



Technical Report

Introduction to NetApp E-Series E5700 arrays

Feature overview with SANtricity

Mitch Blackburn, NetApp
November 2024 | TR-4724

Abstract

The NetApp® E-Series E5700 storage array delivers higher performance than the previous generation of E-Series arrays and supports up to 20% more capacity. The associated NetApp SANtricity® Unified Manager and System Manager provide enhanced security features for both array management and greater flexibility for the drive security feature. This report provides comprehensive E5700 product information including new hardware and software features introduced with the latest version of SANtricity.

TABLE OF CONTENTS

Introduction	6
SANtricity management features	9
Deployment	9
SANtricity Unified Manager navigation	12
SANtricity System Manager.....	18
SANtricity storage features	30
Drive encryption.....	30
SANtricity host and path management features	30
SANtricity reliability features	31
SANtricity data management features	32
SANtricity Remote Storage Volumes.....	33
SANtricity copy services features	34
SANtricity management integration	35
SANtricity Storage Plugin for vCenter.....	39
SANtricity software specifications for E5700 hardware	39
E5700 hardware configurations	41
Controller shelf configurations	41
E5700 hardware specifications.....	42
Controller host interface features.....	44
Hardware LED definitions.....	46
Setting the shelf ID with the ODP pushbutton.....	59
Drive shelves	60
Drive shelf configurations	60
Greenfield installation	66
Drive shelf hot add.....	67
E-Series product support.....	69
Controller shelf serial number.....	69
License keys.....	70
Conclusion	72
Where to find additional information	72
Version history.....	72

LIST OF TABLES

Table 1) Built-in roles and associated permissions.	23
Table 2) LDAP/RBAC required fields and definitions.	24
Table 3) SANtricity common host types and associated failover behavior.	31
Table 4) SANtricity features for long-term reliability.	31
Table 5) E5700 standard features that are included with SANtricity.	32
Table 6) SANtricity copy services features.	34
Table 7) SANtricity APIs and toolkits.	35
Table 8) Third platform plug-ins that use the SANtricity Web Services Proxy.	35
Table 9) SANtricity software boundaries for E5700-based storage systems.	39
Table 10) E5700 technical specifications.	42
Table 11) Table of available FP-SMIDs for E5700 controllers.	44
Table 12) FC host interface port speed and associated SFPs.	45
Table 13) iSCSI host interface port speed and associated SFPs.	45
Table 14) IB host interface port speed with associated cables and HCAs.	45
Table 15) E5700 controller shelf LED definitions (front panel).	48
Table 16) E5724 and E5760 controller shelf power and fan canister LED definitions.	50
Table 17) E-Series controller factory default Ethernet management port IP address assignment.	51
Table 18) Ethernet management port LED definitions.	52
Table 19) LED definitions for the controller base features.	53
Table 20) 16Gb FC/10Gb iSCSI baseboard host port LED definitions.	54
Table 21) Drive expansion port LED definitions.	54
Table 22) LED definitions for the 2-port 100Gb IB HIC.	55
Table 23) LED definitions for the 4-port 12Gb SAS HIC.	56
Table 24) LED definitions for the 4-port 32Gbps FC HIC.	57
Table 25) LED definitions for the 4-port optical 25Gb iSCSI HIC.	58
Table 26) Drive shelf options for E5700.	60
Table 27) IOM LED definitions.	63
Table 28) E5724 drive LED definitions.	64
Table 29) E5760 drive LED definitions.	65

LIST OF FIGURES

Figure 1) E5760 hybrid storage array with the front bezel off.	6
Figure 2) E5724 storage array front and rear views.	7
Figure 3) E5700 controller shown with no base ports and optical base ports.	8
Figure 4) Managing a single E5700 with SANtricity System Manager.	9
Figure 5) Managing multiple new generation systems with SANtricity Unified Manager and SANtricity System Manager.	10
Figure 6) Final dialog box in the Web Services Proxy installation wizard.	11
Figure 7) SANtricity Unified Manager login page.	12
Figure 8) SANtricity Unified Manager landing page—discover and add arrays.	12

Figure 9) SANtricity Unified Manager landing page.....	13
Figure 10) Creating a group to organize arrays in SANtricity Unified Manager.	13
Figure 11) Creating a group in Unified Manager.	14
Figure 12) SANtricity Unified Manager showing a newly created group.	14
Figure 13) SANtricity Unified Manager Operations view.....	15
Figure 14) SANtricity System Manager home page.	20
Figure 15) System Manager Storage page.....	21
Figure 16) System Manager Hardware page.....	21
Figure 17) System Manager Settings page with new security tiles.....	21
Figure 18) System Manager Support page.....	22
Figure 19) System Manager Support Center.....	22
Figure 20) SANtricity System Manager directory server setup wizard.....	25
Figure 21) Role Mapping tab in the directory server settings wizard.	26
Figure 22) SANtricity System Manager views change according to user permission level.....	27
Figure 23) Initial step required to set up web server certificates.....	28
Figure 24) Expanded SANtricity System Manager Certificates tile.....	28
Figure 25) Remote Storage Volumes solution architecture overview.	34
Figure 26) Opening the API documentation.	36
Figure 27) Example expanding the Device-ASUP endpoint.	36
Figure 28) REST API documentation sample.....	37
Figure 29) Sample output from the Try It Out button.	37
Figure 30) Device-asup endpoint possible response codes and definitions.	38
Figure 31) Opening the CLI Command Reference.	39
Figure 32) E5724 front view (bezel removed).....	41
Figure 33) E5724 rear view.	41
Figure 34) E5760 front view (bezel removed).....	42
Figure 35) E5760 rear view.	42
Figure 36) E5760 with optional HIC installations.	46
Figure 37) ODP on the front panel of the E5724 controller shelf.	47
Figure 38) ODP on the front panel of the E5760 controller shelf.	47
Figure 39) Setting the shelf ID by using SANtricity System Manager.....	48
Figure 40) LEDs on the E5724 power fan canister (rear view).	49
Figure 41) LEDs on the E5760 power canister (rear view).	49
Figure 42) Controller settings dialog box.	50
Figure 43) Viewing system status information by using SANtricity System Manager.	51
Figure 44) Dual Ethernet management ports on the E5700 controller canister.	52
Figure 45) Controller module and array status LEDs.	52
Figure 46) Ports 0a and 0b 16Gb FC/10Gb iSCSI baseboard host port status LEDs.	53
Figure 47) LEDs for drive expansion ports.	54
Figure 48) LEDs on the 2-port 100Gb IB HIC.....	55

Figure 49) LEDs for the 4-port 12Gb SAS HIC.....	56
Figure 50) LEDs for the 4-port 32Gb FC HIC.....	57
Figure 51) LEDs for the 4-port 25Gb iSCSI HIC.....	58
Figure 52) ODP on the E5724 or DE224C (front bezel or end caps removed).....	59
Figure 53) ODP on the E5760 or DE460C (front bezel removed).....	59
Figure 54) DE224C front view with end caps.....	61
Figure 55) DE224C front view without end caps.....	61
Figure 56) DE224C rear view.....	61
Figure 57) DE460C front view with the bezel.....	62
Figure 58) DE460C front view without the bezel.....	62
Figure 59) DE460C rear view.....	62
Figure 60) LEDs for IOM.....	63
Figure 61) IOM12B.....	64
Figure 62) E5724 drive carrier LEDs.....	64
Figure 63) DE460C shelf and drawer attention LEDs.....	65
Figure 64) DE460C drive attention LED.....	65
Figure 65) E5724 expansion-drive shelf cabling example for the maximum DE224C shelf configuration.....	66
Figure 66) E5724 in a dual-stack configuration with 12Gbps and 6Gbps drive shelves installed.....	67
Figure 67) Drive shelf hot-add controller A expansion ports 1 and 2 cabling.....	68
Figure 68) Drive shelf hot-add controller B expansion ports 1 and 2 cabling.....	68
Figure 69) Controller shelf SN.....	69
Figure 70) SANtricity System Manager Support Center tile showing the chassis serial number.....	70
Figure 71) Change feature pack from Settings>System view.....	71
Figure 72) Change Feature Pack in SANtricity System Manager.....	71

Introduction

NetApp E-Series E5700 arrays running NetApp SANtricity software supports NVMe over Fabrics (NVMe-oF) host interface options for high-performance computing workloads: 100Gb NVMe over RDMA over Converged Ethernet (NVMe/RoCE) and InfiniBand (NVMe/IB). E5700 arrays also support NVMe over Fiber Channel (NVMe/FC). The E5700 continues to support the SCSI based host interfaces iSCSI, Fibre Channel (FC), SAS, and InfiniBand (IB) as well.

To provide cost-effective solutions for video surveillance, multimedia clustered file systems, backup and recovery applications, and other high-capacity workloads, the E5760 hybrid array continues to support larger-capacity drives that increase the maximum possible system capacity with 480 drives, or 8 total 4RU (rack unit) shelves. Currently, that provides up to 8.64PB of ultra-dense raw capacity in 32RUs using 18TB NL-SAS drives. This storage density continues to grow every 6 to 12 months as larger-capacity drives are qualified for E-Series systems. You can also hot-add drive shelves and new drives up to the maximum number per system, and the add process is nondisruptive to existing operations.

Figure 1 shows the front and rear views of the E5760 array. The front view shows how easy it is to open a drive drawer to install new drives or replace a failed drive without disrupting active I/O operations.

Note: The front bezel should be installed during normal operating conditions.

Figure 1) E5760 hybrid storage array with the front bezel off.

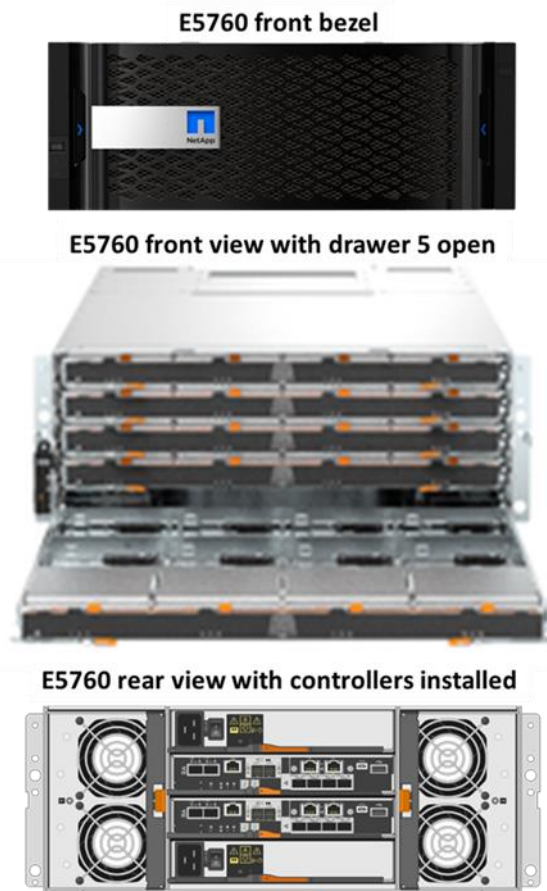


Figure 2 shows the E-Series E5724 hybrid array. For workloads that require fast storage, such as Splunk, high-performance databases, technical computing workloads with distributed parallel file systems, and specialty applications that require ultralow latency storage, E-Series E5724 hybrid arrays support up to

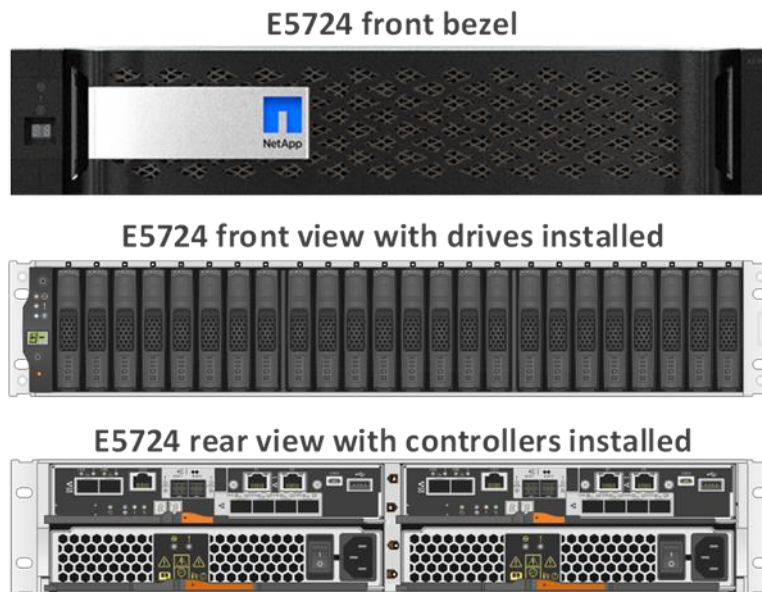
192 drives starting with a base set of 10K RPM SAS drives for the HDD tier. You can add more 10K SAS drives or up to 120 SSDs to build a fast tier in the same array. The E5724 also supports 15.3TB SSDs to build a large-capacity fast tier (~1.8PB fast, raw capacity).

For extreme flexibility, you can add a DE460C expansion-drive shelf that supports both SSDs and NL-SAS drives for workloads that require a fast tier and large-capacity tier.

Note: The DE460C shelf does not support 15.3TB SSDs.

The system can deliver consistent sub millisecond latency response times for small random workloads, or it can deliver up to 21GBps for large sequential read workloads and about 9GBps for large sequential write workloads.

Figure 2) E5724 storage array front and rear views.



Note: E5700 controllers are not offered in the 12-drive DE212C shelf. Only the E-Series E2800 controllers are offered in the 12-drive configuration (that is, E2812).

Figure 3 shows the E5700 controller with ports identified. Each E5700 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 to additional drive-expansion shelves.

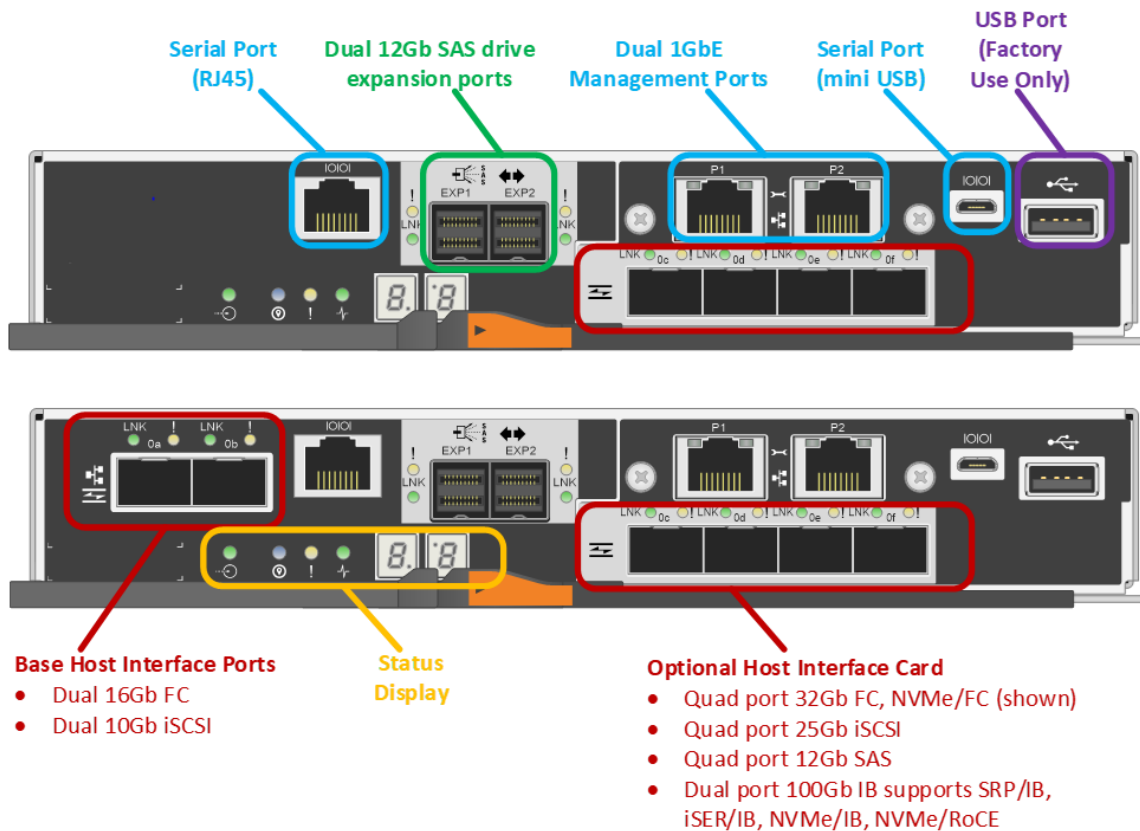
The E5700 controllers can either have no base ports or include two built-in host ports. The base ports can be either two 16Gb FC or two 10Gb iSCSI, and your choice of the following optional host interface cards (HICs):

- 4-port 12Gb SAS (mini-HD SAS 3 connector)
- 4-port 32Gb FC (OM4 fiber cable required)
- 4-port 25Gb iSCSI (OM4 fiber cable required)
- 2-port 100Gb IB (requires 100Gb-capable cables and HCAs) or 100Gb converged Ethernet (NVMe/RoCE protocol)

A software feature pack can be installed in the field to change the host protocol of the optical baseboard ports from FC to iSCSI or from iSCSI to FC. In addition, a software feature pack is used to select one of five protocol or transport options: iSER/IB, SRP/IB, NVMe/IB, NVMe/RoCE, or NVMe/FC.

Note: When the NVMe option is selected, the base ports on the E5700 are disabled and do not appear in the SANtricity System Manager UI. As a result, you also cannot use the SANtricity synchronous or asynchronous mirroring features because the FC or iSCSI ports are not available.

Figure 3) E5700 controller shown with no base ports and optical base ports.



Note: Starting with SANtricity OS 11.80 the USB (Factory Use Only) port is disabled.

For optical connections, you must order the appropriate SFP modules to meet the specific implementation requirements. Consult NetApp's [Hardware Universe](#) for a full listing of available host interface equipment and options. Figure 36 provides a close-up view of the E5700 HIC options.

Note: NetApp does not sell 100Gb host channel adapters (HCAs) or cables. Mellanox sells compatible cabling and HCAs.

For detailed instructions on changing the host protocol, go to the Maintain E-Series Hardware > Maintaining E5700 hardware section at [E-Series and SANtricity documentation resources](#).

For custom environments, E5700 arrays can be configured in mixed-shelf (DE224C and DE460C) architectures under the same 24-drive or 60-drive controller-drive shelf. As a result, the maximum capacity for an array is ultimately based on the choice of shelf and drive combination. Given the possible combinations, all capacities and drive counts discussed in this report assume that the arrays are not in a mixed-shelf architecture. For example, the maximum capacity for the E5760 is assumed to mean eight 4U60 DE460C shelves with 60 drives populated in each shelf for a total of the maximum 480 drive slots allowed. This maximum drive slot count would not apply if the system were configured with a 4U60 controller-drive shelf, two 4U60 expansion-drive shelves, and five 2U24 expansion-drive shelves (totals 8

shelves), even though the system would still technically be named an E5760. System model names are based on the controller-drive shelf and not the attached expansion shelves.

The E5700 continues the E-Series legacy of being fast, simple, reliable, and flexible SAN storage regardless of the workload. If the hosts are qualified with E-Series (most common host types are supported), if they use SAN access to the storage whether direct connect or fabric connected, and if the storage is managed at the host/file system level, E-Series E5700 hybrid arrays can support the workload.

E5700 arrays use the on-box web-based SANtricity System Manager GUI, which is bundled with SANtricity OS. The built-in Web Services REST API makes the E-Series product line easier than ever to integrate with your custom API-driven environment or to configure with an appliance in a bundled solution package.

The following sections provide broad product information, including technical details associated with the SANtricity Unified Manager.

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 E5700-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 configurations can be handled from SANtricity System Manager, simply bookmark each array in a web browser. Figure 4 illustrates this configuration.

