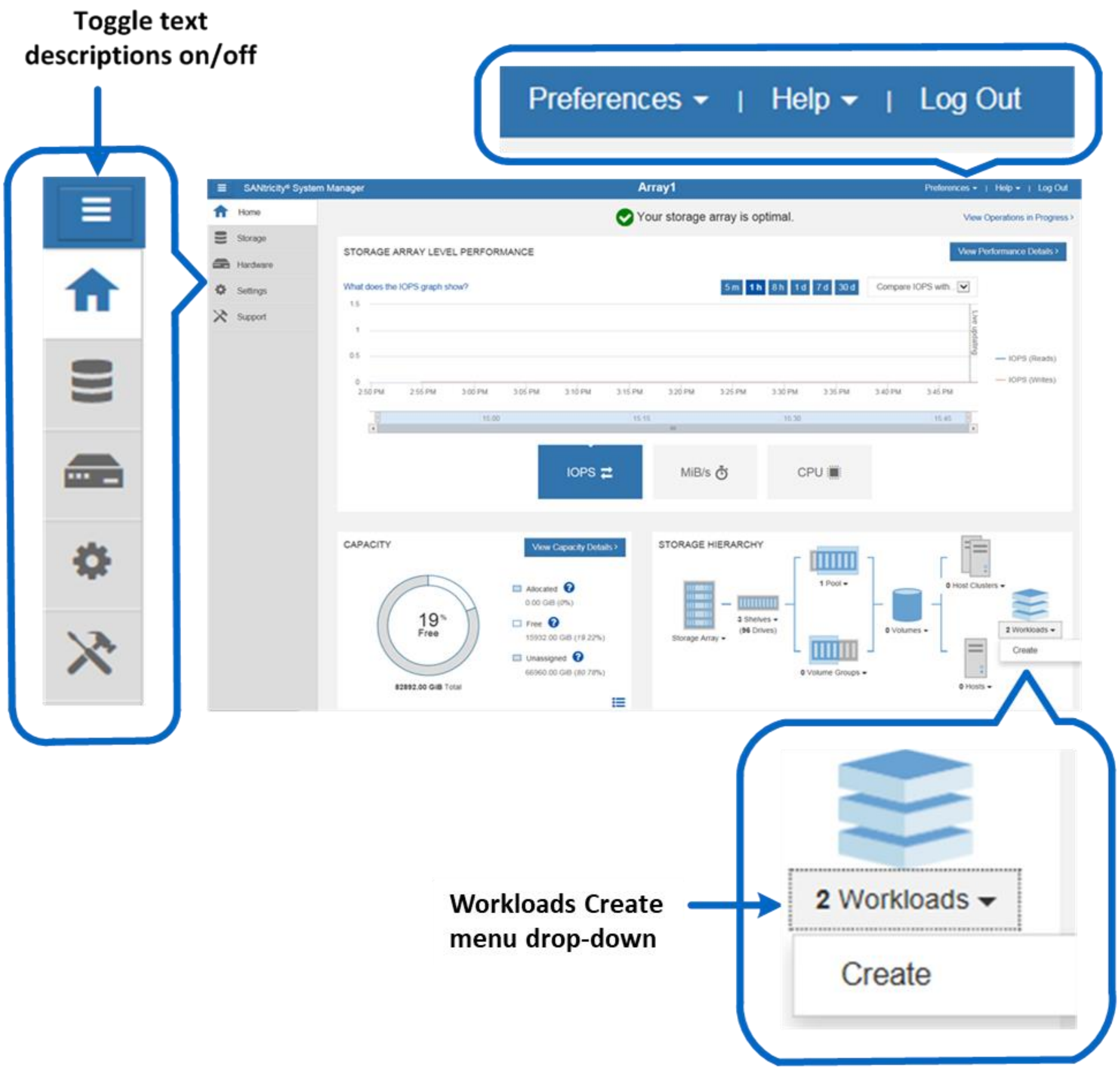
Note: Creating an account on the NetApp Support Site can take 24 hours or more for first-time customers. New customers should register for Support site access well before the initial product installation date.

System Manager navigation

After you log in to SANtricity System Manager, the home page is displayed, as shown in Figure 13. Highlighted on the bottom-right corner is a Storage Hierarchy view of your array that includes the ability to provision the storage. The icons on the left of the home page are used to navigate through the System Manager pages and are available on all pages.

- The text can be toggled on and off.
- The items on the top right of the page (Preferences, Help, Log Out) are also available from any location in System Manager.
- In the Storage Hierarchy view of your array a new feature allows the workload to be defined. This definition does not modify any storage settings.

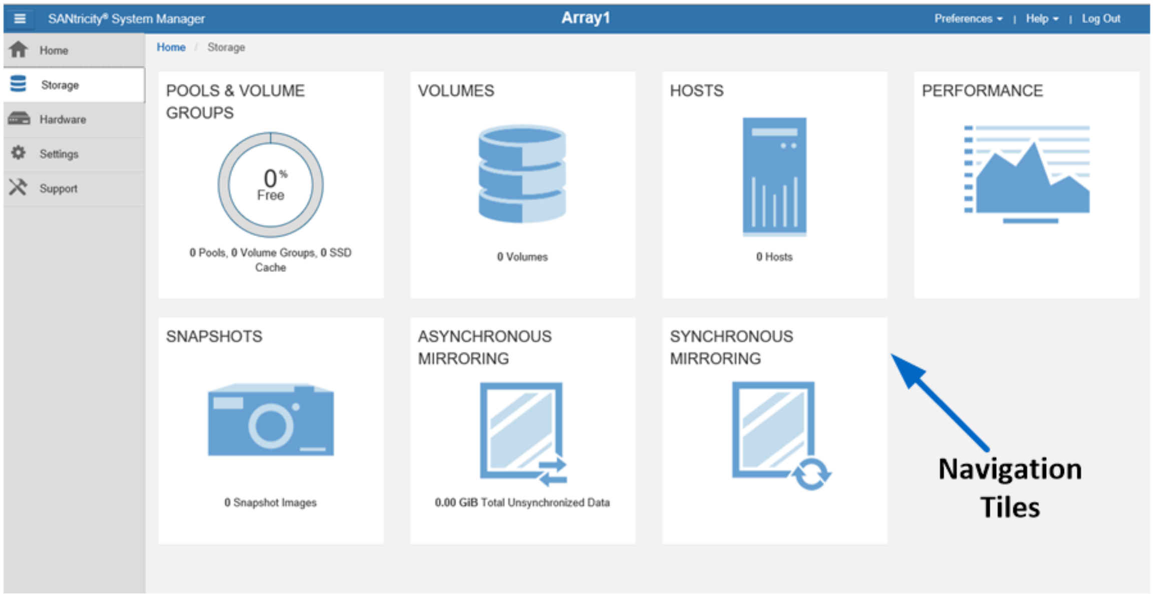
Figure 13) SANtricity System Manager home page.



Your storage array is optimal.

Figure 14, Figure 15, Figure 16, and Figure 17 show the other four main pages that are used in SANtricity System Manager and that are accessible from anywhere in the application.

Figure 14) System Manager Storage page.



Navigation Tiles

Figure 15) System Manager Hardware page.

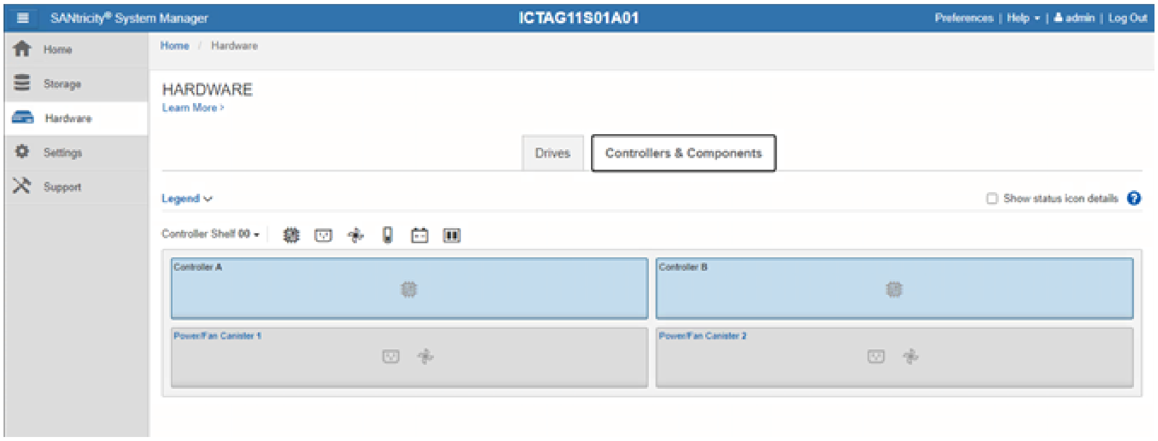
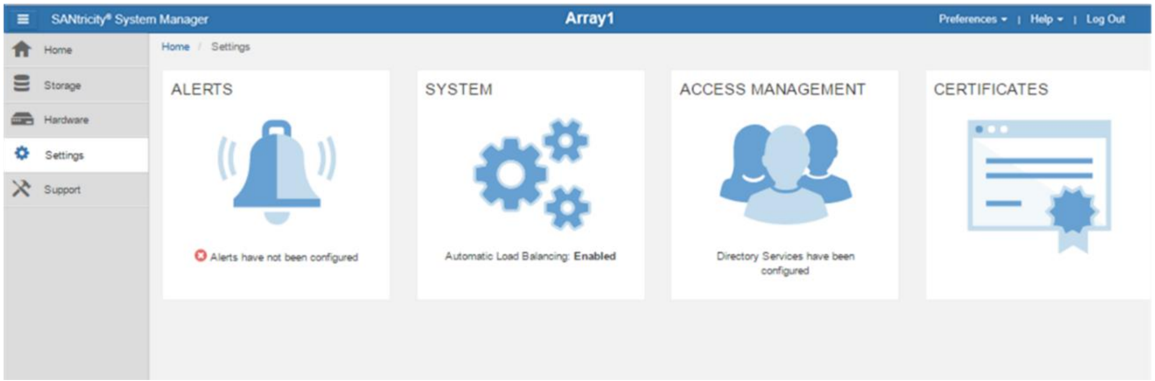


Figure 16) System Manager Settings page with new security tiles.


SANtricity® System Manager
Array1
Preferences ▾ | Help ▾ | Log Out
Home
Storage
Hardware
Settings
Support
Home / Settings
ALERTS
Alerts have not been configured
SYSTEM
Automatic Load Balancing: Enabled
ACCESS MANAGEMENT
Directory Services have been configured
CERTIFICATES

Note: Figure 16 shows the view for an administrator or security administrator. Others with a lower access permission level see only the Alerts and System tiles.

Figure 17) System Manager Support page.

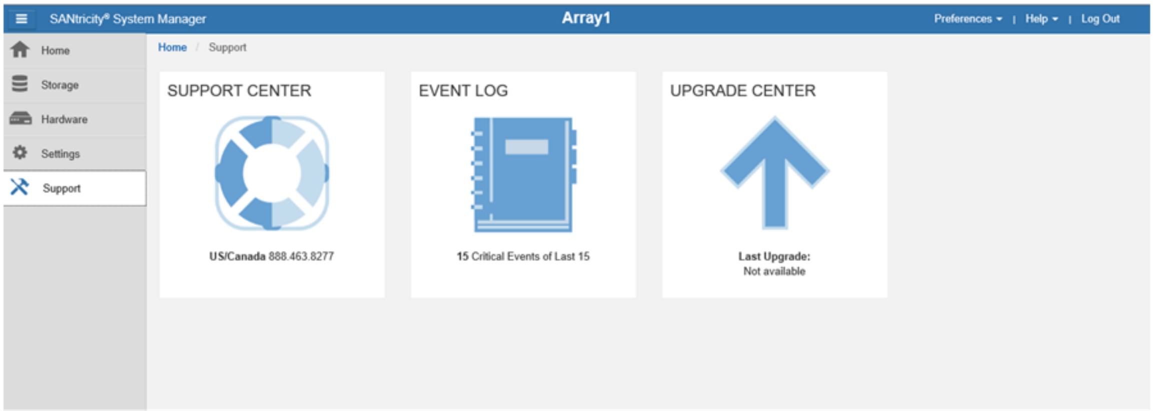
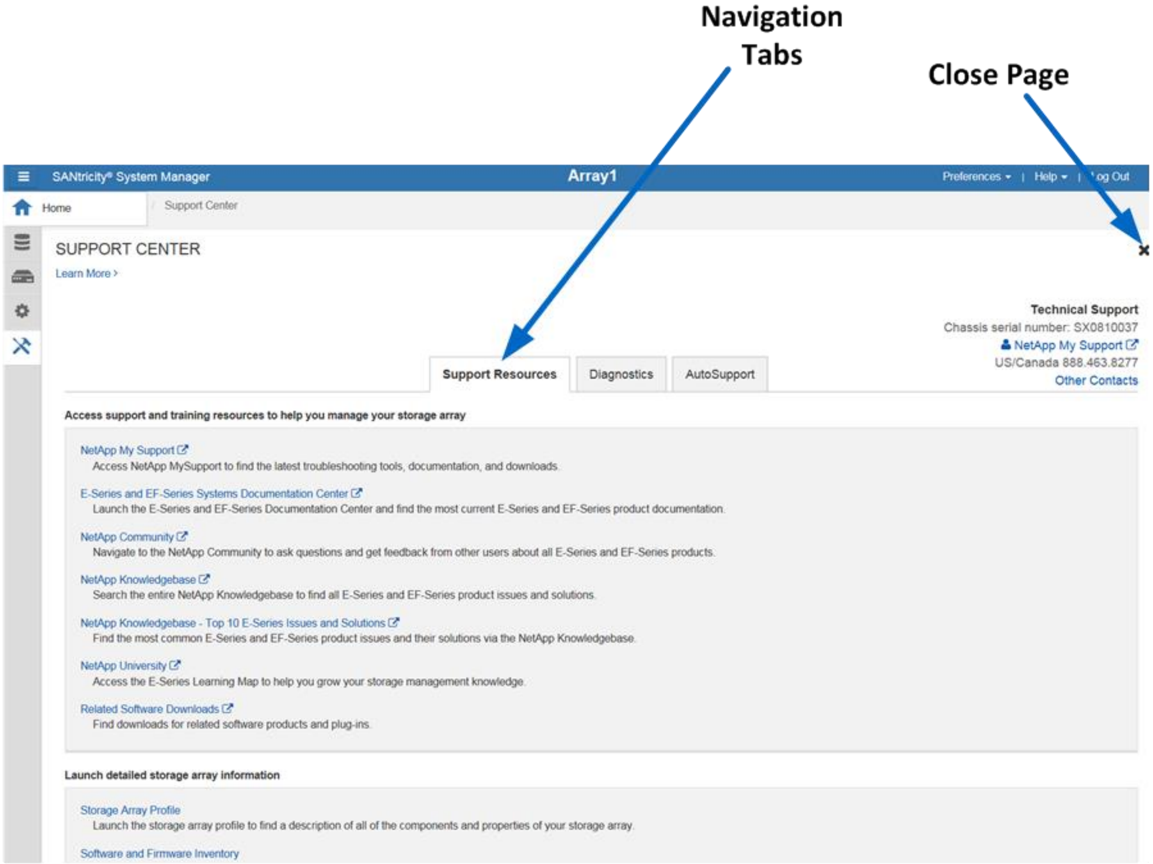


Figure 18 displays the Support Center, which you can reach by selecting the Support Center tile on the Support page. From the Support Center, use navigation tabs to reach support topics.

Figure 18) System Manager Support Center.



Access support and training resources to help you manage your storage array

NetApp My Support
Access NetApp MySupport to find the latest troubleshooting tools, documentation, and downloads.

E-Series and EF-Series Systems Documentation Center
Launch the E-Series and EF-Series Documentation Center and find the most current E-Series and EF-Series product documentation.

NetApp Community
Navigate to the NetApp Community to ask questions and get feedback from other users about all E-Series and EF-Series products.

NetApp Knowledgebase
Search the entire NetApp Knowledgebase to find all E-Series and EF-Series product issues and solutions.

NetApp Knowledgebase - Top 10 E-Series Issues and Solutions
Find the most common E-Series and EF-Series product issues and their solutions via the NetApp Knowledgebase.

NetApp University
Access the E-Series Learning Map to help you grow your storage management knowledge.

Related Software Downloads
Find downloads for related software products and plug-ins.

Launch detailed storage array information

Storage Array Profile
Launch the storage array profile to find a description of all of the components and properties of your storage array.

Software and Firmware Inventory

SANtricity System Manager security

SANtricity System Manager supports multiple levels of management interface security including:

- Support for directory services using LDAP.
- Support for RBAC: five standard roles with varying permission levels.
- Support for certification authority (CA) and SSL certificates.
- Implementation of a secure CLI. The CLI is secure when the certificates are installed. Syntax and invocation are the same as in the legacy CLI, but additional security parameters are supplied.
- Security enhancements that extend to the onboard web services API, where user account passwords are now required.

  Note: If you want to run in the previous security mode with a single administrative password and still use symbols to communicate through the legacy API, the new security features can be disabled by the admin or security users.

LDAP and RBAC

LDAP is a commonly used communication protocol that enables directory servers such as Microsoft Active Directory to provide centralized identity control over user and group definitions.

RBAC is software on the E-Series array that defines standard user levels, each with a well-defined set of access permissions. By authenticating a user as a member of a group and setting group permissions on the array side, SANtricity 11.40 and later versions provide the granularity of access that customers require.

Table 3 defines the permission level with each role.

Table 3) Built-in roles and associated permissions.

Role name (login as)	Access permissions
Root Admin (admin)	This role allows you to change the passwords of any local users and execute any command supported by the array. The admin password is set at initial login or any time after.
Security Admin (security)	This role allows you to modify security configuration settings on the array. It allows you to view audit logs; configure secure syslog server, LDAP, or LDAPS server connections; and manage certificates. This role provides read access but does not provide write access to storage array properties such as pool or volume creation or deletion. This role also has privileges to enable or disable SYMbol access to the array.
Storage Admin (storage)	This role allows full read and write access to the storage array properties and maintenance/diagnostics functions. However, it does not include access to perform any security configuration functions.
Support Admin (support)	This role provides access to all hardware resources on the array, failure data, the MEL/Audit log, and CFW upgrades. You can view the storage configuration but cannot change it.
Monitor (monitor)	This role provides read-only access to all storage array properties. However, you are not able to view the security configuration.

Setting up the directory server and roles

Directory servers, like most data center devices, are complex and designed to fulfill many use cases. However, the E-Series LDAP/RBAC implementation focuses on authentication and two main elements: users and groups. As with most applications, you must understand a few acronyms and follow a few conventions to set up communication between the E-Series array and the directory server. The most critical acronyms to understand are the following:

- **CN**. Stands for commonName, used to identify group names as defined by the directory server tree structure.
- **DC**. Stands for domainComponent, the network in which user and groups exist (for example, netapp.com).
- **DN**. Stands for distinguishedName, the fully qualified domain name made up of one or more comma-separate common names, followed by one or more comma-separated DCs (for example, `CN=functional_group_name,CN=Users,DC=netapp,DC=com`).

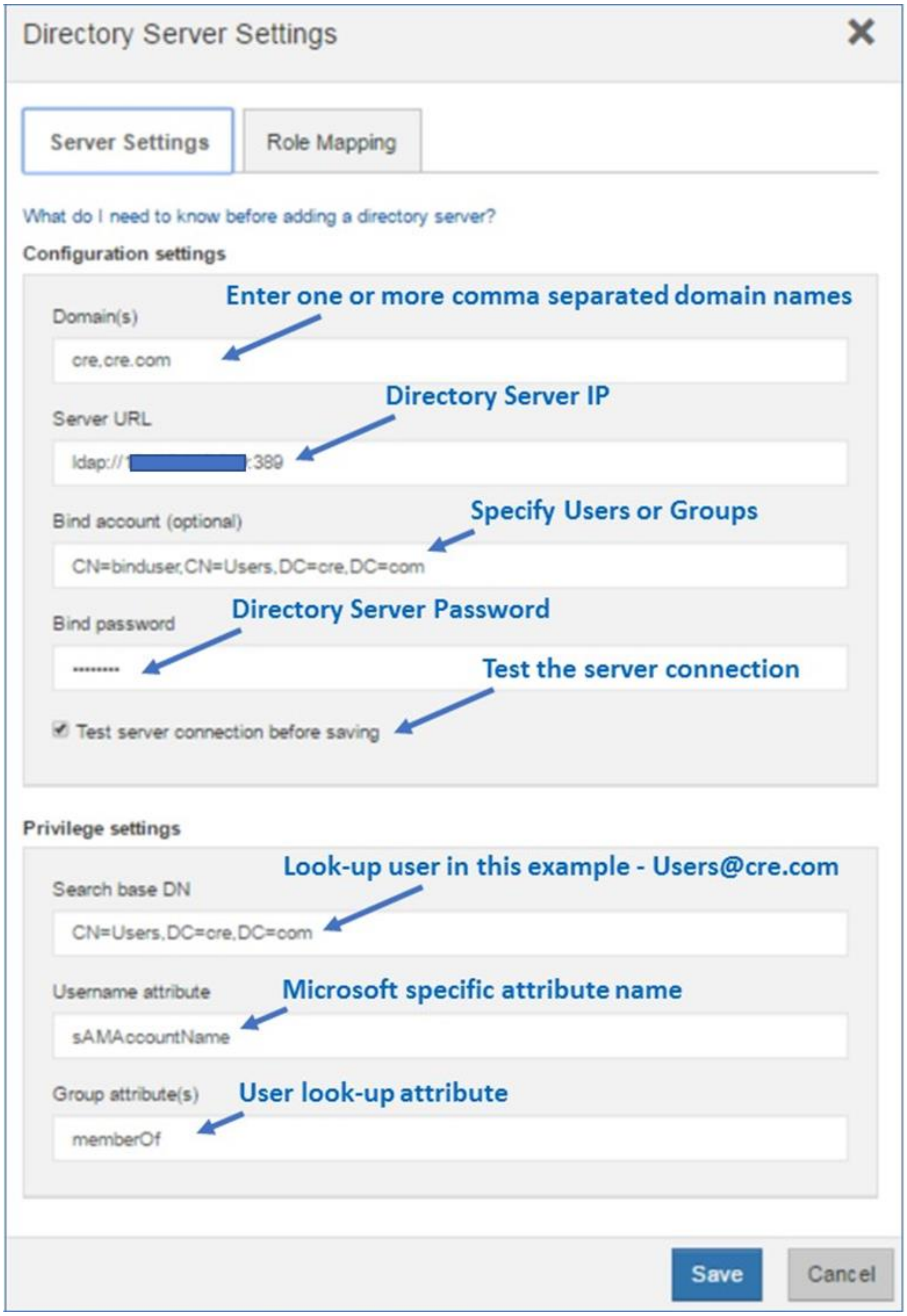
E-Series systems follow a standard web server implementation on the controllers, and information about the general directory services setup is available on the web. As a result, setting up the service on E-Series systems only requires some fields, which are listed in Table 4.

Table 4) LDAP/RBAC required fields and definitions.

Field name	Definitions
Domain (for example, netapp.com)	Network domains defined in the directory server of which users accessing the storage array are members.
Server URL	Can be a fully qualified domain name or IP and port number in the format `ldap://<IP:port_number>` (port 389 or port 636 for LDAPS).
Bind account	Format is `CN=binduser,CN=Users,DC=<some_name>,DC=com`.
Bind account password	Password for bind account user.
Search base DN	Format is `CN=Users,DC=<some_name>,DC=com`.
Username attribute	The LDAP attribute that defines the username. Example: `sAMAccountName` is a standard entry for legacy Windows-based browsers, including Windows 95, Windows 98, and Windows XP. Linux can have other designations.
Group attributes	The LDAP attribute that defines the groups to which a user belongs. Example: `memberOf` is a standard attribute.

Figure 19 shows a sample Active Directory server integration with SANtricity System Manager. The entries are all examples except for username attributes and group attributes in the privileges section. Those items are standard entries for Windows and are not likely to change for most implementations.

Figure 19) SANtricity System Manager directory server setup wizard.



Directory Server Settings

Configuration settings

Domain(s): cre.cre.com

Enter one or more comma separated domain names

Server URL: ldap://1[redacted]:389

Directory Server IP

Bind account (optional): CN=binduser,CN=Users,DC=cre,DC=com

Specify Users or Groups

Bind password: ••••••••

Directory Server Password

☑ Test server connection before saving

Test the server connection

Privilege settings

Search base DN: CN=Users,DC=cre,DC=com

Look-up user in this example - Users@cre.com

Username attribute: sAMAccountName

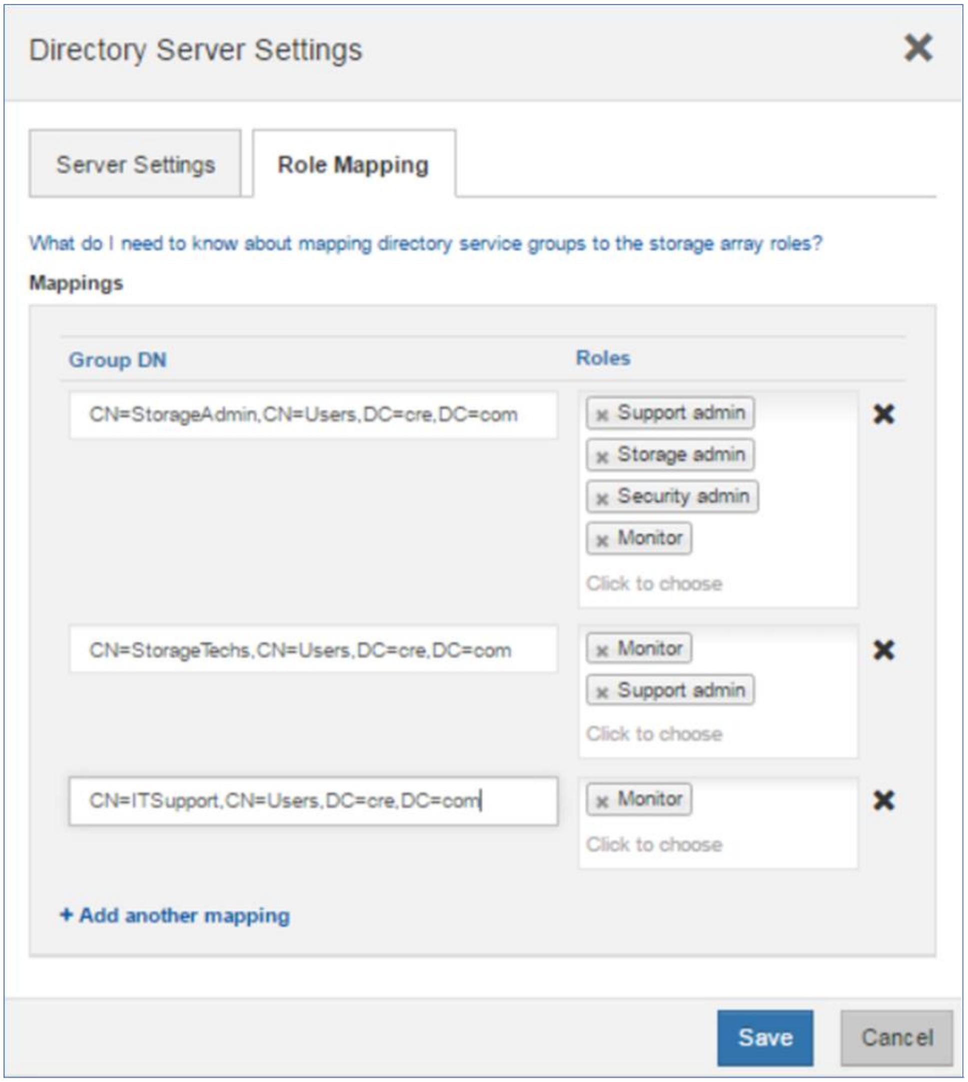
Microsoft specific attribute name

Group attribute(s): memberOf

User look-up attribute

The array roles for the specified user groups are set in the Role Mapping tab. In Figure 20, users who are members of the StorageAdmin, StorageTechs, and ITSupport groups are authenticated as branches of the Users group `@cre.com`. When users in one of those groups log in to the array, they are allowed access to certain views and functions in the management interface according to the permissions granted.

