



Technical Report

Introduction to NetApp EF-Series EF280

Feature Overview with NetApp SANtricity 11.60.2

Mitch Blackburn, NetApp
May 2020 | TR-4727

Abstract

The NetApp® EF280 all-flash array delivers high performance in an entry-level EF-Series all-flash array. This report provides detailed information about the multiple system configuration options of NetApp SANtricity® 11.60.2. It is also a great starting point to introduce EF280 system details to sales engineers, partners, service providers, and customers.

TABLE OF CONTENTS

1	Introduction	6
2	SANtricity Management Features	8
2.1	Deployment	8
2.2	SANtricity Unified Manager	10
2.3	SANtricity Unified Manager Navigation	12
2.4	SANtricity System Manager	19
2.5	SANtricity Storage Features	33
2.6	SANtricity Management Integration	37
3	SANtricity Software Specifications for EF280 Hardware	41
4	EF280 Hardware Configurations	43
4.1	Controller Shelf Configurations	43
4.2	Controller Host Interface Features	45
4.3	Hardware LED Definitions	47
4.4	Setting Shelf ID with ODP Pushbutton	59
5	Drive Shelves	61
5.1	IOM LED Definitions	61
5.2	Drive LED Definitions	62
5.3	Greenfield Installation	63
5.4	Drive Shelf Hot Add	65
6	E-Series Product Support	68
6.1	Controller Shelf Serial Number	68
6.2	License Keys	69
7	Conclusion	71
	Where to Find Additional Information	71
	Version History	71

LIST OF TABLES

Table 1)	Controller options with associated HIC options.	6
Table 2)	Management use cases.	19
Table 3)	Built-in roles and associated permissions.	26
Table 4)	LDAP/RBAC required fields and definitions.	26
Table 5)	SANtricity host types and associated failover behavior in SANtricity 11.60.x.	34
Table 6)	SANtricity 11.60.x features for long-term reliability.	34

Table 7) EF280 standard features that are included with SANtricity 11.60.x.....	36
Table 8) SANtricity 11.60.x copy services features.	36
Table 9) SANtricity APIs and toolkits.	37
Table 10) Third platform plug-ins that use the SANtricity Web Services Proxy.	38
Table 11) SANtricity software boundaries for EF280-based storage systems.....	41
Table 12) EF280 technical specifications.	44
Table 13) FC host interface port speed and associated SFPs.	46
Table 14) iSCSI host interface port speed and associated SFPs.	46
Table 15) EF280 controller shelf LED definitions (front panel).	48
Table 16) EF280 controller shelf power and fan canister LED definitions.	50
Table 17) iSCSI RJ-45 baseboard host port LED definitions.....	53
Table 18) Ethernet management port LED definitions.....	53
Table 19) Controller base features LED definitions.	53
Table 20) 16Gb FC/10Gb iSCSI baseboard host port LED definitions.	54
Table 21) Drive expansion port LED definitions.	55
Table 22) 2-port and 4-port 12Gb SAS HIC LED definitions.....	56
Table 23) 2-port and 4-port optical HIC (16Gb FC or 10Gb iSCSI) LED definitions.	58
Table 24) 4-port 32Gb FC HIC LED definitions.	58
Table 25) 4-port optical 25Gb iSCSI HIC LED definitions.	59
Table 26) IOM LED definitions.	62
Table 27) EF280 drive LED definitions.	63