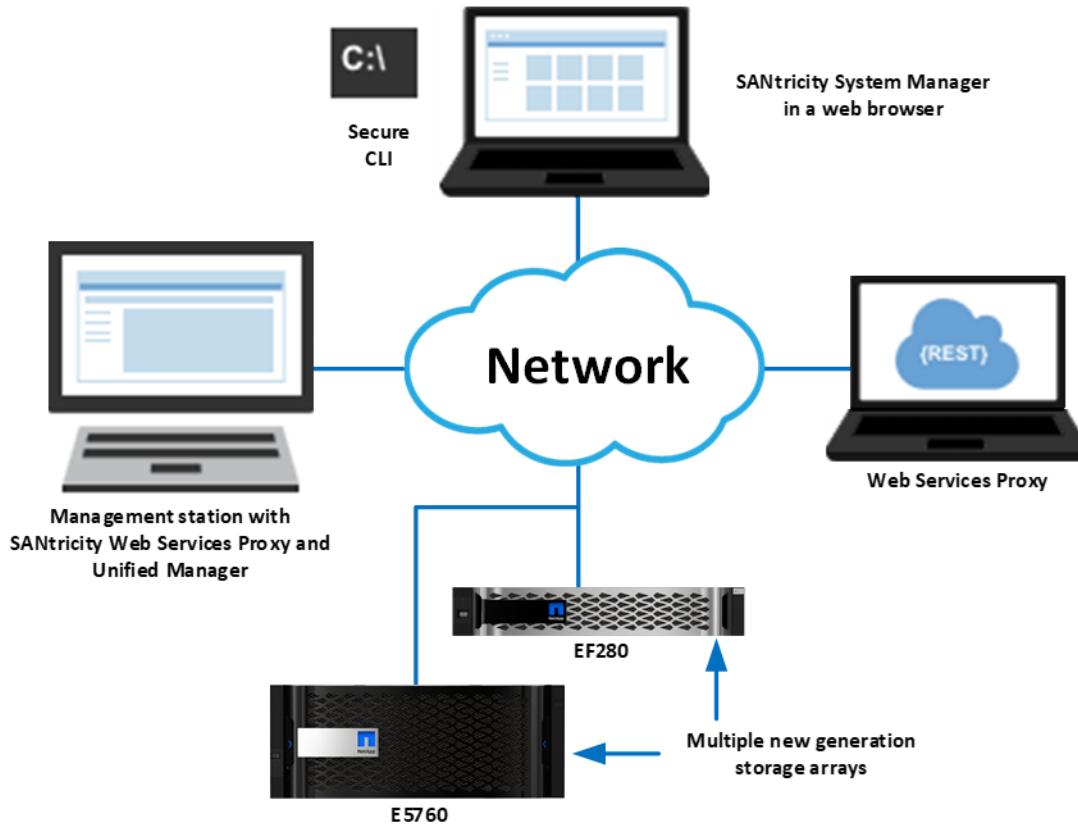
Figure 4) Managing a single E5700 with SANtricity System Manager.



Multiple storage arrays

If you have one or more storage arrays, you can install Unified Manager to manage your overall environment while still handling 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 5.

Figure 5) Managing multiple new generation systems with SANtricity Unified Manager and SANtricity System Manager.



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:

- Upgrade multiple arrays with the same controller type 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 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.

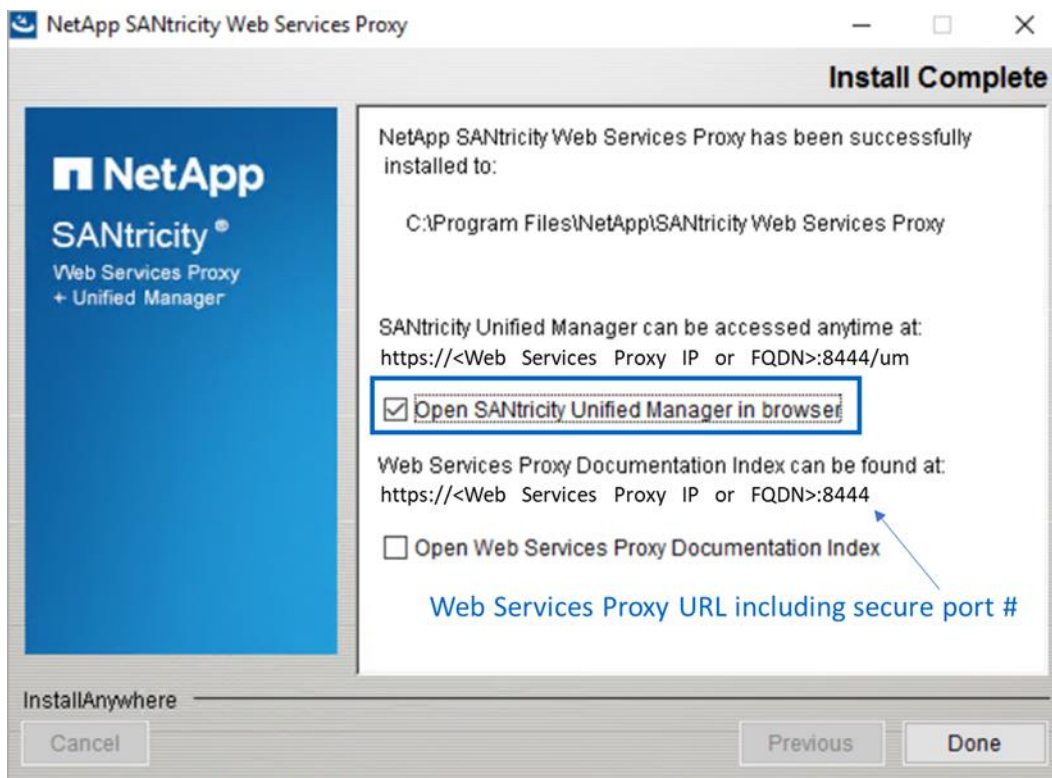
- Supports synchronous and asynchronous mirroring for all new generation arrays through the secure SSL interface. The EMW is only required if the initiator or target array is a legacy E2700, E5600/EF560, or earlier array model.

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.

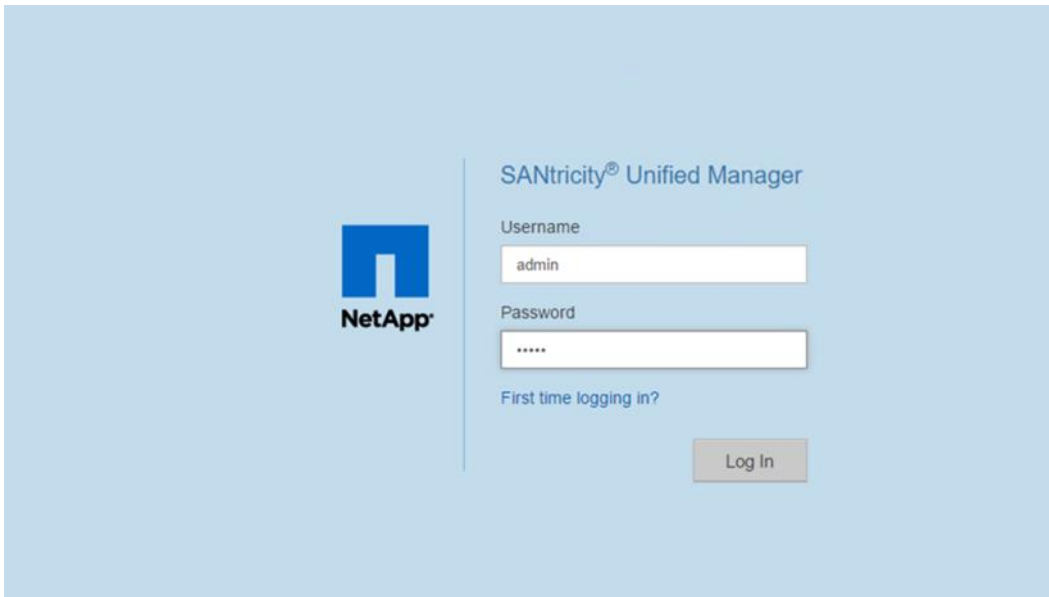
After the installation wizard completes, you can open Unified Manager, or you can directly access the SANtricity Web Services Proxy as shown in Figure 6.

Figure 6) Final dialog box in the Web Services Proxy installation wizard.



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 7) by adding `/um` to the URL. For example, `https://<proxy-FQDN>:<port #>/um`.

Figure 7) SANtricity Unified Manager login page.



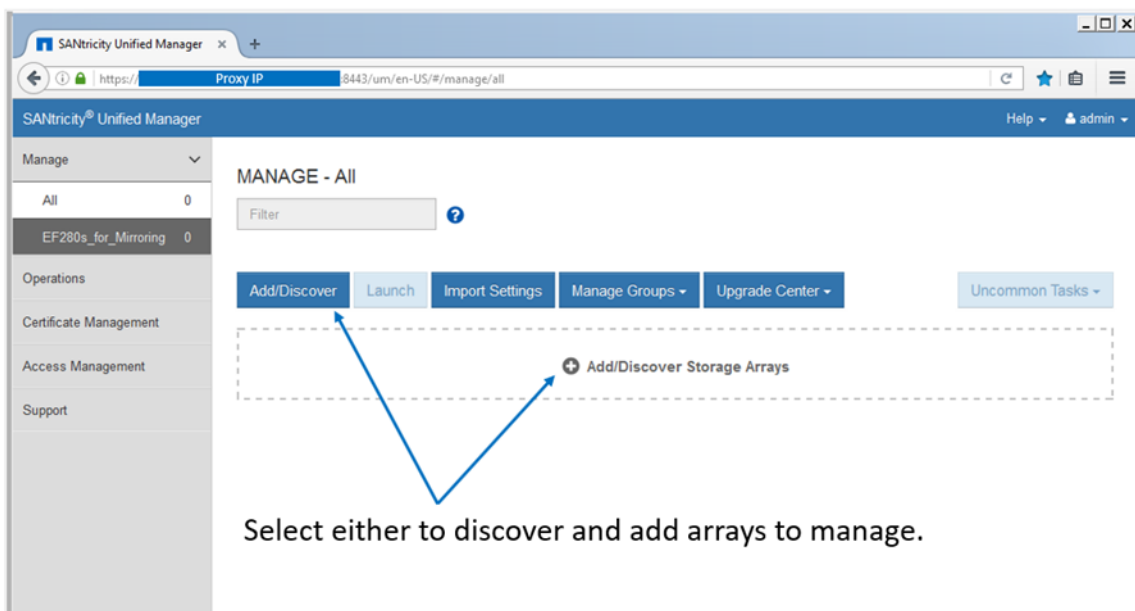
SANtricity Unified Manager navigation

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

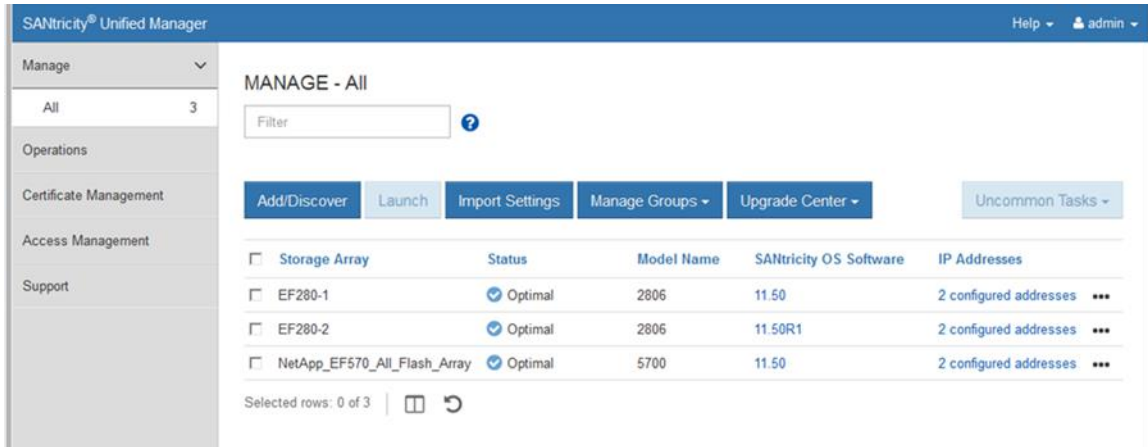
Like the SANtricity EMW, SANtricity Unified Manager must discover arrays to manage, and, like the EMW, you can discover a single array or scan a range of IP addresses to discover multiple arrays simultaneously. Select the tab or link shown in Figure 8 to open the Add/Discover wizard. After discovering arrays, you then choose to manage them with Unified Manager.

Figure 8) SANtricity Unified Manager landing page—discover and add arrays.



After the arrays are discovered and added, they are displayed on the landing page of Unified Manager (Figure 9).

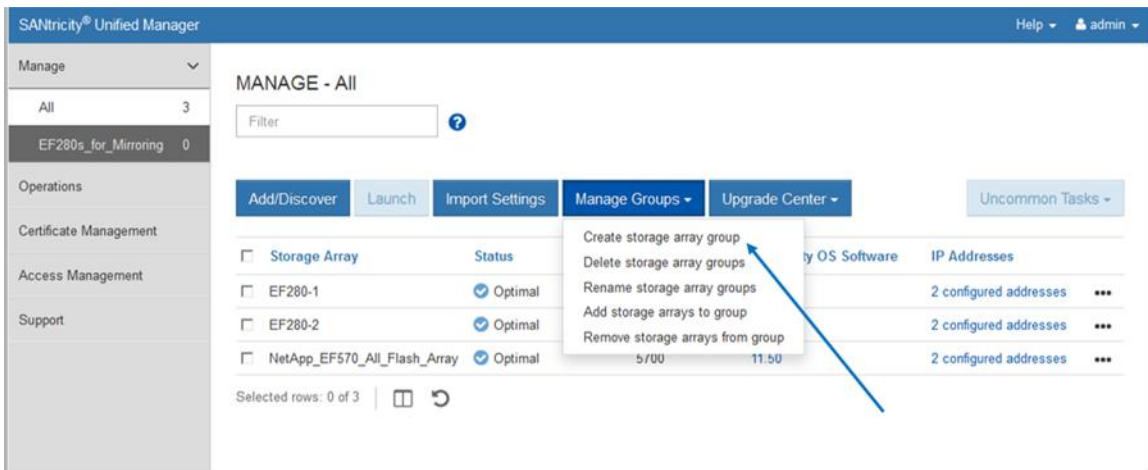
Figure 9) SANtricity Unified Manager landing page.



Organizing arrays by group

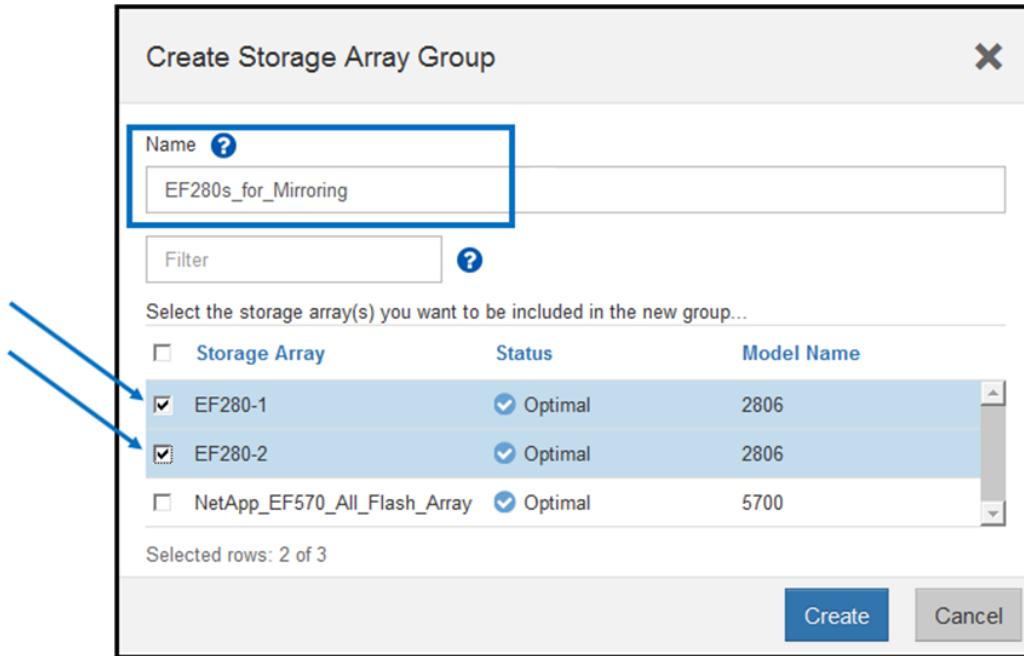
After you add arrays to Unified Manager, you can group them to organize your array management environment. Figure 10 shows EF280 arrays added to a group. This capability is available for all new generation E-Series and EF-Series arrays.

Figure 10) Creating a group to organize arrays in SANtricity Unified Manager.



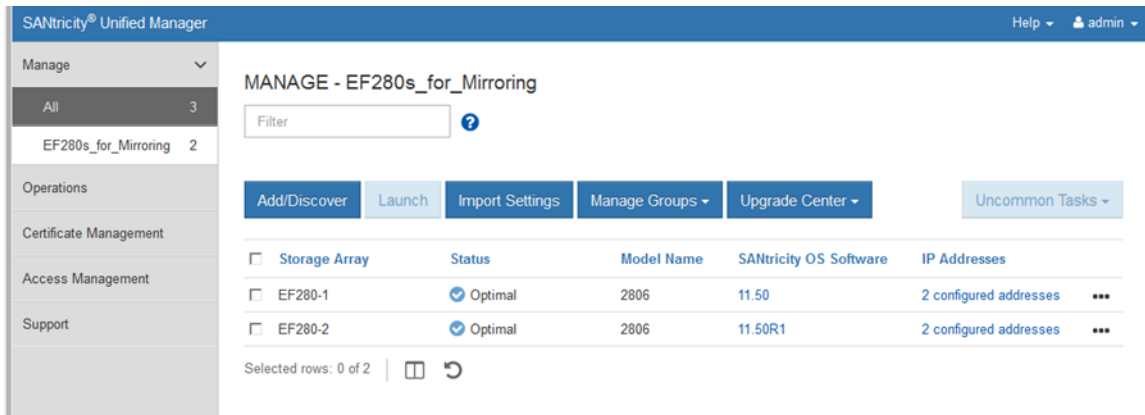
The built-in wizard makes adding arrays to groups quick and easy, as shown in Figure 11.

Figure 11) Creating a group in Unified Manager.



SANtricity Unified Manager allows you to see just the subset of arrays in the new group, as shown in Figure 12.

Figure 12) SANtricity Unified Manager showing a newly created group.



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 11.60 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 13.

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 13) SANtricity Unified Manager Operations view.

The screenshot shows the SANtricity Unified Manager interface. On the left is a navigation menu with options: Manage, All (3), EF280s_for_Mirroring (2), Operations, Certificate Management, Access Management, and Support. The main area is titled 'OPERATIONS' and contains a 'Filter' input field, 'Refresh' and 'Save' buttons, and a table of 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

Below the table, it indicates 'Total rows: 2' with pagination icons.

Updating SANtricity OS through Unified Manager

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

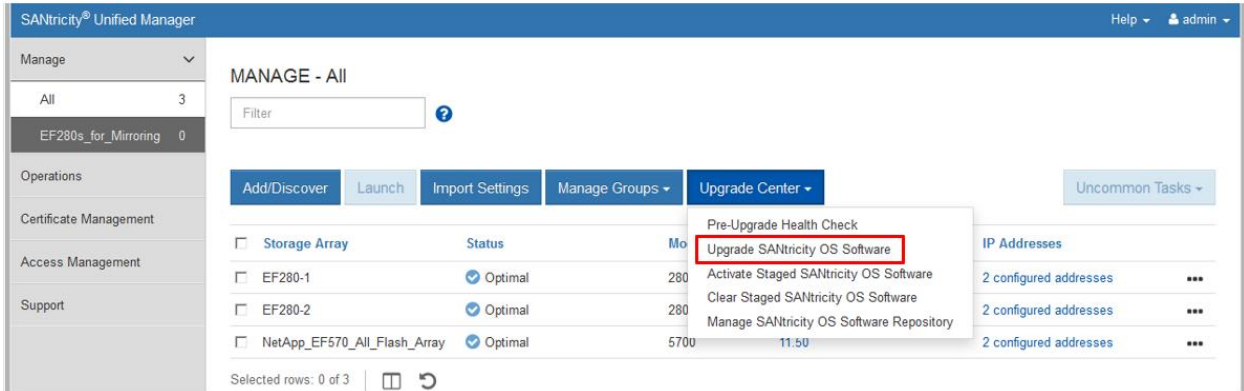
1. Import the SANtricity OS software into the Unified Manager's SANtricity OS Software Repository using the Manage SANtricity OS Software Repository dialog under Upgrade Center on the landing page.