Figure 20) Role Mapping tab in the directory server settings wizard.


Directory Server Settings
Server Settings
Role Mapping
What do I need to know about mapping directory service groups to the storage array roles?
Mappings
Click to choose
+ Add another mapping
Save
Cancel

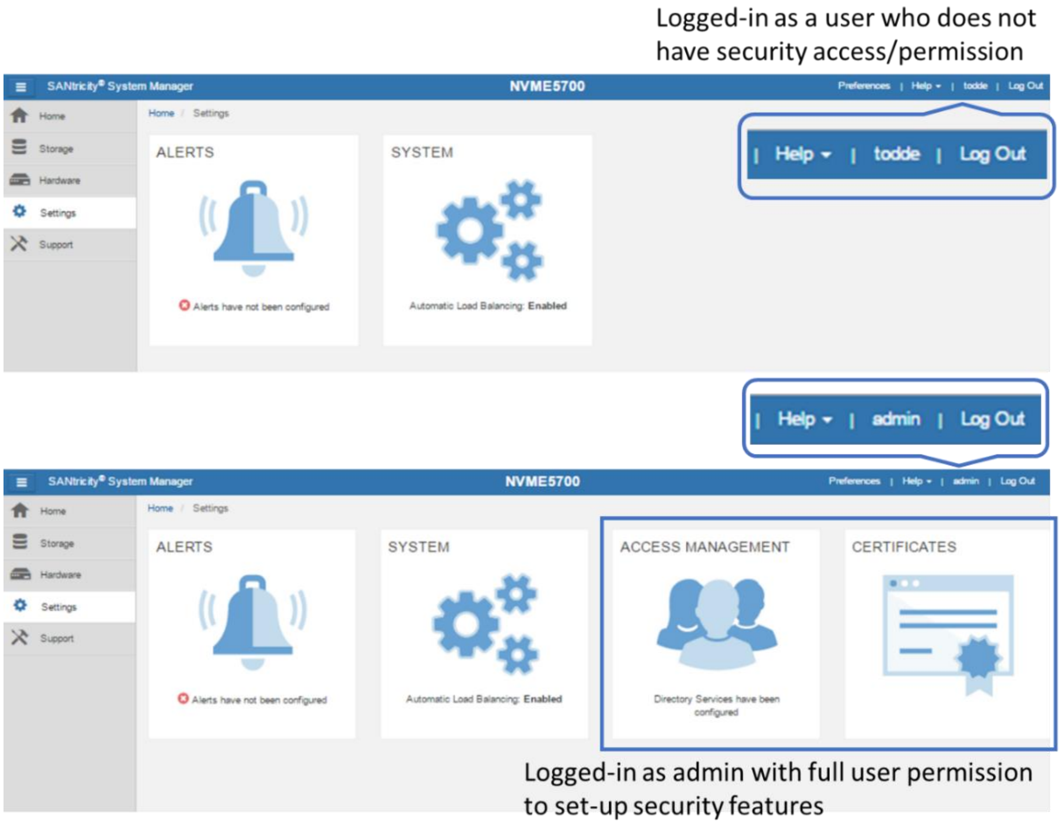
Group DN	Roles
CN=StorageAdmin,CN=Users,DC=cre,DC=com	Support admin Storage admin Security admin Monitor
CN=StorageTechs,CN=Users,DC=cre,DC=com	Monitor Support admin
CN=ITSupport,CN=Users,DC=cre,DC=com	Monitor

Note: The monitor role is automatically added to all group DNs. Without monitor permission, users in the associated mapped group are not able to log in to the array.

Multiple groups can be defined and mapped to specific roles that meet individual business requirements. Figure 21 shows the difference in user views and access to features according to the access permission level.

The top half of the figure shows the view after you log in without security access or permission. With this login, you can monitor and access support, but it does not provide the security access of the second group mapping in Figure 21.

Figure 21) SANtricity System Manager views change based on user permission level.



Logged-in as a user who does not have security access/permission

SANtricity® System Manager
NVME5700
Preferences | Help ▾ | todde | Log Out
Home
Storage
Hardware
Settings
Support
Home / Settings
ALERTS
SYSTEM
| Help ▾ | todde | Log Out
| Help ▾ | admin | Log Out
SANtricity® System Manager
NVME5700
Preferences | Help ▾ | admin | Log Out
ACCESS MANAGEMENT
CERTIFICATES

Alerts have not been configured

Automatic Load Balancing: Enabled

Directory Services have been configured

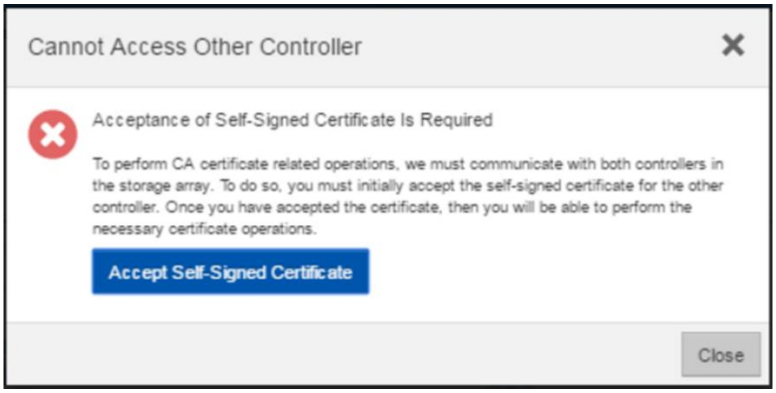
Logged-in as admin with full user permission to set-up security features

SANtricity web server security certificates

In addition to authentication and access control, SANtricity System Manager supports standard CA certificates. This support enables secure communications (SSL/TLS) between browser clients and the E-Series built-in web servers on the controllers. On E2800 arrays, the SANtricity System Manager UI is accessed through one of the two controllers. (In the legacy SANtricity Storage Manager application, access was through both controllers simultaneously.) As a result, all communication to the other controller in the E2800 array is done through the midplane in the shelf.

Because you can log in to either of the controllers through the web browser, both controllers must run a web server instance. For proper communication, both controllers must present a self-signed certificate to each other. This process happens automatically when the admin or security user logs in to each controller and opens the Certificates tile. Figure 22 shows the dialog box that is displayed the first time the tile is opened.

Figure 22) Initial step required to set up web server certificates.



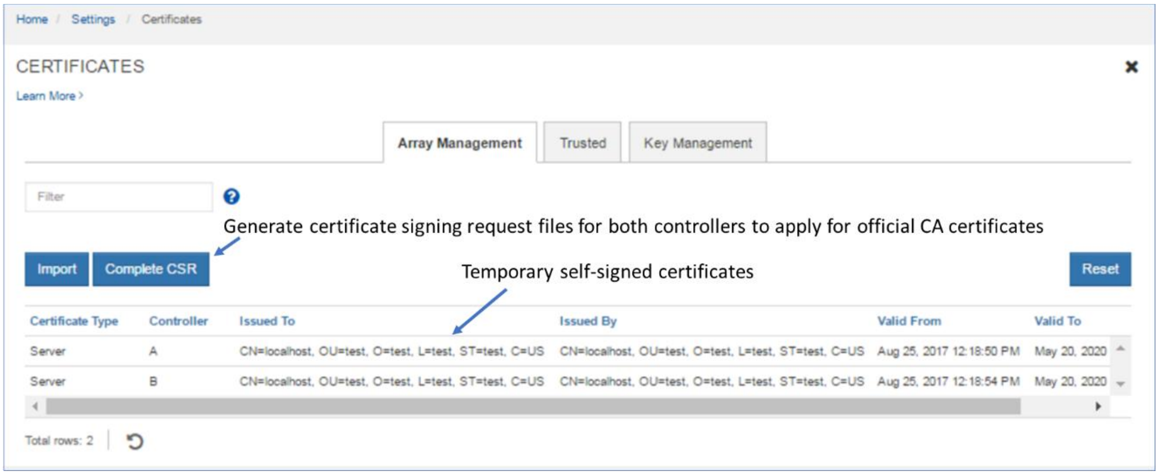
Cannot Access Other Controller

Acceptance of Self-Signed Certificate Is Required

To perform CA certificate related operations, we must communicate with both controllers in the storage array. To do so, you must initially accept the self-signed certificate for the other controller. Once you have accepted the certificate, then you will be able to perform the necessary certificate operations.

You must accept the self-signed certificate to continue setting up certificates. The process takes you to another webpage where the certificate is created in the background. Follow the prompts to complete the process. When the process is complete, the array requires the admin user or a user with security permissions to log in again. Both controllers are then displayed with valid local host certificates, as shown in Figure 23.

Figure 23) SANtricity System Manager Certificates tile expanded.



Home / Settings / Certificates
CERTIFICATES
Learn More ›
Array Management
Trusted
Key Management
Filter
Generate certificate signing request files for both controllers to apply for official CA certificates
Import
Complete CSR
Temporary self-signed certificates
Reset

Certificate Type	Controller	Issued To	Issued By	Valid From	Valid To
Server	A	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	Aug 25, 2017 12:18:50 PM	May 20, 2020
Server	B	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	CN=localhost, OU=test, O=test, L=test, ST=test, C=US	Aug 25, 2017 12:18:54 PM	May 20, 2020

Total rows: 2

To enable the E-Series onboard web servers to validate certificates from external client browsers, the controllers are preloaded with industry-standard CA root certificates. To view a list of factory-installed CA root and intermediate certificates, select the Trusted tab in the Certificates tile window shown in Figure 23 and then select Show Preinstalled Certificates from the drop-down menu.

For complete details and procedures to manage certificates for SANtricity System Manager and SANtricity Unified Manager, see [TR-4712: NetApp SANtricity Management Security Feature Details and Configuration Guide](#).

Multifactor authentication

Feature overview

Multifactor authentication (MFA) includes several new functional areas on E2800 arrays:

- **Authentication with Security Assertion Markup Language (SAML) 2.0 to support MFA**. You can manage authentication through an identity provider (IdP) by using SAML 2.0. An administrator establishes communication between the IdP system and the storage array and then maps IdP users to the local user roles embedded in the storage array. Using IdP allows the administrator to configure MFA.

- **Digitally signed firmware**. The controller firmware verifies the authenticity of any downloadable SANtricity firmware. Digitally signed firmware is required in controller firmware version 8.42 (SANtricity 11.40.2) and later. If you attempt to download unsigned firmware during the controller upgrade process, an error is displayed, and the download is aborted.
- **Certificate revocation checking using Online Certificate Status Protocol (OCSP)**. Certificate management includes certificate revocation checking through an OCSP server. The OCSP server determines whether the certificate authority (CA) has revoked any certificates before the scheduled expiration date. The OCSP server then blocks the user from accessing a server if the certificate is revoked. Revocation checking is performed whenever the storage array connects to an AutoSupport server, external key management server, LDAP over SSL (LDAPS) server, or syslog server. Configuration tasks are available from Settings > Certificates and require security admin permissions.
- **Syslog server configuration for audit log archiving**. In access management, you can configure a syslog server to archive audit logs. After configuration, all new audit logs are sent to the syslog server; however, previous logs are not transferred. Configuration tasks are available from Settings > Access Management and require security admin permissions.

How MFA works

MFA is provided through the industry standard SAML protocol. SAML does not directly provide the MFA functionality; instead, it allows the web service to send a request to an external system. The external system requests credentials from the user and verifies those credentials. Information about the authenticated user is then returned to the web service to allow the user to be assigned appropriate roles. With the previous E-Series authentication methods, the web service was responsible for requesting the user credentials and authenticating the user. With SAML, an external system provides all authentication activity. The external system can be configured to require any amount and types of user authentication factors.

SAML identifies two types of systems that cooperate to provide authentication of users:

- **Identity provider**. The identity provider (IdP) is the external system that does the actual authentication of users by requesting the user credentials and verifying their validity. Maintenance and configuration of the IdP is your responsibility.
- **Service provider**. The service provider (SP) is the system that sends a request to the IdP to have a user authenticated. For E-Series storage arrays, the controllers are the service providers; each controller is a separate SP.

Using SAML to provide MFA also enables single sign-on (SSO) capabilities. If multiple applications are configured to use the same IdP, SSO enables them to accept the same user credentials without requiring users to reenter them. The SSO feature is available only if the user is accessing these applications with the same browser.

Note that when SAML is enabled, SANtricity System Manager is the only management access point. There is therefore no access through the SANtricity CLI, the SANtricity Web Services REST API, in-band management (I/O path that uses a host agent), or native SYMbol interface. The lack of SYMbol access means that you cannot use the Storage Manager EMW or other SYMbol-based tools such as the NetApp Storage Management Initiative Specification (SMI-S) provider.

For more information about MFA, see the E-Series online help center and the E-Series and SANtricity 11 Documentation Center. For detailed explanations about the full set of SANtricity management security features and settings, see TR-4712: NetApp SANtricity Management Security Feature Details and Configuration Guide.

SANtricity storage features

SANtricity offers several layers of storage features ranging from security for data at rest, features that manage host paths, features to manage large-capacity drives that ensure data integrity and efficiently manage drive faults, and features that provide data protection. The following sections describe many of the features and provide links to additional information resources.

Drive encryption

When external key management is enabled from the Settings tile, use the Key Management tab to generate a CSR file. Use the CSR file on the key management server to generate a client certificate. Import the client certificate from the Key Management tab to enable secure communication between the E-Series controllers and the external key management server. For more information about the SANtricity drive security feature, see the E-Series online help center and TR-4474: SANtricity drive security.

SANtricity host and path management features

When considering the elements of E-Series multipath functionality, you must understand two concepts. The first is controller-to-volume ownership and how path failover between controllers is managed through asymmetrical logical unit access (ALUA). This scenario occurs when the primary paths to an E-Series volume (I/O paths through the owning controller) are lost. The second concept concerns how the multipath driver on the host interacts with multiple ports on each E-Series controller (target port group support, or TPGS) to spread I/O across the interfaces and maximize performance. This section provides a brief explanation of each concept. For a deep explanation of E-Series multipath behavior, see TR-4604: Clustered File Systems with E-Series Products: BPG for Media.

The design of the E-Series multipath behavior has evolved from a host multipath driver-managed scenario (explicit failover) to the new E-Series-led path management model (implicit failover). However, the E-Series fundamentals have not changed. For example, E-Series systems have asymmetric dual active controllers for which:

- Volume ownership alternates as volumes are provisioned.
- Write I/O is mirrored to the peer controller.
- Both controllers have access to every volume on the array.
- Both controllers have multiple host ports.
- If one E-Series controller fails, the other controller takes control of all the LUNs and continues to process I/O.

These attributes allow host multipath drivers to spread I/O across ports on each controller that are associated to the volumes owned by that controller (TPGS). The drivers use path policies such as least queue depth and round robin. Depending on the host operating system, the default path policy is one of these two methods.

When all the paths from a host to one E-Series controller are lost, I/O from that host to the volumes owned by that controller is routed to ports on the other E-Series controller, which performs “I/O shipping” across the shelf midplane to the controller that owns the volumes. In parallel, an ALUA timer is set, and changes in controller-to-volume ownership are delayed until the timer expires. This delay time is long enough for links to reset and return to service (the default is 5 minutes). After the timer expires, the array decides whether to initiate a change of volume ownership to the peer controller. The decision is based on whether the non-owning controller is still receiving more than 75% of the I/O.

Table 5 provides a list of SANtricity host types and the associated support for implicit failover/failback.

Table 5) SANtricity common host types and associated failover behavior.

Host type	ALUA/AVT status	Implicit failover	Implicit failback	Automatic load balance
Linux DM-Multipath (kernel 3.10 or later)	Enabled	Supported	Supported	Supported
VMware	Enabled	Supported	Supported	Supported
Windows (clustered or non-clustered)	Enabled	Supported	Supported	Supported
ATTO cluster (all operating systems)	Enabled	Supported	Not supported	Not supported

Note: Several uncommon host types also exist as well as host types that are only to be used if instructed to by support. Appearance on the host type list does not imply the option is fully supported; for more information, refer to the NetApp Interoperability Matrix Tool (IMT) as well as the SANtricity online help.

SANtricity reliability features

Table 6 provides a list of SANtricity reliability features and a brief explanation of each with references to additional information.

Table 6) SANtricity features for long-term reliability.

Reliability features with SANtricity
Media scan with redundancy check. A background scan of media that is run on a set schedule and detects data integrity issues. This feature is critically important to turn on by default when you provision new volumes. **Note:** If you have been running I/O to an array with media scan turned off, consult with NetApp Technical Support before you turn it on.
Data assurance (T10 PI). Confirms data integrity from the HIC to the drive (end-to-end in the storage array). This data integrity is especially important with large-capacity drives.
Cache mirroring. Each E-Series controller owns a set of LUNs and is responsible for processing I/O to and from those LUNs. Both controllers have access to all LUNs, and by default, all incoming writes are cached in memory on the peer controller. This mechanism enables a second level of data integrity checking and enables E-Series and EF-Series arrays to handle controller failover scenarios gracefully.
Nondisruptive controller firmware upgrade. Using the ALUA host type with multiple paths to hosts and an upgrade wizard that activates one controller at a time, this feature prevents upgrades from affecting host-to-LUN access. **Note:** Most host OSs support the ALUA host type; however, you must verify that you are using ALUA-capable host types before executing an in-service upgrade.
Proactive drive monitor and data evacuator. Nonresponsive drives are automatically power cycled to see if the fault condition can be cleared. If the condition cannot be cleared, then the drive is flagged as failed. For predictive failure events, the evacuator feature starts to remove data from the affected drive to move the data before the drive fails. If the drive fails, rebuild resumes where the evacuator was disrupted, reducing the rebuild time.
Automatic drive fault detection. Failover and rebuild by using global hot spare drives for standard RAID and spare pool capacity in the case of DDP.
SSD wear-life tracking and reporting. This metric is found in the Hardware tab's Drive Settings dialog box. It indicates the wear life of SSDs and replaces two SSD wear-life metrics (average erase count and spare blocks remaining) that were in previous versions of SANtricity. The metric is Percent Endurance Used; to access it, select a drive from the hardware view and then select Settings.

Reliability features with SANtricity
Online drive firmware upgrade. This feature upgrades one drive at a time and tracks writes to the affected drives during the upgrade window; it should be used only during low write I/O periods. Parallel drive firmware upgrades are supported offline to upgrade multiple drives more quickly during a maintenance window.
Automatic load balancing. This feature provides automated I/O workload balancing and confirms that incoming I/O traffic from hosts is dynamically managed and balanced across both controllers. The workload of each controller is continually monitored and analyzed in the background. When I/O on one controller significantly exceeds the I/O on the other controller for a prolonged and predictable period, SANtricity can change LUN ownership from the busy controller to the less busy controller. The feature does not react to short-term changes in I/O patterns. However, when a change of ownership is needed, SANtricity interacts with the affected host multipath driver to initiate an implicit path failover. Most current server operating systems and associated multipath drivers support implicit failover. For more information, search for “What is automatic load balancing?” in the System Manager online help.
Embedded SNMP agent. For the E2800 controller, SNMP is supported natively. The embedded SNMP agent complies with the SNMP V2C standard and RFC 1213 (MIB-II). For more information, search for “manage SNMP alerts” in the System Manager online help.
Automatic alerts. This feature sends email alerts to notify data center support staff about events on the storage array.
Event monitor and system log. The SANtricity event monitor automatically records events that occur on the storage array. Syslog enables a second level of activity tracking that allows you to connect events with associated changes recorded in the system log.
AutoSupport. E-Series products have supported AutoSupport for several releases.
Ability to enable or disable AutoSupport maintenance window. AutoSupport includes an option for enabling or suppressing automatic ticket creation on error events. Under normal operation mode, the storage array uses AutoSupport to open a support case if there is an issue. To enable or disable the AutoSupport maintenance window, select Support > Access Management > AutoSupport.

SANtricity data management features

E-Series E2800 systems ship with significant storage management features that can be activated from SANtricity System Manager. Table 7 lists standard features included with SANtricity OS.

Table 7) E2800 standard features that are included with SANtricity.

Standard features with SANtricity
SANtricity System Manager (embedded single-array management). Browser-based, on-box SANtricity System Manager is used to manage individual new-generation storage arrays. • Access all array setup, storage provisioning, and array monitoring features from one UI. • Includes an embedded RESTful API that can be used for management.
Volume workload tags. SANtricity System Manager provides a built-in volume tagging feature that allows administrators to organize the volumes in their array by workload type. Usually, the tag is only for organization purposes. In some cases—for example, Microsoft and VMware tags—the volume creation wizard provides suggested configuration or volume segment size settings associated with the workload type. You do not have to accept the recommendations. The configurations are suggestions for saving time when you provision volumes for common applications.
Storage partitions. Partitions can consist of an individual host without shared LUNs, host groups with shared LUNs, or a combination of both. This concept has been abstracted in the new System Manager, but you can view the partitions by using a CLI.
Thin provisioning. This feature enables you to overcommit storage and add capacity when you need it. This approach is a DDP feature. Starting with 11.40.2, it is available through the CLI and the SANtricity Web Services REST API only.

Standard features with SANtricity
Note: DDP thin provisioning is intended only for use cases that do not have a specific performance requirement, such as slow-growing, age-out archives where data is written once and seldom read. Thin volumes are not appropriate for transactional workloads requiring low latencies and high IOPS or throughput.
SSD read cache. This feature enables you to accelerate 85% or higher random read workloads by using a few SSDs. **Note:** The SSD read cache is not recommended for environments with sequential write workloads and should never be used with DDP thin provisioning. Both cases can result in reduced performance.
Secure SSD read cache. The SSD read cache can be secured with a nonsecure base volume or a secure base volume (FIPS drive). However, when there is an FIPS secure base volume, the storage management software alerts you if the SSD read cache does not have the same security capabilities as the base volume. **Note:** If drive security is enabled and the SSD is secure capable, the SSD read cache can be secured only when you create it.
Changing host protocol. Supported through new feature pack keys. To obtain free activation codes and detailed instructions for each starting and ending protocol, go to the E-Series and SANtricity documentation resources page.

SANtricity Remote Storage Volumes

The Remote Storage Volumes feature allows customers to import data from an existing remote storage device onto an E-Series volume with minimal downtime. It can be used to help streamline the process for equipment upgrades and/or provide data migration capabilities to move data from non-E-Series devices to E-Series systems.

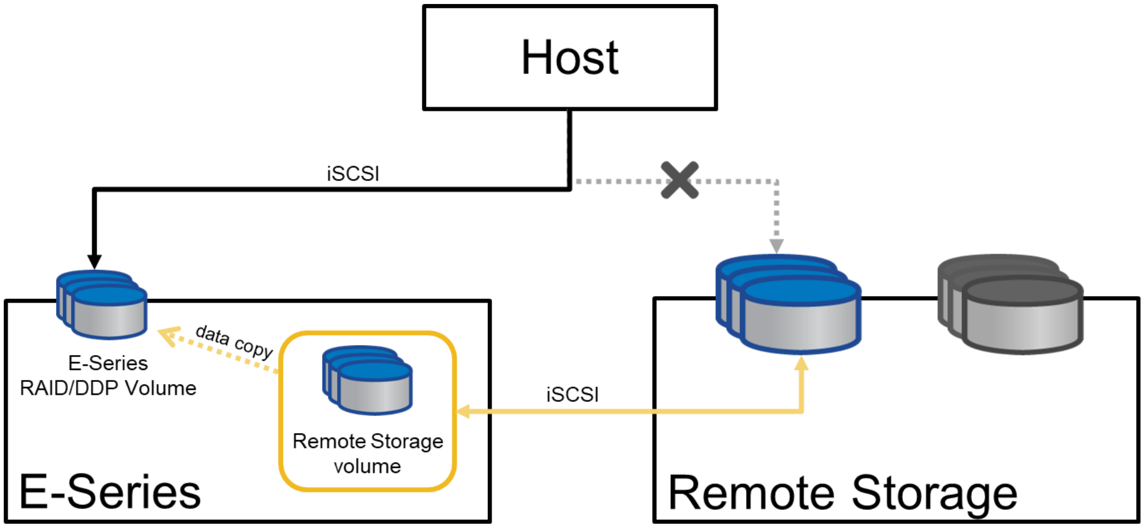
The base function of this feature is to support importing data from a remote storage device directly to a local E-Series volume. To use this feature, an iSCSI connection must first be manually established between the remote storage device and the E-Series system. The remote storage will need to be configured to have one or more IP addresses where the iSCSI IQNs of the remote storage devices can be discovered.

With the iSCSI connection in place, the remote storage device can then be mapped to the E-Series system. After the mapping is in place, SANtricity System Manager or REST API commands for the E-Series system can then be used to initiate and manage the import operation.

During the import operation the target volume can be set up to process the I/Os that the remote storage device was originally processing. Any I/Os going to the target volume will then be propagated back to the remote storage device until the import operation has completed and the import has been disconnected.

Figure 24 shows the technical components of the solution.

Figure 24) Remote Storage Volumes solution architecture overview.



Information that needs to be provided to initiate the import operation includes:

- Remote storage iSCSI IQN
- Remote storage iSCSI IP addresses
- LUN number where the remote device is mapped

The provided information will need to persist on the E-Series system so that it can remain accessible after reboots, power cycles, and so on.

After it is configured, the remote storage iSCSI IQN and/or iSCSI IP addresses can be updated, if needed, using either SANtricity System Manager or through REST API commands.