LIST OF FIGURES

Figure 1) New generation NetApp EF280 all-flash array with the bezel removed.	6
Figure 2) EF280 controller ports.	7
Figure 3) Which SANtricity management components should you install?.....	8
Figure 4) Managing a single EF280 with SANtricity System Manager.	9
Figure 5) Managing multiple new generation systems with SANtricity Unified Manager and SANtricity System Manager.	9
Figure 6) Managing a mixed-array environment with SANtricity Storage Manager and System Manager.	10
Figure 7) Final dialog box in the Web Services Proxy installation wizard.	11
Figure 8) SANtricity Unified Manager login page.....	12
Figure 9) New SANtricity Unified Manager landing page—discover and add arrays.....	13
Figure 10) SANtricity Unified Manager landing page.....	13
Figure 11) Creating a group to organize arrays in SANtricity Unified Manager.	14
Figure 12) Creating a group in Unified Manager.	14
Figure 13) SANtricity Unified Manager showing a newly created group.	15
Figure 14) SANtricity Unified Manager Operations view.	15
Figure 15) SANtricity System Manager home page.	22
Figure 16) System Manager Storage page.....	23

Figure 17) System Manager Hardware page.....	23
Figure 18) System Manager Settings page with new security tiles.....	24
Figure 19) System Manager Support page.....	24
Figure 20) System Manager Support Center.....	25
Figure 21) SANtricity System Manager directory server setup wizard.....	28
Figure 22) Role Mapping tab in the directory server settings wizard.	29
Figure 23) SANtricity System Manager views change based on user permission level.	30
Figure 24) Initial step required to set up web server certificates.....	31
Figure 25) SANtricity System Manager Certificates tile expanded.	31
Figure 26) Opening the API documentation.	38
Figure 27) Example expanding the Device-ASUP endpoint.	39
Figure 28) REST API documentation sample.....	39
Figure 29) Sample output from the Try It Out button.	40
Figure 30) Device-asup endpoint possible response codes and definitions.	40
Figure 31) Opening the CLI Command Reference.	41
Figure 32) EF280 front view with bezel.	43
Figure 33) EF280 front view (open).....	43
Figure 34) EF280 rear view.	43
Figure 35) EF280 with optional HICs.....	47
Figure 36) ODP on front panel of EF280 controller shelf.....	48
Figure 37) Setting shelf ID by using SANtricity System Manager.....	49
Figure 38) LEDs on EF280 power fan canister (rear view).....	50
Figure 39) Viewing system status information by using SANtricity System Manager.....	51
Figure 40) LEDs on left side of EF280 controller canister with Base-T iSCSI host ports.....	52
Figure 41) LEDs on left side of EF280 controller canister with 16Gb FC/10Gb optical iSCSI host ports.....	54
Figure 42) LEDs for drive expansion ports (no HIC installed).....	55
Figure 43) LEDs for 4-port 12Gb SAS HIC.....	56
Figure 44) LEDs for 2-port 12Gb SAS HIC.....	56
Figure 45) LEDs for 4-port optical HIC (16Gb FC or 10Gb iSCSI).	57
Figure 46) LEDs for 2-port optical HIC (16Gb FC or 10Gb iSCSI).	57
Figure 47) LEDs for 4-port 32Gb FC HIC.	58
Figure 48) LEDs for 4-port 25Gb iSCSI HIC.....	59
Figure 49) ODP on the DE224C (front bezel or end caps removed).	60
Figure 50) DE224C front view with end caps.	61
Figure 51) DE224C front view without end caps.	61
Figure 52) DE224C rear view.	61
Figure 53) LEDs for IOM.	62
Figure 54) EF280 drive carrier LEDs.....	63
Figure 55) EF280 expansion drive shelf cabling example for maximum DE224C shelf configuration.	64
Figure 56) EF280 with mixed 6Gbps and 12Gbps expansion shelves.	65

Figure 57) Drive shelf hot-add controller expansion A-side cabling.....	66
Figure 58) Drive shelf hot-add controller expansion B-side cabling.....	67
Figure 59) Controller shelf SN.	68
Figure 60) SANtricity System Manager Support Center tile showing chassis serial number.	69
Figure 61) Change feature pack from Settings > System view.....	70
Figure 62) Change Feature Pack option.....	70

1 Introduction

The NetApp EF280 has a modern look, see Figure 1, uses 12Gbps DE224C drive shelves, and supports the more secure SANtricity System Manager GUI (as does the mid-range EF570) in an entry-level all-flash array. It delivers optimal performance for both mixed random workloads and large sequential workloads.