The dialog box is titled 'Manage SANtricity OS Software Repository' and includes a close button (X). It contains instructions: '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.' Below this is a 'Filter' input field and a help icon. There are 'Import' and 'Delete' buttons. A table lists files for import:

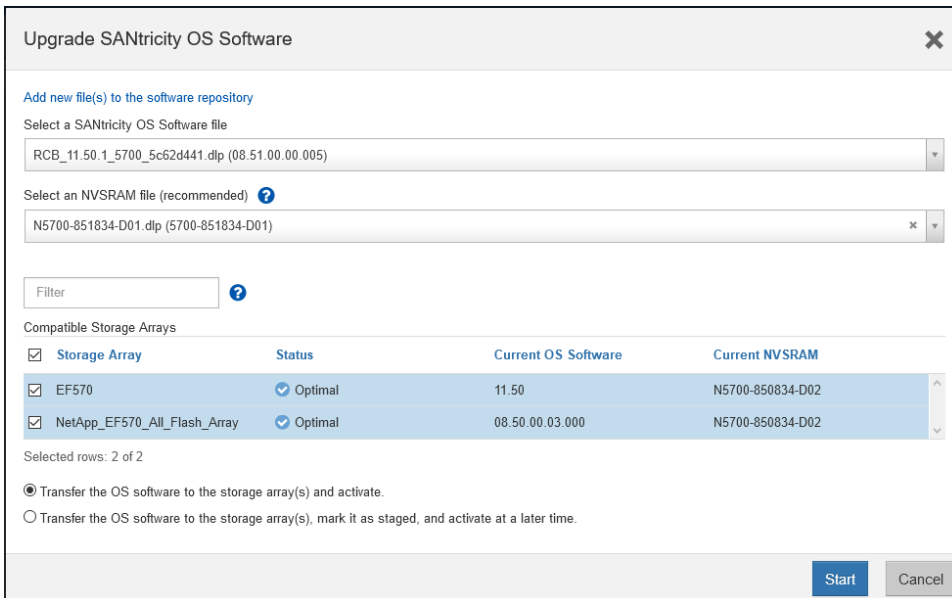
<input type="checkbox"/>	Filename	Version	File Type
<input type="checkbox"/>	RCB_11.50.1_5700_5c62d441.dlp	08.51.00.00.005	SANtricity OS Software
<input type="checkbox"/>	N5700-851834-D01.dlp	5700-851834-D01	NVSRAM

At the bottom, it shows 'Selected rows: 0 of 2' and a 'Close' button.

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



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.



5. On the Confirm Transfer and Activation page, enter Upgrade and then click Upgrade button 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.

Filter ?

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 Cancel

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 ✕

Filter ?

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

Close

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

Upgrade SANtricity OS Software ✕

Filter ?

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

Close

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
<input type="checkbox"/> E2860	Optimal	2806	11.50R1	2 configured addresses
<input type="checkbox"/> EF280-1	Optimal	2806	11.50R1	2 configured addresses
<input type="checkbox"/> EF570	Optimal	5700	11.50.1	2 configured addresses
<input type="checkbox"/> 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](#), [TR-4855: Security Hardening Guide for NetApp SANtricity](#), and [TR-4813: Managing Certificates for NetApp E-Series Storage Systems](#).

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: Drive 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.

Prior to 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 \(11.61 and below\)](#).

SANtricity System Manager

Overview

SANtricity System Manager provides embedded management software, web services, event monitoring, secure CLI, and AutoSupport for E5700 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.

E5700 storage systems are shipped preloaded with SANtricity OS, which includes SANtricity System Manager 11.60 or later. To discover E5700 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 14. 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.
- Highlighted on the bottom-right corner is a Storage Hierarchy view of your array that includes the ability to provision the storage.

Figure 14) SANtricity System Manager home page.



Figure 15, Figure 16, Figure 17, and Figure 18 show the other four main pages that are used in SANtricity System Manager and that are accessible from anywhere in the application.

Figure 15) System Manager Storage page.

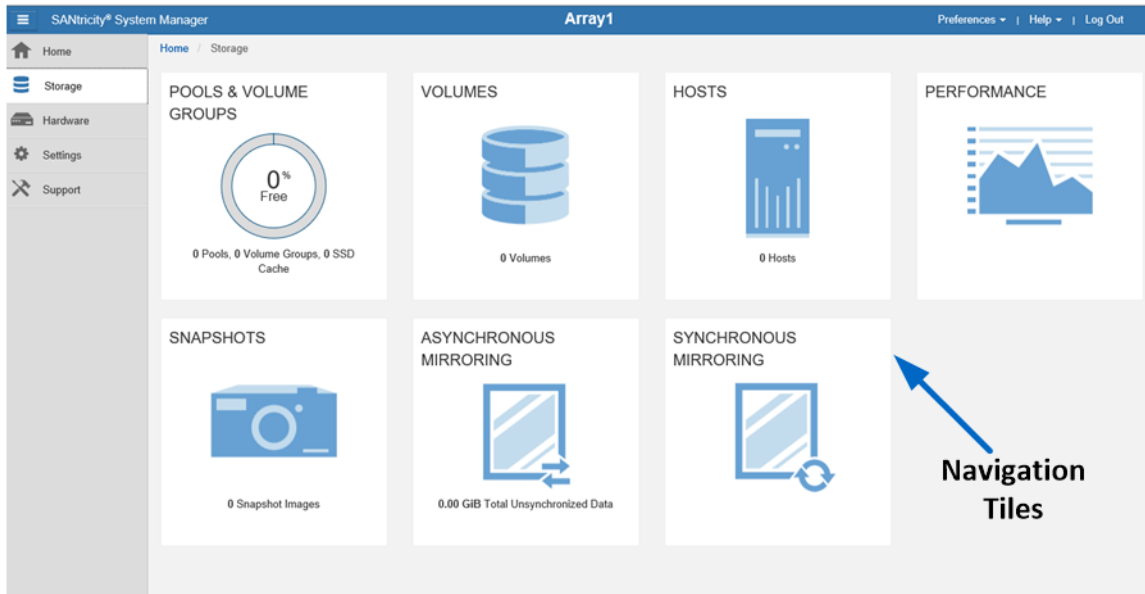


Figure 16) System Manager Hardware page.



Figure 17) System Manager Settings page with new security tiles.



Note: Figure 17 shows the view for an administrator or security administrator. Others with a lower access permission level see only the Alerts and System tiles.

Figure 18) System Manager Support page.

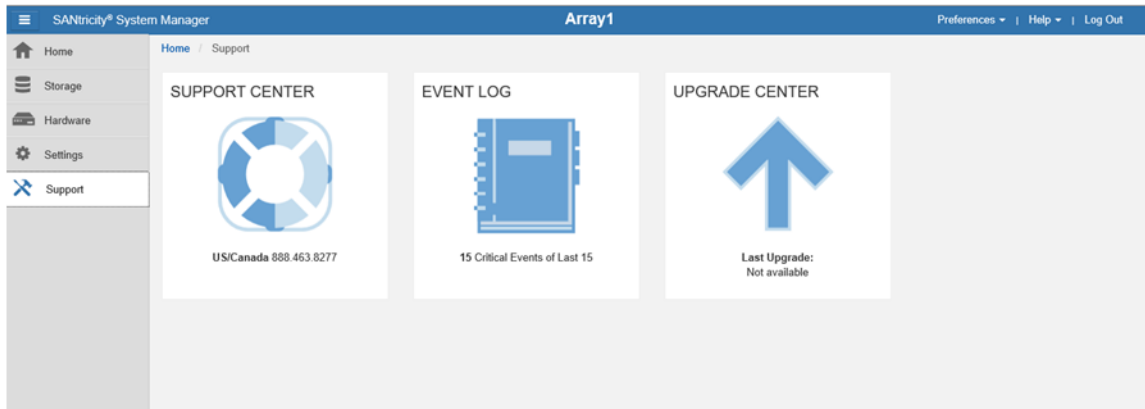
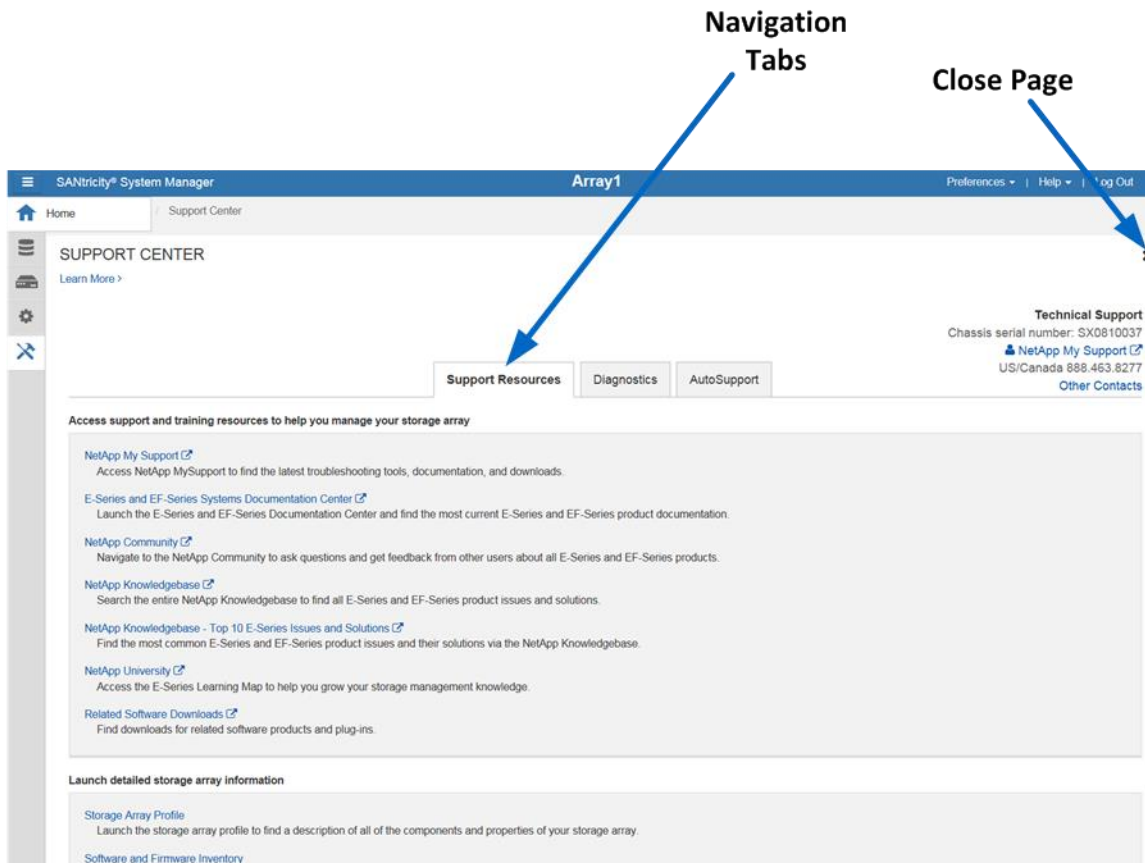


Figure 19 displays the Support Center, which you can reach by selecting the Support Center tile on the Support page. From the Support Center, use navigation tabs to reach support topics.

Figure 19) System Manager Support Center.



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 1 defines the permission level with each role.

Table 1) 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-separated 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 2.

Table 2) LDAP/RBAC required fields and definitions.

Field name	Definitions
Domain (for example, <code>netapp.com</code>)	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 <code>ldap://<IP:port_number></code> (port 389 or port 636 for LDAPS).
Bind account	Format is <code>CN=binduser,CN=Users,DC=<some_name>,DC=com</code> .
Bind account password	Password for bind account user.
Search base DN	Format is <code>CN=Users,DC=<some_name>,DC=com</code> .
Username attribute	The LDAP attribute that defines the username. Example: <code>sAMAccountName</code> 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: <code>memberOf</code> is a standard attribute.

Figure 20 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 20) SANtricity System Manager directory server setup wizard.

Directory Server Settings

Server Settings | Role Mapping

What do I need to know before adding a directory server?

Configuration settings

Domain(s) **Enter one or more comma separated domain names**
cre,cre.com

Server URL **Directory Server IP**
ldap://10.113.149.249:389

Bind account (optional) **Specify Users or Groups**
CN=binduser,CN=Users,DC=cre,DC=com

Bind password **Directory Server Password**
.....

Test server connection before saving **Test the server connection**

Privilege settings

Search base DN **Look-up user in this example - Users@cre.com**
CN=Users,DC=cre,DC=com

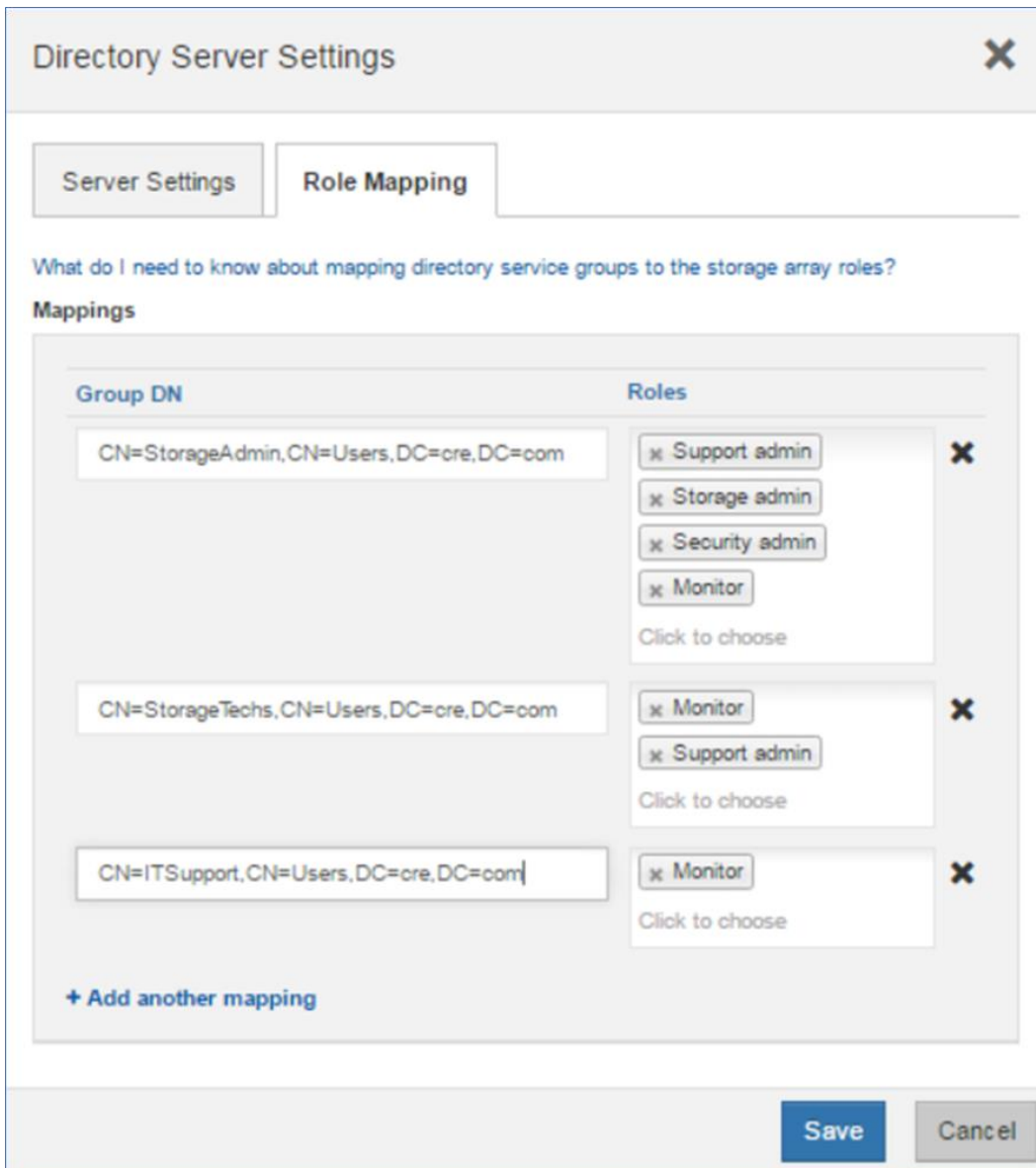
Username attribute **Microsoft specific attribute name**
sAMAccountName

Group attribute(s) **User look-up attribute**
memberOf

Save Cancel

The array roles for the specified user groups are set in the Role Mapping tab. In Figure 21, 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 21) Role Mapping tab in the directory server settings wizard.



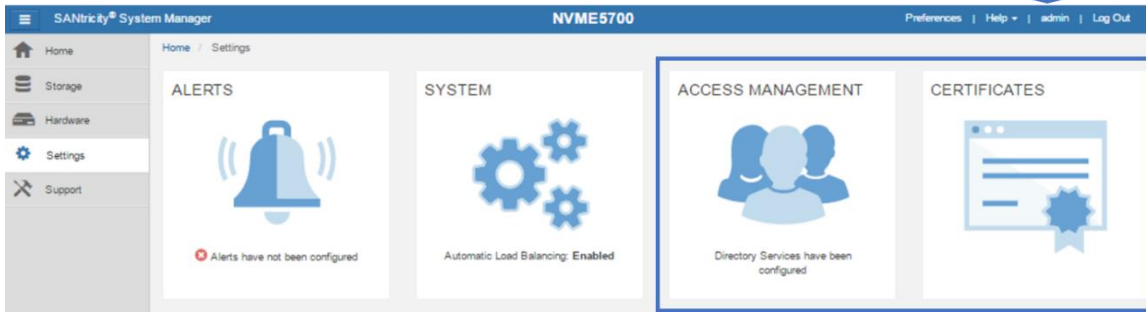
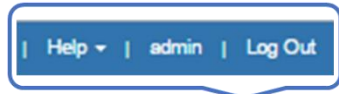
Note: The monitor role is automatically added to all group DN's. Without monitor permission, users in the associated mapped group are not able to log in to the array.

Multiple groups can be defined and mapped to specific roles that meet individual business requirements. Figure 22 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 22.

Figure 22) SANtricity System Manager views change according to user permission level.

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



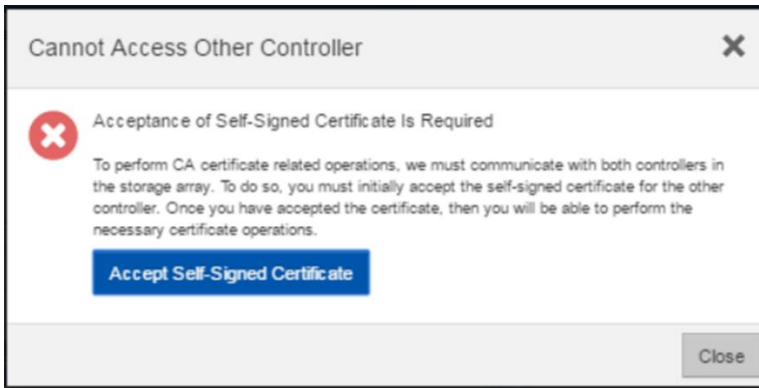
Logged-in as admin with full user permission to set-up security features

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 E5700 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 E5700 array is done through the midplane in the shelf.

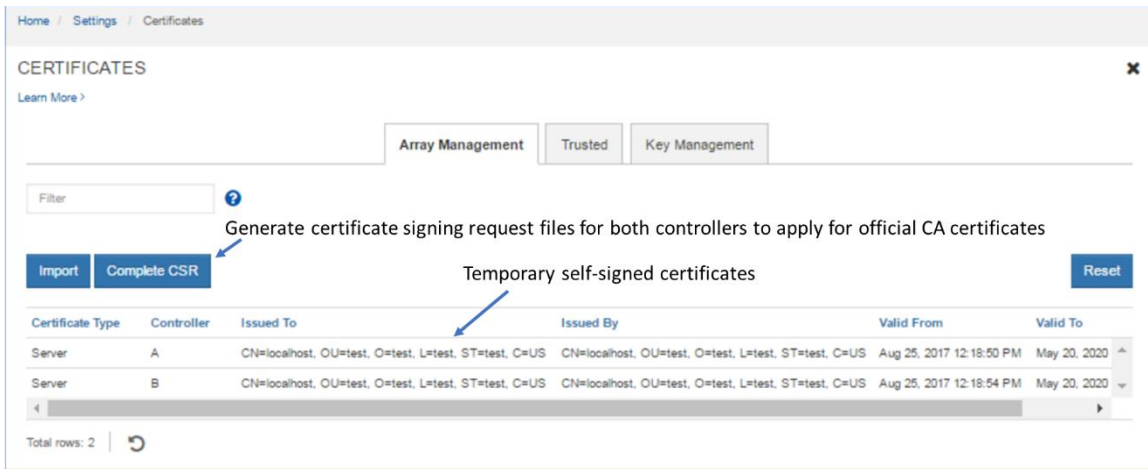
Because you can log in to either of the controllers through the web browser, both controllers must run a web server instance. For proper communication, both controllers must present a self-signed certificate to each other. This process happens automatically when the admin or security user logs in to each controller and opens the Certificates tile. Figure 23 shows the dialog box that is displayed the first time the tile is opened.

Figure 23) Initial step required to set up web server certificates.



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 24.

Figure 24) Expanded SANtricity System Manager Certificates tile.



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 24 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 E5700 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: 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 3 provides a list of SANtricity host types and the associated support for implicit failover/failback.

Table 3) 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 [IMT](#) as well as the SANtricity online help.

SANtricity reliability features

Table 4 provides a list of SANtricity reliability features and a brief explanation of each with references to additional information.

Table 4) 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.

Note: 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 E5700 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 E5700 systems ship with significant storage management features that can be activated from SANtricity System Manager. Table 5 lists the E5700 features that are standard with SANtricity OS.

Table 5) E5700 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 (Maintain E-Series hardware).

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.