For more information about Remote Storage Volumes, see TR-4893-DEPLOY: SANtricity Remote Storage Volumes.

SANtricity copy services features

Table 8 lists standard copy services features with E2800 storage arrays.

Table 8) SANtricity copy services features.

Standard SANtricity copy services features
SANtricity Snapshot copies. Point-in-time NetApp Snapshot copies.
Synchronous mirroring. Real-time mirroring to a remote site (usually within 10km).
Asynchronous mirroring. Mirroring to a remote site where RPO = 0 is not a requirement.
Volume copy. Used to clone volumes for testing/development or analytics purposes.

For additional details and use case information about SANtricity copy services features, see TR-4458: Deploying NetApp E-Series Copy Services with Oracle and SQL Server Databases.

For details on using SANtricity Snapshots see TR-4747: SANtricity Snapshot Feature Overview and Deployment Guide.

Starting with SANtricity 11.62 the Unified Manager is used to create mirror relationships for new generation arrays. See TR-4839: SANtricity Synchronous and Asynchronous Mirroring Feature Descriptions and Deployment Guide (11.62 and Later) or the Online Help in SANtricity Unified Manager for a complete description. SANtricity Unified Manager must be version 4.2 or later and SANtricity System Manager must be OS version 11.62 or later.

Before SANtricity 11.62, for a description of mirroring between two new generation E-Series arrays or between a new generation E-Series array and a legacy E-Series array, see TR-4656: SANtricity Synchronous and Asynchronous Mirroring Feature Descriptions and Deployment Guide (11.61 and Earlier).

SANtricity management integration

Starting with SANtricity 11.40, the E-Series SANtricity integration model changed focus. To support today's modernized data center operations and partner appliances, NetApp is de-emphasizing legacy plug-ins and emphasizing API integration.

Table 9 shows the SANtricity APIs and toolkits that can be used for scripting and custom integration into other management tools and appliance architectures. To download the latest version of the E-Series SANtricity Web Services (REST API) visit NetApp Support. Information for how to use Ansible with E-Series for managing your storage can be found in TR-4574: Deploying NetApp E-Series with Ansible (Automating E-Series). For the Windows PowerShell toolkit, go to the NetApp PowerShell Toolkit page of the NetApp Support Site.

Table 9) SANtricity APIs and toolkits.

APIs and toolkits	Description
SANtricity Web Services Proxy **Note:** You can use either the proxy or the embedded REST API for all new generation storage systems.	These web APIs provide a collection of REST interfaces to configure, manage, and monitor E-Series systems.
NetApp E-Series and Ansible	Ansible is a simple yet powerful orchestration tool. NetApp E-Series has joined the Ansible community to provide you with a high-quality solution for managing your E-Series storage systems, regardless of scale.
NetApp PowerShell Toolkit	The unified toolkit provides end-to-end automation and storage management across NetApp storage systems.
SANtricity Secure CLI	The SANtricity Secure CLI (SMcli) from System Manager provides a secure, text-based method for configuring and monitoring storage arrays.

Table 10 provides a list of third platform plug-ins that use E-Series storage systems as building blocks. Usually, the plug-ins listed are available on the various provider websites. For more information about third platform integration with E-Series storage systems, contact your NetApp sales representative.

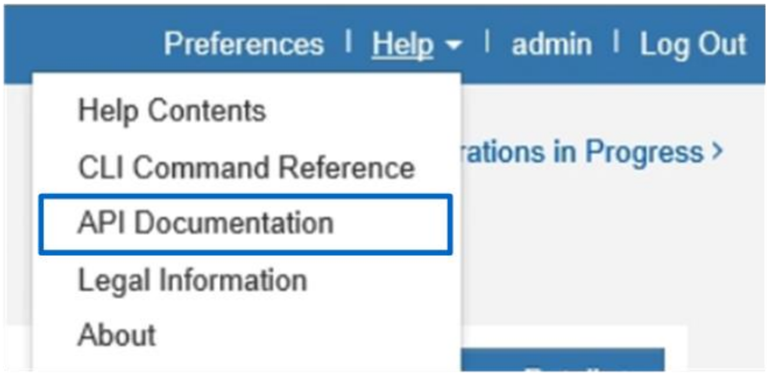
Table 10) Third platform plug-ins that use the SANtricity Web Services Proxy.

Software package	Use
NetApp SANtricity Performance App for Splunk Enterprise Technology Add-On for NetApp SANtricity	A display and monitor tool to report configuration and performance details of multiple E-Series systems in one interface. Requires both application and technology add-on.
NetApp E-Series + Grafana: Performance Monitoring	The E-Series Performance Analyzer is a powerful and easy-to-use tool to monitor the performance of your E-Series storage system.

SANtricity Web Services native REST API

The SANtricity Web Services REST API is an embedded API for experienced developers. Actions performed through the REST API are applied on execution and without user prompts or confirmation dialog boxes. The REST API is URL-based, and the accompanying API documentation is completely interactive. Each URL contains a description of the corresponding operation and enables you perform the action directly through the API documentation. To access the documentation, select API Documentation in the Help drop-down menu from any page in System Manager, as shown in Figure 25.

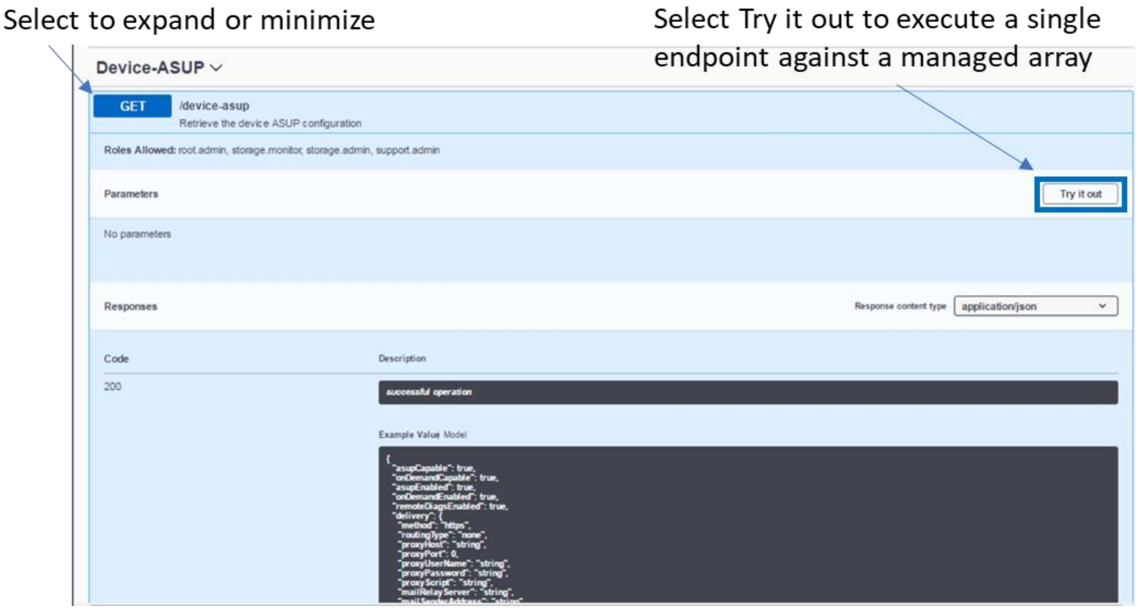
Figure 25) Opening the API documentation.



Each URL endpoint presented in the API documentation has a corresponding POST, DELETE, or GET option. These URL endpoint options, known as HTTP verbs, are the actions available through the API documentation. A sample from the REST API documentation is shown in Figure 26. You can expand or hide operations by selecting the drop-down beside the topic name or clicking the individual endpoints. Click Try It Out to execute the endpoint. You must click Execute to run an endpoint (Figure 27).

Note: To execute successfully, some endpoints require additional input parameters in the Try It Out dialog box. No additional input is required for this example.

Figure 26) Example expanding the Device-ASUP endpoint.


Select to expand or minimize
Select Try it out to execute a single endpoint against a managed array
Device-ASUP
GET
Try it out
Model

/device-asup

Retrieve the device ASUP configuration

Roles Allowed: root.admin, storage.monitor, storage.admin, support.admin

Parameters

No parameters

Responses

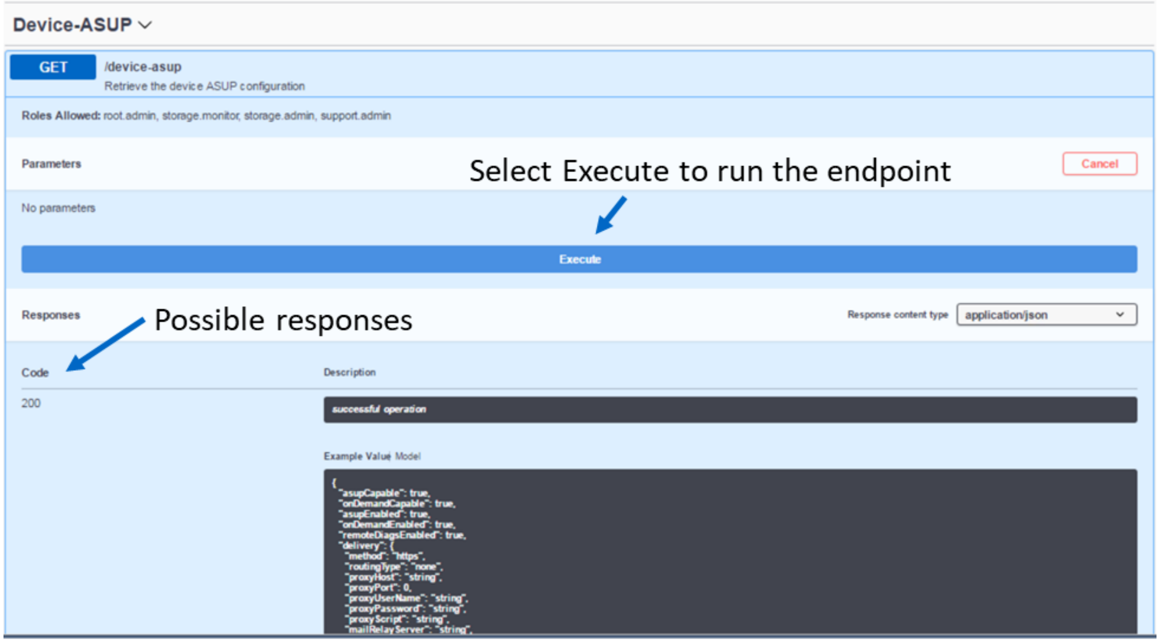
Response content type: application/json

Code	Description
200	successful operation

Example Value

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyScript": "string",
    "mailRelayServer": "string",
    "mailSenderAddress": "string",
```

Figure 27) REST API documentation sample.



Roles Allowed: root.admin, storage.monitor, storage.admin, support.admin

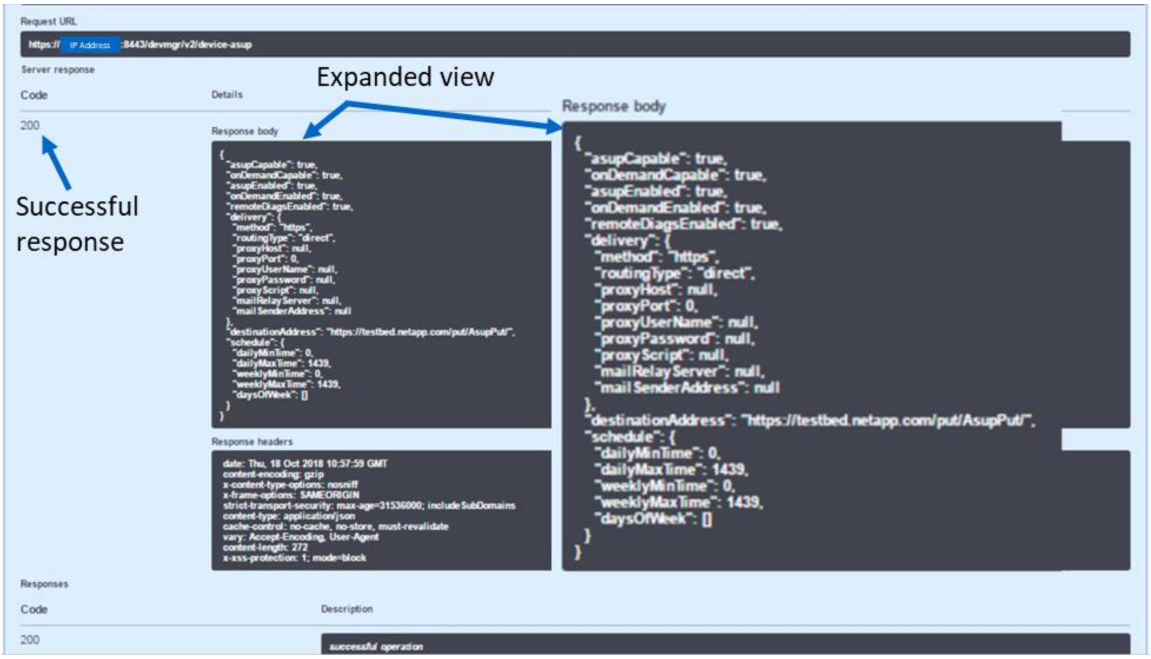
Select Execute to run the endpoint

Possible responses

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyScript": "string",
    "mailRelayServer": "string",
```

The corresponding output for the GET device-asup verb is shown in Figure 28 and Figure 29.

Figure 28) Sample output from the Try It Out button.



Request URL: https:// IP Address :8443/devmgr/v2/device-asup

Expanded view

Successful response

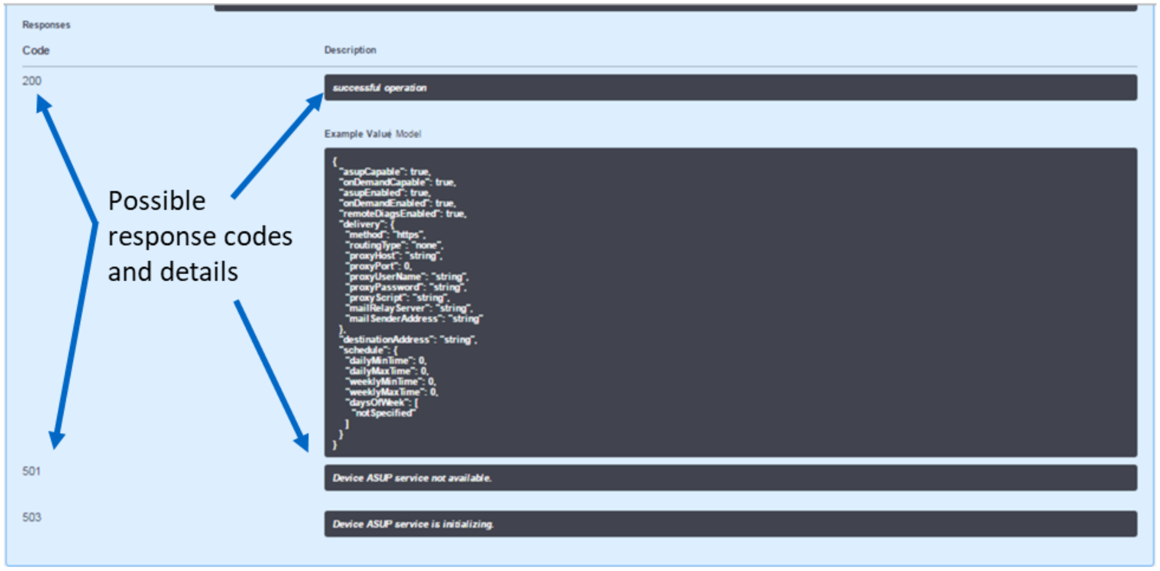
```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "direct",
    "proxyHost": null,
    "proxyPort": 0,
    "proxyUserName": null,
    "proxyPassword": null,
    "proxyScript": null,
    "mailRelayServer": null,
    "mailSenderAddress": null
  },
  "destinationAddress": "https://testbed.netapp.com/put/AsupPut/",
  "schedule": {
    "dailyMinTime": 0,
    "dailyMaxTime": 1439,
    "weeklyMinTime": 0,
    "weeklyMaxTime": 1439,
    "daysOfWeek": []
  }
}
```

```
date: Thu, 18 Oct 2018 10:57:59 GMT
content-encoding: gzip
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
strict-transport-security: max-age=31536000; includeSubDomains
content-type: application/json
cache-control: no-cache, no-store, must-revalidate
vary: Accept-Encoding, User-Agent
content-length: 272
x-xss-protection: 1; mode=block
```

Response body

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "direct",
    "proxyHost": null,
    "proxyPort": 0,
    "proxyUserName": null,
    "proxyPassword": null,
    "proxyScript": null,
    "mailRelayServer": null,
    "mailSenderAddress": null
  },
  "destinationAddress": "https://testbed.netapp.com/put/AsupPut/",
  "schedule": {
    "dailyMinTime": 0,
    "dailyMaxTime": 1439,
    "weeklyMinTime": 0,
    "weeklyMaxTime": 1439,
    "daysOfWeek": []
  }
}
```

Figure 29) Device-asup endpoint possible response codes and definitions.



200

successful operation