Figure 1) New generation NetApp EF280 all-flash array with the bezel removed.



The EF280 can deliver consistent submillisecond latency response times for up to 300,000 4KB random read IOPS with as few as 12 solid-state drives (SSDs). The 24-drive configuration can deliver up to 10GBps of large sequential read throughput and 3.7GBps of cache mirrored large sequential write throughput.

This performance versatility is enhanced by multiple SSD choices to achieve the price-performance combination that fits your business need. Current drive choices include:

- Entry-price-point 800GB SSDs for fast, small random workloads
- 1.6TB and 3.8TB fast, large-capacity SSDs to support higher-capacity sequential workloads, random workloads, or mixed workloads
- 7.6TB and 15.3TB SSDs for fast, large-capacity requirements

NetApp EF-Series products have a documented history of delivering up to 99.9999% availability when systems are properly sized, deployed, and maintained with NetApp agreements. This includes the use of NetApp AutoSupport® technology to enhance your ongoing product experience.

Note: EF280 controllers are not offered in the 12-drive DE212C shelf or in the 60-drive DE460C shelf.

Each EF280 controller provides two Ethernet management ports for out-of-band management and has two 12Gbps wide-port (x4 lanes) SAS drive expansion ports for redundant drive expansion paths. The EF280 controllers also include two built-in host ports, either two 16Gb FC/10Gb iSCSI or two 10Gb iSCSI RJ-45. However, one of the following host interface cards (HICs) can be installed in each controller, including the new 32Gb FC or 25Gb iSCSI options as shown in Table 1.

Table 1) Controller options with associated HIC options.

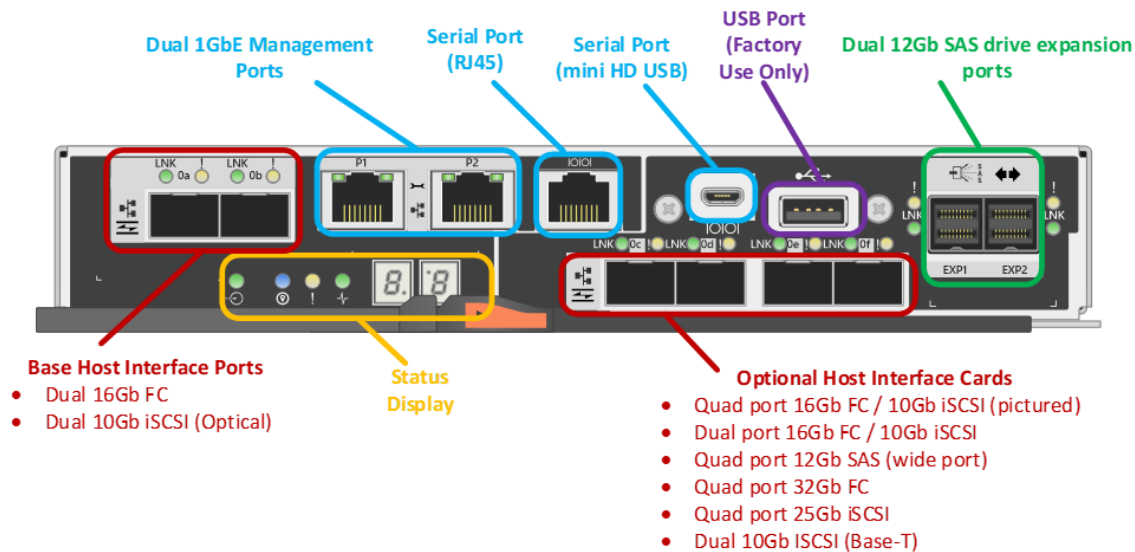
Controller Type	2-Port / 4-Port 12Gb SAS HIC	2-Port / 4-Port 16Gb FC / 10Gb iSCSI HIC	4-Port 32Gb FC	4-Port 25Gb iSCSI	2-Port 10Gb iSCSI (Base-T)
EF280 w/ optical baseboard ports	Yes	Yes	Yes	Yes	Yes