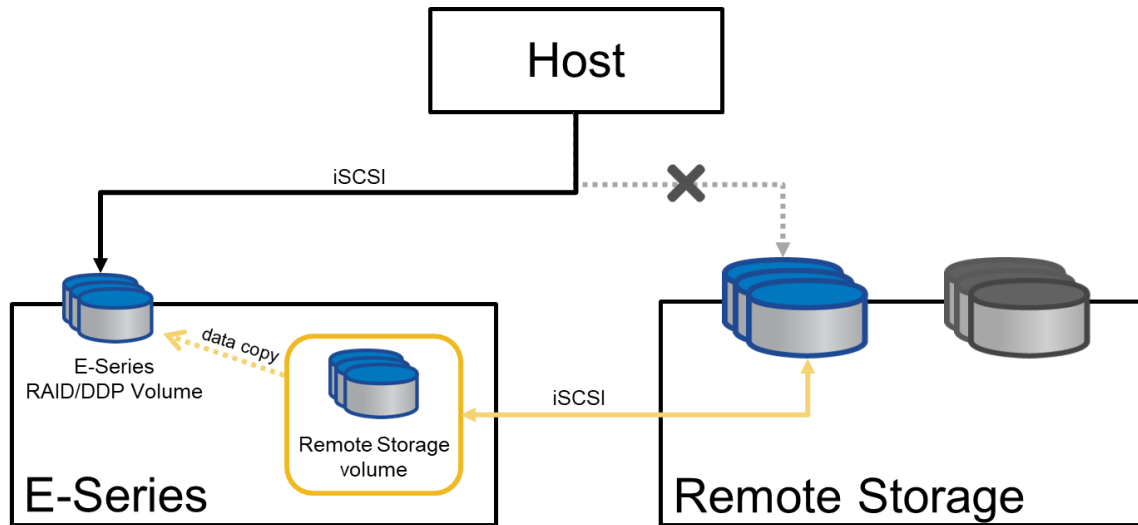
The base function of this feature is to support importing data from a remote storage device directly to a local E-Series volume. To use this feature, an iSCSI connection must first be manually established between the remote storage device and the E-Series system. The remote storage will need to be configured 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. Once 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 25 shows the technical components of the solution.

Figure 25) Remote Storage Volumes solution architecture overview.



Information that will need 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.

Once configured, the remote storage iSCSI IQN and/or iSCSI IP addresses can be updated, if needed, using 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 6 lists standard copy services features with E5700 storage arrays.

Table 6) 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. 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.

Prior to 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 7 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 [E-Series SANtricity Unified Manager and Web Services Proxy](#). 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 7) 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 8 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 8) Third platform plug-ins that use the SANtricity Web Services Proxy.

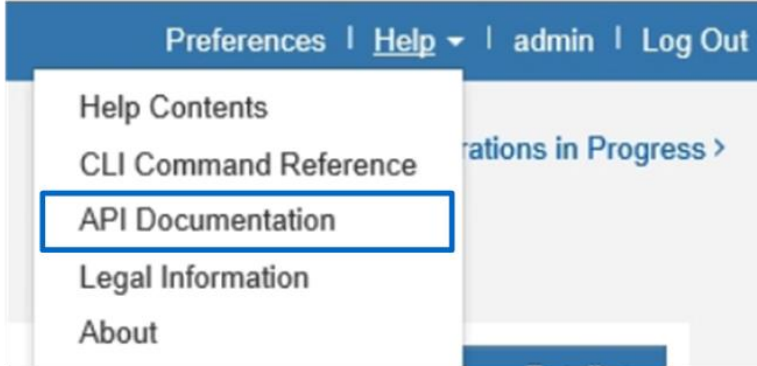
Software Package	Use
NetApp SANtricity Performance App for Splunk Enterprise Technology Add-On for NetApp SANtricity	A display and monitor tool to report configuration and performance details of multiple E-Series systems in one interface. Requires both application and technology add-on.
NetApp E-Series + Grafana: Performance Monitoring https://github.com/netapp/eseries-perf-analyzer	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 lets 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 26.

Figure 26) 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 27. 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 28).

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 27) Example expanding the Device-ASUP endpoint.

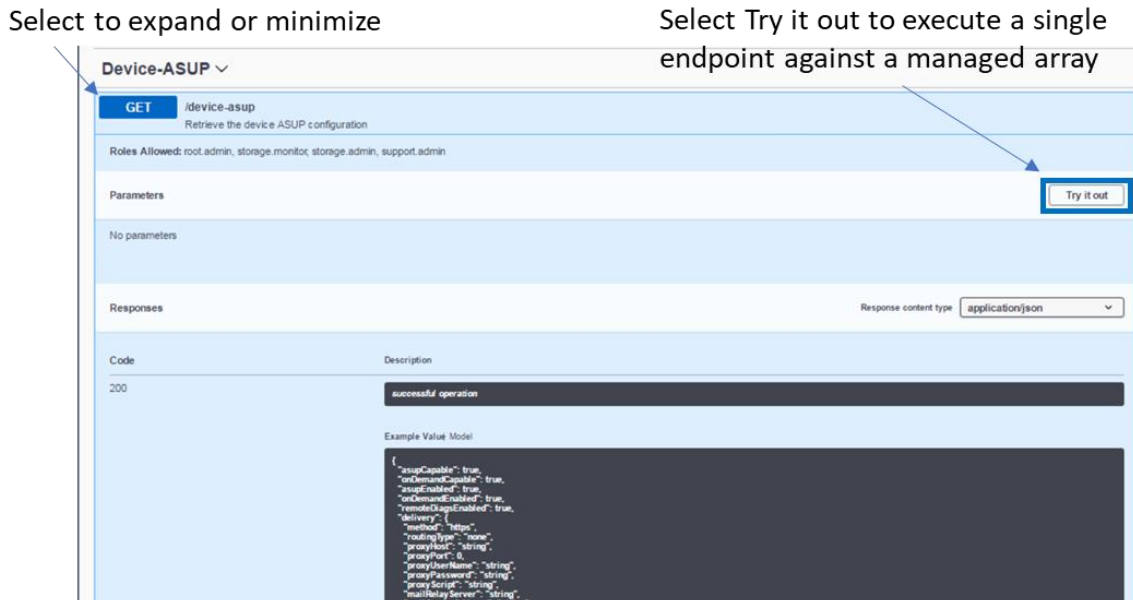


Figure 28) REST API documentation sample.

Device-ASUP ▾

GET /device-asup
Retrieve the device ASUP configuration

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

Parameters
No parameters

Select Execute to run the endpoint

Execute

Responses
Response content type: application/json

Code	Description
200	successful operation

Example Value Model

```
{
  "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 29 and Figure 30.

Figure 29) Sample output from the Try It Out button.

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

Server response

Code: 200

Expanded view

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": []
  }
}
```

Response headers

```
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-ss-protection: 1; mode=block
```

Responses

Code	Description
200	successful operation

Figure 30) Device-asup endpoint possible response codes and definitions.

Code	Description
200	successful operation
501	Device ASUP service not available.
503	Device ASUP service is initializing.

Example Value Model

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

Possible response codes and details

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, allowing 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 through 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.

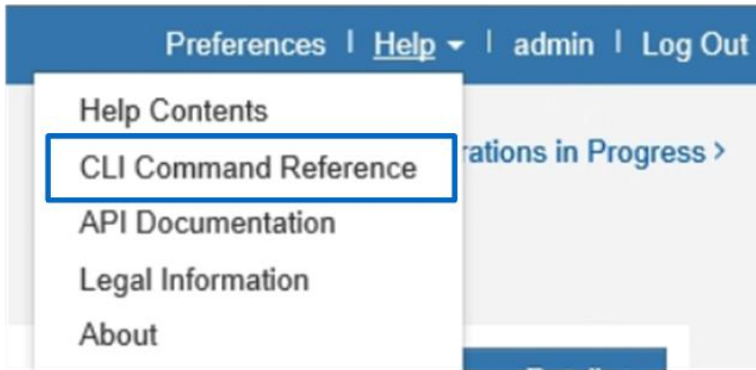
Downloading the CLI

- 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 the System Manager A CLI (Figure 31).

Figure 31) 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](#), choose 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 E5700 hardware

Table 9 lists the SANtricity software specifications for E5700-based storage systems.

Table 9) SANtricity software boundaries for E5700-based storage systems.

Components	Maximum
Storage hardware components	
Shelves (controller and expansion)	8 (1x controller + 7x expansion)
Drives	480 (120 SSDs)
SSD cache capacity	8TB
Logical components	
Host Partitions	1024
Volumes per partition	256

Components	Maximum
Volumes per system	2,048
Disk pools per system	20
Volumes per disk pool	2,048
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: <ul style="list-style-type: none"> • 2PiB maximum DDP capacity per array SANtricity 11.40.1 and later: <ul style="list-style-type: none"> • 6PiB maximum DDP capacity per array SANtricity 11.90 and later: <ul style="list-style-type: none"> • 12PiB maximum DDP capacity per array
Maximum DDP single volume capacity as of SANtricity 11.50 and later	4PiB
Maximum DDP single thin volume capacity (SANtricity 11.30 and later)	256TiB
Maximum standard RAID capacity limits	Limits for standard RAID based on maximum supported drives per RAID type: <ul style="list-style-type: none"> • 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	64
Consistency groups per system	32
NetApp Snapshot copies	
Per Snapshot group	32
Per volume	128
Per storage system	2,048
Snapshot volumes	
Per Snapshot copy	4
Per system	1,024
Snapshot groups	
Per volume	4
Per system	1,024
Mirrors	
Mirrors per system	128
Mirrors per volume	1
Mirrors per asynchronous mirror group	64
Asynchronous mirror groups per system	4

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](#).

E5700 hardware configurations

E5700 storage systems, like all E-Series arrays, 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 record of accomplishment with reliability and scalability to satisfy requirements in remote dedicated environments or primary data centers providing mission-critical infrastructure.

Controller shelf configurations

E5700 controllers can be paired with DE224C or DE460C E-Series shelves, but they are not offered in the smaller entry-level 12-drive shelf. The following sections provide detailed information about each shelf configuration.

E5724 controller shelf

The E5724 is a two-rack-unit-high (2U) shelf that holds up to twenty-four 2.5-inch drives. It features two RAID controllers and two ENERGY STAR Platinum certified high-efficiency power supplies (913W) with integrated fans. An E5724-based storage system supports a maximum of 192 HDDs (120 SSDs) and a mix of drive shelf models in a single system.

Figure 32 and Figure 33 show the front and rear views, respectively, of the E5724 controller shelf. In this example, the E5700 controllers have two optical base ports and have the optional 4-port 32Gb FC HIC installed.

Figure 32) E5724 front view (bezel removed).

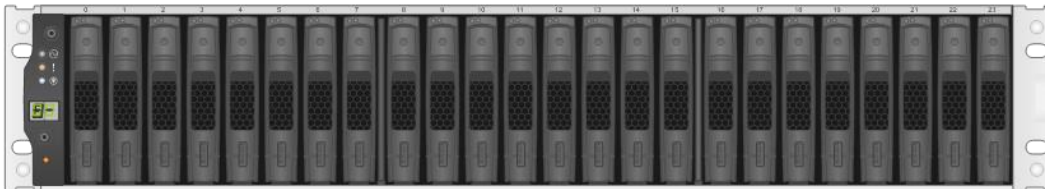
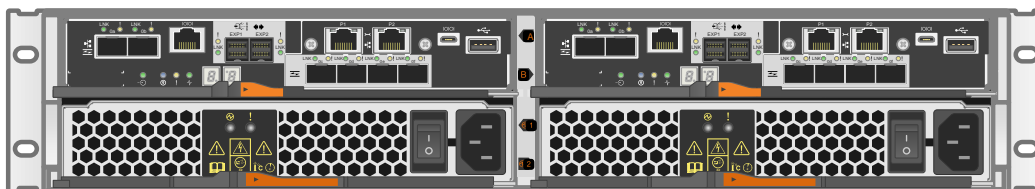


Figure 33) E5724 rear view.



E5760 controller shelf

The E5760 is a DE460C, 4U shelf that holds up to sixty 3.5-inch drives or 2.5-inch drives with an adapter. It features two RAID controllers and two ENERGY STAR Platinum certified high-efficiency power supplies (2325W) with separate fan modules. E5760 storage systems support a higher drive count, up to 480 HDDs (120 SSDs) when built with eight total DE460C shelves. E5700 systems can also support a mix of drive shelf models to accommodate any of the available drive choices; however, the maximum drive count and total capacity are limited by the number of slots available in the up to eight total shelves chosen for the system.

Figure 34 and Figure 35 show the front (without front bezel) and rear views, respectively, of the E5760 controller shelf. In the example, the E5700 controllers have two optical base ports with the optional 4-port 25Gbps iSCSI HIC installed.

Figure 34) E5760 front view (bezel removed).

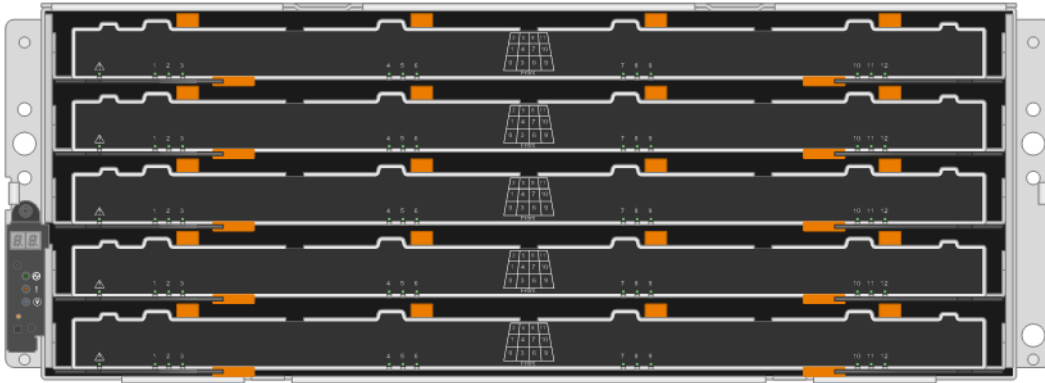
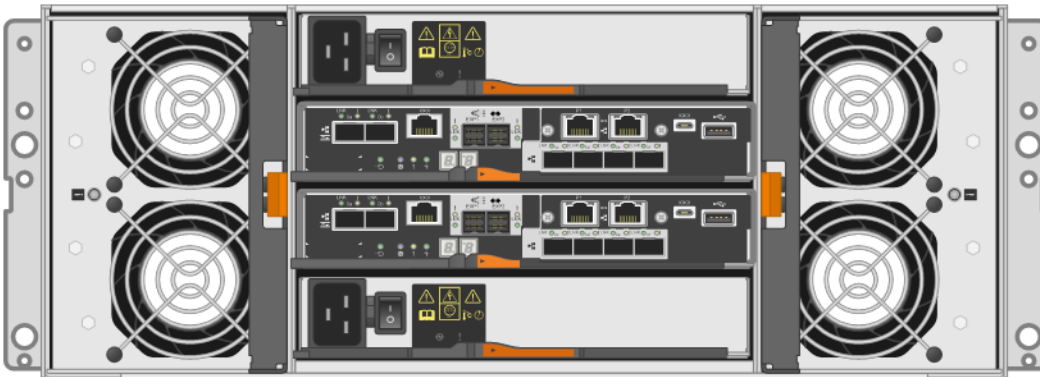


Figure 35) E5760 rear view.



Note: The 12Gb 4U60 shelf, DE460C, is physically deeper than the predecessor 6Gb 4U60 shelf, DE6600. NetApp now offers a new deeper cabinet that supports this shelf including the ~220VAC PDUs needed to power the DE460C shelves. See the [Hardware Universe](#) for physical dimensions and power requirement details on all available E-Series systems.

E5700 hardware specifications

The E5700 controller has the following base hardware features:

- Dual Ethernet ports for management-related activities
- Either no baseboard ports or dual optical 16Gbps FC/10Gbps iSCSI baseboard ports for host connection
- Dual 12Gb SAS drive expansion ports to attach expansion-drive shelves

Note: Adding optional HICs for the E5700 controller provides faster host interfaces for iSCSI, FC, and IB. For more information about the faster host interfaces, see [Controller host interface features](#).

Table 10 lists the technical specifications for the E5700-based storage systems.

Table 10) E5700 technical specifications.

Specification	E5724	E5760
Maximum raw system capacity (assumes not mixing shelf models)	1965TB (120x 15.3TB SSD) + (72 x 1.8TB SAS)	8.64PB (480 x 18TB)

Specification	E5724	E5760
Maximum number of drives per system (assumes not mixing shelf models)	192 HDDs (120 SSDs max.)	480 HDDs (120 SSDs max.)
Shelf form factor	2U, 24 drives	4U, 60 drives
Memory	16GB or 64GB per controller; 64GB memory option required when using NVMe/IB, NVMe/RoCE and NVMe/FC protocols.	
	32GB or 128GB per duplex system.	
Onboard host interface (if present)	2-port 10Gb iSCSI (optical) or 16Gb FC per controller. Note: Only one protocol can be configured per system using the onboard host ports.	
Optional host interface (HIC) per controller <ul style="list-style-type: none"> • Controllers must match • A software feature pack* can be applied for host protocol conversion 	2-port 100Gb IB (iSER, SRP, NVMe/IB, or NVMe/RoCE based on feature pack installed*) Note: Onboard host ports are disabled when using NVMe protocols.	
	4-port 12Gb SAS (wide port): uses mini-SAS cables.	
	4-port 32Gb FC (FC or NVMe/FC based on feature pack installed*) Note: Onboard host ports are disabled when using NVMe protocols.	
	4-port 25Gb iSCSI (see the Hardware Universe for SFP details: must set port speed for 10Gbps or 25Gbps using SANtricity System Manager: the 25Gbps SFP does work for 25Gb and 10Gb speeds, but the port does not change speeds automatically).	
Drive shelves supported for expansion-drive offerings	DE224C (2U, 24 drives): 7 expansion shelves maximum.; supports the same drive types as E5724 controller shelf.	
	DE460C (4U, 60 drives): 7 expansion shelves maximum; supports the same drive types as E5760 controller shelf.	
	DE6600 (4U, 60 drives): up to 7 expansion shelves max. Note: Supports only SAS 2 (6Gbps) transfer speeds.	
	DE5600 (2U, 24 drives): 7 expansion shelves maximum. Note: Supports only SAS 2 (6Gbps) transfer speeds.	
	DE1600 (2U, 12 drives): 3 expansion shelves maximum; supports only NL-SAS drive types Note: Supports only SAS 2 (6Gbps) transfer speeds.	
High-availability (HA) features	Dual active controllers with automated I/O path failover.	
	Support for RAID 1 (10 for 4 drives or more), 5, 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 SANtricity System Manager online help.	
	Redundant, hot-swappable storage controllers, disks, and power fan canisters.	
	Mirrored data cache with battery-backed destage to flash.	

Specification	E5724	E5760
---------------	-------	-------

* For more information about the available feature pack SMIDs for E5700 controllers, see the section titled [Controller host interface features](#).

For current supported drive availability information and encryption capability by drive capacity (FDE, FIPS), see the [Hardware Universe](#).

Controller host interface features

By default, the E5700 controller includes two Ethernet management ports that provide out-of-band system management access and either two 16Gbps FC or 10Gbps iSCSI optical baseboard ports for host connections. As a result, E5700 controllers are ordered as either FC base or iSCSI base. Optional host interface ports can be added, as indicated in Table 10. For the optional 25Gbps iSCSI and 12Gbps SAS HICs, any of the feature pack SMIDs (FP-SMID) can be used because those interfaces do not have multiple protocol choices. The 32Gbps FC HIC uses specific FP-SMIDs for NVMe/FC protocol. The 100Gbps IB HIC has four IB protocols available on the E5700 100Gb IB HIC, including:

- iSER
- SRP
- NVMe/IB
- NVMe/RoCE

Table 11 provides a detailed breakdown of the available base host port protocols combined with the protocol options for the 100Gb IB/Ethernet HIC and FC HIC. See [Change E5700 Host Protocol](#) for specific instructions.

Table 11) Table of available FP-SMIDs for E5700 controllers.

Controller base protocol	Encryption-enabled FP-SMID	HIC protocol	Encryption-disabled FP-SMID
E5700 FC base or No base ports	360	Any or no HIC (IB = iSER)	365
E5700 FC base or No base ports	361	Any or no HIC (IB = SRP)	366
E5700 FC base or No base ports	382	Any or no HIC (IB = NVMe/IB)	384
E5700 FC base or No base ports	403	Any or no HIC (NVMe/FC or NVMe/RoCE)	405
E5700 iSCSI base	362	Any or no HIC (IB = iSER)	367
E5700 iSCSI base	363	Any or no HIC (IB = SRP)	368
E5700 iSCSI base	383	Any or no HIC (IB = NVMe/IB)	385
E5700 iSCSI base	404	Any or no HIC (NVMe/FC or NVMe/RoCE)	406

The optical 32Gbps FC and 25Gbps iSCSI HICs support several SFP options, including two FC and one iSCSI option and there are two options for the 16Gb FC or 10Gb iSCSI base ports. Table 12 provides details of the FC options.

Table 12) FC host interface port speed and associated SFPs.