```
{
  "asupCapable": true,
  "onDemandCapable": true,
  "asupEnabled": true,
  "onDemandEnabled": true,
  "remoteDiagsEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUserName": "string",
    "proxyPassword": "string",
    "proxyScript": "string",
    "mailRelayServer": "string",
    "mailSenderAddress": "string"
  },
  "destinationAddress": "string",
  "schedule": {
    "dailyMinTime": 0,
    "dailyMaxTime": 0,
    "weeklyMinTime": 0,
    "weeklyMaxTime": 0,
    "daysOfWeek": [
      "notSpecified"
    ]
  }
}
```

501

Device ASUP service not available.

503

Device ASUP service is initializing.

Data in the REST API is encoded through JSON. The structured JSON data from the REST API can be easily parsed by programming languages (C, C++, cURL, Java, Python, Perl, and so on). JSON is simple encoding based on key-value pairs with support for list and subject objects. Objects start and end with curly braces (that is, { }), whereas lists start and end with brackets (that is, [ ]). JSON understands values that are strings, numbers, and Booleans. Numbers are floating-point values. The API documentation provides a JSON template for each applicable URL operation, enabling the developer to enter parameters under a properly formatted JSON command.

For more information, see E-Series and SANtricity documentation resources.

SANtricity Secure CLI

The SANtricity Secure CLI is an embedded API for experienced developers. From System Manager you can download the CLI package. The CLI provides a text-based method for configuring and monitoring storage arrays. It communicates via HTTPS and uses the same syntax as the CLI available in the externally installed management software package. No key is required to download the CLI.

A Java Runtime Environment (JRE), version 8 and above, must be available on the management system where you plan to run the CLI commands.

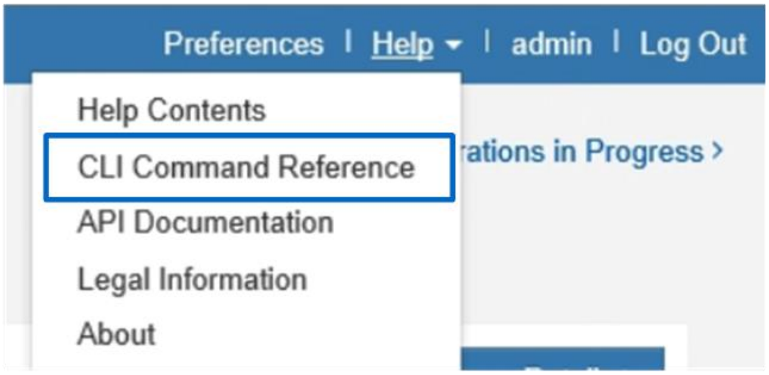
Downloading the CLI

- Select the Settings view > System.
- Under Add-Ons, select Command Line Interface. The ZIP package downloads to the browser.
- Save the ZIP file to the management system where you plan to run CLI commands for the storage array, and then extract the file.

You can now run CLI commands from an operating system prompt, such as the DOS C: prompt.

To access the documentation, select CLI Command Reference in the Help drop-down menu from any page in System Manager A CLI (Figure 30).

Figure 30) Opening the CLI Command Reference.



SANtricity Storage Plugin for vCenter

The vSphere Client is a single management interface that you can use to manage the VMware infrastructure and all your day-to-day storage needs. The following functions are available in the Plugin for vCenter:

- View and manage discovered storage arrays in the network.
- Perform batch operations on groups of multiple storage arrays.
- Perform upgrades on the software OS.
- Import settings from one storage array to another.
- Configure volumes, SSD cache, hosts, host clusters, pools, and volume groups.
- Launch the System Manager interface for additional management tasks on an array.

Note: The plugin is not a direct replacement for the System Manager software. System Manager is still required for performing certain storage administration tasks on a single array.

The plugin requires a VMware vCenter Server Appliance deployed in the VMware environment and an application host to install and run the plugin webserver.

The plugin can be downloaded from the NetApp Support Site: NetApp Support Site > Downloads > All Downloads, then select E-Series SANtricity Storage Plugin for vCenter.

Installation and Configuration documentation can be found on the NetApp Documentation site, E-Series and SANtricity 11 Documentation Center (netapp.com).

SANtricity software specifications for E2800 hardware

Table 11 lists the SANtricity software specifications for the E2800-based storage systems.

Table 11) SANtricity software boundaries for E2800-based storage systems.

Components	Maximum
Storage hardware components	
Shelves (controller and expansion)	4 (1x controller + 3x expansion) **Note:** E2812 with DE212C 7x expansion shelves maximum
Maximum drives - Drive slot count	180 (96 SSDs)
SSD cache capacity	8TB

Components	Maximum
Logical components	
Host partitions	256
Volumes per partition	256
Volumes per system	512
Disk pools per system	20
Volumes per disk pool	512
Total DDP capacity in an array (maximum capacity includes RAID overhead, DDP reserve capacity, and a small DDP-specific overhead based on the number of drives in the pool and other factors)	SANtricity 11.40 and earlier: • 2PiB maximum DDP capacity per array SANtricity 11.40.1 and later: • 6PiB maximum DDP capacity per array SANtricity 11.90 and later (see note): • 12PiB maximum DDP capacity per array
Maximum DDP single volume capacity as of SANtricity 11.50 and later	4PiB
Maximum single-DDP thin volume capacity (SANtricity 11.30 and later)	256TB
Maximum standard RAID capacity limits	Limits for standard RAID based on maximum supported drives per RAID type: • 30 drives any supported capacity for RAID 5 and RAID 6 • All drives any supported capacity for RAID 10
Maximum single volume capacity for standard RAID	4PiB
Maximum standard RAID volumes per volume group	256
Consistency groups	
Volumes per consistency group	32
Consistency groups per system	16
Snapshot copies	
Per Snapshot group	32
Per volume	128
Per storage system	512
Snapshot volumes	
Per Snapshot copy	4
Per system	256
Snapshot groups	
Per volume	4
Per system	256
Mirrors	
Mirrors per system	32
Mirrors per volume	1
Mirrors per asynchronous mirror group	32
Asynchronous mirror groups per system	4

Components	Maximum
Note: A system prior to SANtricity OS 11.90 that has existing DDP will continue to have the 6PiB maximum DDP capacity per array despite upgrading to SANtricity OS 11.90. To reuse old drives and get the 12PiB maximum DDP capacity per array, all existing DDP would need to be first deleted and recreated.	

For additional software limits and specifications, see the Hardware Universe.

E2800 hardware configurations

E2800 storage systems use a modular approach to hardware configuration. This approach can meet most customer SAN storage requirements for flexible host interfaces and versatile drive choices without sacrificing supportability, ease of implementation, and long-term stability. E-Series has a proven track record of reliability and scalability to satisfy requirements in remote dedicated environments or primary data centers.

Controller shelf configurations

E2800 controllers can be paired with DE212C, DE224C, or DE460C E-Series shelves. The following sections provide detailed information about each shelf configuration.

E2812 controller shelf

The E2812 is a 2RU shelf that holds up to 12 3.5" drives or 2.5" drives with adapter. It features one or two RAID controllers and one or two ENERGY STAR Platinum certified high-efficiency power supplies (913W) with integrated fans. An E2812-based storage system supports a maximum of 180 HDDs (120 SSDs) and a mix of drive shelf models.

Figure 31, Figure 32, and Figure 33 show the front and rear views of the E2812 controller shelf. In the example, the E2800 controllers have two RJ-45 base ports and no HIC.

Figure 31) E2812 front view with bezel.

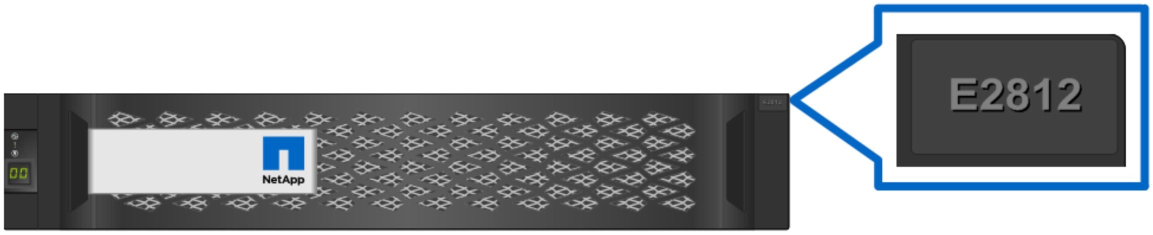


Figure 32) E2812 front view (open).

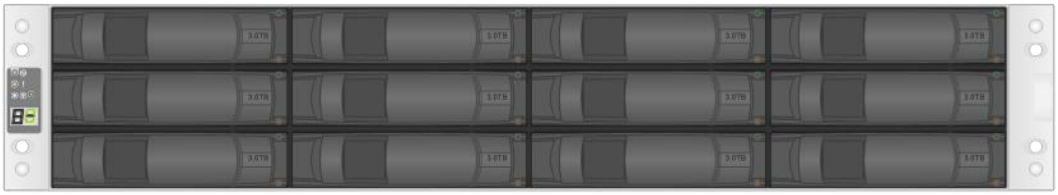
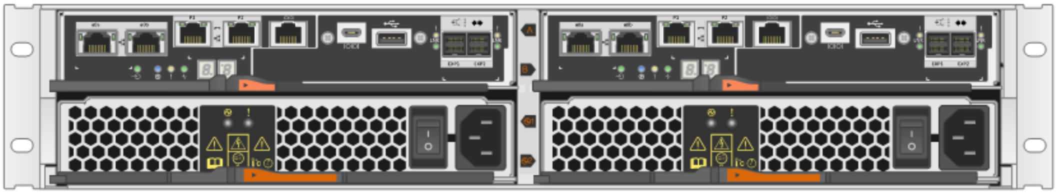


Figure 33) E2812 rear view.



E2824 controller shelf

The E2824 is a 2RU shelf that holds up to 24 2.5" drives. It features one or two RAID controllers and one or two ENERGY STAR Platinum certified high-efficiency power supplies (913W) with integrated fans. An E2824-based storage system supports a maximum of 180 HDDs (120 SSDs) and a mix of drive shelf models in a single system.

Figure 34, Figure 35, and Figure 36 show the front and rear views of the E2824 controller shelf. In the example, the E2800 controllers have two optical base ports and no HIC.

Figure 34) E2824 front view with bezel.

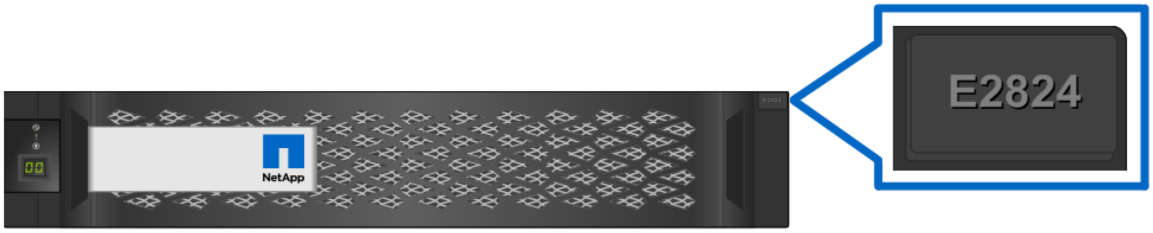


Figure 35) E2824 front view (open).

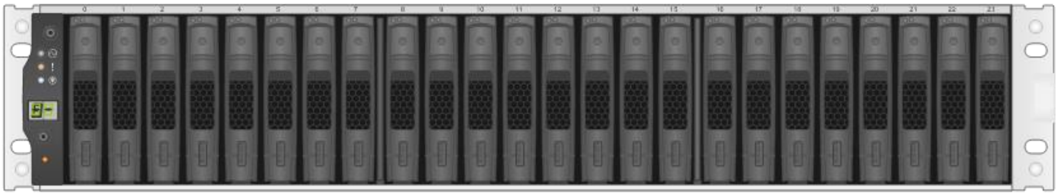
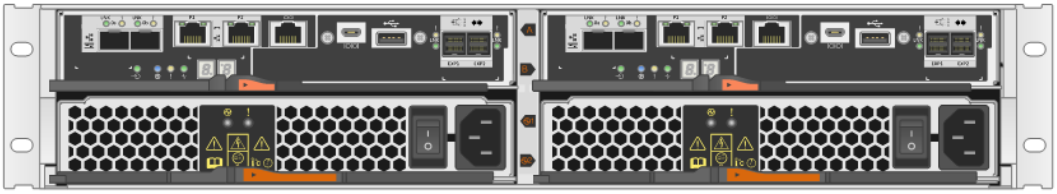


Figure 36) E2824 rear view.



E2860 controller shelf

The E2860 is a 4RU shelf that holds up to 60 3.5" drives or 2.5" drives with adapter. It features two RAID controllers and two ENERGY STAR Platinum certified high-efficiency power supplies (2325W) with separate dual fan modules. Power supplies require dual 220-240VAC power sources. An E2860-based storage system supports a maximum of 180 HDDs (120 SSDs). When mixing shelf models, the maximum drive counts vary and are governed by a maximum shelf count of 3 total shelves (a controller drive shelf and up to 2 expansion drive shelves), and the system must not exceed 180 total drive slots.

Figure 37, Figure 38, and Figure 39 show the front and rear views of the E2860 controller shelf. In the example, the E2800 controllers have two optical base ports and no HIC.

Figure 37) E2860 front view with bezel.

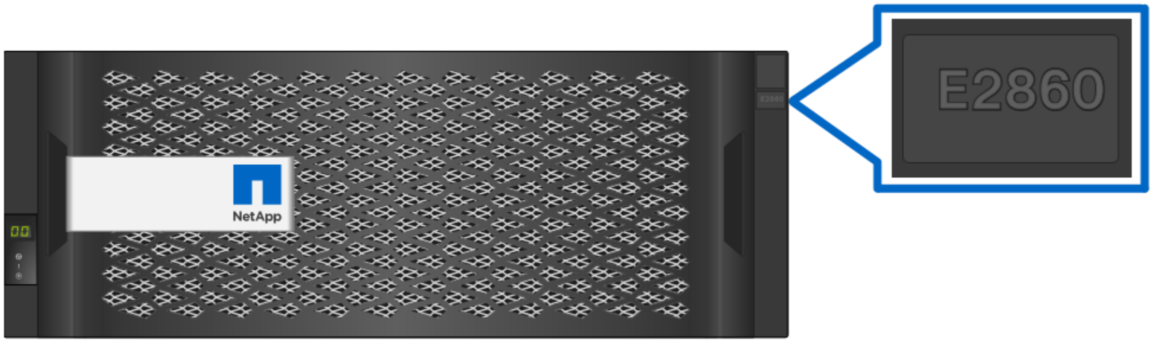


Figure 38) E2860 front view (open).

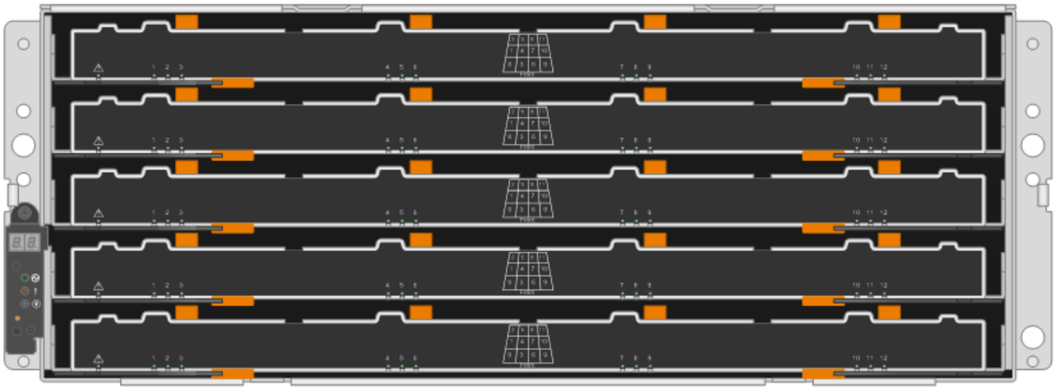
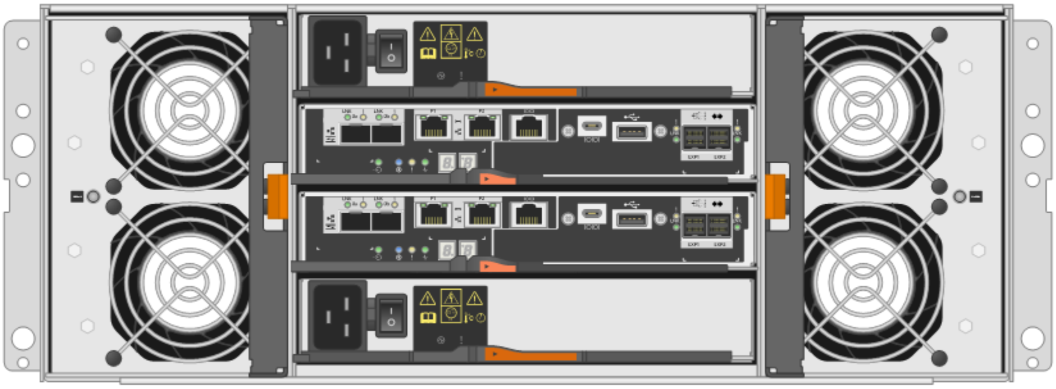


Figure 39) E2860 rear view.



E2800 hardware specifications

The E2800 controller has the following base hardware features:

- Dual Ethernet ports for management-related activities
- Either no baseboard ports (no longer available for purchase), two optical FC/iSCSI baseboard ports or two RJ-45 iSCSI baseboard ports for host connection
- Dual 12Gb SAS drive expansion ports to attach expansion drive shelves

Note: A HIC is required for the no baseboard port configuration.

Table 12 lists the technical specifications for the E2800-based storage systems.

Table 12) E2800 technical specifications.

Specification	E2812	E2824	E2860
Maximum raw system capacity (assumes not mixing shelf models)	1.7PB (18TB HDDs)	1.4PB (15.3TB SSDs)	3.24PB (18TB HDDs)
Maximum number of drives per system (assumes not mixing shelf models)	96 HDDs (96 SSDs)	96 HDDs (96 SSDs)	180 HDDs (120 SSDs)
Shelf form factor	2RU, 12 drives	2RU, 24 drives	4RU, 60 drives
Memory	4GB or 16GB per controller: simplex system.		