Controller Type	2-Port / 4-Port 12Gb SAS HIC	2-Port / 4-Port 16Gb FC / 10Gb iSCSI HIC	4-Port 32Gb FC	4-Port 25Gb iSCSI	2-Port 10Gb iSCSI (Base-T)
E2800 w/ base-T baseboard ports	Yes	No	No	No	Yes

Note: A software feature pack can be applied in the field to change the host protocol of the optical baseboard ports and the optical HIC ports from FC to iSCSI or from iSCSI to FC.

Figure 2 identifies the various interface ports on the EF280 controller.

Figure 2) EF280 controller ports.



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

For detailed instructions about how to change host protocols, go to the Upgrading > Hardware Upgrade section at <https://mysupport.netapp.com/eseries>.

The EF280 continues the E-Series legacy of fast, simple, reliable, and flexible SAN storage regardless of the workload. E-Series EF280 all-flash arrays can support workloads if the following conditions are met:

- Hosts are qualified with E-Series arrays (most common host types are supported).
- The hosts use SAN access to the storage, whether directly connected or fabric connected.
- The storage is managed at the host or file system level.

In fact, SMB to large enterprise customers use EF280 arrays because they are simple to install and operate, and they are reliable (up to 99.9999% data availability). These highly flexible SAN building blocks can be applied when you need them and can be plugged into your current application environment on demand. EF-Series arrays can operate in a space as small as two rack units (RU), can seamlessly integrate with many software layers, and can still deliver consistent low-latency performance. These capabilities make EF280 an optimal SAN building block for any size enterprise for the cost of an entry-level, all-flash system.

Whether you are running specialty applications with demanding metadata requirements or surveillance analytics, the EF280 maintains its performance profile as systems scale up to 96 SSDs or four total shelves. Only minor settings changes are required when you create disk pools, volume groups, or

volumes to switch between high-IOPS configurations and high-throughput configurations, making EF-Series arrays easy to deploy regardless of workload.

2 SANtricity Management Features

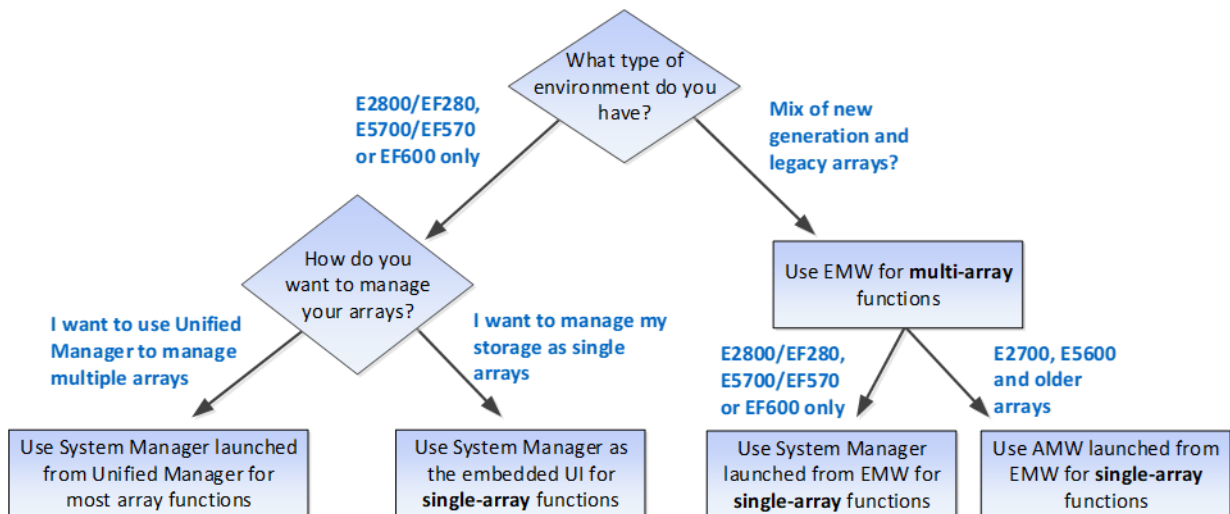
NetApp E-Series and EF-Series arrays have a rock-solid reputation for reliability, availability, simplicity, and security. The NetApp SANtricity 11.60.2 release builds on that legacy by adding a secure CLI to SANtricity System Manager and improving the configuration of mirroring in SANtricity Unified Manager.