HIC Protocol	32Gbps SFP	16Gbps SFP	8Gbps SFP
32Gbps FC	32Gbps/16Gbps	16Gbps/8Gbps	Not applicable
16Gbps FC base ports	Not applicable	16Gbps/8Gbps/4Gbps	8Gbps/4Gbps

Table 13 provides the iSCSI port speed details based on the installed SFP. For the 16Gbps FC or 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 13) iSCSI host interface port speed and associated SFPs.

HIC Protocol	25Gbps SFP	10Gbps SFP (Unified SFP)	1Gbps SFP
25Gbps iSCSI	25Gbps/10Gbps*	Not applicable	Not applicable
10Gbps iSCSI base ports	Not applicable	10Gbps	1Gbps

* You must change port speed from 25Gbps to 10Gbps or 10Gbps to 25Gbps 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.

Table 14 provides the port speed details for the 100Gbps IB HIC.

Table 14) IB host interface port speed with associated cables and HCAs.

HIC protocol	100Gbps cable/HCA	56Gbps cable/HCA	40Gbps cable/HCA
100Gbps IB	100Gbps	56Gbps	40Gbps

Note: NetApp does not sell IB cables or HCAs for either port speed; however, cables are readily available from suppliers such as Mellanox and QLogic.

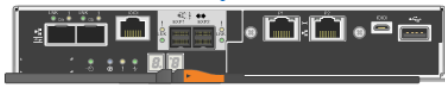
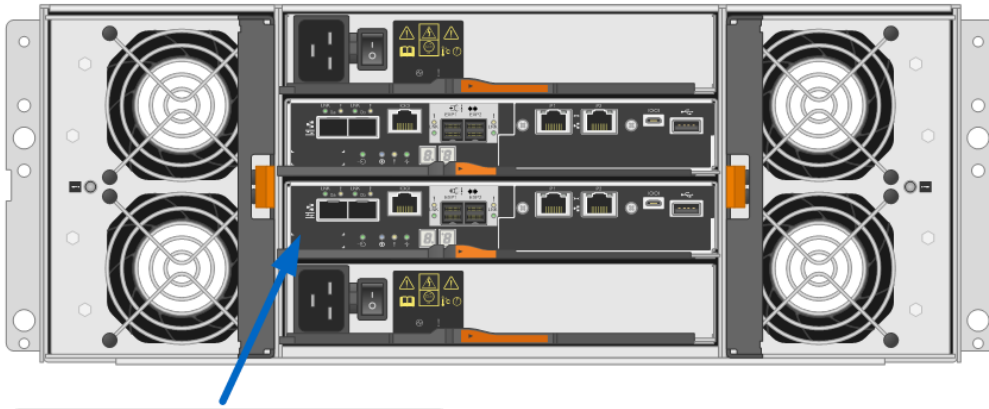
For optical connections, the appropriate SFPs must be ordered for the specific implementation. Consult the [Hardware Universe](#) for a full listing of available host interface equipment. All E5700 optical connections use OM4 optical cable.

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

Figure 36 shows the five HIC options.

Figure 36) E5760 with optional HIC installations.

E5760 showing controller HIC options



E5700 controller with no optional HIC



E5700 controller with 2-port 100Gbps IB or NVMe/RoCE HIC installed



E5700 controller with 4-port 32Gbps FC or NVMe/FC HIC installed



E5700 controller with 4-port 25Gbps iSCSI HIC installed



E5700 controller with 4-port 12 Gbps SAS HIC

Hardware LED definitions

E5700 controller shelf LEDs

The E5700 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 E5700 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 and controller canisters indicate the status of the individual units.

Figure 37 shows the ODP of the E5724 controller shelf. Figure 38 shows the ODP of the E5760 controller shelf.

Figure 37) ODP on the front panel of the E5724 controller shelf.

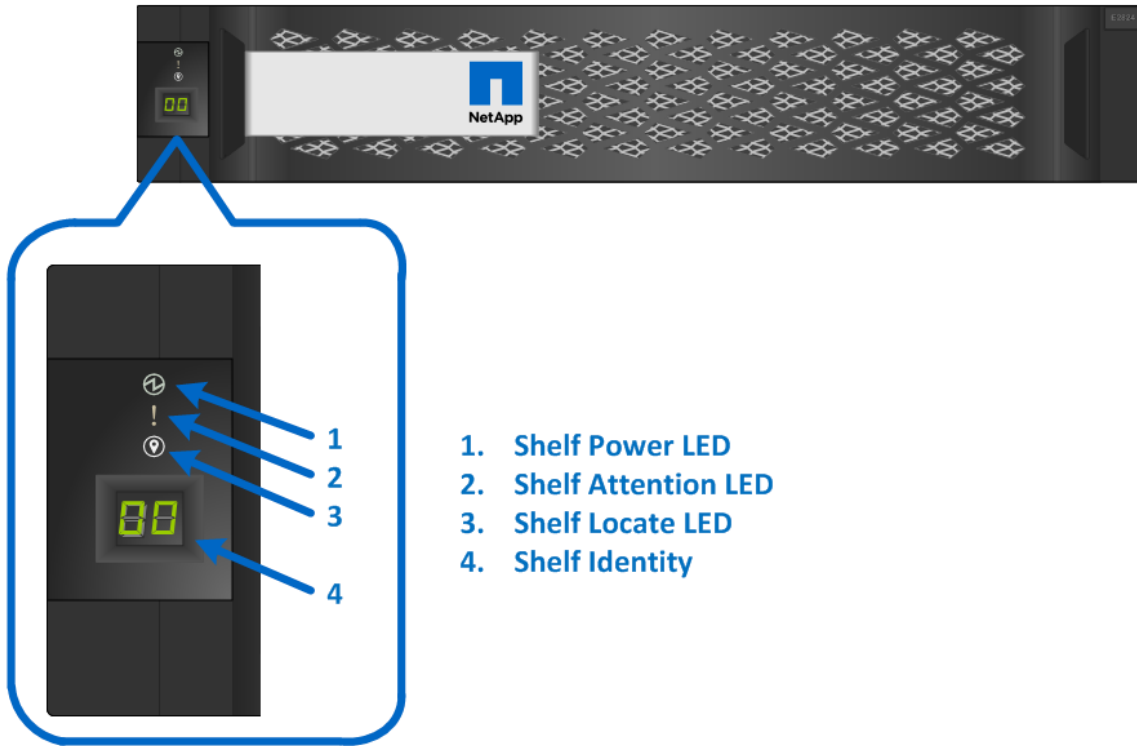


Figure 38) ODP on the front panel of the E5760 controller shelf.

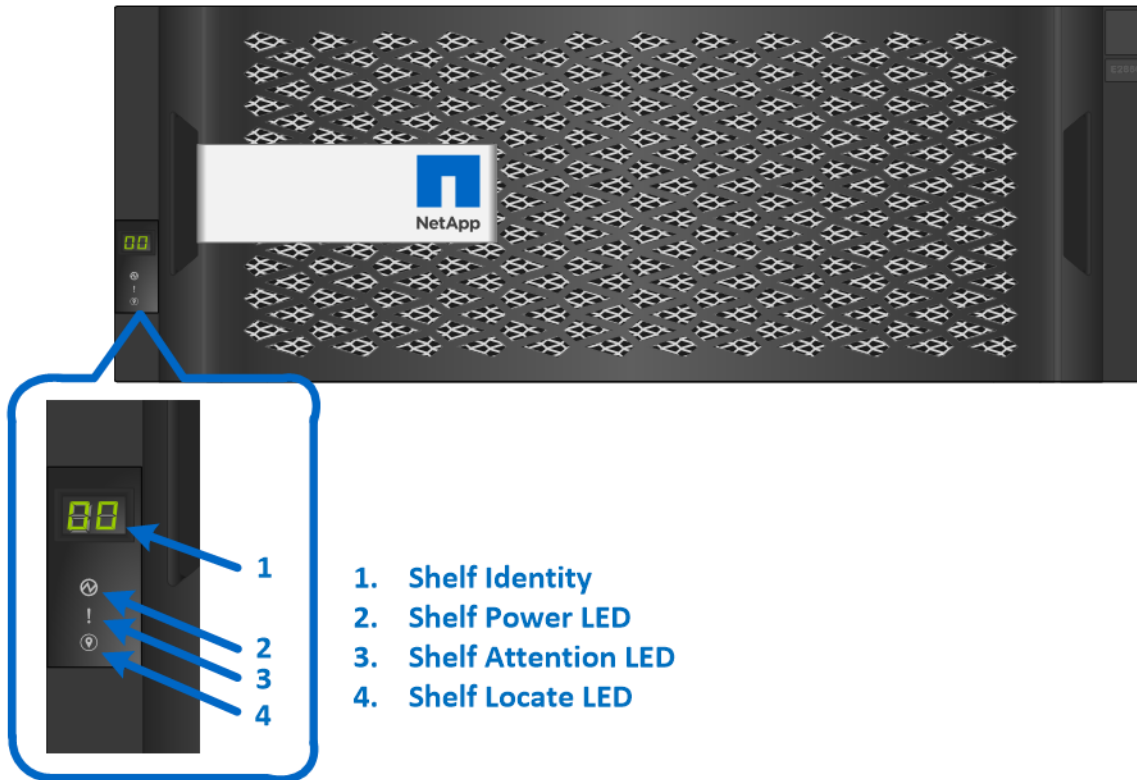


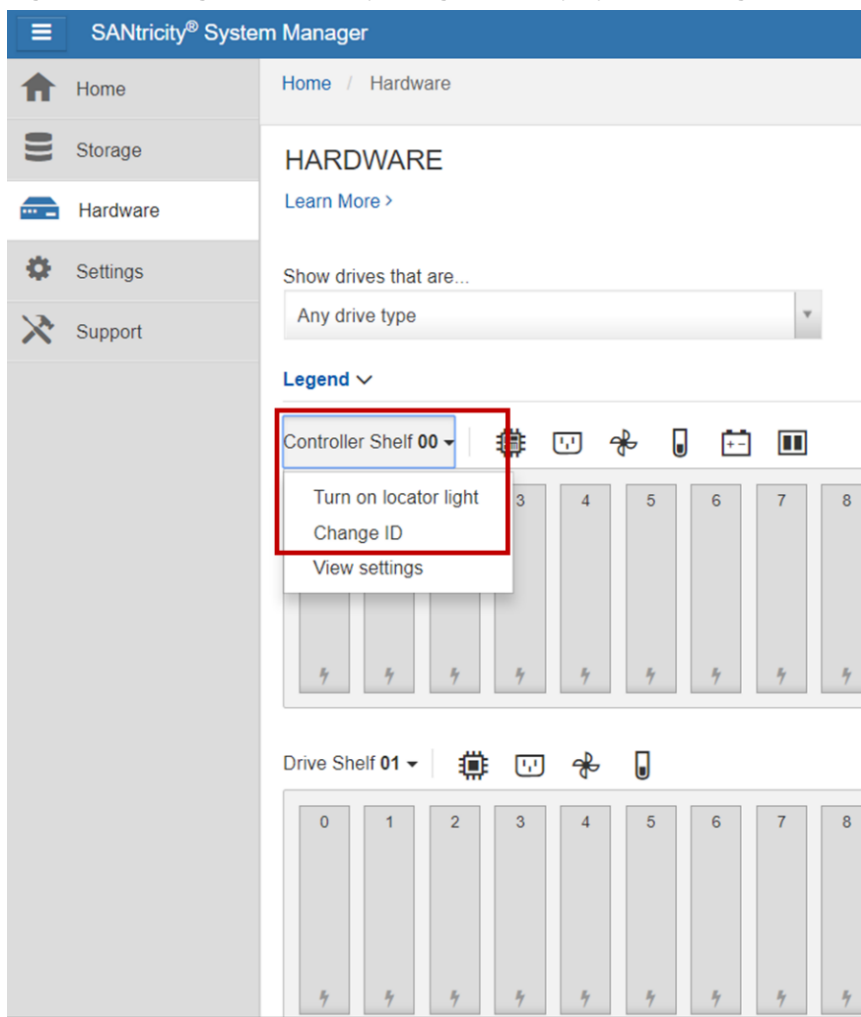
Table 15 defines the ODP LEDs on the E5700 controller shelf.

Table 15) E5700 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.

The shelf identity feature displays a numerical value to identify the shelf. The dual seven-segment display indicates values from 00 to 99 that can be set from the SANtricity System Manager Hardware tab that is shown in Figure 39.

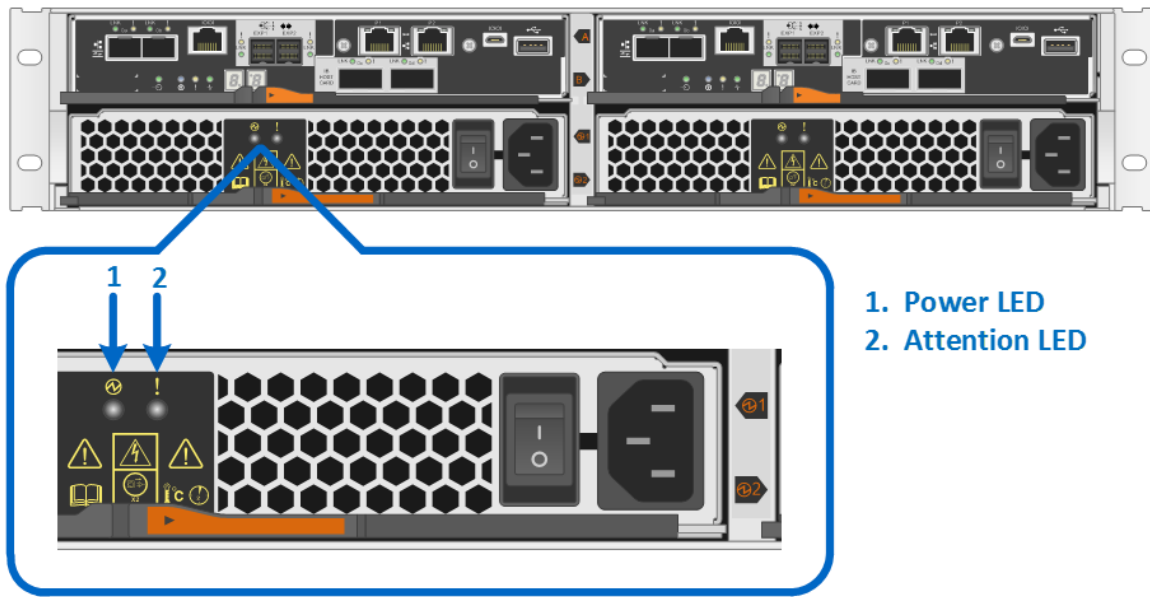
Figure 39) Setting the shelf ID by using SANtricity System Manager.



Power fan canister status LEDs

The LEDs on the rear panel of the E5724 integrated power and fan canisters are shown in Figure 40 and are defined in Table 16.

Figure 40) LEDs on the E5724 power fan canister (rear view).



The power and fan canisters are separate for the E5760 controller shelf. The LEDs on the rear panel of each are shown in Figure 41 and are defined in Table 16.

Figure 41) LEDs on the E5760 power canister (rear view).

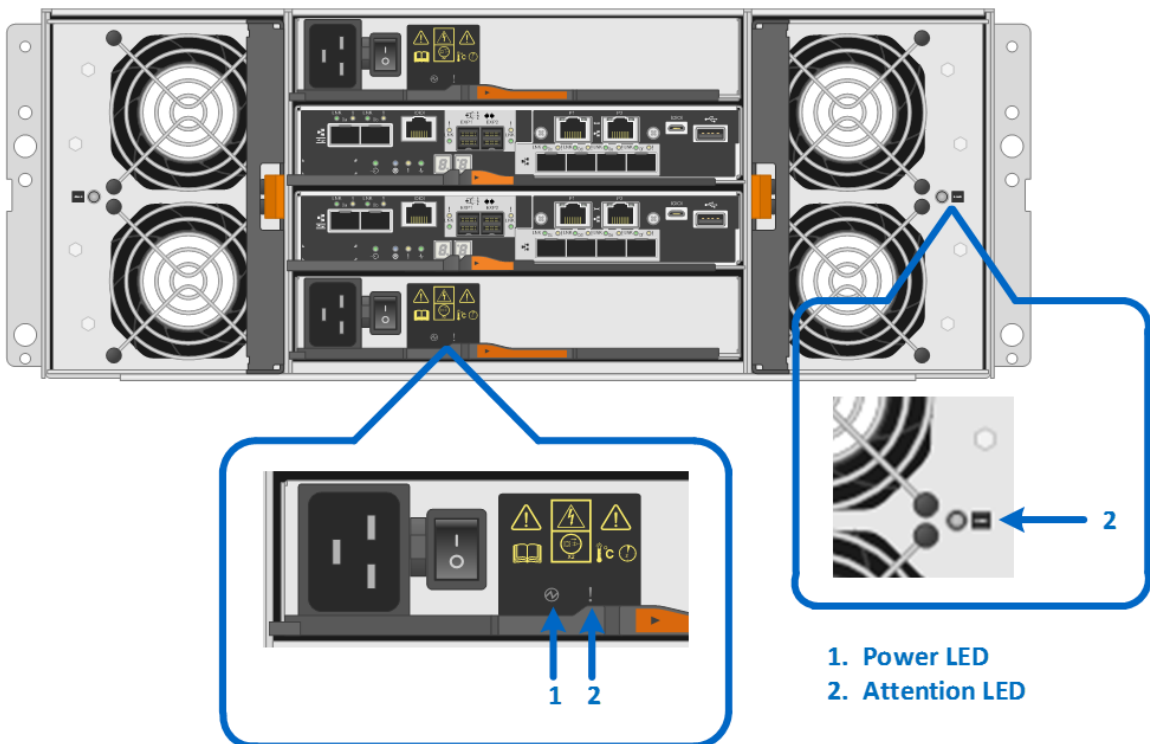


Table 16) E5724 and E5760 controller shelf power and fan canister LED definitions.

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.

E5700 controller canister LEDs

The E5700 controller canister has several LED status indicators. The host port status and other system-level statuses can be verified by directly checking the port LEDs or by using the SANtricity System Manager GUI. For example, the Host Interfaces tab of the Controller Settings dialog box, shown in Figure 42, details the status of each host I/O interface that is connected to the storage system.

Note: The controller settings must be viewed for each controller individually by selecting the controller to see the options. Select View Settings to access the view in Figure 42.

Figure 42) Controller settings dialog box.

Controller A Settings [Close]

Base | Cache | **Host Interfaces** | Drive Interfaces | Management Ports | DNS / NTP

Host interfaces [Show fewer settings](#)

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

Host ports

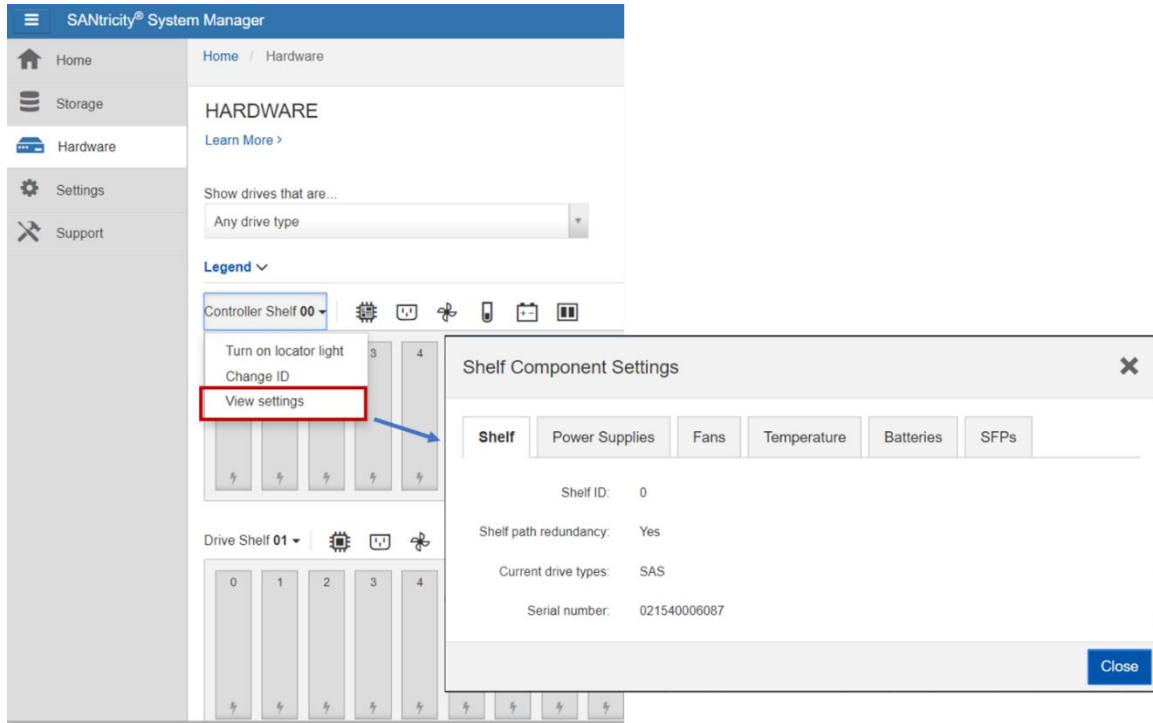
Fibre host ports

Channel	Port	Link Status	HIC Location	Maximum Data Rate	Current Data Rate	Data Rate Control	Topology	World-wide Port Ident
1	e0a 0a	Down	Baseboard	16 Gb/s	Unknown	Auto	Unknown	20:12:00 ^
2	e0b 0b	Down	Baseboard	16 Gb/s	Unknown	Auto	Unknown	20:22:00
3	e1a 1a	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:32:00
4	e1b 1b	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:42:00
5	e1c 1c	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:52:00
6	e1d 1d	Down	Slot 1	16 Gb/s	Unknown	Auto	Unknown	20:62:00 v

[Close]

Other system-wide status information is displayed in the View Settings page (Figure 43).