	8 GB or 32GB per duplex system.		
Onboard host interface (if present)	2-port 10Gb iSCSI (Base-T) per controller or 2-port 10Gb iSCSI (optical)/16Gb FC per controller. **Note:** Only one interface can be configured per system on the onboard host ports.		
Optional host I/O (HIC) • Controllers must match • A software feature pack can be applied to convert the FC HIC ports to iSCSI or to convert iSCSI HIC ports to FC	2-port 10Gb iSCSI (Base-T) per controller.		
	2-port 12Gb SAS (wide-port) per controller.		
	4-port 12Gb SAS (wide-port) per controller.		
	2-port 10GB iSCSI (optical) or 16Gb FC per controller.		
	4-port 10Gb iSCSI (optical) or 16Gb FC per controller.		
	4-port optical 32Gb FC per controller.		
	4-port optical 25Gb iSCSI.		
Drive shelves supported for expansion drive offerings	DE212C (2RU, 12 drives): 7 expansion shelves maximum; supports the same drive types as E2812 controller shelf.		
	DE224C (2RU, 24 drives): 3 expansion shelves maximum; supports the same drive types as E2824 controller shelf.		
	DE460C (4RU, 60 drives): 2 expansion shelves maximum; supports the same drive types as E2860 controller shelf.		
	DE6600 (4RU, 60 drives): 2 expansion shelves maximum; supports the same drive types as E2824 and/or E2812 controller drive shelves. **Note:** Supports only SAS 2 (6Gbps) transfer speeds.		
	DE5600 (2RU, 24 drives): 3 expansion shelves maximum; supports the same drive types as E2824 controller shelf. **Note:** Supports only SAS 2 (6Gbps) transfer speeds.		
	DE1600 (2RU, 12 drives): 3 expansion shelves maximum; supports only NL-SAS drive types. **Note:** Supports only SAS 2 (6Gbps) transfer speeds.		

Specification	E2812	E2824	E2860
High-availability (HA) features	Dual active controllers with automated I/O path failover.		
	Support for RAID 0, 1 (10 for 4 drives or more), 5, and 6 and DDP. **Note:** It is only possible to create RAID 3 volumes through the CLI. For more information, search for “using the create volume group wizard” in the System Manager online help.		
	Redundant, hot-swappable storage controllers, disks, and power fan canisters.		
	Mirrored data cache with battery-backed destage to flash.		

See the Hardware Universe for current supported drive availability information and encryption capability by drive capacity (FDE, FIPS).

For additional information, see the Datasheet - NetApp E2800 Series.

Controller host interface features

By default, the E2800 controller includes two Ethernet management ports that provide out-of-band system management access and either two optical FC/iSCSI or two RJ-45 iSCSI baseboard ports for host connection. The E-Series E2800 controller also supports seven HIC options, including:

- 2-port 10Gb iSCSI BASE-T
- 2-port 12Gb SAS (SAS 3 connector)
- 4-port 12Gb SAS (SAS 3 connector)
- 2-port optical HIC, which can be configured as either 16Gb FC or 10Gb iSCSI
- 4-port optical HIC, which can be configured as either 16Gb FC or 10Gb iSCSI
- 4-port optical 32Gb FC optical HIC
- 4-port optical 25Gb iSCSI optical HIC

Note: A software feature pack can be applied in the field to change the host protocol of the optical baseboard ports and for the 2-port or 4-port 16Gb FC, or 10Gb iSCSI optical HICs. However, the 32Gb FC and 25Gb iSCSI HICs are not programmable. Also, the 25Gb iSCSI port speed must be manually set by using the SANtricity System Manager GUI or SMcli interface, one port per controller. Changing one port will automatically change all four ports on a HIC.

For instructions to obtain and apply software feature packs to change baseboard and HIC protocol, see Change E2800 Host Protocol for specific instructions.

The optical 32Gbps FC and 25Gbps iSCSI HICs support several SFP options, including two FC and one iSCSI option. There are two options for the 16Gb FC or 10Gb iSCSI base ports. Table 13 provides details about the FC options.

Table 13) FC host interface port speed and associated SFPs.

HIC protocol	32Gbps SFP	16Gbps SFP	8Gbps SFP
32Gbps FC	32Gbps/16Gbps	16Gbps/8Gbps	Not available
16Gbps FC base ports	Not available	16Gbps/8Gbps/4Gbps	8Gbps/4Gbps

Table 14 provides details about the iSCSI port speed based on the installed SFP. For the 16Gbps FC/10Gbps iSCSI base ports, use the unified SFP part number X-48895-00-R6-C. For 1Gbps iSCSI base ports, use SFP part number X-48896-00-C.

Note: The unified SFP does not support 1Gb iSCSI. It does support 4/8/16Gb FC and 10Gb iSCSI.

Table 14) iSCSI host interface port speed and associated SFPs.

HIC protocol	25Gbps SFP	10Gbps SFP (Unified SFP)	1Gbps SFP
25Gbps iSCSI	25Gbps/10Gbps*	Not available	Not available
10Gbps iSCSI base ports	Not available	10Gbps	1Gbps

* You must change port speed from 25Gbps to 10Gbps or 10Gbps to 25Gbps by using SANtricity System Manager in the iSCSI setup section. Change one HIC port per controller as required to match the SFP and the switch port setting. The remaining HIC ports on each controller change automatically to match the one port per controller that you manually changed.

For optical connections, appropriate SFPs must be ordered for the specific implementation. Consult the Hardware Universe for a full listing of available host interface equipment.

Note: Both controllers in a duplex configuration must be configured identically.

Figure 40 shows the seven HIC options.

Figure 40) E2800 with optical base ports HIC options.

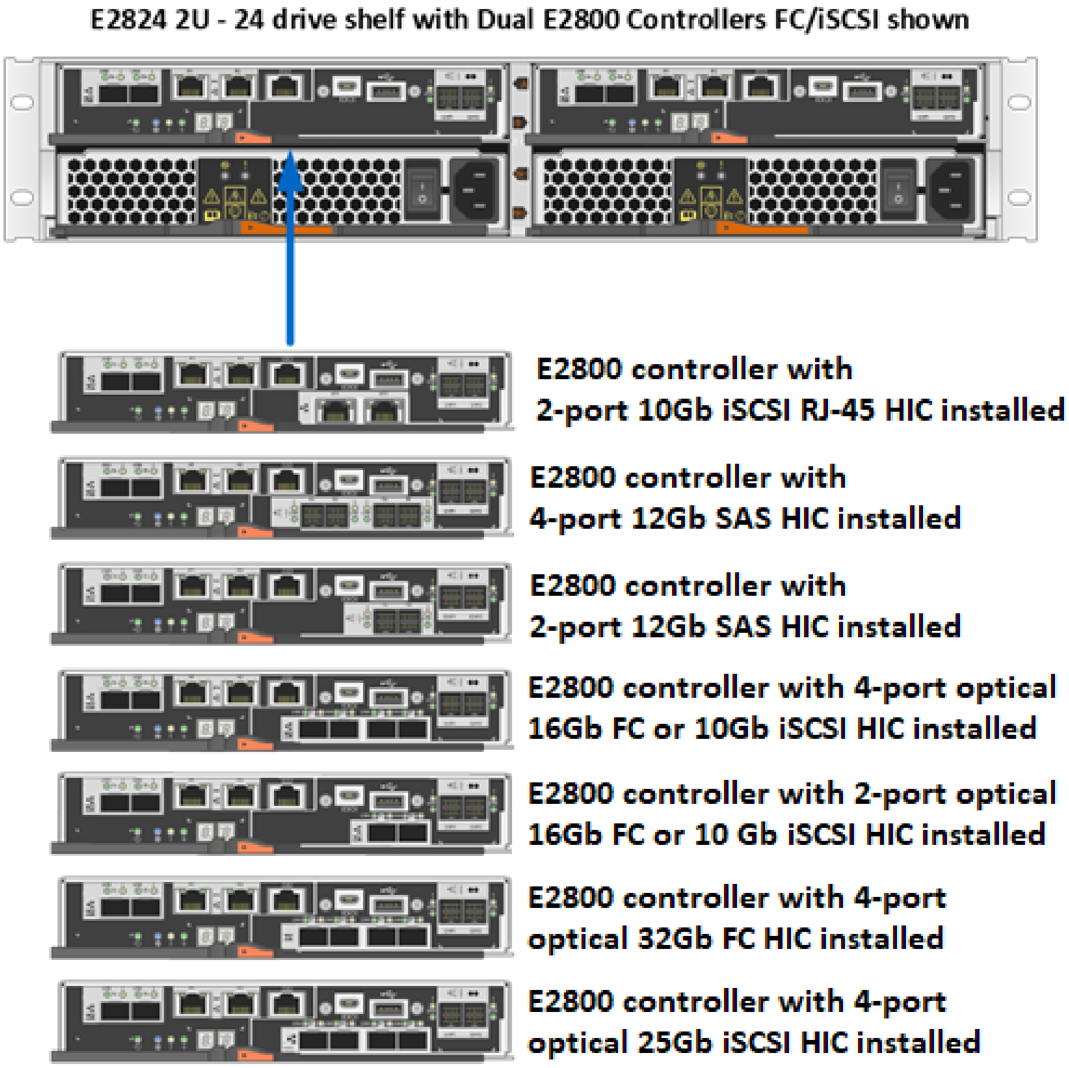
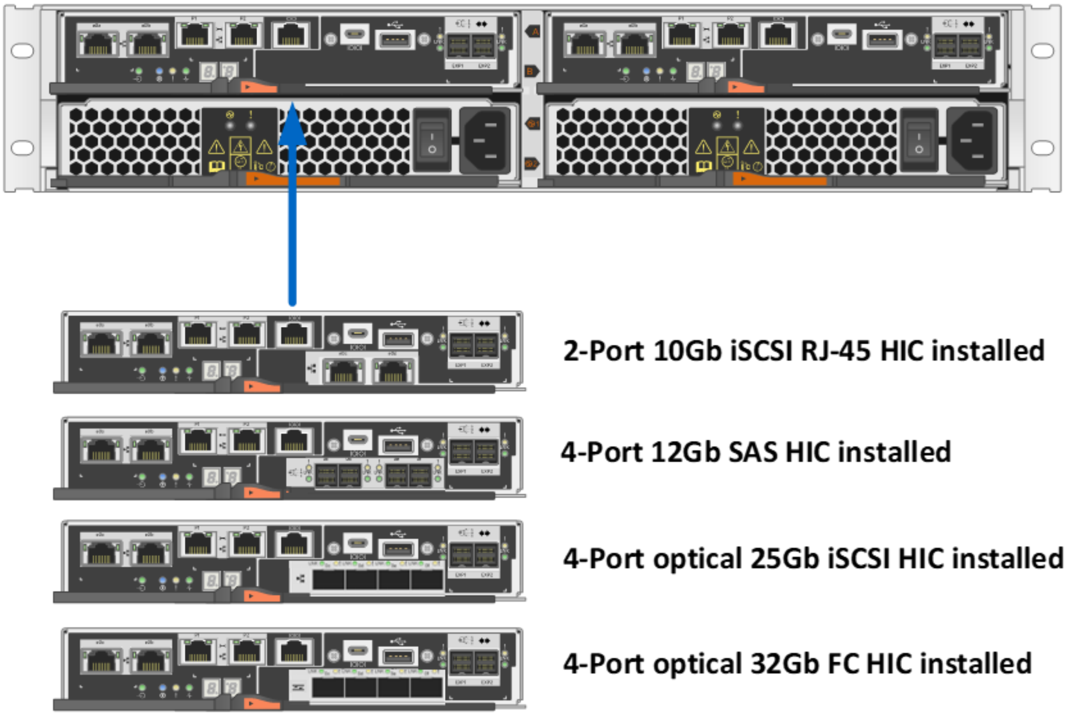

E2824 2U - 24 drive shelf with Dual E2800 Controllers FC/iSCSI shown
E2800 controller with 2-port 10Gb iSCSI RJ-45 HIC installed
E2800 controller with 4-port 12Gb SAS HIC installed
E2800 controller with 2-port 12Gb SAS HIC installed
E2800 controller with 4-port optical 16Gb FC or 10Gb iSCSI HIC installed
E2800 controller with 2-port optical 16Gb FC or 10 Gb iSCSI HIC installed
E2800 controller with 4-port optical 32Gb FC HIC installed
E2800 controller with 4-port optical 25Gb iSCSI HIC installed

Figure 41 shows the HIC options available when the baseboard host ports are 10Gb iSCSI Base-T.

Figure 41) E2800 with Base-T iSCSI onboard host ports: HIC options.


2-Port 10Gb iSCSI RJ-45 HIC installed
4-Port 12Gb SAS HIC installed
4-Port optical 25Gb iSCSI HIC installed
4-Port optical 32Gb FC HIC installed

Note: All HIC options support link speed autonegotiation except for 25Gb iSCSI. In that case, the port speed must be manually set by using SANtricity System Manager or SMcli.

Hardware LED definitions

E2800 controller shelf LEDs

The E2800 controller shelf has LED status indicators on the front of the shelf, the Operator Display Panel (ODP), the rear of the shelf, the power fan canisters, and the controller canisters. The new E2800 shelf ODP also includes a dual seven-segment display to indicate the shelf identity. The LEDs on the ODP indicate systemwide conditions, and the LEDs on the power fan canisters indicate the status of the individual units.

Figure 42 shows the ODP of the E2812 and E2824 controller shelves. Figure 43 shows the ODP of the E2860 controller shelf.

Figure 42) ODP on the front panel of E2824 and E2812 controller shelves.

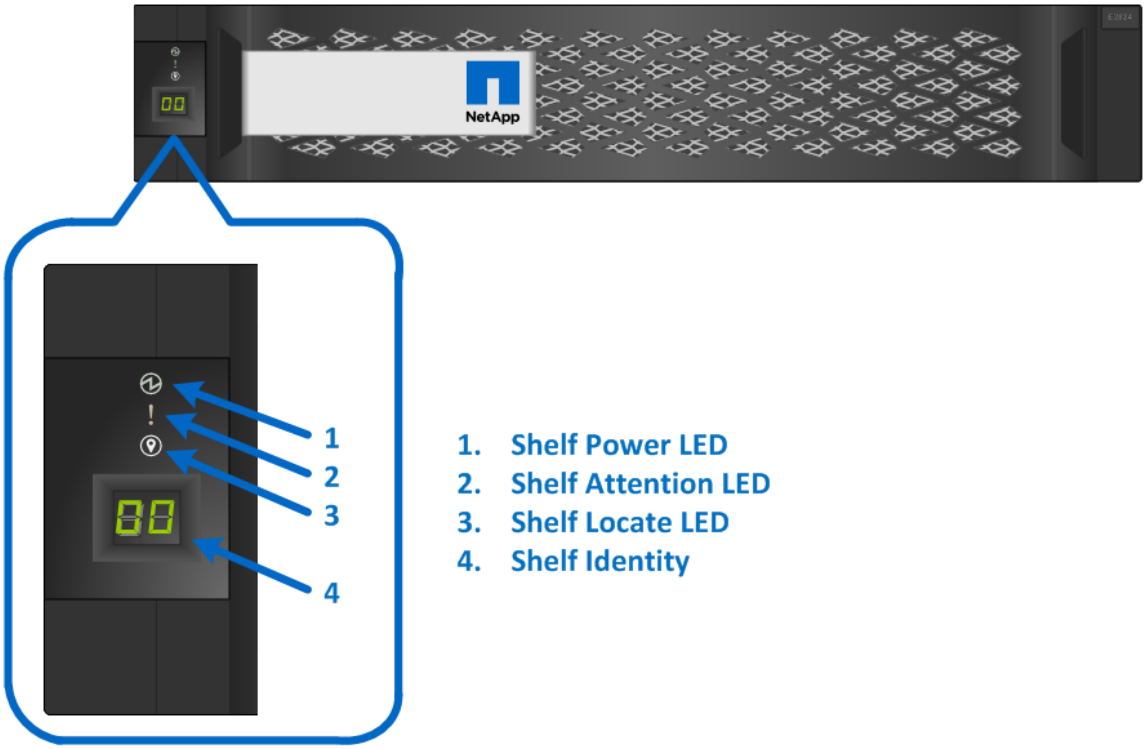


Figure 43) ODP on the front panel of E2860 controller shelves.

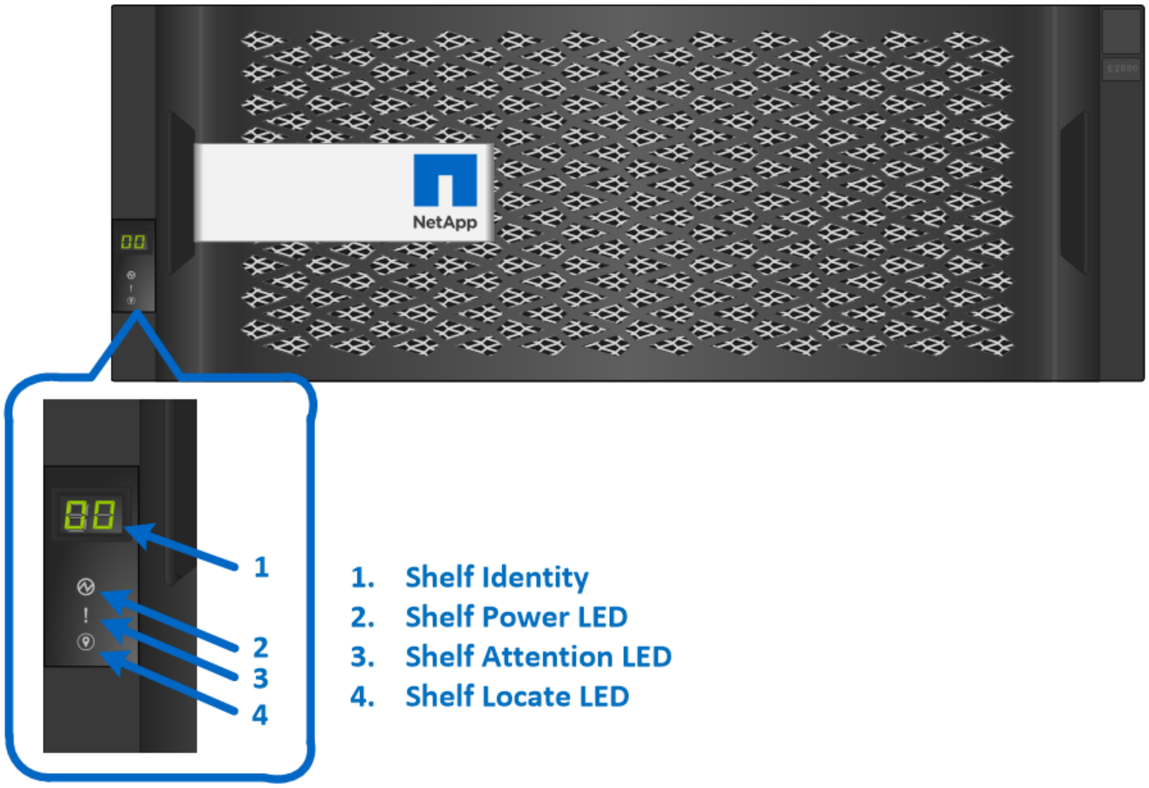


Table 15 defines the ODP LEDs on the E2800 controller shelf.

Table 15) E2800 controller shelf LED definitions (front panel).

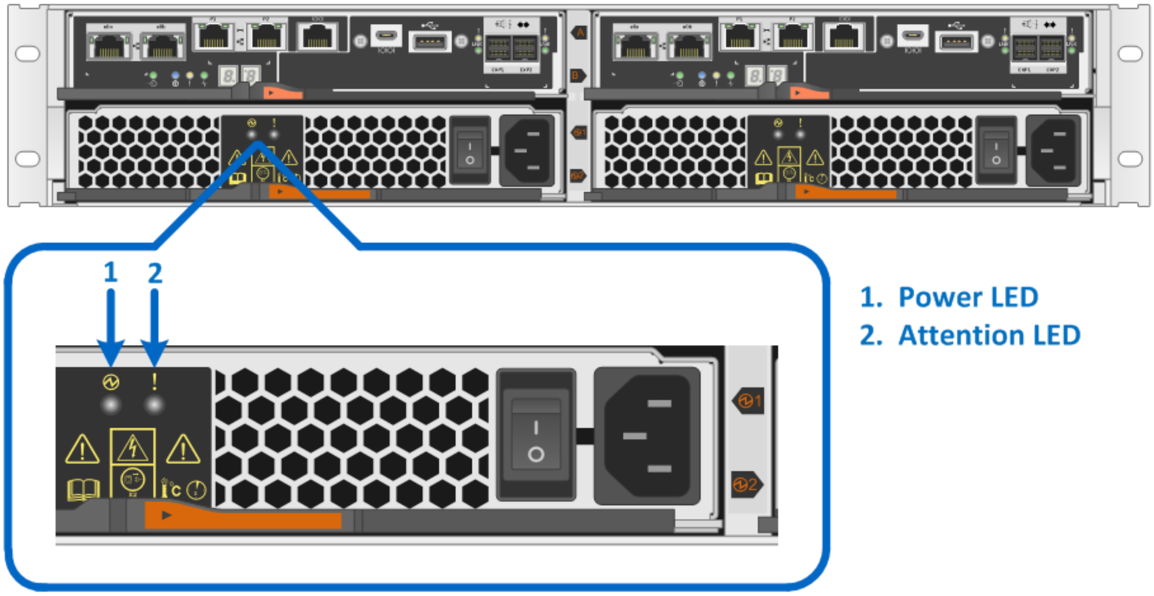
LED Name	Color	LED on	LED off
Power	Green	Power is present.	Power is not present.
Attention	Amber	A component in the controller shelf requires attention.	Normal status.
Locate	Blue	There is an active request to physically locate the shelf.	Normal status.

Note: The shelf-identity feature displays a numerical value to identify the shelf. The dual seven-segment display indicates values from 00 to 99.

Power fan canister status LEDs

The power fan canisters for the E2824 and E2812 controller shelves are identical. The LEDs on the rear panel are shown in Figure 44 and are defined in Table 16.

Figure 44) LEDs on the E2824 and E2812 power fan canister (rear view).



The power and fan canisters are separate for the E2860 controller shelf. The LEDs on the rear panel of each are shown in Figure 45 and defined in Table 16.

Figure 45) LEDs on the E2860 power canister (rear view).

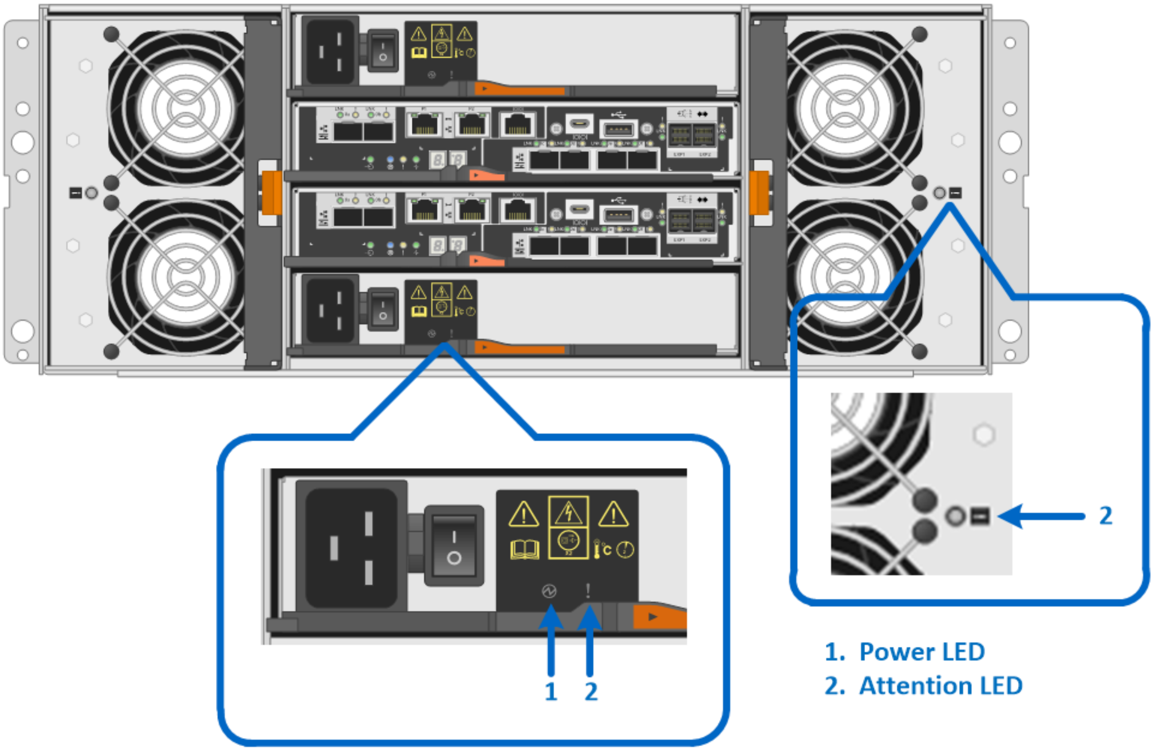


Table 16) E2812, E2824, and E2860 controller shelf power and fan canister LED definitions.

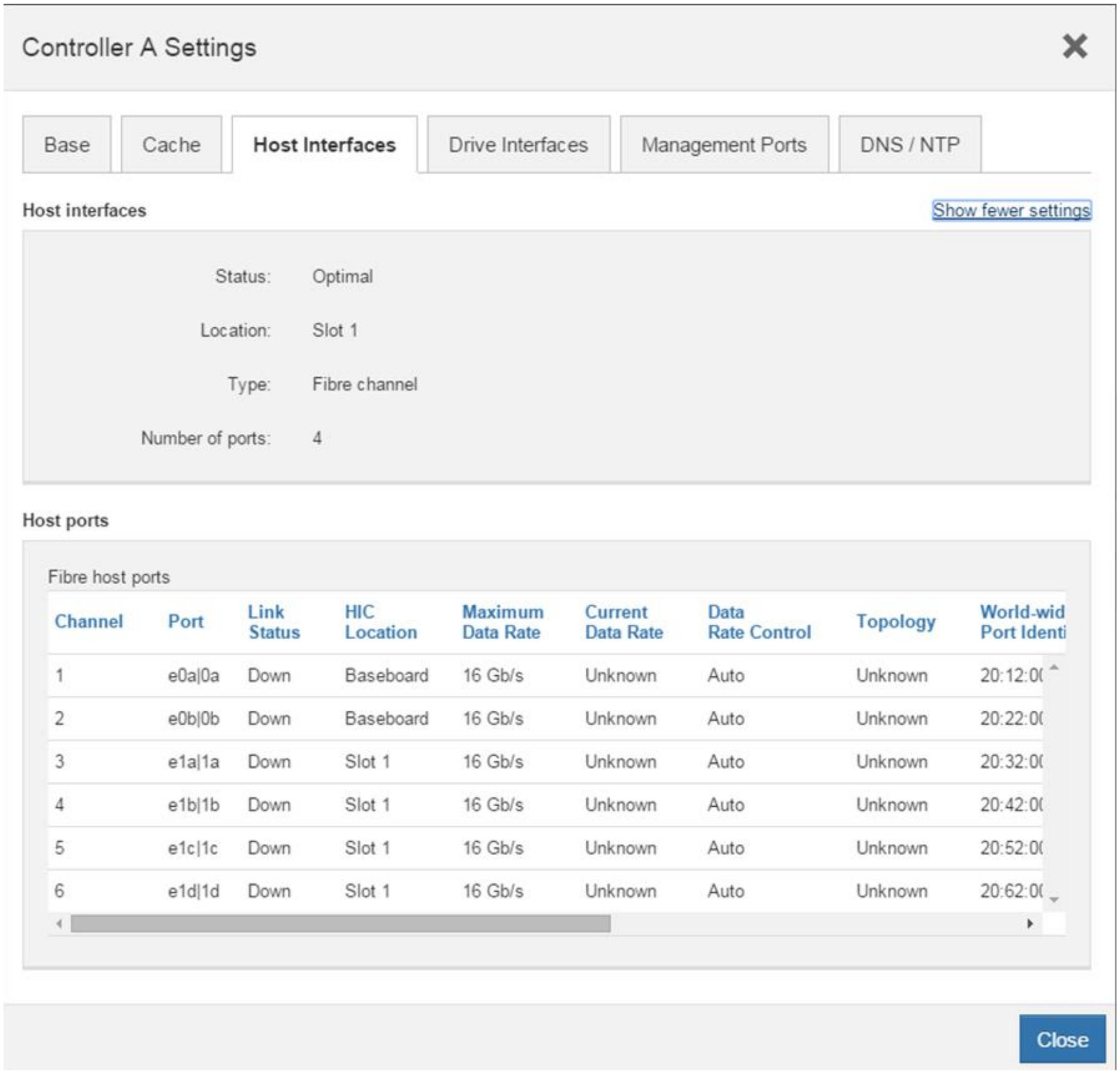
LED Name	Color	LED on	LED off
Power	Green	AC power is present.	AC power is not present.
Attention	Amber	The power supply or the integrated fan has a fault.	Normal status.

E2800 controller canister LEDs

The E2800 controller canister has several LED status indicators. The LEDs on the left side of the module refer to the overall controller status and to the onboard host ports. The LEDs on the right side of the module refer to the drive expansion ports and to the optional HIC ports.

Host port status can be verified by directly checking the port LEDs or by using the SANtricity System Manager GUI. The Host Interfaces tab of the Controller Settings dialog box (Figure 46) details the status of each host I/O interface that is connected to the storage system.

Figure 46) Controller settings dialog box.



Controller A Settings

Host interfaces

Status:	Optimal
Location:	Slot 1
Type:	Fibre channel
Number of ports:	4

Host ports

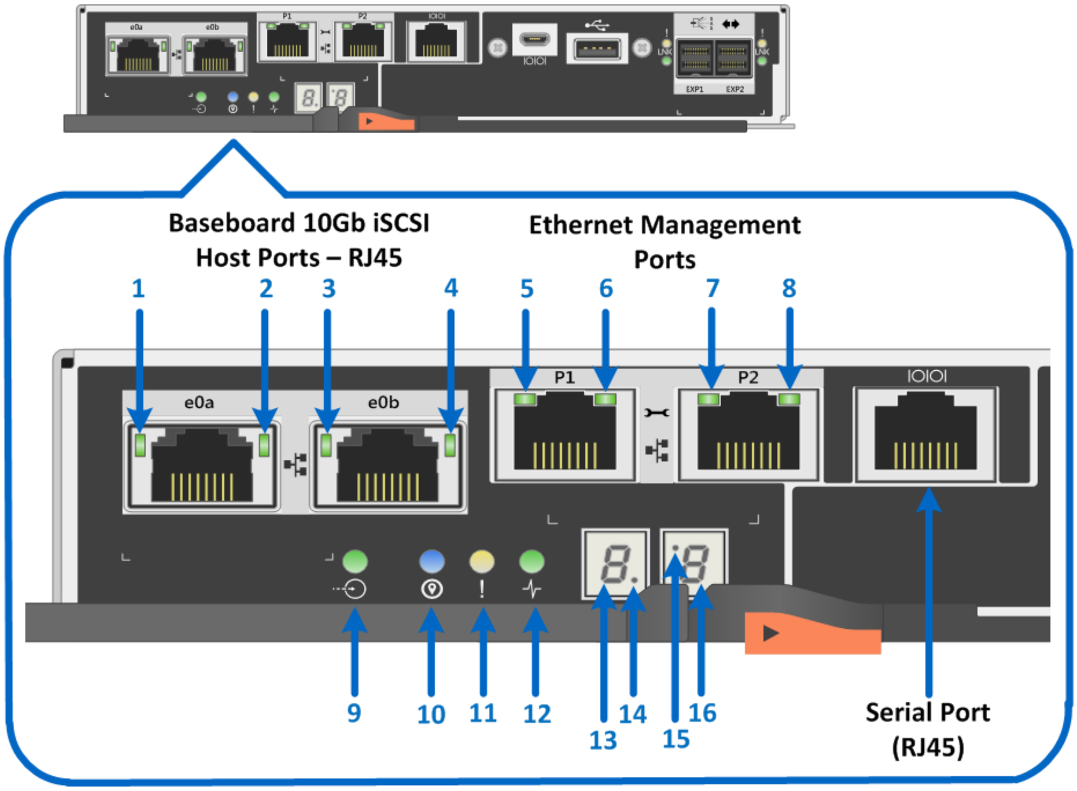
Fibre host ports

Channel	Port	Link Status	HIC Location	Maximum Data Rate	Current Data Rate	Data Rate Control	Topology	World-wid Port Identi
1	e0a|0a	Down	Baseboard	16 Gb/s	Unknown	Auto	Unknown	20:12:0(
2	e0b|0b	Down	Baseboard	16 Gb/s	Unknown	Auto	Unknown	20:22:0(
3	e1a|1a	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:32:0(
4	e1b|1b	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:42:0(
5	e1c|1c	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:52:0(
6	e1d|1d	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:62:0(

Controller base port status LEDs