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.

2.1 Deployment

Deciding which components to install on an EF280-based storage array depends on how you answer the questions in Figure 3.

Figure 3) Which SANtricity management components should you install?



Note: If you are not using synchronous or asynchronous mirroring features and only have new generation E5700 or E2800 storage arrays, an alternative to installing the Unified Manager to manage multiple arrays is to simply bookmark each array in a web browser.

Single EF280 Storage Array

If you only have a single new array and are not using synchronous or asynchronous mirroring features, then all configuration can be handled from SANtricity System Manager. Figure 4 illustrates this configuration.

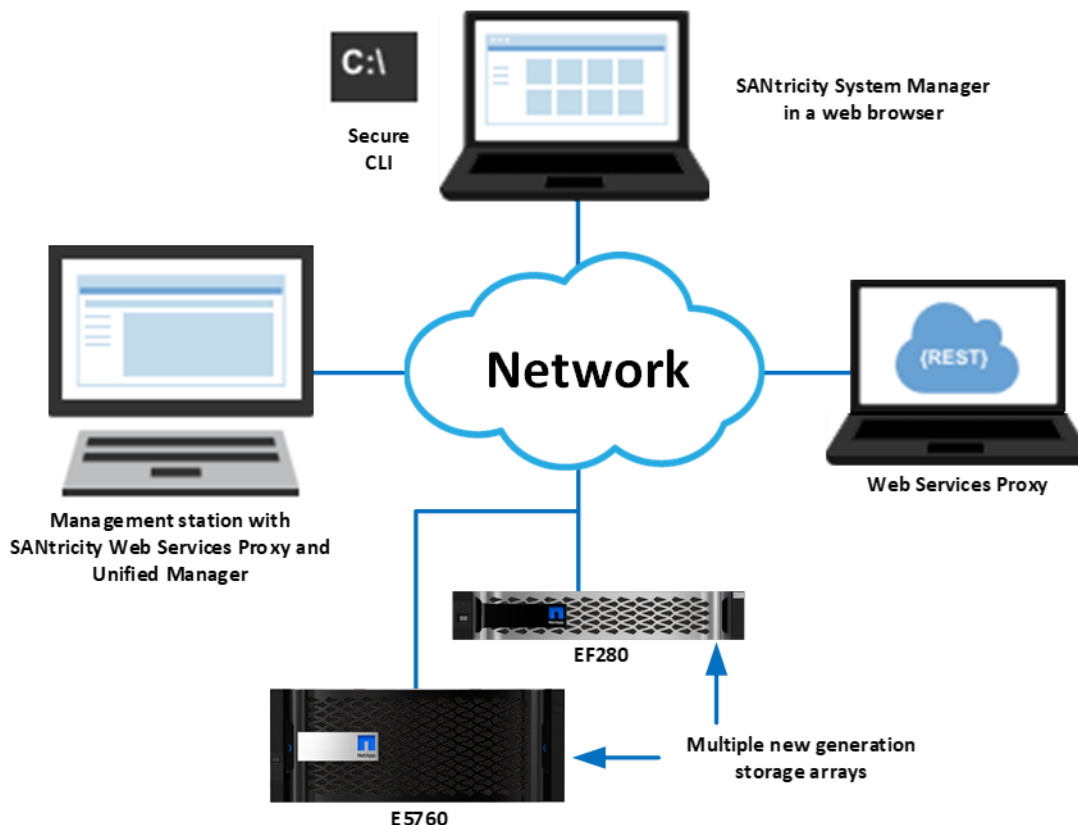
Figure 4) Managing a single EF280 with SANtricity System Manager.