Figure 43) Viewing system status information by using SANtricity System Manager.



Controller base port status LEDs

Using out-of-band management to configure and support a newly installed E5700 based storage array requires connecting to an onboard Ethernet management port on each controller. The best practice for redundant array access is to connect your management network to one Ethernet port on each controller in an array and leave the other management port open for local access in case on-site support is required. The ports default to Dynamic Host Configuration Protocol (DHCP). If a DHCP server is not detected, the ports time out within five minutes and default to the factory assigned static addresses shown in Table 17.

Table 17) E-Series controller factory default Ethernet management port IP address assignment.

Controller ID	Management port 1 static IP	Management port 2 static IP
Controller A	192.168.128.101	192.168.128.102
Controller B	192.168.129.101	192.168.129.102

Figure 44 shows the dual 1Gb Ethernet management ports on the E5700 controller.

Figure 44) Dual Ethernet management ports on the E5700 controller canister.

Dual 1Gb Ethernet Management Ports

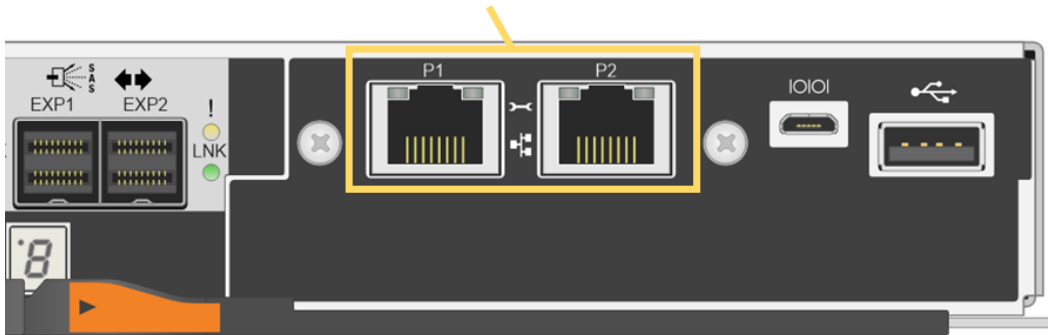


Table 18 defines the Ethernet management port LEDs on each port (P1 and P2). The ports are highlighted in Figure 44.

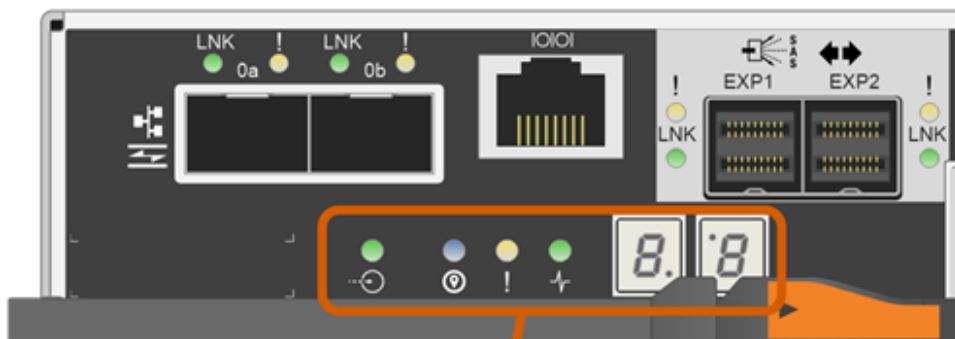
Table 18) Ethernet management port LED definitions.

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.

Figure 45 shows the onboard LED status indicators that are on the left side of the E5700 controller canister. Most of the LEDs are lit when a fault condition exists; however, the cache active LED is lit only 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 45 shows the controller status LEDs, and Table 19 defines them. The table lists the LEDs as they appear from left to right in the figure.

Figure 45) Controller module and array status LEDs.



Controller LED Status Display

Table 19) LED definitions for the controller base features.

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 7-segment LEDs	Yellow	<ul style="list-style-type: none"> Shelf ID if diagnostic LED off. Diagnostic code if diagnostic LED on. 	The controller is not powered on.

Figure 46 shows the onboard 16Gb FC or 10Gb iSCSI baseboard host port LEDs.

Figure 46) Ports 0a and 0b 16Gb FC/10Gb iSCSI baseboard host port status LEDs.

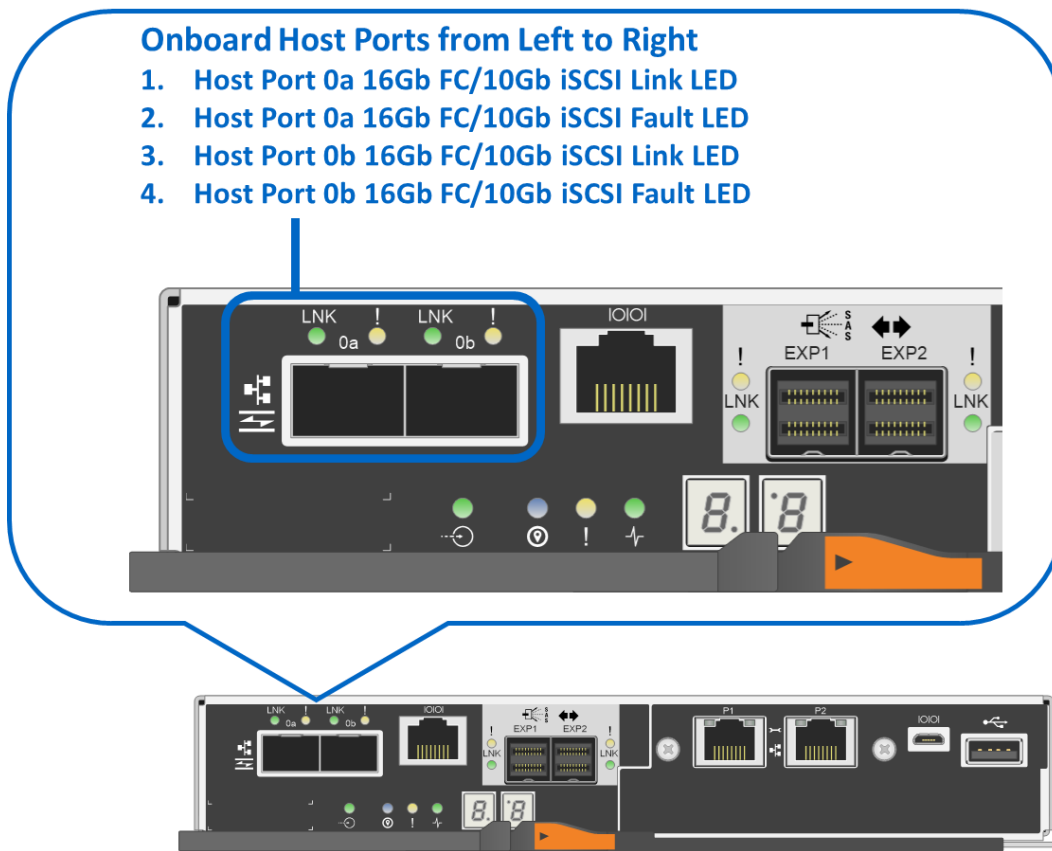


Table 20 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 46). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

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

LED name	Color	LED on	LED off
Host port link/activity	Green	<ul style="list-style-type: none"> • 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 E5700 controller canister is equipped with two 12Gb SAS expansion ports that are used to connect expansion-drive shelves to the E5700 controller shelf. Figure 47 shows the SAS expansion port LEDs.

Figure 47) LEDs for drive expansion ports.

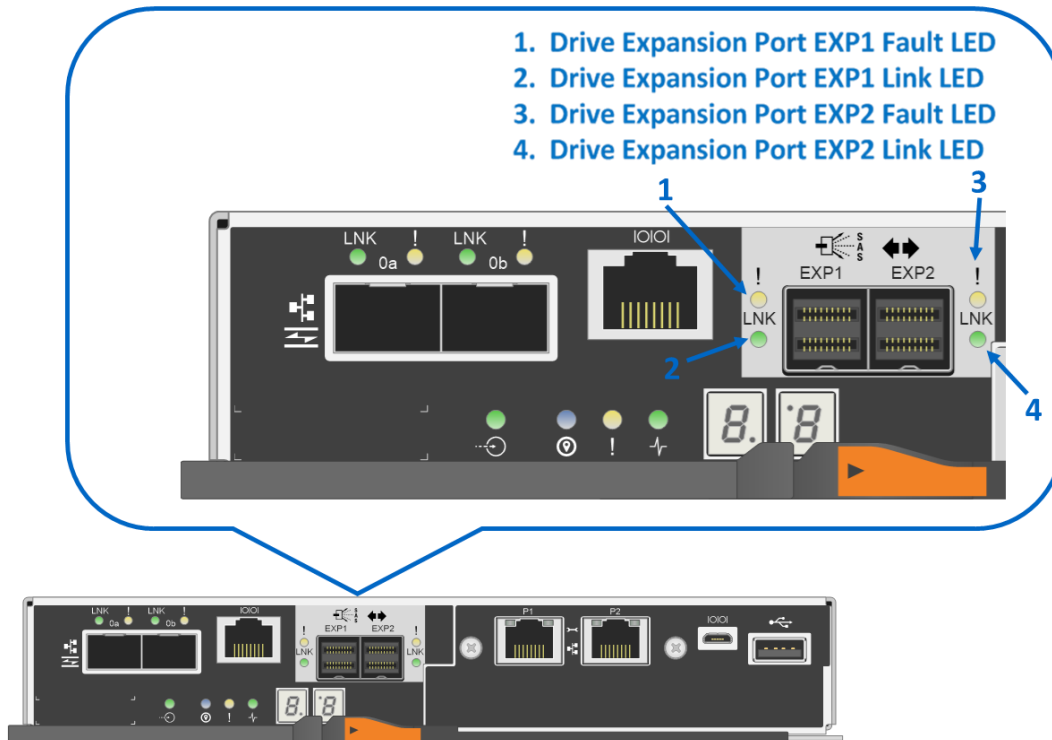


Table 21 defines each drive-side LED. The definitions for port EXP1 are repeated for port EXP2.

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.

E5700 optional host interface cards

The E5700 supports several host interface expansion options, including SAS, FC, iSCSI, and IB. This section provides detailed LED status definitions for all the HIC choices.

2-Port 100Gb IB HIC LEDs

Figure 48 shows the 2-port 100Gb IB HIC.

Figure 48) LEDs on the 2-port 100Gb IB HIC.

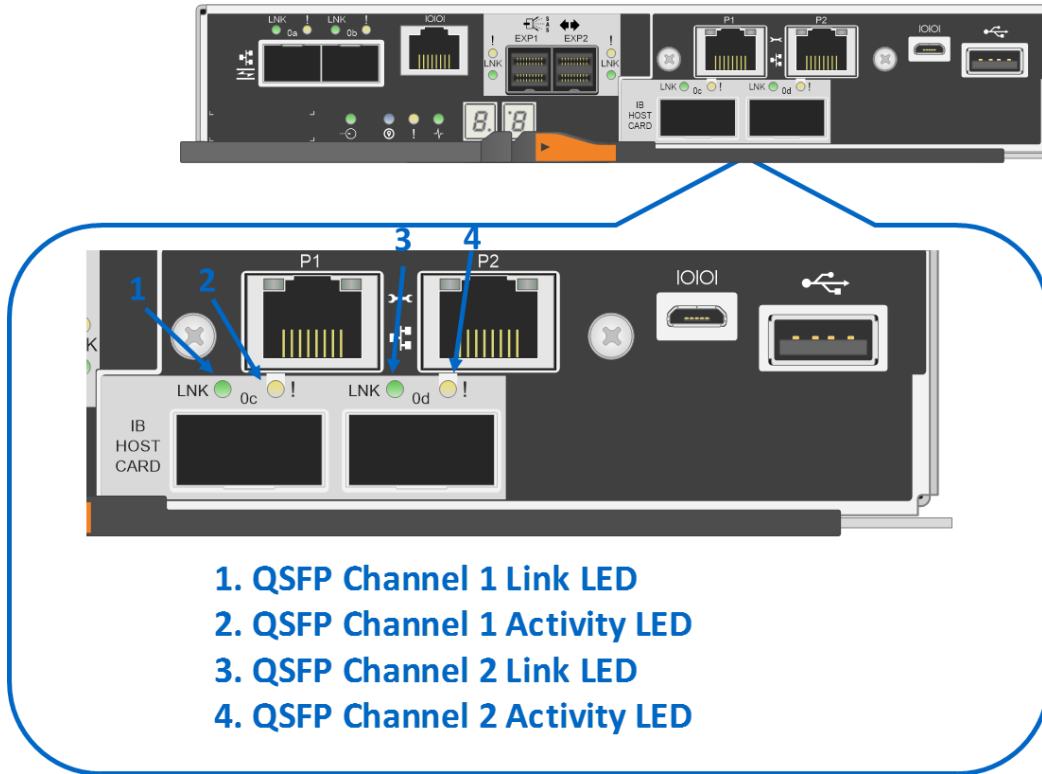


Table 22 defines the LEDs on the 2-port 100Gb IB HIC.

Table 22) LED definitions for the 2-port 100Gb IB HIC.

LED name	Color	LED on	LED off
QSFP link	Amber	The physical link is active.	The physical link is not active.
QSFP activity	Green	<ul style="list-style-type: none"> • Solid: Link is up without activity. • Blinking: Link is up with activity. 	The controller has not yet loaded the driver for the ConnectX host channel adapter.

4-Port 12Gb SAS HIC LEDs

Figure 49 shows the LEDs for the 4-port 12Gb SAS HIC. As shown, the ports use mini-SAS3 cables.

Figure 49) LEDs for the 4-port 12Gb SAS HIC.

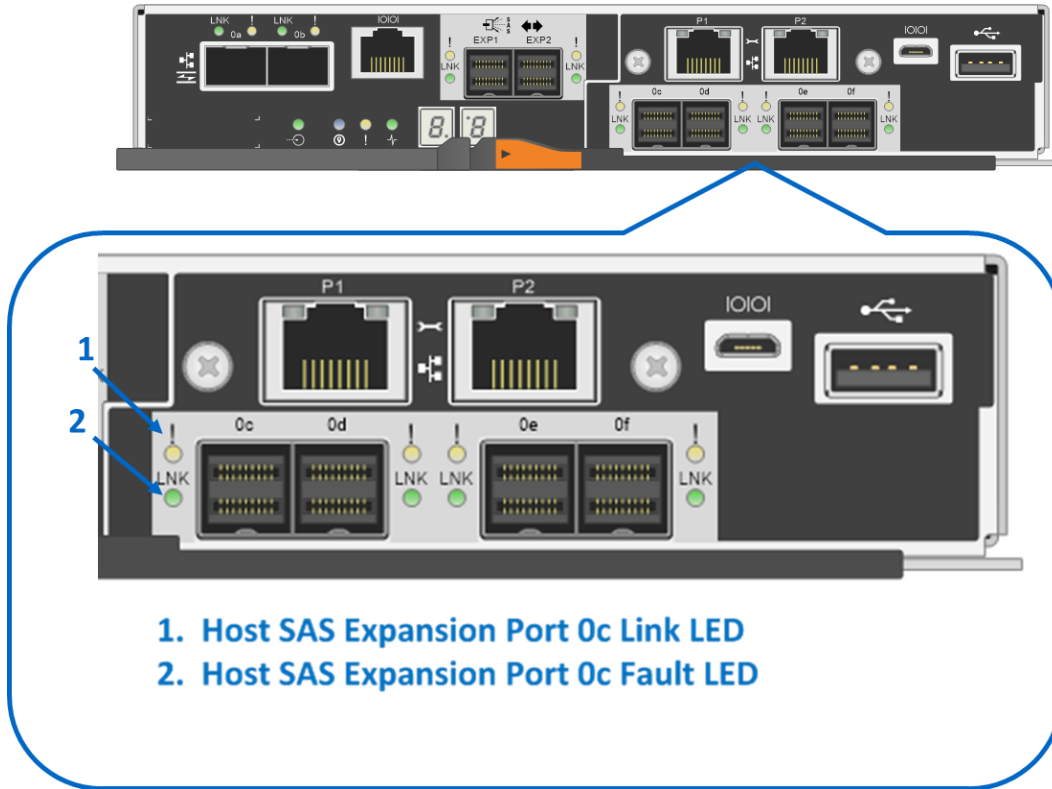


Table 23 defines the LEDs for the 4-port 12Gb SAS HICs.

Table 23) LED definitions for the 4-port 12Gb SAS HIC.

LED name	Color	LED on	LED off
Host SAS channel fault	Amber	At least one of the four PHYs is working, but another PHY cannot establish the same link to the device connected to the host input port connector.	Normal status.
Host SAS channel activity	Green	At least one of the four PHYs in the host input port is working, and a link has been established to the device connected to the input port connector.	A link error has occurred.

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

4-Port 32Gb FC HIC LEDs

The E5700 controller supports a 4-port 32Gbps FC HIC that offers the ability to autonegotiate down to 16Gbps by using the 32Gbps SFP. The 32Gb FC HIC does require OM4 fiber cable to connect to switches or to connect directly to hosts. Figure 50 shows the LEDs for the 4-port 32Gbps FC HIC.

Figure 50) LEDs for the 4-port 32Gb FC HIC.

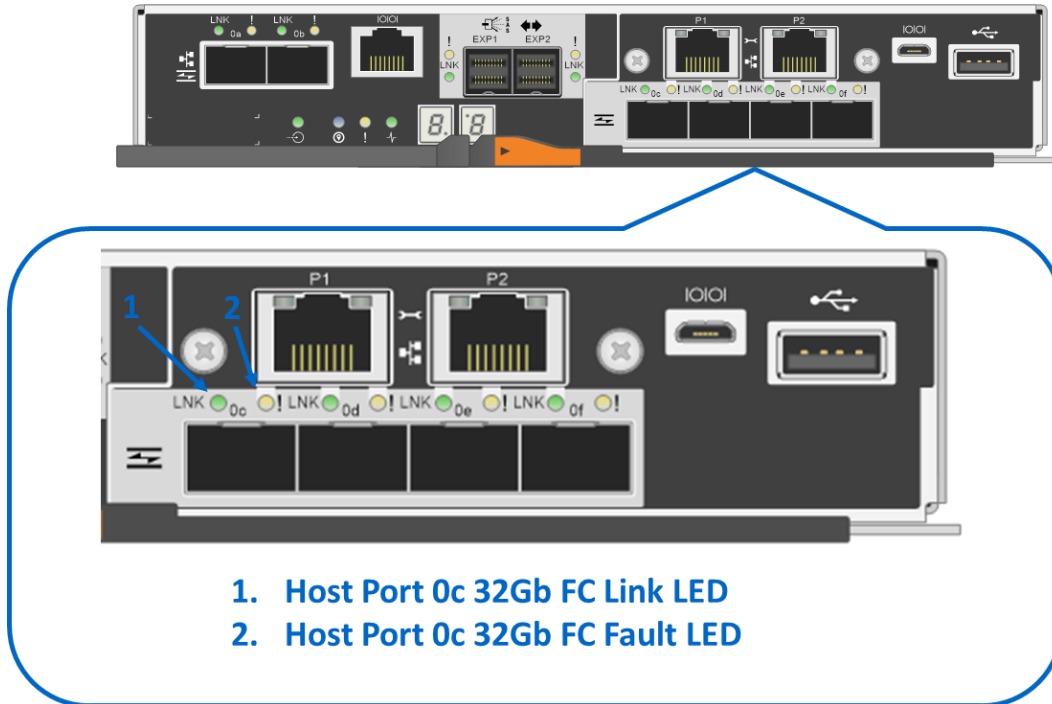


Table 24 defines the LEDs on the 4-port 32Gbps FC HIC.

Table 24) LED definitions for the 4-port 32Gbps FC HIC.