Figure 47 shows the onboard LED status indicators on the left side of the E2800 controller canister with the RJ-45 iSCSI baseboard host ports. Most of the LEDs are lit when a fault condition exists. However, the cache active LED is lit when the cache is active. The seven-segment LEDs provide status codes for both normal operation and fault conditions. The dot in the first seven-segment LED is the controller heartbeat indicator, which comes on when an intercontroller communication link has been established. The dot in the second seven-segment LED is on to indicate a diagnostic code. Otherwise, the display indicates the shelf ID.

Figure 47) LEDs on the left side of E2800 controller canister with RJ-45 iSCSI host ports.



1. Baseboard Host Port e0a iSCSI Link State LED
2. Baseboard Host Port e0a iSCSI Link Activity LED
3. Baseboard Host Port e0b iSCSI Link State LED
4. Baseboard Host Port e0b iSCSI Link Activity LED
5. Ethernet Management Port P1 Link State LED
6. Ethernet Management Port P1 Link Activity LED
7. Ethernet Management Port P2 Link State LED
8. Ethernet Management Port P2 Link Activity LED
9. Cache Active LED
10. Locate LED
11. Attention LED
12. Activity LED
13. Seven-segment Display – Upper Digit
14. Flashing dot heartbeat indicator
15. On to indicate diagnostic code LED
16. Seven-segment Display – Lower Digit

Table 17 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 47). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

Table 17) iSCSI RJ-45 baseboard host port LED definitions.

LED name	Color	LED on	LED off
Host port link state (top left)	Green	Link is up.	Link is down.

LED name	Color	LED on	LED off
Host port link activity (top right)	Green	Link activity.	No link activity.

Table 18 defines the Ethernet management port LEDs on the controller (LEDs 5 through 8 in Figure 47).

Table 18) Ethernet management port LED definitions.

LED name	Color	LED on	LED off
Ethernet management port link state (top left)	Green	Link is up.	Link is down.
Ethernet management port link activity (top right)	Green	Blinking: The link is up with activity.	No link activity.

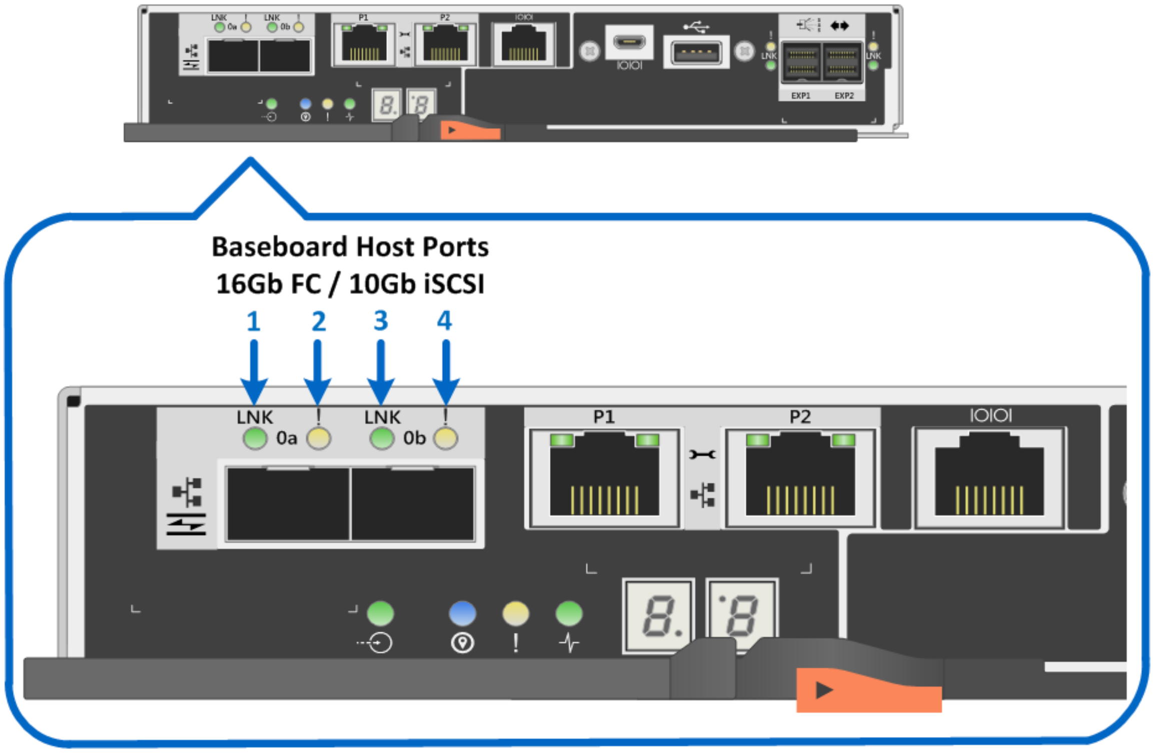
Table 19 defines the controller status LEDs (LEDs 9 through 15 in Figure 47).

Table 19) Controller base features LED definitions.

LED name	Color	LED on	LED off
Cache active	Green	Write data in cache.	Normal status.
Locate	Blue	Request to locate the enclosure is active.	Normal status.
Attention	Amber	Some fault exists in the controller canister.	Normal status.
Activity	Green	Blinking: controller active.	Controller is not in service.
Heartbeat (upper digit of seven-segment LED, lower right)	Yellow	Blinking: heartbeat.	Controller is not in service.
Diagnostic (lower digit of seven-segment LED, upper left)	Yellow	Seven-segment display indicates diagnostic code.	Seven-segment display indicates shelf ID.
Two seven-segment LEDs	Yellow	• Shelf ID if diagnostic LED off. • Diagnostic code if diagnostic LED on.	The controller is not powered on.

Figure 48 shows the onboard LED status indicators on the left side of the E2800 controller canister with the 16Gb FC or 10Gb iSCSI baseboard host port LEDs.

Figure 48) LEDs on left side of E2800 controller canister with 16Gb FC/10Gb iSCSI host ports.



1. Baseboard Host Port 0a 16GB FC/10Gb iSCSI Link LED
2. Baseboard Host Port 0a 16GB FC/10Gb iSCSI Fault LED
3. Baseboard Host Port 0b 16GB FC/10Gb iSCSI Link LED
4. Baseboard Host Port 0b 16GB FC/10Gb iSCSI Fault LED

Table 20 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 48). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

Table 20) 16Gb FC/10Gb iSCSI baseboard host port LED definitions.

LED Name	Color	LED on	LED off
Host port link/activity	Green	• Solid: link up with no activity. • Blinking: link up with activity.	Link is down.
Host port attention	Amber	Port requires operator attention.	Normal status.

Drive-side SAS expansion port LEDs

The E2800 controller canister is equipped with two SAS expansion ports that are used to connect expansion drive shelves to the E2800 controller shelf. Figure 49 shows the SAS expansion port LEDs.

Figure 49) LEDs for drive expansion ports (no HIC installed).

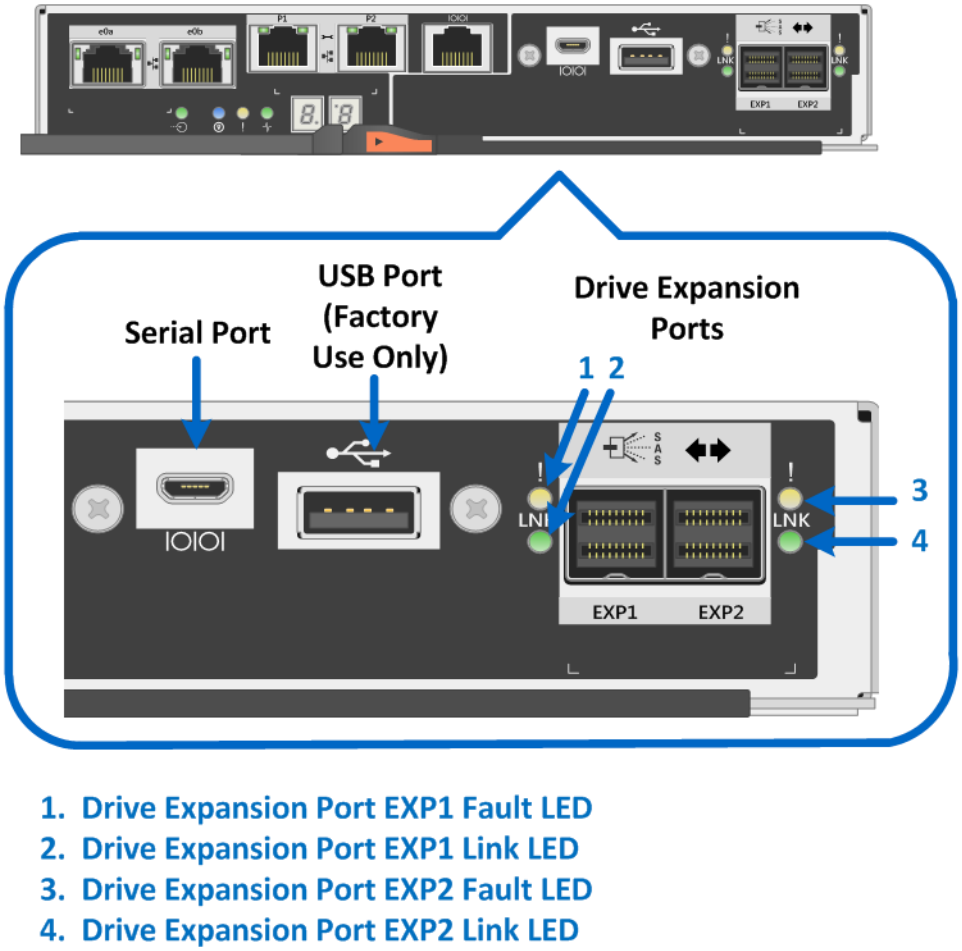

e0a
e0b
P1
P2
IOIOI
EXP1
EXP2
LNK
Serial Port
USB Port (Factory Use Only)
Drive Expansion Ports
1
2
3
4
IOIOI
LNK
LNK
EXP1
EXP2
1. Drive Expansion Port EXP1 Fault LED
2. Drive Expansion Port EXP1 Link LED
3. Drive Expansion Port EXP2 Fault LED
4. Drive Expansion Port EXP2 Link LED

Table 21 defines each drive-side LED (LEDs 1 through 4 in Figure 49).

Table 21) Drive expansion port LED definitions.

LED Name	Color	LED on	LED off
Drive expansion fault	Amber	At least one of the four PHYs in the output port is working, but another PHY cannot establish the same link to the expansion output connector.	Port is optimal (all PHYs in the port are up).
Drive expansion link	Green	Link is up.	Link is down.

E2800 optional host interface cards

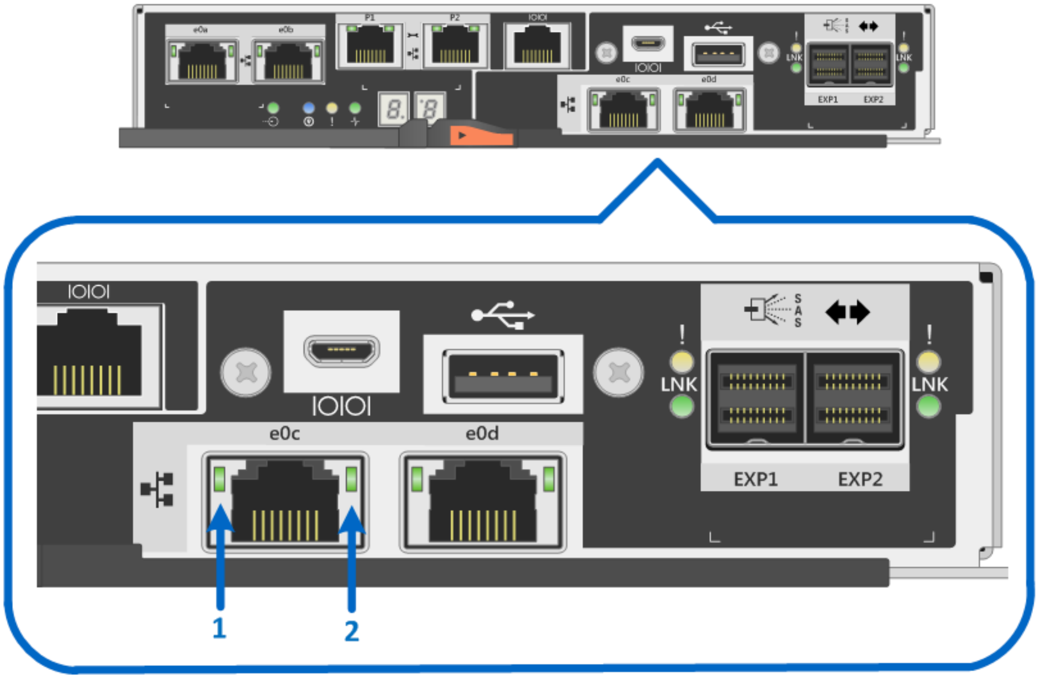
The E2800 supports several host interface expansion options, including SAS, FC, and iSCSI:

- When the baseboard host ports are optical, as shown in Figure 40, all five HIC options are available.
- When the baseboard host ports are 10Gb iSCSI Base-T, as shown in Figure 41, only the 2-port 10Gb iSCSI Base-T HIC or 2-port and 4-port 12Gb SAS HICs expansion HICs are supported.

2-Port 10Gb iSCSI RJ-45 HIC LEDs

The 2-port 10Gb iSCSI copper HIC has two standard RJ-45 connectors, as shown in Figure 50, and uses standard RJ-45 Twinax cables to connect to switches or directly to hosts.

Figure 50) LEDs on the 2-port 10Gb iSCSI RJ-45 HIC.



1. Host iSCSI Expansion (RJ45) Port e0c Link State LED
2. Host iSCSI Expansion (RJ45) Port e0c Link Activity LED

Table 22 defines the LEDs on the 2-port 10Gb iSCSI HIC.

Note: The drive expansion port LEDs are defined in Table 21.

Table 22) 2-port 10Gb iSCSI HIC LED definitions.

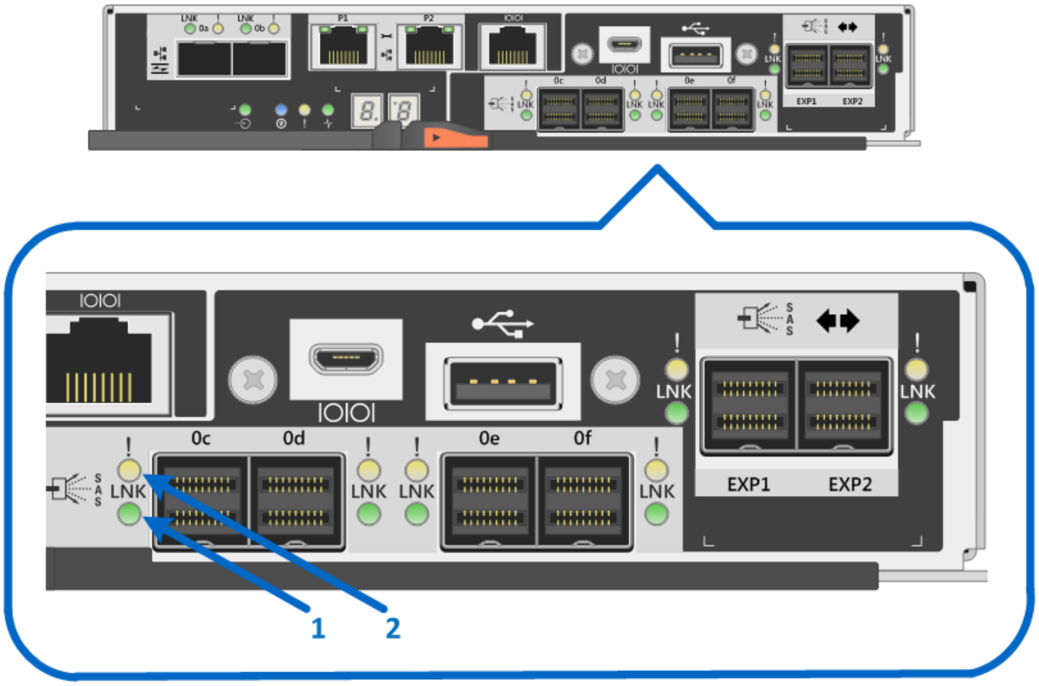
LED name	Color	LED on	LED off
Host port link state (top left)	Green	Link is up.	Link is down.
Host port link activity (top right)	Green	Link activity.	No link activity.

2-Port and 4-Port 12Gb SAS HIC LEDs

Figure 51 and Figure 52 show the LEDs for the 4-port and 2-port 12Gb SAS HICs. LEDs are called out for only the 4-port SAS HIC; the 2-port HIC LEDs are the same.

Note: The SAS expansion HICs are the same for both E2800 controller models. Figure 51 shows the E2800 controller with the 2-port optical onboard ports and the 4-port optional SAS HIC installed.

Figure 51) LEDs for the 4-port 12Gb SAS HIC.



1. Host SAS Expansion Port 0c Link LED
2. Host SAS Expansion Port 0c Fault LED

Figure 52) LEDs for the 2-port 12Gb SAS HIC.

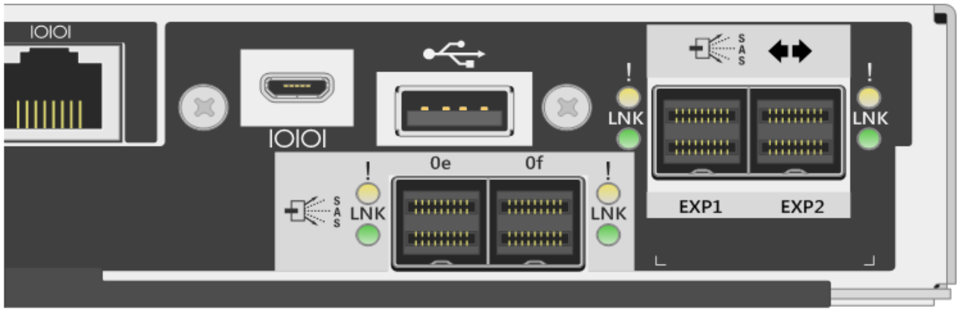


Table 23 defines the LEDs for the 12Gb SAS HICs.

Note: Table 21 defines the drive expansion port LEDs.

Table 23) 2-port and 4-port 12Gb SAS HIC LED definitions.

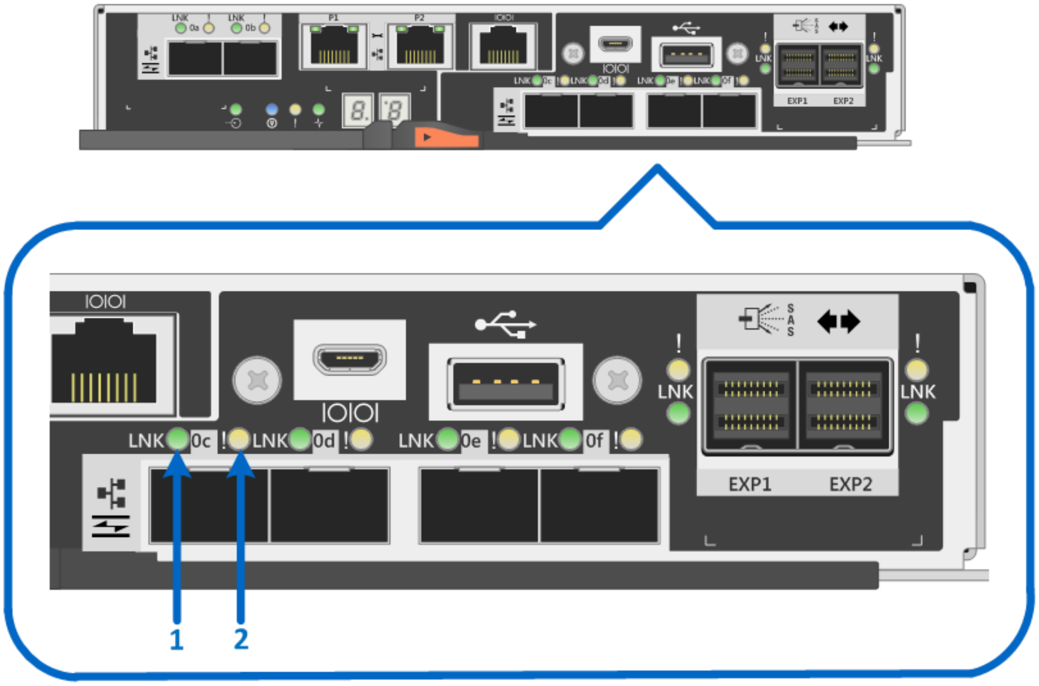
LED name	Color	LED on	LED off
Drive expansion link	Green	Link is up.	Link is down.
Drive expansion fault	Amber	At least one of the four PHYs in the output port is working, but another PHY cannot establish the same link to the expansion output connector.	Port is optimal (all PHYs in the port are up).

2-Port and 4-Port optical HIC (16Gb FC or 10Gb iSCSI) LEDs

The E2800 controller supports a 2-port or 4-port optical HIC that offers 16Gb FC protocol or 10Gb iSCSI protocol. The 2-port HIC is functionally equivalent to the 4-port HIC. When using the 4-port HIC and dual controllers, the E2800 storage system provides a maximum of 12 16Gb FC or 12 10Gb iSCSI ports or a mixture of 16Gb FC and 10Gb iSCSI ports.

Figure 53 and Figure 54 show the LEDs for the 4-port and 2-port optical HIC. LEDs are called out for only the 4-port optical HIC; the 2-port HIC LEDs are the same.

Figure 53) LEDs for the 4-port optical HIC (16Gb FC or 10Gb iSCSI).



1. Host 16Gb FC / 10Gb iSCSI Expansion Port 0c Link LED
2. Host 16Gb FC / 10Gb iSCSI Expansion Port 0c Fault LED

Figure 54) LEDs for the 2-port optical HIC (16Gb FC or 10Gb iSCSI).

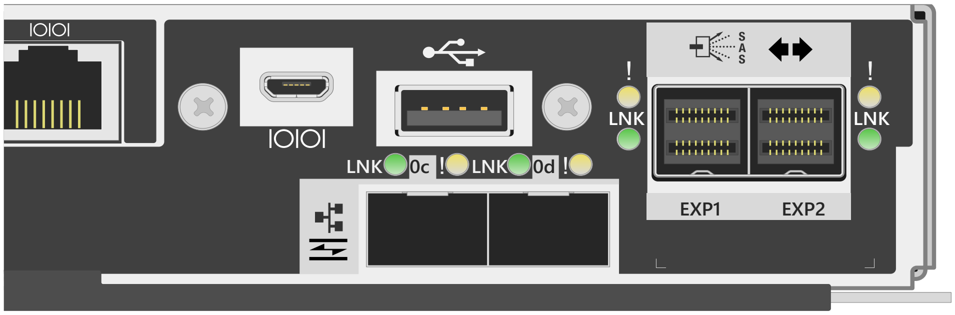


Table 24 defines the LEDs on the 2-port and 4-port optical HICs (16Gb FC or 10Gb iSCSI).

Note: Table 21 defines the drive expansion port LEDs.

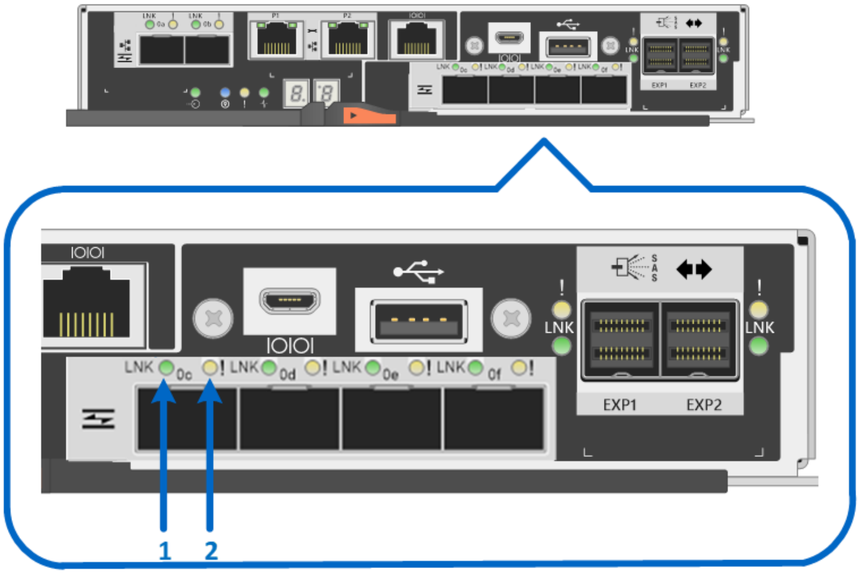
Table 24) 2-port and 4-port optical HIC (16Gb FC or 10Gb iSCSI) LED definitions.

LED name	Color	LED on	LED off
Host port link/activity	Green	• Solid: link up with no activity. • Blinking: link up with activity.	Link is down.
Host port attention	Amber	Port requires operator attention.	Normal status.

4-Port 32Gb FC HIC LEDs

The E2800 controller beginning with SANtricity 11.50 supports a 4-port 32Gbps FC HIC that offers the ability to auto-negotiate down to 16Gbps by using the 32Gbps SFP or the 16Gbps SFP. The new 32Gb FC HIC does require OM4 fiber cable to connect to switches or to connect directly to hosts. Figure 55 shows the LEDs for the 4-port 32Gbps FC HIC.

Figure 55) LEDs for the 4-port 32Gb FC HIC.



1. Host 32Gb FC Port 0c Link LED
2. Host 32Gb FC Port 0c Fault LED

Table 25 defines the LEDs on the 4-port 32Gbps FC HIC.

Table 25) LED definitions for the 4-port 32Gbps FC HIC.

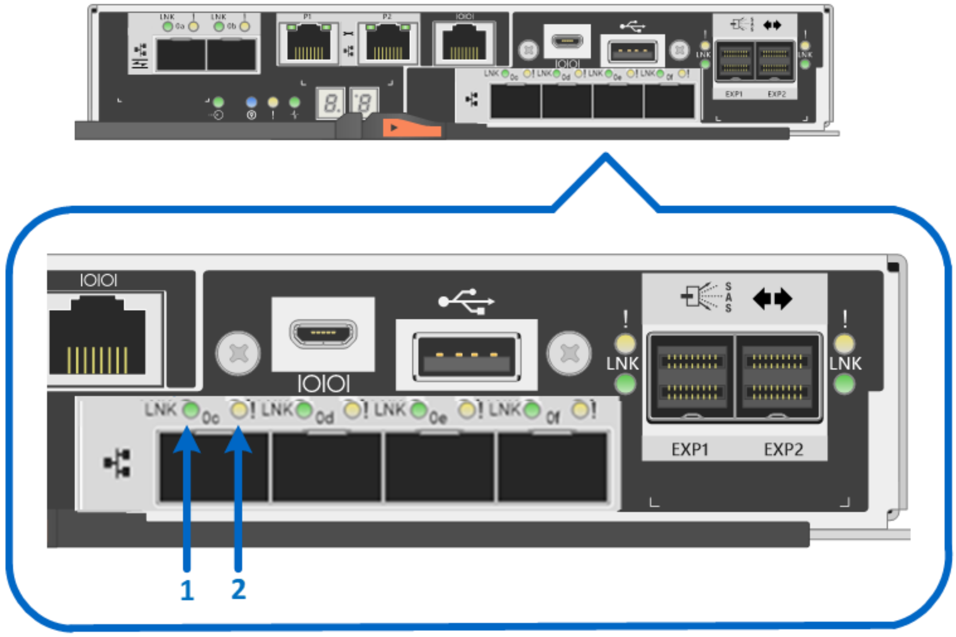
LED name	Color	LED on	LED off
Host port link/activity	Green	• Solid: link up with no activity. • Blinking: link up with activity.	Link is down.
Host port attention	Amber	Port requires operator attention.	Normal status.

Note: The LED definitions for port 0c repeat for ports 0d, 0e, and 0f.

4-Port 25Gb iSCSI HIC LEDs

The E2800 controller beginning with SANtricity 11.50 supports a 4-port 25Gbps iSCSI HIC that offers the ability to also run at 10Gbps by changing the port speed on each controller by using SANtricity System Manager without changing the 25Gbps SFP (25Gbps SFP supports 10Gbps speed). The new 25Gb iSCSI HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 56 shows the LEDs for the 4-port 25Gbps iSCSI HIC.

Figure 56) LEDs for the 4-port 25Gb iSCSI HIC.



1. Host 25Gb iSCSI Port 0c Link LED
2. Host 25Gb iSCSI Port 0c Fault LED

Table 26 provides the LED definitions for the 4-port 25Gb iSCSI HIC.

Table 26) LED definitions for the 4-port optical 25Gb iSCSI HIC.

LED speed (left side)	LED activity (right side)	Link rate	Color
On	On	Link operating at 25Gbps; no activity	Green