Multiple New Generation Storage Arrays

If you have one or more new generation 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.



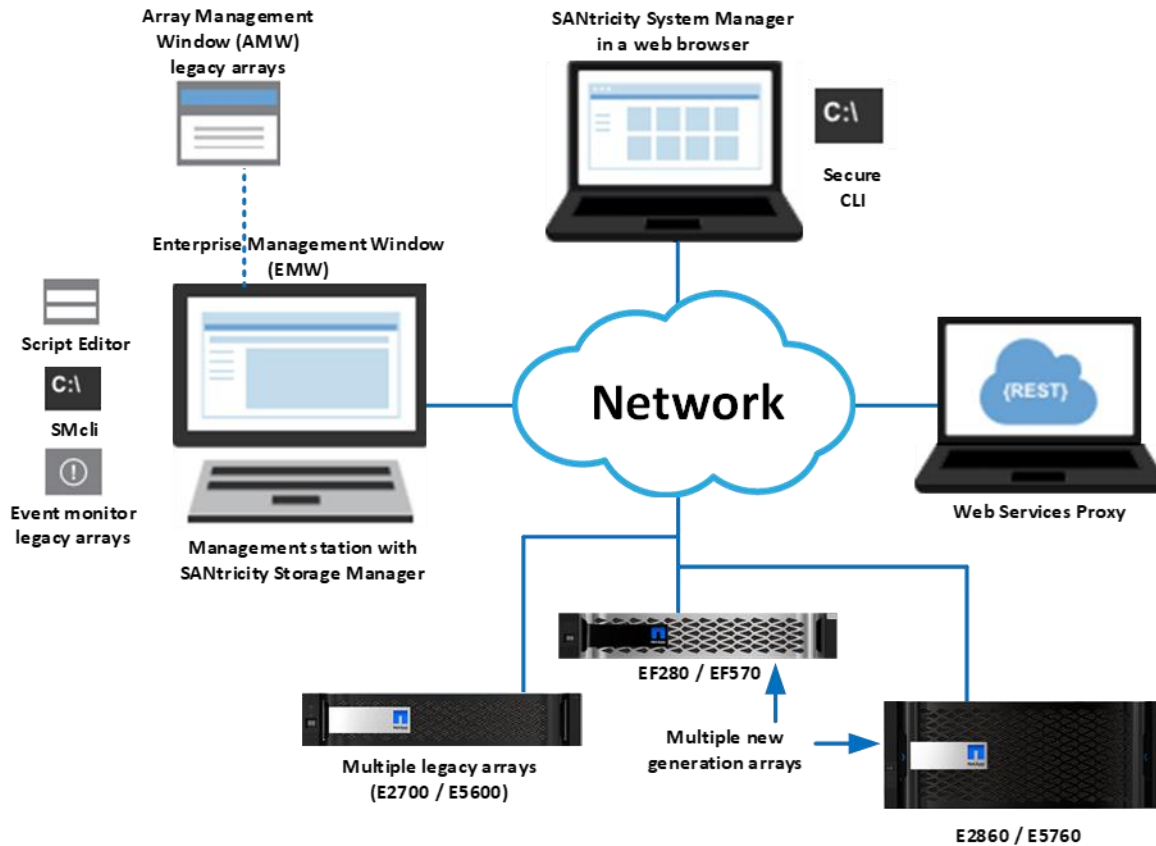
Mix of New Generation and Legacy Storage Arrays

For mixed-generation environments that have older E2700 or EF560 arrays and new EF280 or EF570 arrays, do the following (Figure 6):

- Use the SANtricity Storage Manager Enterprise Management Window (EMW) to launch SANtricity System Manager for array-based tasks on the EF280 storage arrays.