LED name	Color	LED on	LED off
Host port link/activity	Green	<ul style="list-style-type: none"> • 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 E5700 controller supports a 4-port 25Gbps iSCSI HIC that offers the ability to also run at 10Gbps by changing the port speed on each controller in SANtricity System Manager without changing the 25Gbps

SFP (25Gbps SFP supports 10Gbps speed). The 25Gb iSCSI HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 51 shows the LEDs for the 4-port 25Gbps iSCSI HIC.

Figure 51) LEDs for the 4-port 25Gb iSCSI HIC.

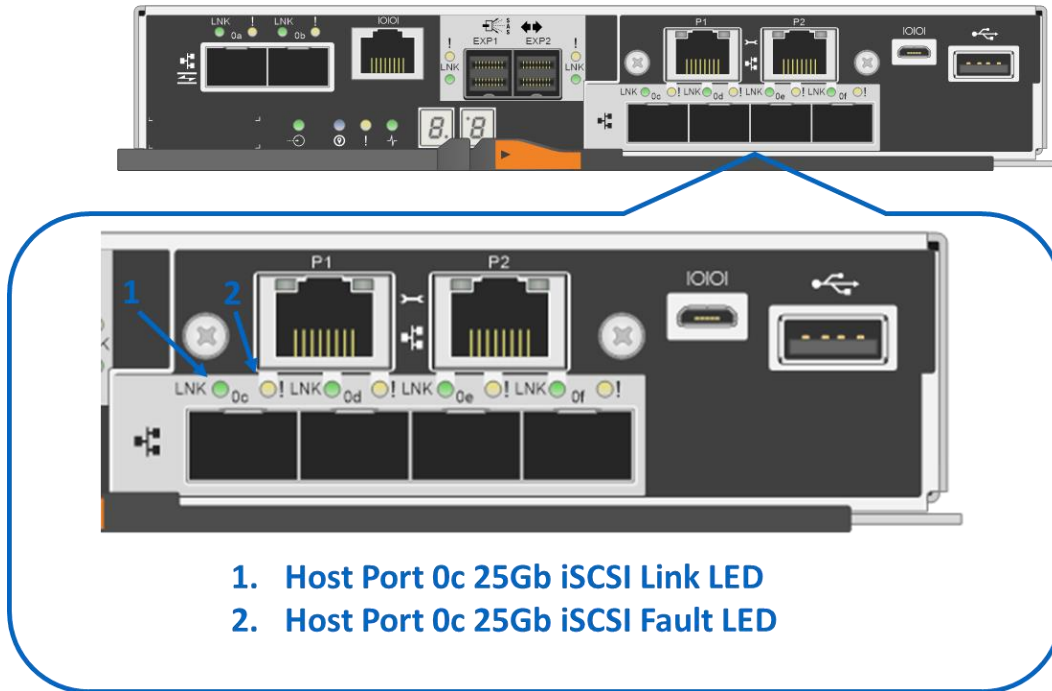


Table 25 provides the LED definitions for the 4-port 25Gb iSCSI HIC.

Table 25) 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	N/A

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 52 and Figure 53 show the push button for the E5724 (DE224C) and the E5760 (DE460C) systems, respectively.

Figure 52) ODP on the E5724 or DE224C (front bezel or end caps removed).

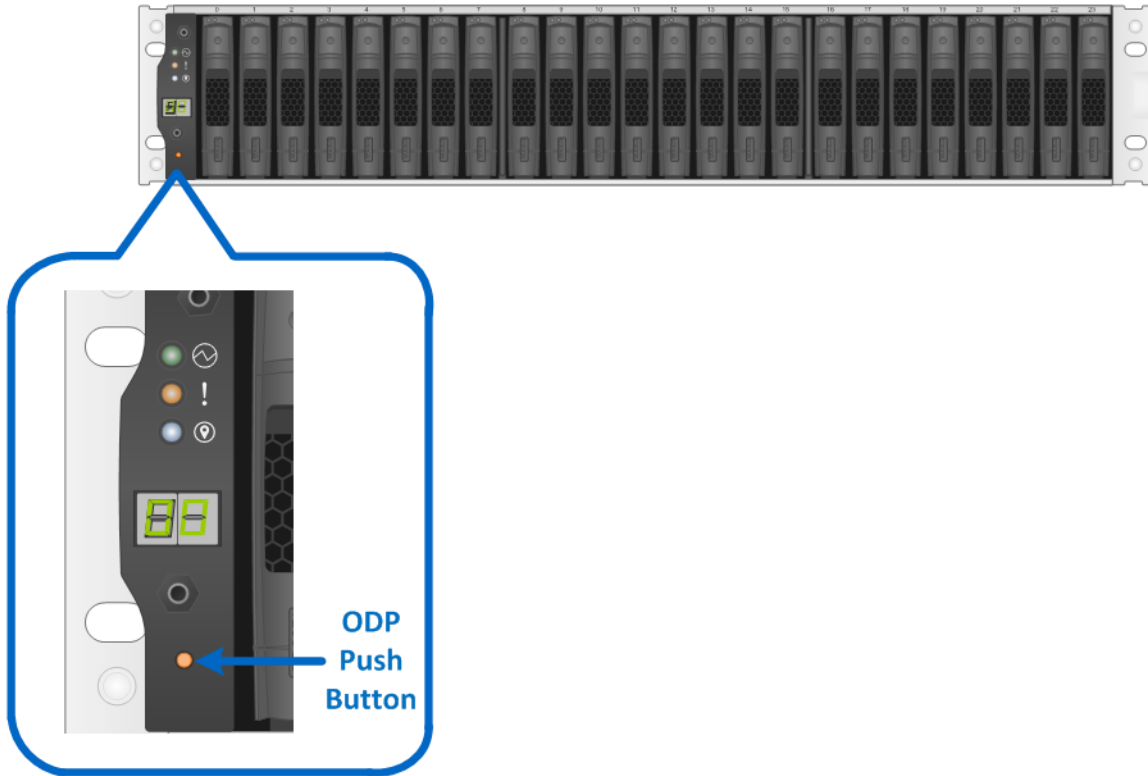


Figure 53) ODP on the E5760 or DE460C (front bezel removed).



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 two to three seconds.

4. If the ID takes longer than two to three 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 two to three 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 two to three 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 E5700 storage systems and related hardware, see the E5700 series documentation on the [E-Series and SANtricity documentation resources page](#).

Drive shelves

The E5700 controller shelf supports 24 or 60 drives based on the shelf model (DE224C or DE460C), but the system capacity can be further expanded by adding additional expansion-drive shelves to the controller-drive shelf. The E5700 supports up to 8 total shelves, the controller shelf plus seven expansion-drive shelves, for a maximum of 480 HDDs (120 SSDs). Table 26 shows the drive shelf options.

Table 26) Drive shelf options for E5700.

Property	DE224C	DE460C	DE5600	DE6600
Form factor	2U	4U	2U	4U
Drive size	2.5"	3.5" 2.5" (with bracket)	2.5"	3.5" 2.5" (with bracket)
Drive types	SAS SSD	SAS NL-SAS SSD	SAS SSD	SAS NL-SAS SSD
Total drives	24	60	24	60
Drive interface	12Gb SAS	12Gb SAS	6Gb SAS	6Gb SAS

Note: DE5600 and DE6600 are supported only as part of in-place data migration from E2700/E5400/E5500/E5600 to E5700.

Drive shelf configurations

E5700 controllers can be paired with all five E-Series shelves, and the shelves can be mixed in the same storage system. This document does not cover in detail the older 6Gb SAS 2 drive shelves (DE5600 and DE6600). It only mentions that mixing the 6Gbps shelf infrastructure with the 12Gbps shelf infrastructure requires the drive side interface to run at 6Gbps. For more information, see the [E-Series Disk Shelves](#) documentation. The following sections provide detailed information about the 12Gb SAS 3 drive shelves (DE224C and DE460C).

DE224C drive shelf

The DE224C is a 2U shelf that holds up to twenty-four 2.5-inch drives. 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 54 and Figure 55 show the front view of the DE224C drive shelf, and Figure 56 shows the rear view.

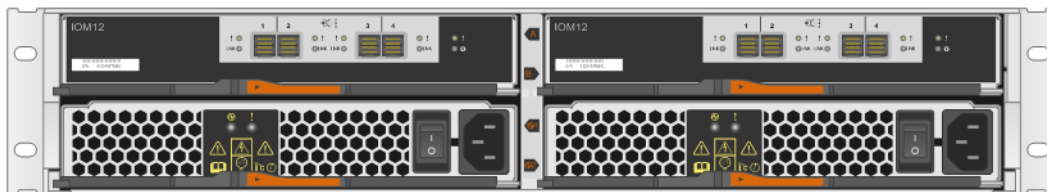
Figure 54) DE224C front view with end caps.



Figure 55) DE224C front view without end caps.



Figure 56) DE224C rear view.



The modular design of the DE224C makes the hardware easy to deploy and maintain over the life of the storage system.

DE460C drive shelf

The DE460C is a 4U 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 with no disruption to other running drives in the drawer.

Figure 57 and Figure 58 show the front view of the DE460C drive shelf, and Figure 59 shows the rear view.

Figure 57) DE460C front view with the bezel.

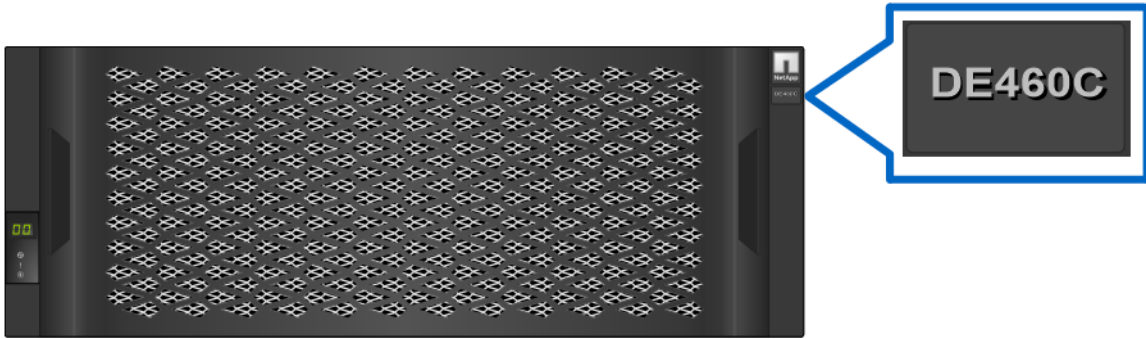


Figure 58) DE460C front view without the bezel.

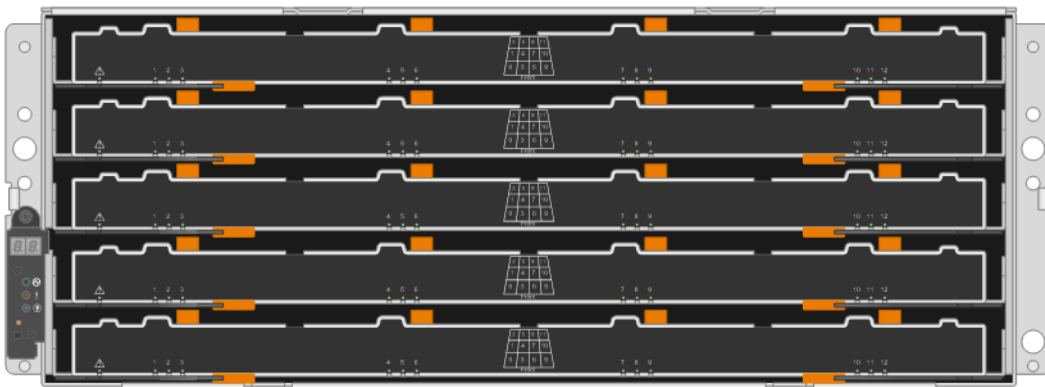
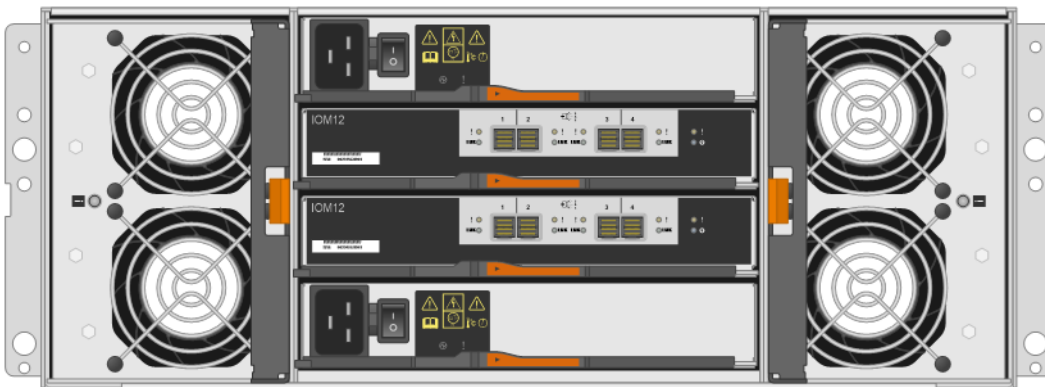


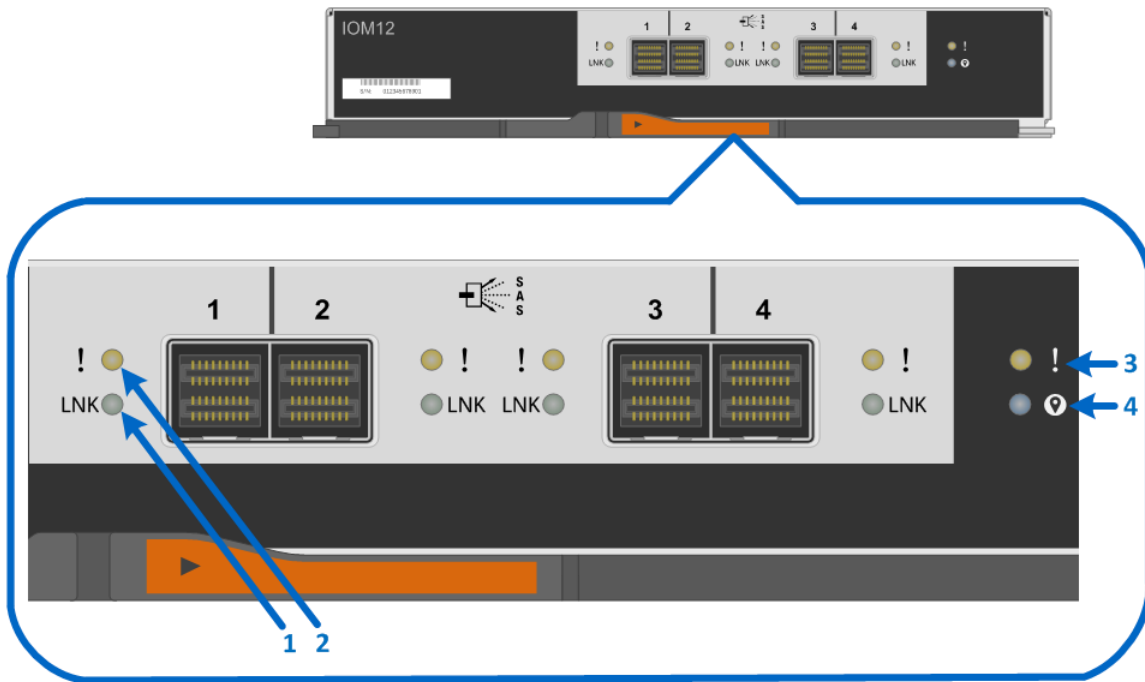
Figure 59) DE460C rear view.



IOM LED definitions

Figure 60 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 the same LEDs.

Figure 60) LEDs for IOM.



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

Table 27 defines the LEDs for the IOM.

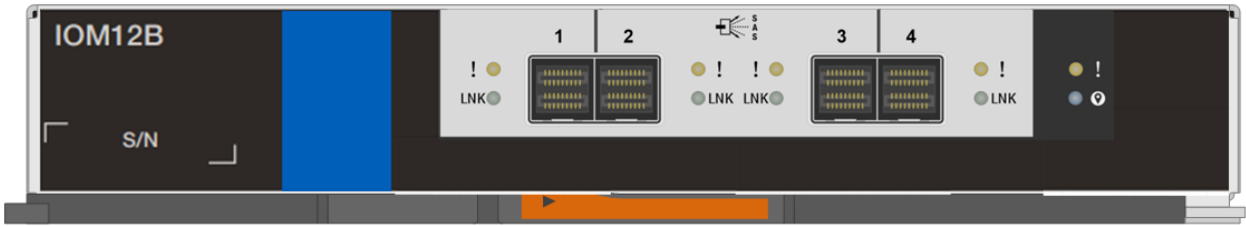
Table 27) IOM LED definitions.

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 later SANtricity versions. IOM12 and IOM12B are not supported in the same shelf but can exist in the same stack. Figure 61 shows the new IOM12B.

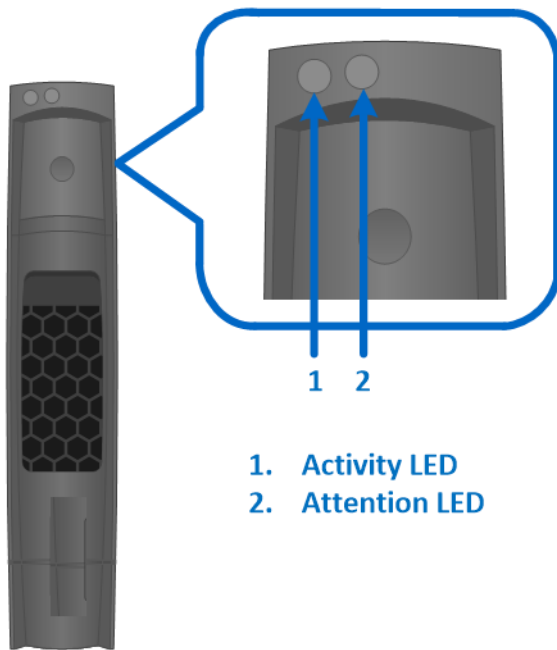
Figure 61) IOM12B.



Drive LED definitions

Figure 62 shows the LEDs on the drive carriers for the E5724. The DE224C shelf supports only 2.5-inch form-factor drives (10K SAS and SSDs).

Figure 62) E5724 drive carrier LEDs.



1. Activity LED
2. Attention LED

Table 28 defines the LEDs for the drives.

Table 28) E5724 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.
	Blinking amber	Drive locate turned on.	Normal status.

For the DE460C shelf, there is a shelf attention LED (1), drawer attention LED (2), and drive activity LED (3), as shown in Figure 63. The shelf attention LED is displayed when a drawer is open. The drawer and drive (see Figure 64) attention LEDs indicate the location of failed drives. The activity LED for each drive

is shown on the front of the drawer to indicate the location of the drive. The LED definitions are provided in Table 29.

Note: The drive activity LED on the drawer is not illuminated for failed drives. See item 3 in Figure 63 for an example.

Figure 63) DE460C shelf and drawer attention LEDs.

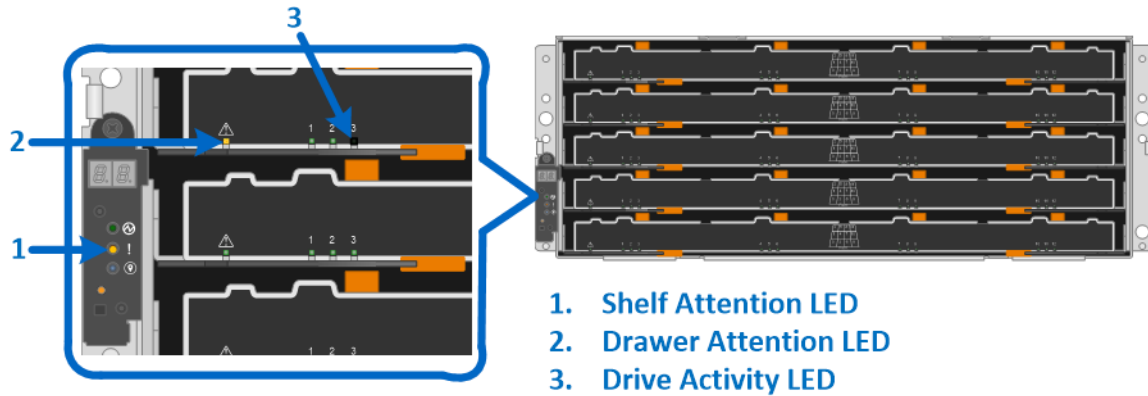


Figure 64) DE460C drive attention LED.



Drive Attention LED

Table 29) E5760 drive LED definitions.