	Blinking	Link operating at 25Gbps with active I/O in progress	Green
Off	On	Link operating at 10Gbps; no activity	Green
	Blinking	Link operating at 10Gbps with active I/O in progress	Green
Off	Off	Link down	Not applicable

Note: The LED definitions for port 0c repeat for ports 0d, 0e, and 0f.

Setting the shelf ID with the ODP pushbutton

The shelf ID for the controller shelves and drive shelves can be changed externally by using the ODP push button. Figure 57, Figure 58, and Figure 59 show the push button for the E2812 (DE212C), E2824 (DE224C), and E2860 (DE460C), respectively.

Figure 57) ODP on the E2812 or DE212C (front bezel or end caps removed).

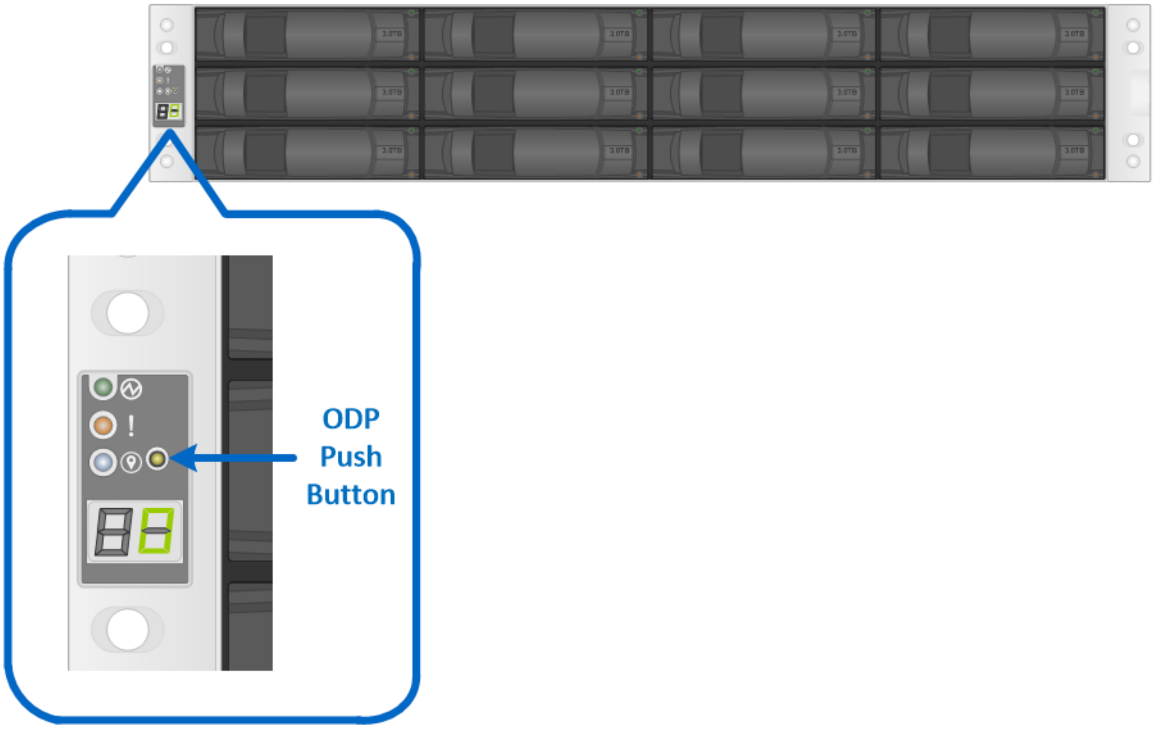


Figure 58) ODP on the E2824 or DE224C (front bezel or end caps removed).

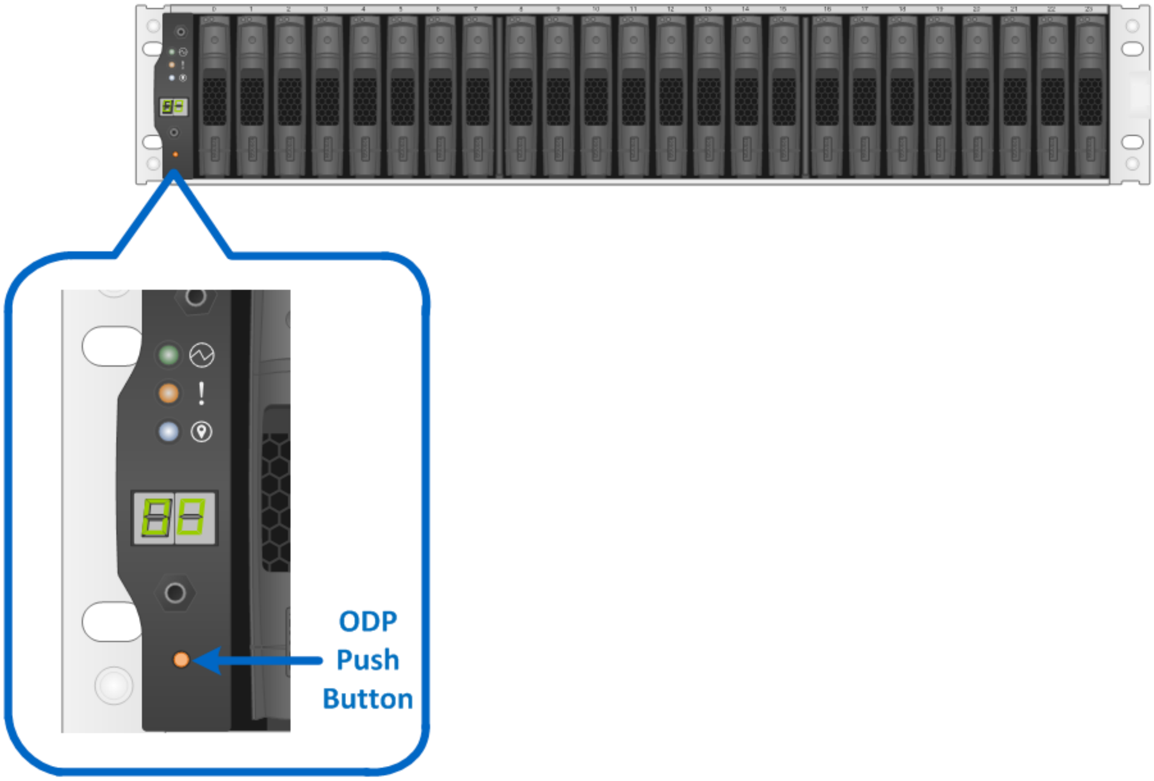
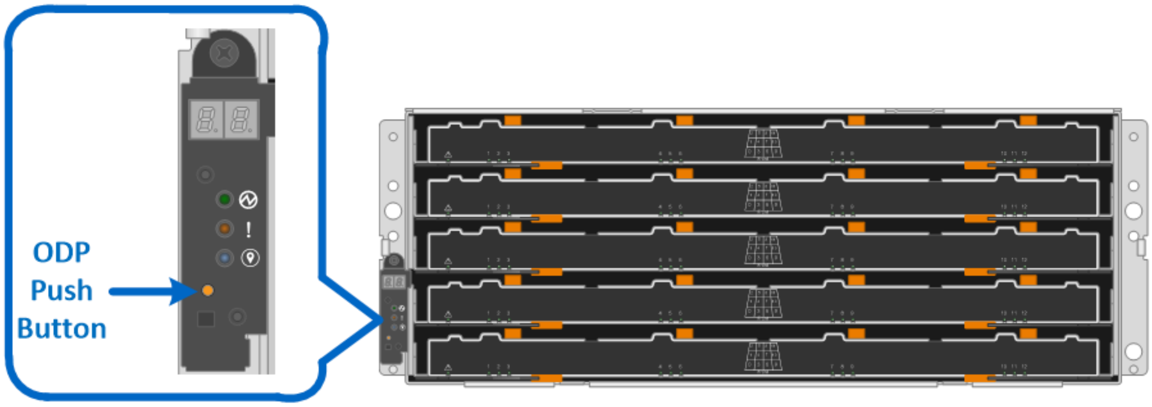


Figure 59) ODP on the E2860 or DE460C (front bezel removed).



Follow these steps to modify the shelf ID:

1. Turn on the power to the shelf if it is not already on.
2. Remove either the front bezel or the left end cap to locate the ODP push button.
3. Change the first number of the shelf ID by pressing and holding the button until the first number on the digital display blinks, which can take 2 to 3 seconds.
4. If the ID takes longer than 2 to 3 seconds to blink, press the button again, making sure to press it in all the way. This action activates the shelf ID programming mode.
5. Press the button to advance the number until you reach the desired number from 0 to 9. The first number continues to blink.
6. Change the second number of the shelf ID by pressing and holding the button until the second number on the digital display blinks, which can take 2 to 3 seconds. The first number on the digital display stops blinking.
7. Press the button to advance the number until you reach the desired number from 0 to 9. The second number continues to blink.
8. Lock in the desired number and exit the programming mode by pressing and holding the button until the second number stops blinking, which can take 2 to 3 seconds.
9. Repeat steps 1 through 8 for each additional shelf.

   Note: It is also possible to modify the shelf ID using SANtricity System Manager.

For additional information about the E2800 storage systems and related hardware, see the E2800 series documentation on the E-Series and SANtricity documentation resources page.

Drive shelves

The E2800 controller shelf supports 12, 24, or 60 drives based on the shelf model (DE212C, DE224C, or DE460C, respectively), but the system capacity can be further expanded by adding additional expansion drive shelves to the controller shelf. The E2800 supports up to 4 total shelves, the controller shelf plus three expansion drive shelves, for a maximum of 180 HDDs (120 SSDs). Table 27 shows the drive shelf options.

Table 27) Drive shelf options for E2800.

Property	DE212C	DE224C	DE460C	DE1600	DE5600	DE6600
Form factor	2RU	2RU	4RU	2RU	2RU	4RU
Drive size	3.5"	2.5"	3.5"	3.5"	2.5"	3.5"

Property	DE212C	DE224C	DE460C	DE1600	DE5600	DE6600
	2.5" (with bracket)		2.5" (with bracket)			2.5" (with bracket)
Drive types	NL-SAS SSD	SAS SSD	SAS NL-SAS SSD	NL-SAS	SAS SSD	SAS NL-SAS SSD
Total drives	12	24	60	12	24	60
Drive interface	12Gb SAS	12Gb SAS	12Gb SAS	6Gb SAS	6Gb SAS	6Gb SAS

Note: DE1600, DE5600, and DE6600 are supported only as part of in-place data migration from E2700/E5400/E5500/E5600 to E2800.

Drive shelf configurations

E2800 controllers can be paired with all six E-Series shelves, and the shelves can be mixed in the same storage system. The older 6Gb SAS 2 drive shelves (DE1600, DE5600, and DE6600) are not covered in detail in this document. For more information, see the E-Series Disk Shelves documentation. The following sections provide detailed information about the 12Gb SAS 3 drive shelves (DE212C, DE224C, and DE460C).

DE212C drive shelf

The DE212C is a 2RU shelf that holds up to twelve 3.5-inch drives or 2.5-inch SSDs with adapter. It features dual high-speed 12Gb SAS 3 I/O modules (IOMs) and dual ENERGY STAR Platinum certified high-efficiency power supplies (913W) with integrated fans, in a duplex system. It is fully redundant with hot-swappable components.

Figure 60, Figure 61, and Figure 62 show the front and rear views of the DE212C drive shelf.

Figure 60) DE212C front view with end caps.

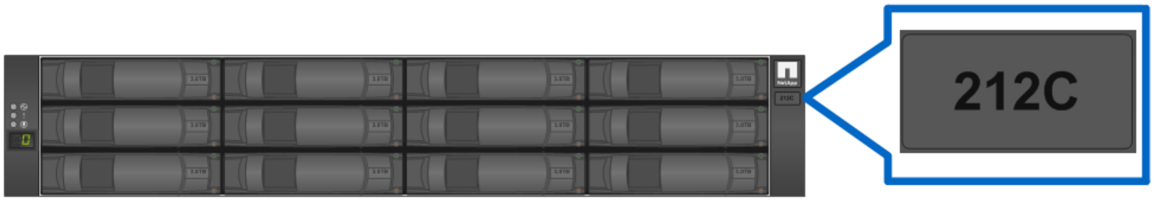


Figure 61) DE212C front view without end caps.

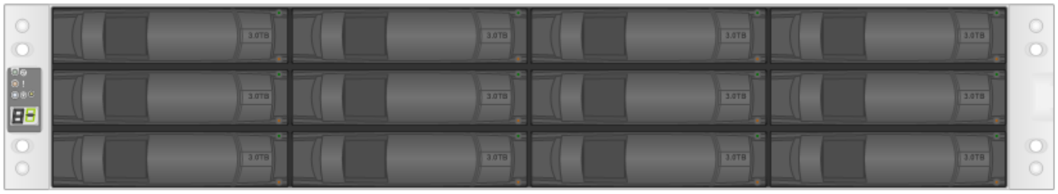
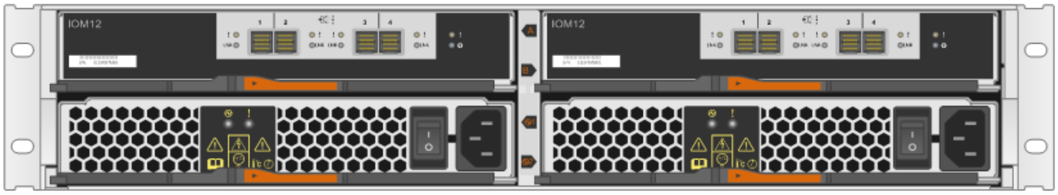


Figure 62) DE212C rear view.



DE224C drive shelf

The DE224C is a 2RU shelf that holds up to 24x 2.5-inch drives. It features dual high-speed 12Gb SAS 3 IOMs and dual ENERGY STAR Platinum certified high-efficiency power supplies (913W) with integrated fans, in a duplex system. It is fully redundant with hot-swappable components.

Figure 63, Figure 64, and Figure 65 show the front and rear views of the DE224C drive shelf.

Figure 63) DE224C front view with end caps.

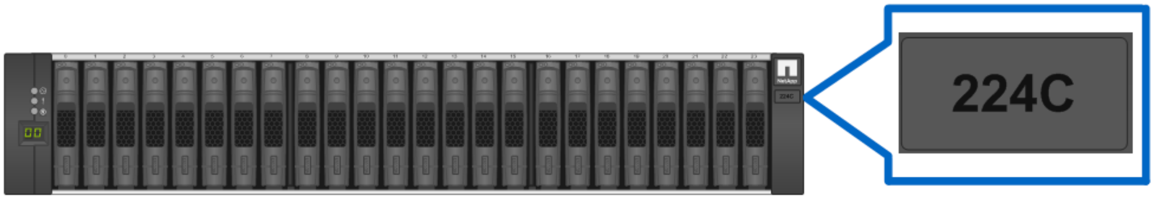


Figure 64) DE224C front view without end caps.

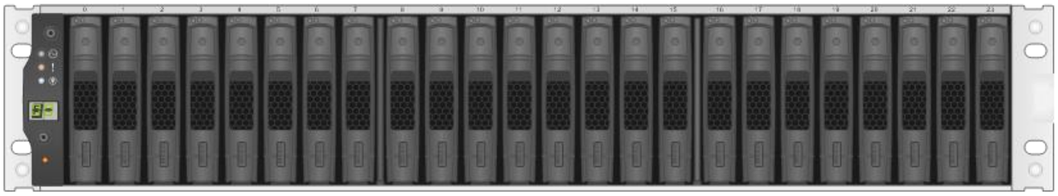
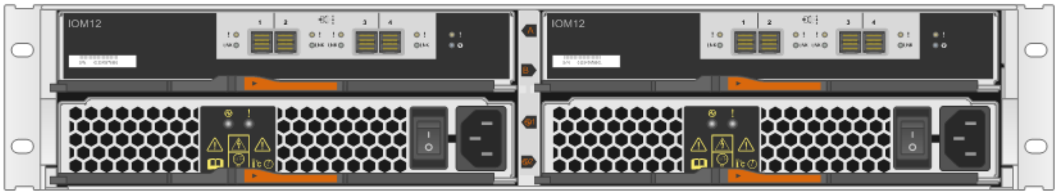


Figure 65) DE224C rear view.



DE460C drive shelf

The DE460C is a 4RU shelf that holds up to sixty 3.5-inch or 2.5-inch drives. It features dual high-speed 12Gb SAS 3 IOMs and dual ENERGY STAR Platinum certified high-efficiency power supplies (2325W) with separate dual fan modules, in a duplex system. From a controller, power, and cooling perspective, it is fully redundant with hot-swappable components. From a drive maintenance perspective, simply open a running drawer and insert new drives in open slots or replace a defective drive nondisruptively to other running drives in the drawer.

Figure 66, Figure 67, and Figure 68 show the front and rear views of the DE460C drive shelf.

Figure 66) DE460C front view with bezel.

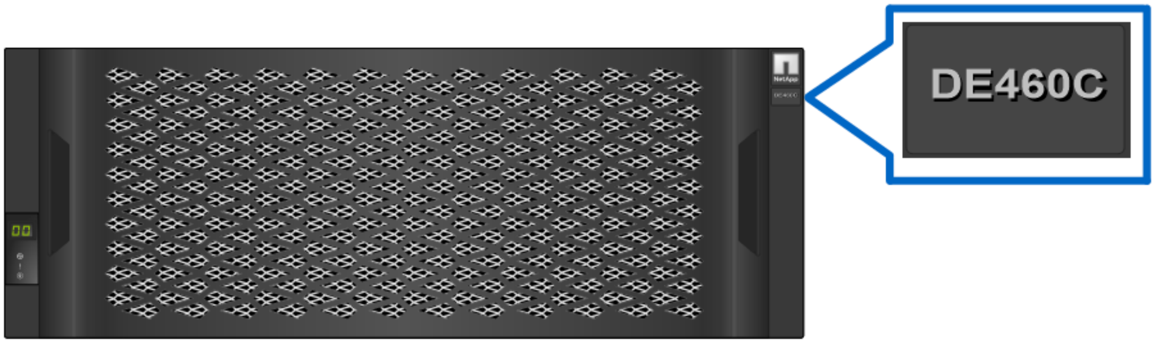


Figure 67) DE460C front view without bezel.

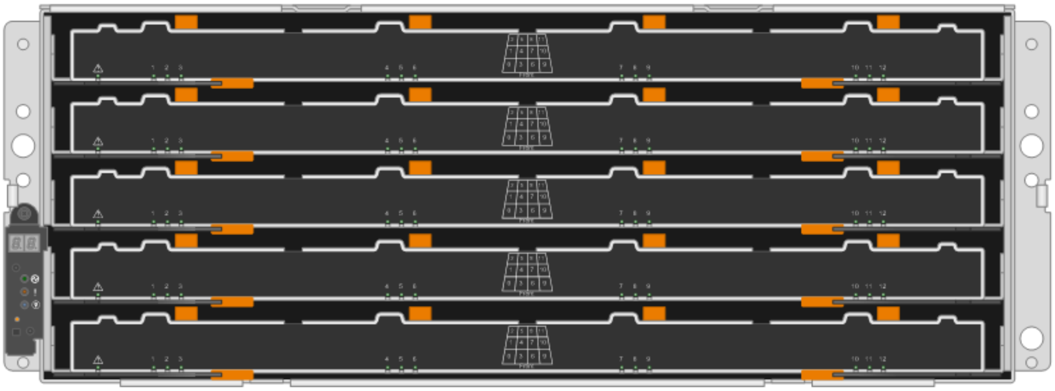
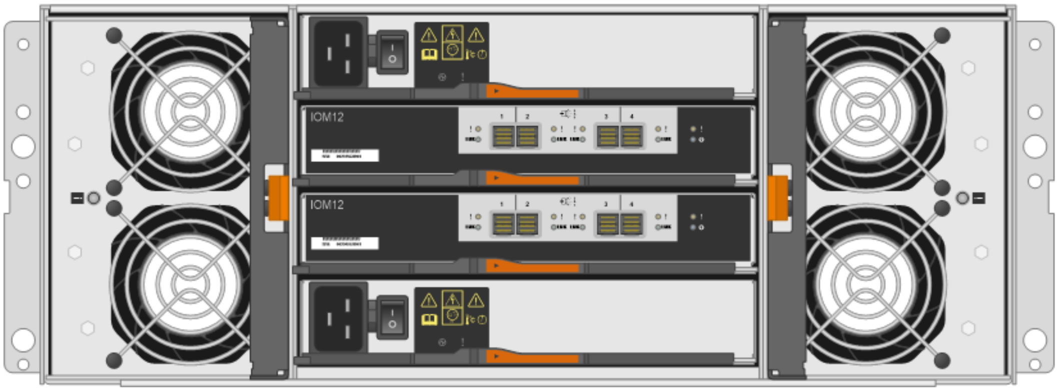


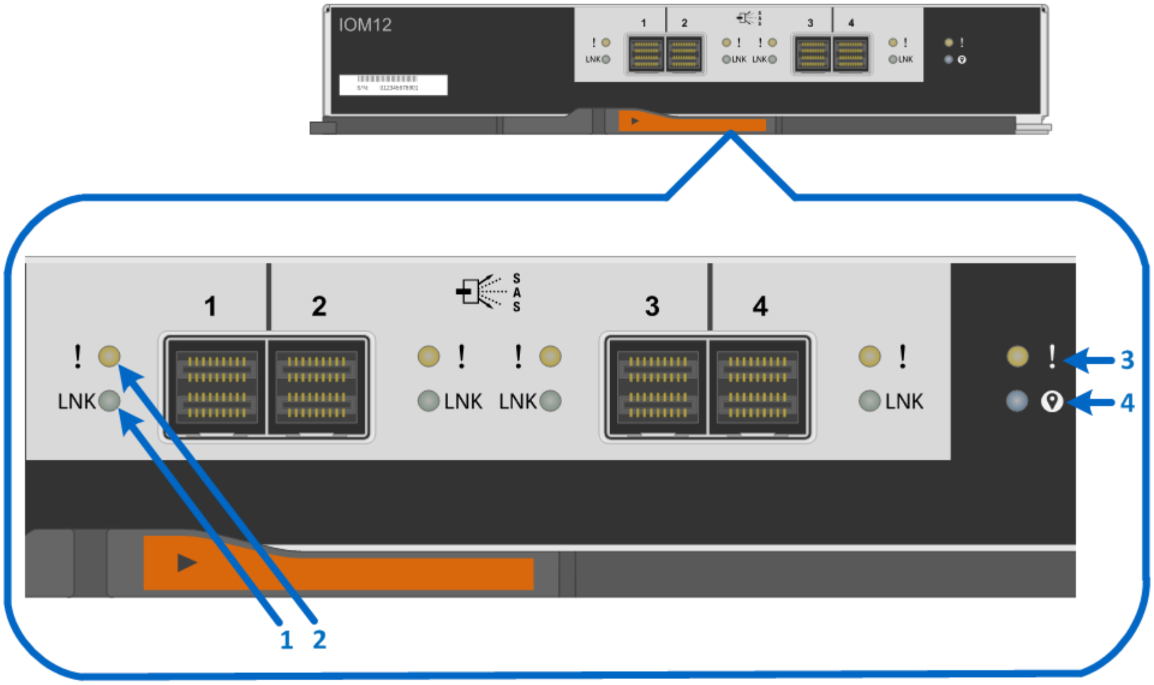
Figure 68) DE460C rear view.



IOM LED definitions

Figure 69 shows the LEDs for the 4-port 12Gb SAS 3 IOM. LEDs are highlighted only for SAS expansion port 1 and for the IOM. SAS expansion ports 2 through 4 have similar LEDs.

Figure 69) LEDs for IOM.



1. Drive Expansion Port 1 Link LED
2. Drive Expansion Port 1 Fault LED
3. Attention LED
4. Locate LED

Table 28 defines the LEDs for the IOM.

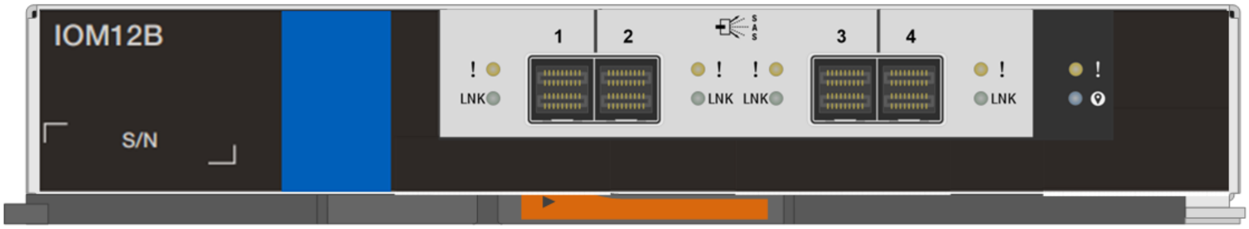
Table 28) IOM LED definitions.

LED name	Color	LED on	LED off
Drive expansion link	Green	Link is up.	Link is down.
Drive expansion fault	Amber	At least one of the four PHYs in the output port is working, but another PHY cannot establish the same link to the expansion output connector.	Port is optimal (all PHYs in the port are up).
Attention	Amber	Some fault exists in the IOM.	Normal status.
Locate	Blue	Request to locate the enclosure is active.	Normal status.

IOM12B

A new IOM the IOM12B has been added for disk expansion shelves. The IOM12B is only supported with SANtricity 11.70.2 and newer SANtricity versions. IOM12 and IOM12B are not supported in the same shelf but can exist in the same stack. Figure 70 shows the new IOM12B.

Figure 70) IOM12B.



Drive LED definitions

Figure 71 and Figure 72 show the LEDs on the drive carriers for the E2812 and E2824, respectively.

Figure 71) E2812 drive carrier LEDs.

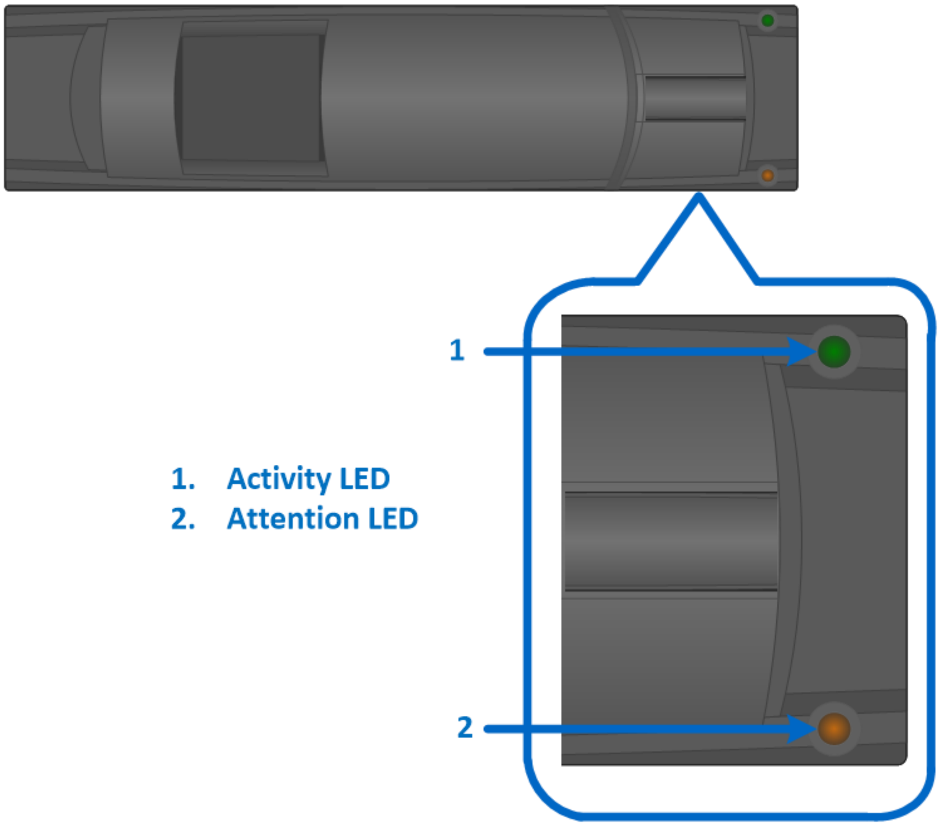


Figure 72) E2824 drive carrier LEDs.

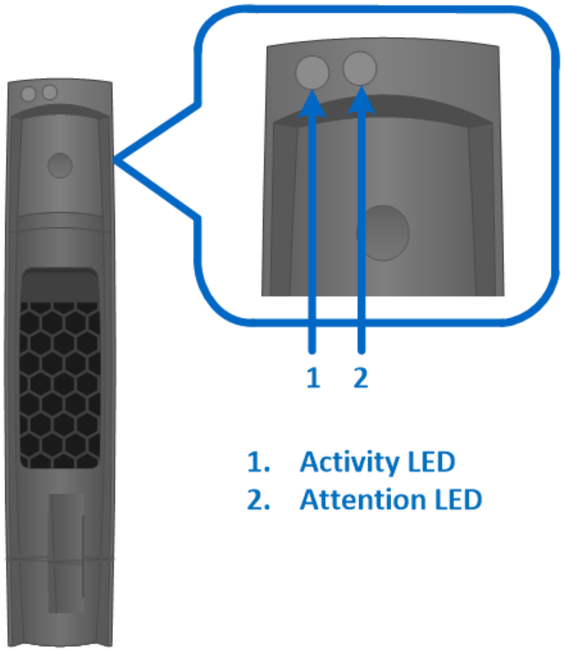


Table 29 defines the LEDs for the drives.

Table 29) E2812 and #2824 drive LED definitions.

LED name	Color	LED on	LED off
Activity	Green	Drive has power.	Drive does not have power.
	Blinking green	The drive has power, and I/O is in process.	No I/O is in process.
Attention	Amber	An error occurred with the functioning of the drive.	Normal status.
Attention	Blinking amber	Drive locate turned on.	Normal status.

For the DE460C shelf, the drive activity and attention LEDs are displayed on the drawer (Figure 73). It has an attention LED (Figure 74) that displays when the drawer is open. The drawer and shelf also have attention LEDs to indicate the location of the drive (Figure 73). Note that the drive activity LED is not illuminated for a failed drive.

Figure 73) E2860 shelf and drawer attention LEDs.

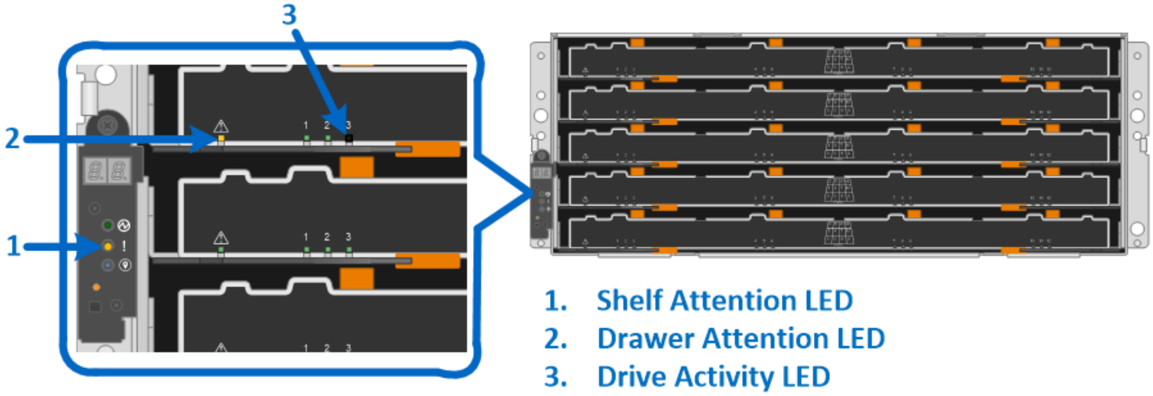


Figure 74) E2860 drive attention LED.

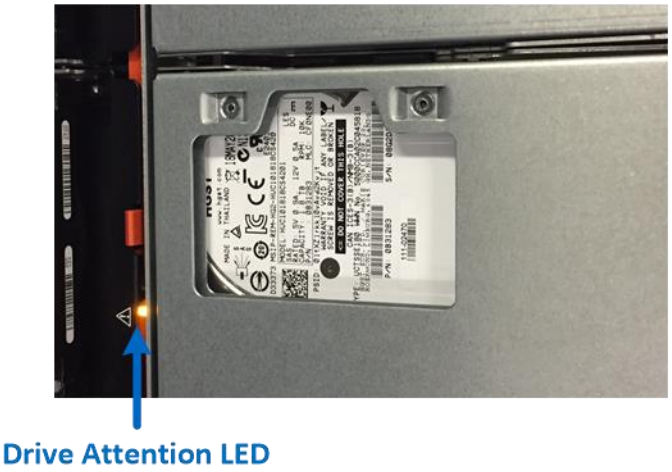


Table 30 defines the LEDs for the drives, drawers, and shelf of the E2860.

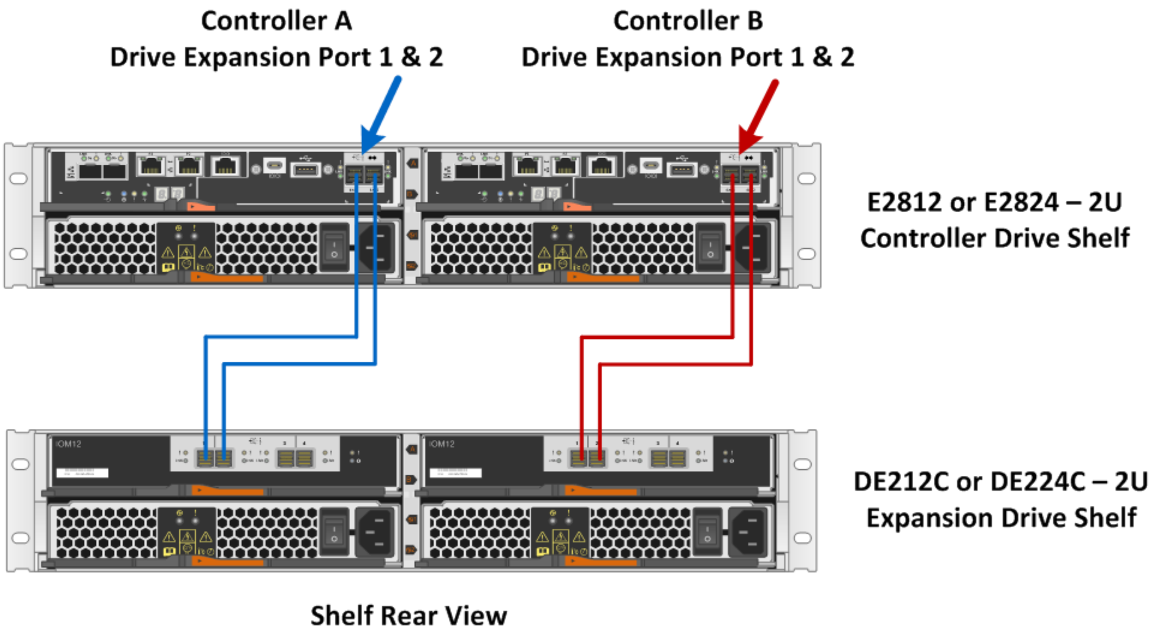
Table 30) E2860 drive LED definitions.

LED name	Color	LED on	LED off
Drive activity	Green	Drive has power.	Drive does not have power, or an error occurred with the functioning of the drive.
	Blinking green	The drive has power, and I/O is in process.	Drive does not have power, or an error occurred with the functioning of the drive.
Shelf attention	Amber	An error occurred with the functioning of a drive.	Normal status.
Drawer attention	Amber	An error occurred with the functioning of a drive.	Normal status.
Drawer attention	Blinking amber	Drive locate turned on.	Normal status.
Drive attention	Amber	An error occurred with the functioning of the drive.	Normal status.
Drive attention	Blinking amber	Drive locate turned on.	Normal status.

Greenfield installation

E2800 storage systems use two cabling methods: single stack and dual stack. The single-stack method is used only when the storage system has a controller shelf and a single drive shelf, as shown in Figure 75.

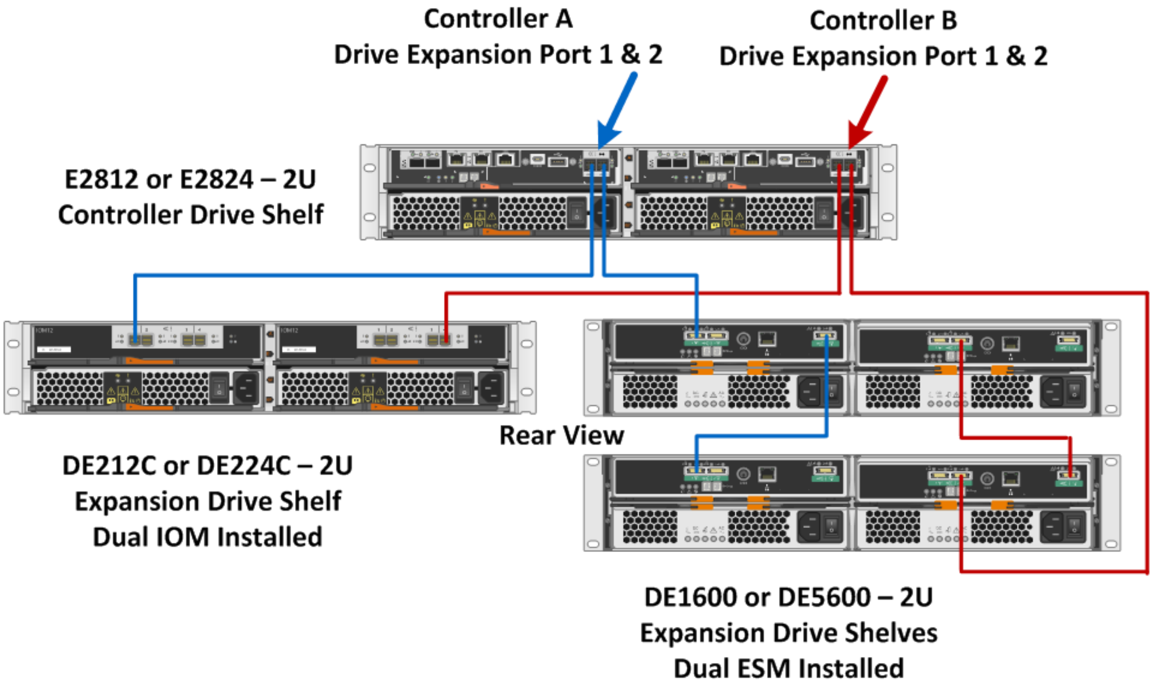
Figure 75) E2800 single-stack system configuration.



For E2800 storage systems with two or more drive shelves or a mix of SAS 3 and SAS 2 drive shelves, use the dual-stack cabling method (Figure 76).

Note: For optimal performance, SAS 2 and SAS 3 drive shelves should be isolated into different stacks.

Figure 76) E2800 storage system dual-stack configuration with SAS 3 and SAS 2 shelves.



For simplex controller systems, use the same cabling methods shown in Figure 75 and Figure 76 (blue paths) for the A-side controller as appropriate based on whether the system has just 12Gb drive shelves versus 12Gb shelves and 6Gb shelves connected to the same E2800 controller shelf.

Note: Only use dual-stack cabling if you have a mix of 12Gb and 6Gb expansion drive shelves. Otherwise, use the single-stack cabling method when all expansion drive shelves are new generation 12Gb shelves.

Failure to cable drive shelves correctly can lead to a semi-lockdown state on the storage system that does not allow changes to the system configuration until the cabling issue is resolved.

Drive shelf hot add

E-Series storage systems support the addition of expansion drive shelves and drive capacity to running storage systems. To prevent the loss of data availability to existing drive shelves when new drive shelves are added, the storage system must be cabled according to the cabling best practices recommended by NetApp. Two independent SAS channel paths must be available to the drive shelves so that one path can be interrupted when a drive shelf is added to the storage system while the other path maintains data availability to existing shelves.

After additional drive shelves have been successfully added to a storage system, SANtricity can be used to add capacity to existing volume groups and disk pools or to create volume groups and disk pools.

When adding a drive shelf to an existing E-Series storage system, it is critical to follow the specific hot-add installation steps in the order specified by the E-Series Hardware Cabling Guide.

Note: For more information and assistance with adding a drive shelf to an existing production E-Series system, go to http://mysupport.netapp.com/eseries and click the Cable the Hardware link or contact NetApp Customer Support Delivery.

Figure 77 and Figure 78 show the hot-add connectivity when a drive shelf is added as the last shelf in the system. The E2812 and E2824 are shown; the cabling for E2860 is similar.

Figure 77) Drive shelf hot-add A-side cabling.

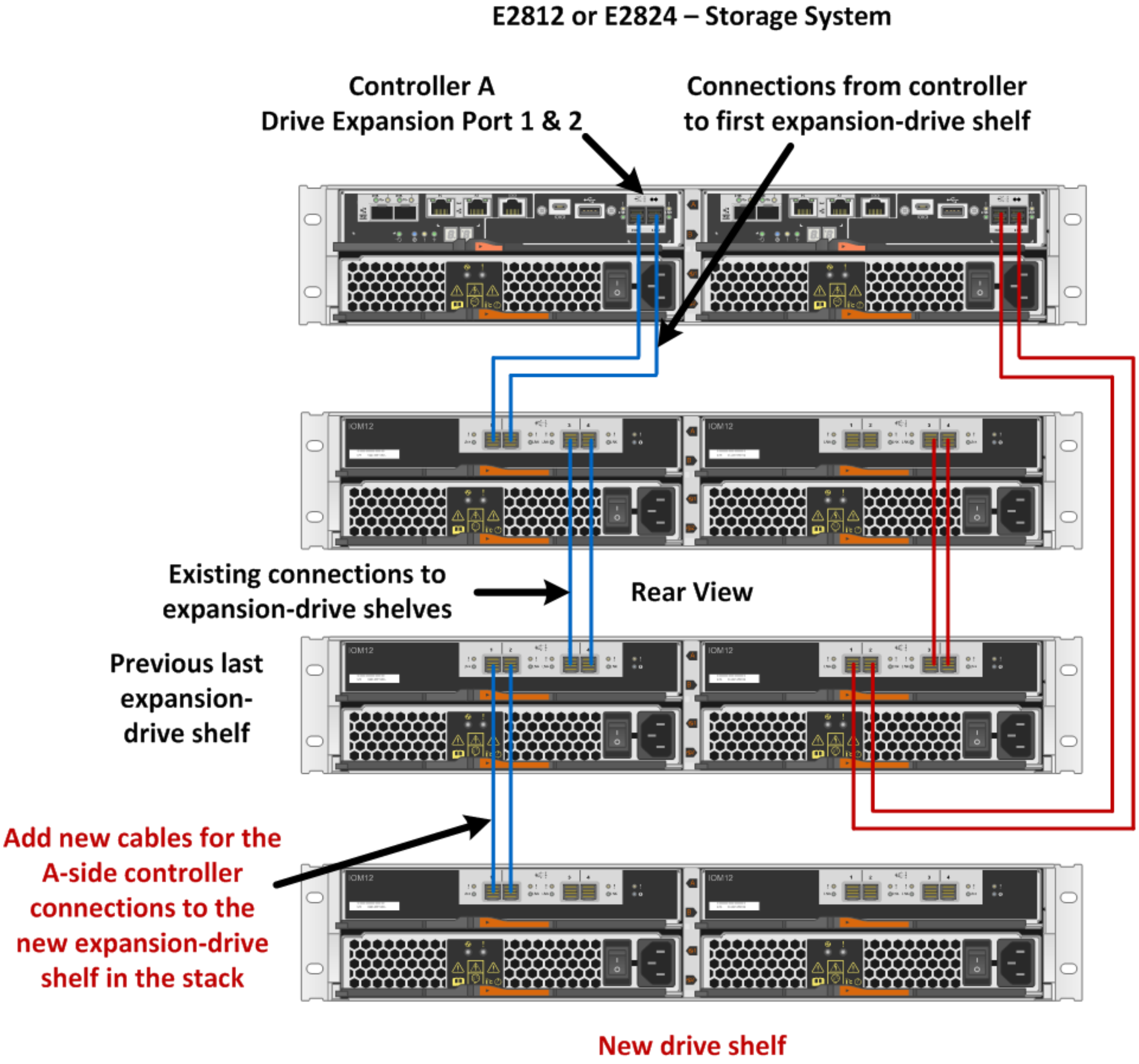
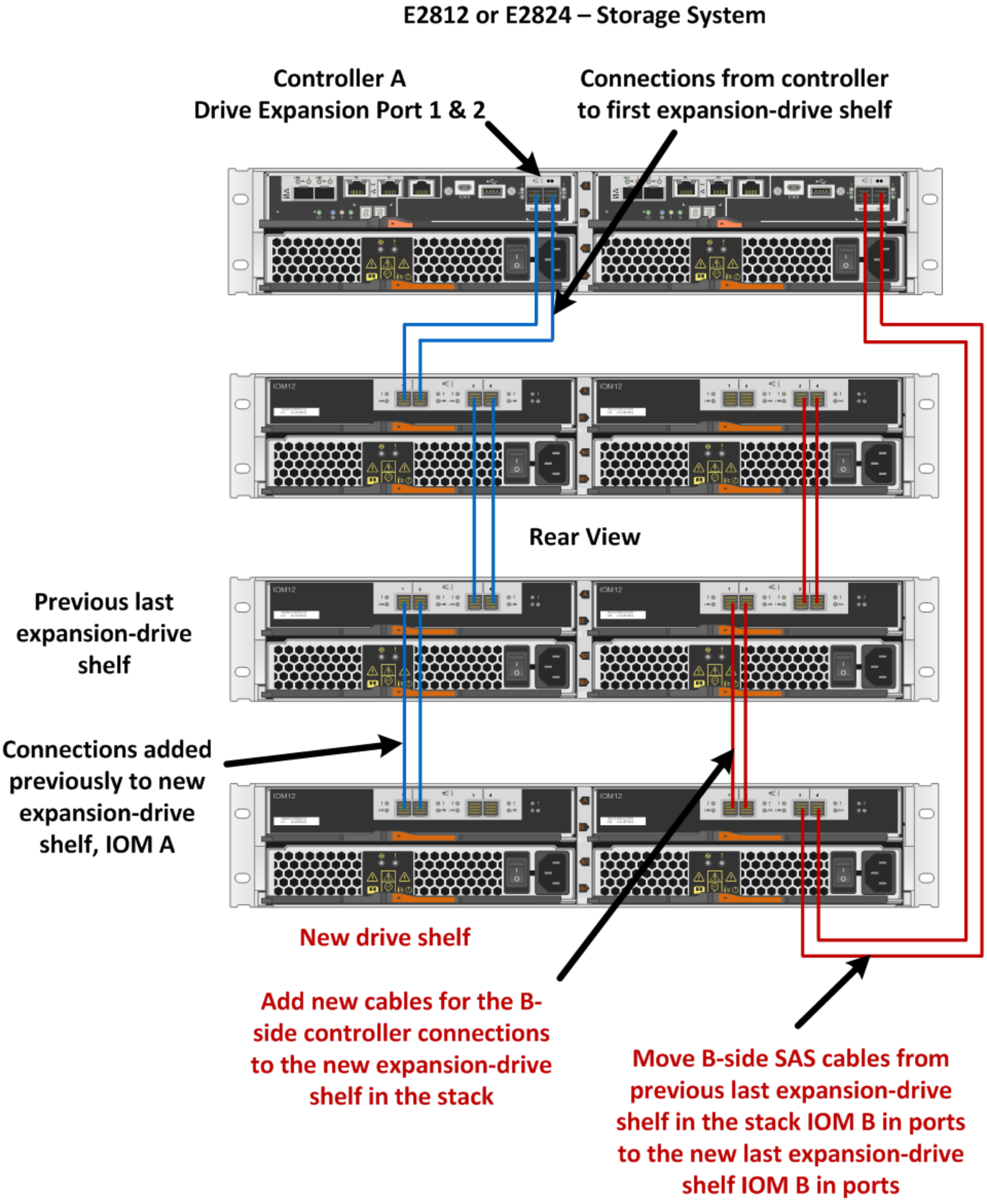


Figure 78) Drive shelf hot-add B-side cabling.


E2812 or E2824 – Storage System
Controller A
Drive Expansion Port 1 & 2
Connections from controller
to first expansion-drive shelf
Rear View
Previous last
expansion-drive
shelf
Connections added
previously to new
expansion-drive
shelf, IOM A
New drive shelf
Add new cables for the B-side controller connections to the new expansion-drive shelf in the stack
Move B-side SAS cables from previous last expansion-drive shelf in the stack IOM B in ports to the new last expansion-drive shelf IOM B in ports

Best practices

Plan carefully for any drive shelf hot-add activity on production storage systems. Verify that the following conditions are met:

- The existing power infrastructure can support the additional hardware.

Best practices

- The cabling plan for the new shelf does not simultaneously interrupt the SAS expansion paths for controller A and controller B.
- The new expansion port 1 path is confirmed to be valid, and the new shelf is visible in the SANtricity management software before the expansion path 2 is disconnected and moved to the new shelf.

Note: Failure to preserve one active path to existing drive shelves during the procedure could potentially result in degradation/failure of LUNs during I/O activity.

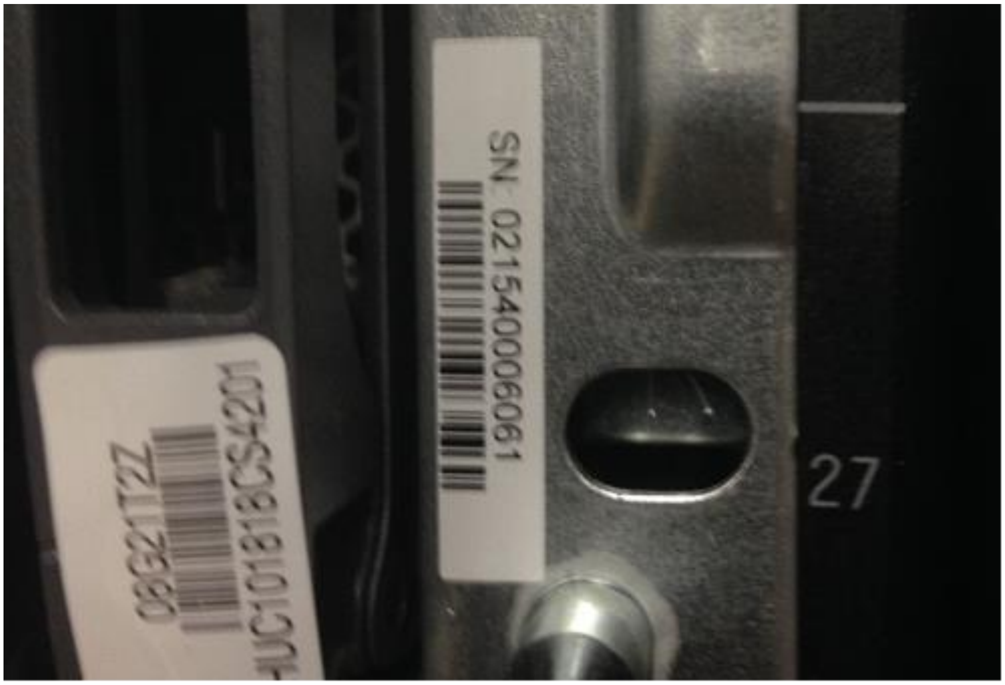
E-Series product support

NetApp E-Series storage systems are identified by the serial number (SN) of the E-Series system shelf, not the SNs of the individual controllers in the E-Series system shelf. The correct SN must be registered for an E-Series system because only the SN of the E-Series system shelf can be used to log a support case with NetApp.

Controller shelf serial number

The E2800 storage systems are shipped preconfigured from the factory (controllers have HICs and batteries installed, and controllers are installed in the controller shelf). The chassis serial number is printed on a white label affixed to the controller shelf behind the right end cap on the front of the chassis. The SN is identified by the text "SN," which is shown in Figure 79.

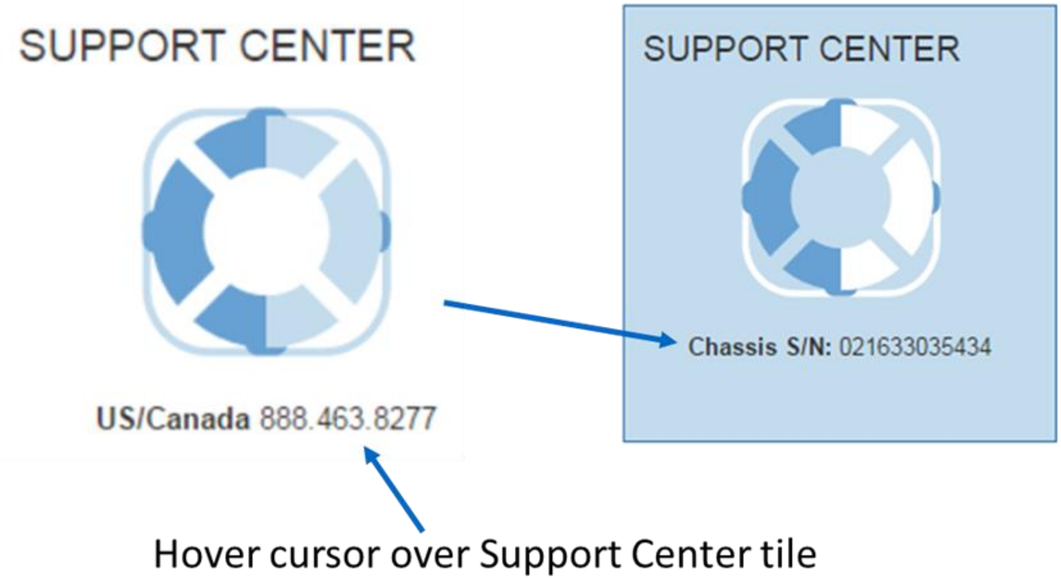
Figure 79) Controller shelf SN.



The SN is also included on the shelf UL sticker. However, this sticker is often not visible after the shelves are installed in a rack.

On a running storage system, the chassis serial number is also available through SANtricity System Manager by selecting the Support tab and positioning your cursor over the Support Center tile, as shown in Figure 80.

Figure 80) SANtricity System Manager Support Center tile showing chassis serial number.



SUPPORT CENTER

US/Canada 888.463.8277

SUPPORT CENTER

Chassis S/N: 021633035434

License keys

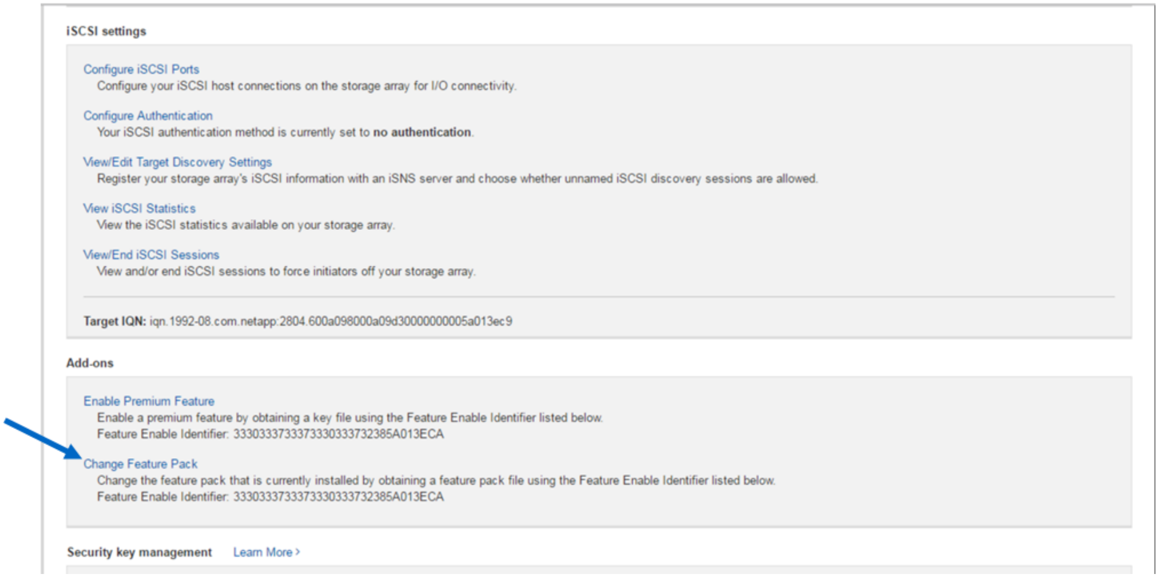
E-Series storage arrays use two types of license keys. One type of key file is for premium features, and the other type of key file is used to change the storage system feature pack (changes the host interface protocol). For the E2800, all features are enabled out of the box.

Note: The encryption feature is disabled for systems sold in export-limited countries.

When E2800 controllers are equipped with either the 2-port optical baseboard or the 2 or 4-port optical 16Gb FC or 10Gb iSCSI HIC, feature pack keys are used to change the host interface protocol from FC to iSCSI or from iSCSI to FC. The process to generate a new feature pack key for your storage array is the same as generating a premium feature key, except that the 11-digit key activation code for each package is available at no additional cost. This process is listed in the hardware upgrade instructions per controller type, on the E-Series and SANtricity documentation resources page.

After the feature pack file is downloaded to the host server, click Change Feature Pack (Figure 81). Follow the prompts, beginning with browsing to the feature pack file (Figure 82).

Figure 81) Change feature pack from Settings>System view.



iSCSI settings

Configure iSCSI Ports
Configure your iSCSI host connections on the storage array for I/O connectivity.

Configure Authentication
Your iSCSI authentication method is currently set to **no authentication**.

View/Edit Target Discovery Settings
Register your storage array's iSCSI information with an iSNS server and choose whether unnamed iSCSI discovery sessions are allowed.

View iSCSI Statistics
View the iSCSI statistics available on your storage array.

View/End iSCSI Sessions
View and/or end iSCSI sessions to force initiators off your storage array.

Target IQN: iqn.1992-08.com.netapp:2804.600a098000a09d30000000005a013ec9

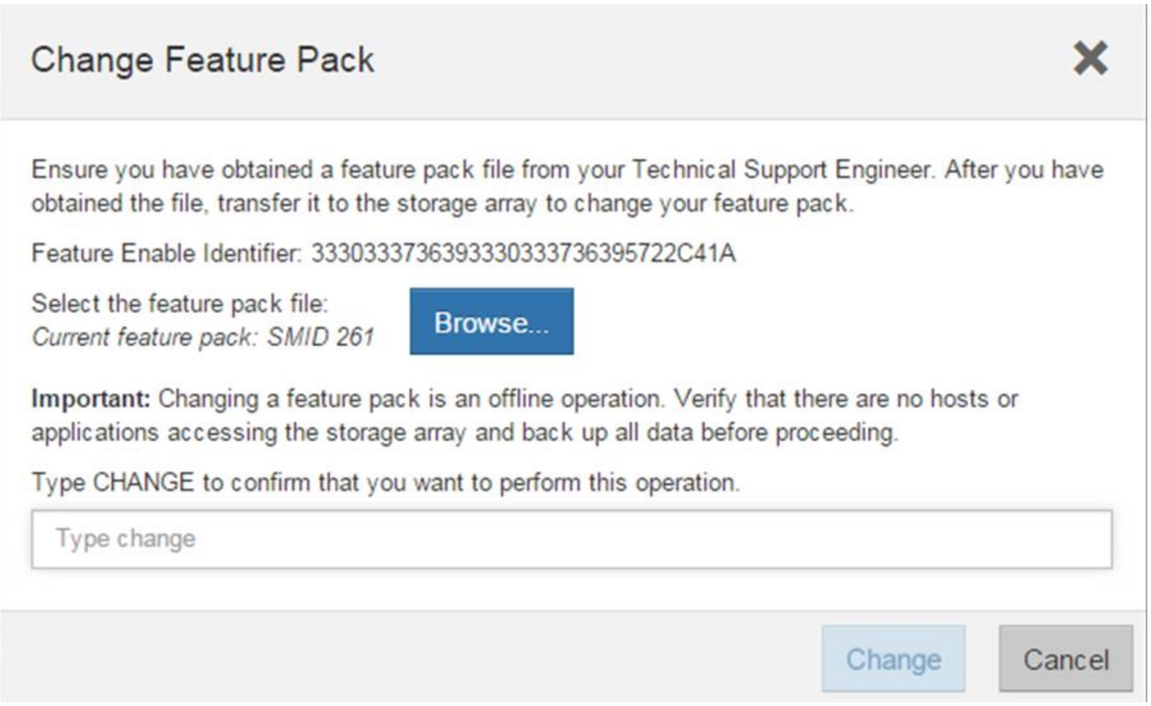
Add-ons

Enable Premium Feature
Enable a premium feature by obtaining a key file using the Feature Enable Identifier listed below.
Feature Enable Identifier: 33303337333733303337323885A013ECA

Change Feature Pack
Change the feature pack that is currently installed by obtaining a feature pack file using the Feature Enable Identifier listed below.
Feature Enable Identifier: 33303337333733303337323885A013ECA

Security key management Learn More >

Figure 82) Change feature pack.



Change Feature Pack

Ensure you have obtained a feature pack file from your Technical Support Engineer. After you have obtained the file, transfer it to the storage array to change your feature pack.

Feature Enable Identifier: 3330333736393330333736395722C41A

Select the feature pack file:
Current feature pack: SMID 261

Important: Changing a feature pack is an offline operation. Verify that there are no hosts or applications accessing the storage array and back up all data before proceeding.

Type CHANGE to confirm that you want to perform this operation.

Note: This causes the storage array to reboot. The new protocol is active after the system is back online.

For issues with accessing license key files, open a support ticket with NetApp Customer Support Delivery using the serial number of the registered controller shelf for the associated storage system.

Conclusion

The E-Series E2800 storage system enables customers to cut operational costs with ultra-dense drive shelves for capacity-hungry applications while improving storage utilization with the intuitive, easy-to-learn SANtricity System Manager web-based GUI.

E2800 storage systems offer balanced throughput performance for backup, video, and analytical environments, and other sequential workloads. It also supports demanding IOPS workloads in small and medium enterprise data centers. The wide choice of drive speeds, capacities, and storage features with multiple host connectivity interface options make the E2800-based storage system the optimal choice for environments where simplicity, seamless integration with wide-ranging workloads, and a streamlined price/performance product focus are the key elements for customer success.

With SANtricity Unified Manager capabilities, you can securely manage new-generation arrays. The enhanced SANtricity security features make the E2800 suitable for large enterprise environments with many employees, while maintaining setup simplicity for small and medium environments where a small team supports everything.

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- E-Series E2800 datasheet
  https://www.netapp.com/us/media/ds-3805.pdf
- E-Series and SANtricity 11 Documentation Center
  https://docs.netapp.com/ess-11/index.jsp
- E-Series and SANtricity Documentation Resources
  https://www.netapp.com/documentation/eseries-santricity/

Version history

Version	Date	Document version history
Version 1.0	November 2018	Initial release concurrent with SANtricity 11.50
Version 1.1	February 2019	Updated for SANtricity 11.50.1 release
Version 1.2	June 2019	Updated for SANtricity 11.50.2 release
Version 1.3	May 2020	Updated for SANtricity 11.60.2 release
Version 1.4	July 2021	Updated for SANtricity 11.70.1 release
Version 1.5	February 2022	Updated for controllers with no base ports
Version 1.6	November 2022	Updated for IOM12B.
Version 2.0	July 2023	Updated for SANtricity 11.80.0 release.
Version 2.1	November 2024	Updated for SANtricity 11.90.0 release.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Trademark Information

TR-4725-1124