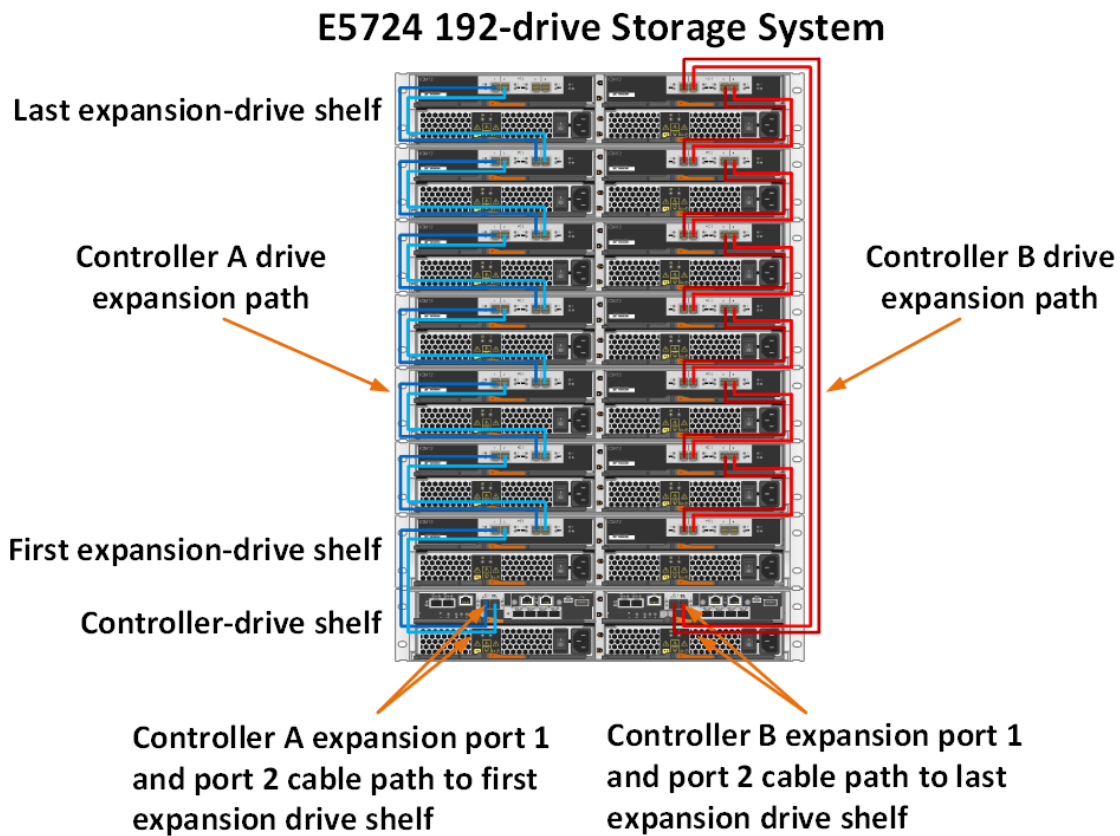
LED name	Color	LED on	LED off
Drive activity	Green	Drive has power.	Drive does not have power, or an error occurred with the functioning of the drive.
	Blinking green	The drive has power, and I/O is in process.	Drive does not have power, or an error occurred with the functioning of the drive.
Shelf attention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

LED name	Color	LED on	LED off
Drive attention	Amber	An error occurred with the functioning of the drive.	Normal status.
	Blinking amber	Drive locate turned on.	Normal status.

Greenfield installation

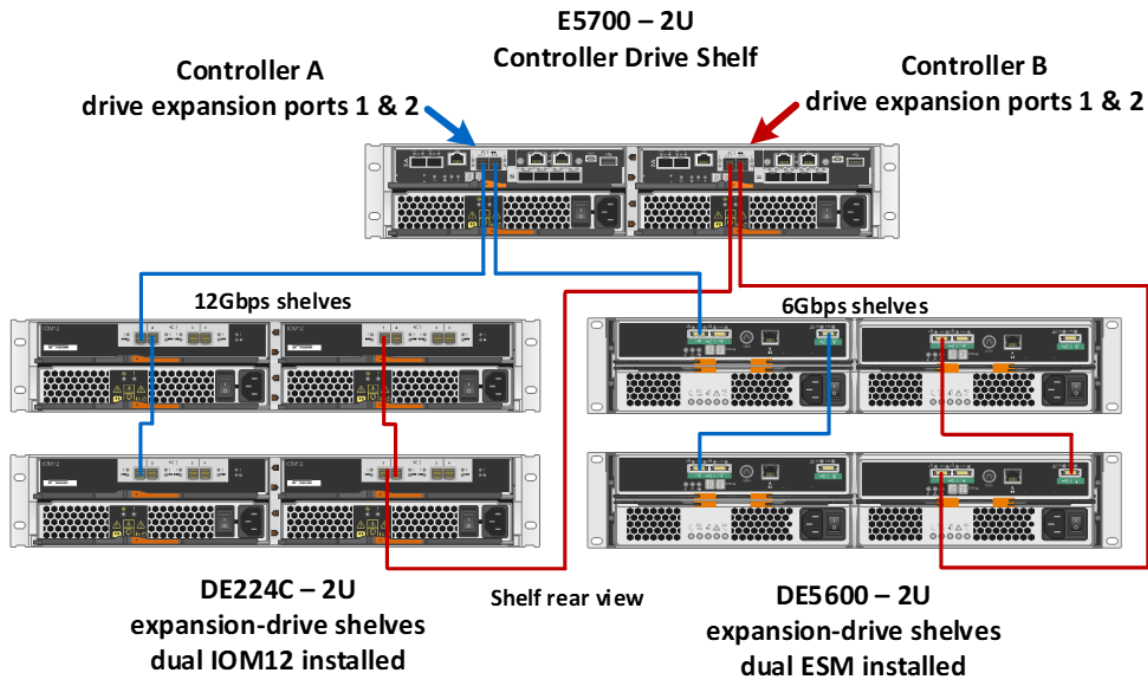
E5700 storage systems use a cabling method that matches the E2800 storage system, as shown in Figure 65.

Figure 65) E5724 expansion-drive shelf cabling example for the maximum DE224C shelf configuration.



For optimal performance, SAS 2 and SAS 3 drive shelves should be isolated into different storage systems. However, if you decide to add 6Gbps SAS drive expansion shelves to an E5700 array, you should use dual-stack cabling, as shown in Figure 66.

Figure 66) E5724 in a dual-stack configuration with 12Gbps and 6Gbps drive shelves installed.



Note: 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 has been resolved.

Best practices

- When you initially power on an E-Series storage system that includes expansion-drive shelves, power on the expansion-drive shelves first and wait one to two minutes per drive shelf before you power on the controller shelf.
- To power off an E-Series storage system that includes expansion-drive shelves, confirm that all host I/O operations have stopped. Then, turn off both power switches on the controller shelf and wait for all LEDs on the shelf to go dark. Finally, turn off both power switches on any attached expansion-drive shelves and wait two minutes for the drive activity to stop.

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 that NetApp recommends. 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.

The SANtricity cable connections report can be used to verify that the cabling is configured appropriately. 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 the <http://mysupport.netapp.com/eseriesHot adding a drive shelf> section of the E-Series online documentation or contact NetApp Customer Support Delivery.

Figure 67 and Figure 68 show the hot-add connectivity when a drive shelf is added as the last shelf in the system.

Figure 67) Drive shelf hot-add controller A expansion ports 1 and 2 cabling.

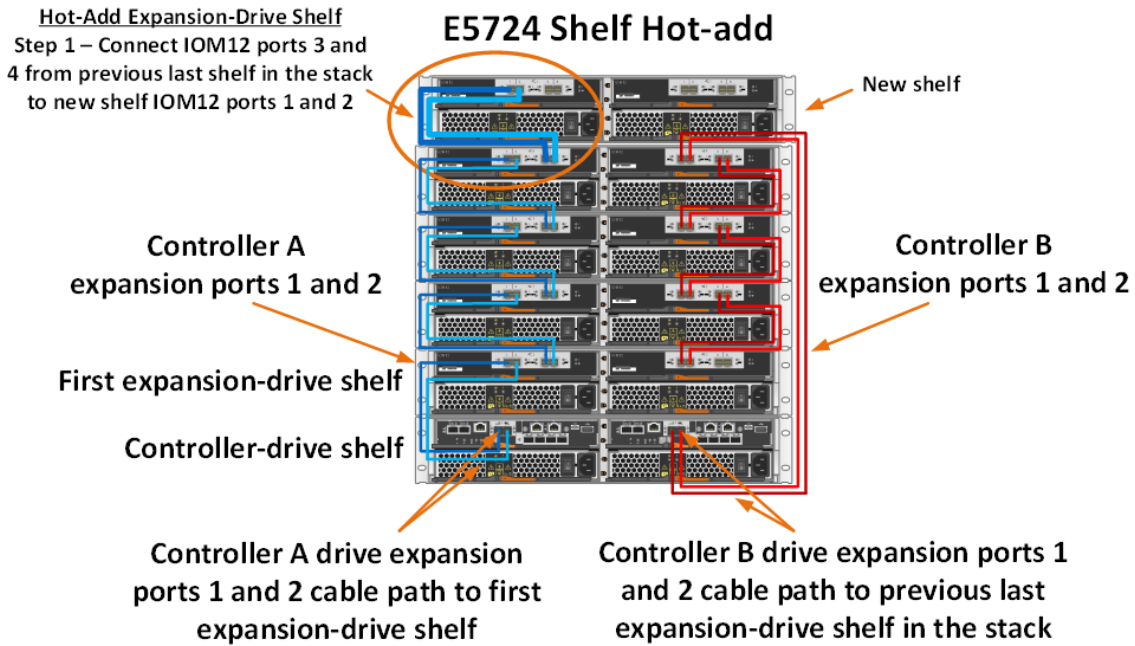
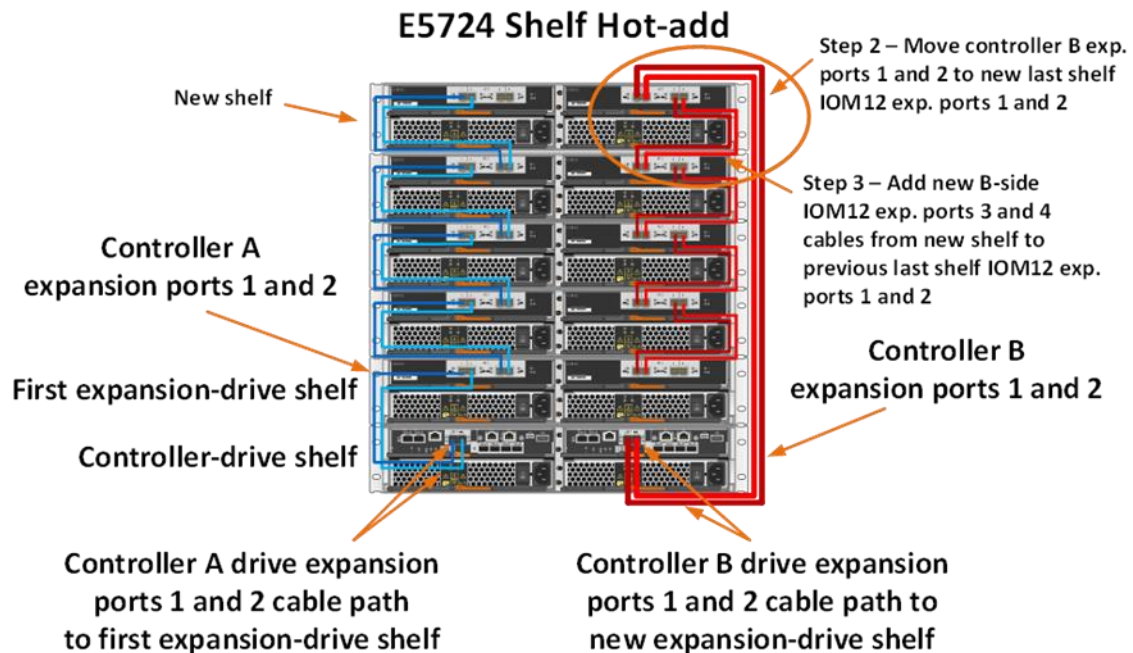


Figure 68) Drive shelf hot-add controller B expansion ports 1 and 2 cabling.



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.
- The cabling plan for the new shelf does not simultaneously interrupt both SAS expansion paths for controller A and controller B to the expansion-drive shelves at the same time.
- The new expansion port 1 path is confirmed to be valid, and the new shelf is visible in SANtricity before the expansion path 2 is 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 E5700 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 69.

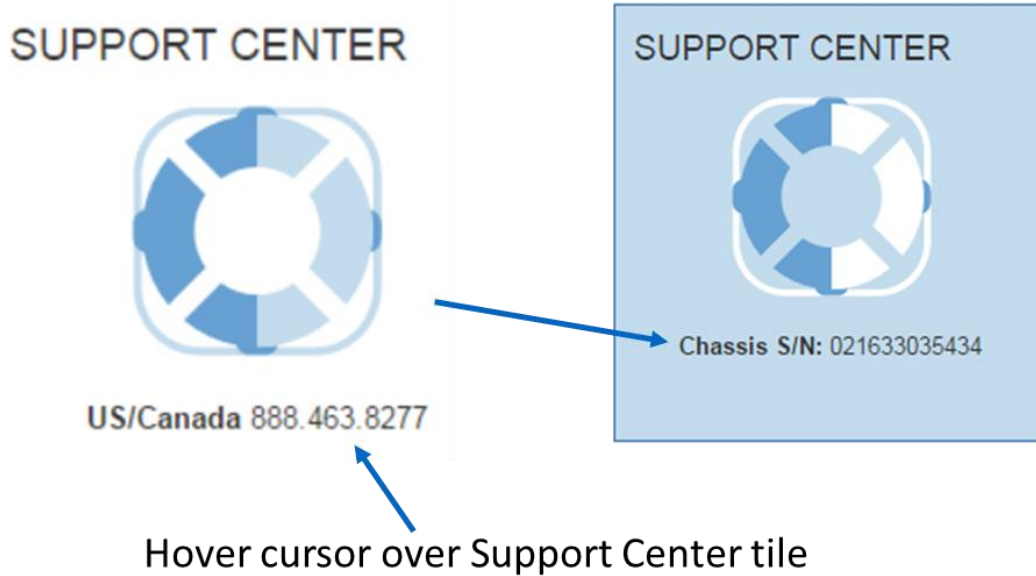
Figure 69) Controller shelf SN.



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 70.

Figure 70) SANtricity System Manager Support Center tile showing the chassis serial number.



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 E5700 systems, there are currently no premium features. All features are enabled out of the box.

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

The E5700 controllers are equipped with onboard FC or iSCSI base ports from the factory, but feature pack keys are used to change the host interface protocol from FC to iSCSI or from iSCSI to FC. The feature pack keys are also used to change the protocol on IB/Ethernet HIC. The process to generate a new feature pack key for your storage array is the same as the process to generate a premium feature key, except that the 11-digit key activation code for each package is available at no additional cost. For the hardware upgrade instructions per controller type, see the resources on the [E-Series and SANtricity documentation resources page](#).

The following information is required to generate a feature pack key file:

- 11-digit key activation code
- Array serial number shown in System Manager by selecting Support, then Support Center
- Feature Enable Identifier shown in System Manager by selecting Settings, then System, and reference the identifier in the Add-ons section

After the feature pack file is downloaded to the host server, click Change Feature Pack (Figure 71). Follow the prompts, beginning with browsing to the feature pack file (Figure 72).

Figure 71) Change feature pack from Settings>System view.

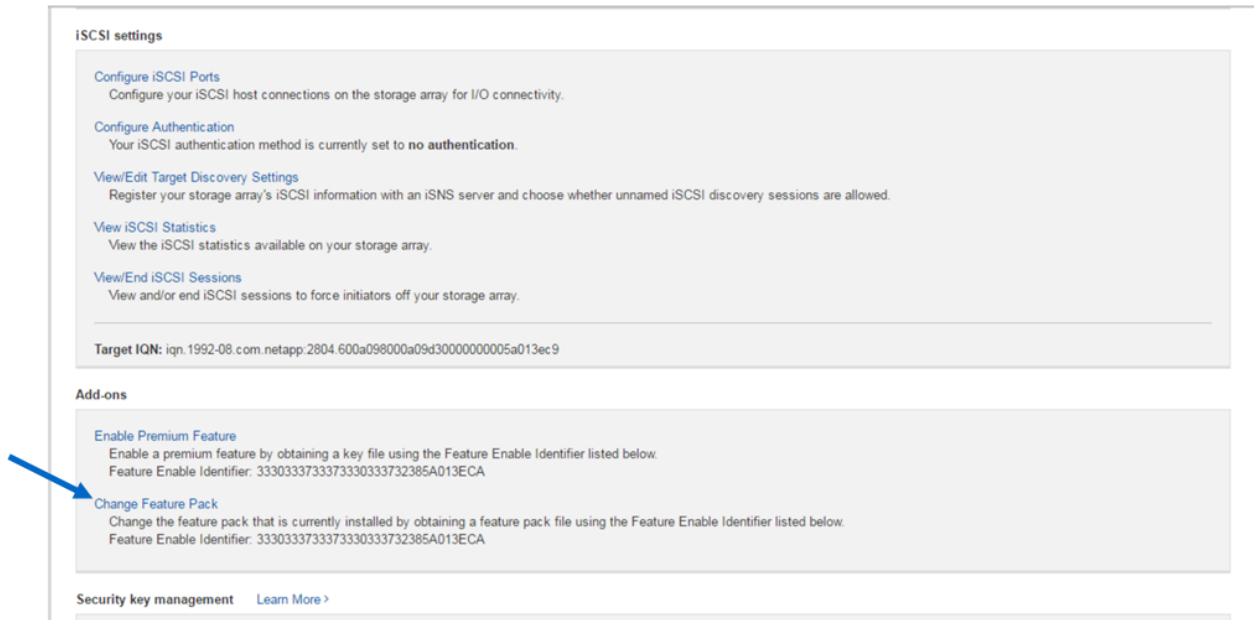
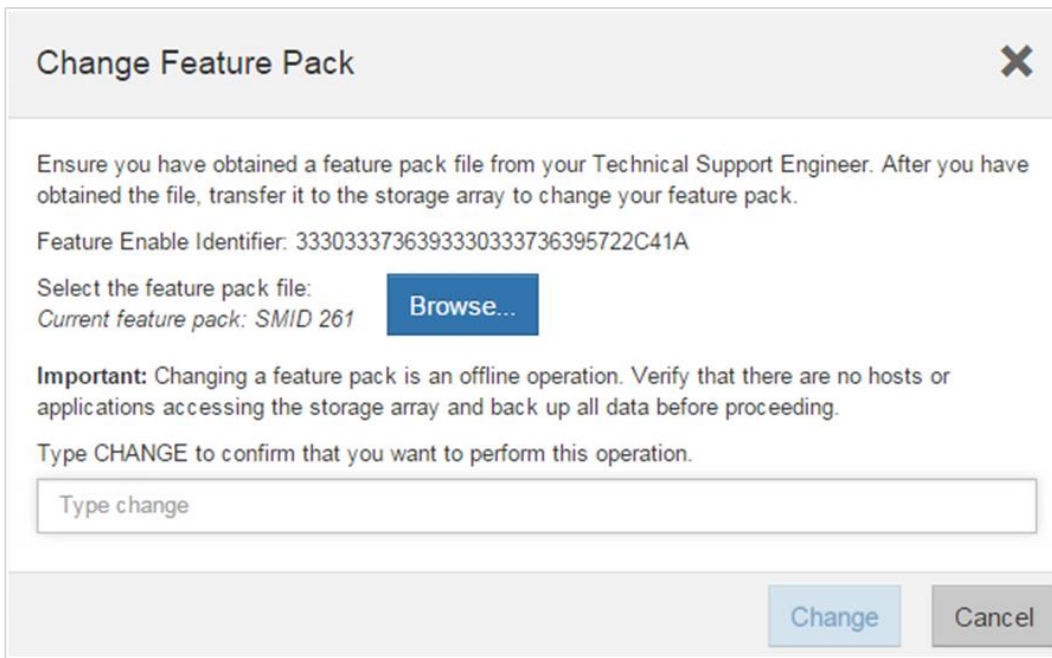


Figure 72) Change Feature Pack in SANtricity System Manager.



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

E-Series E5700 storage systems allow customers to cut operational costs with ultra-dense drive shelves that support capacity-hungry applications. The E5700 arrays deliver predictable performance with three distinct classes of drives to support new parallel file systems or analytics applications like Splunk. This capability enables customers to easily scale to implement SAN building blocks to meet growing performance and capacity requirements.

The enhanced SANtricity security features make the E5700 suitable for large enterprise environments with many employees, while maintaining setup simplicity for small and medium environments where a small team supports everything.

E5700 storage systems provide extreme throughput performance up to 21GBps with flexible, faster host interfaces. The E5760 scales up to 480 drives, currently 8.64PB of raw capacity to support backup, video, and analytics workloads. The E5760 equipped with SSDs can deliver I/O at sub millisecond latency with up to 99.9999% reliability. This combination of packaging flexibility, capacity options, performance capabilities, reliability, and simplicity delivered with SANtricity makes the E-Series E5700 family of arrays the perfect choice to support traditional transactional workloads and innovative enterprise applications.

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 E5700 datasheet
<https://www.netapp.com/us/media/ds-3894.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.
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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

TR-4724-1124