- Use the AMW for array-based tasks on legacy E-Series storage arrays.

Figure 6) Managing a mixed-array environment with SANtricity Storage Manager and System Manager.



For a detailed description of installing and configuring the components you choose, refer to the appropriate [Express Guides](#) for deployment instructions.

2.2 SANtricity Unified Manager

SANtricity Unified Manager is a web-based central management interface that replaces the legacy SANtricity Storage Manager EMW for managing current-generation EF280/E2800 and EF570/E5700 arrays. The Unified Manager GUI is bundled with the SANtricity Web Services Proxy and installs on a management server with IP access to the managed arrays. Unified Manager can manage hundreds of arrays.

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

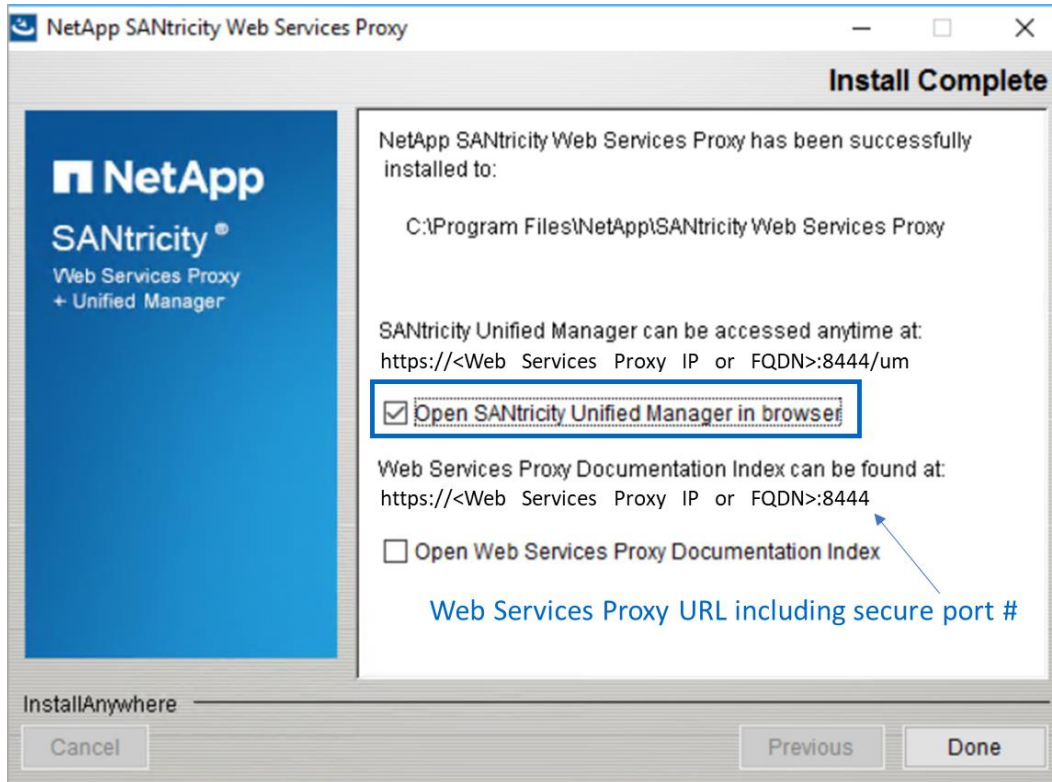
- Upgrade multiple arrays with the same controller type at one time.
- Supports Lightweight Directory Access Protocol (LDAP) and role-based access control (RBAC) just like SANtricity System Manager. Unified Manager includes a simplified certificate management workflow to manage the Unified Manager or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

- Supports synchronous and asynchronous mirroring for E2800/EF280 and E5700/EF570 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.

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

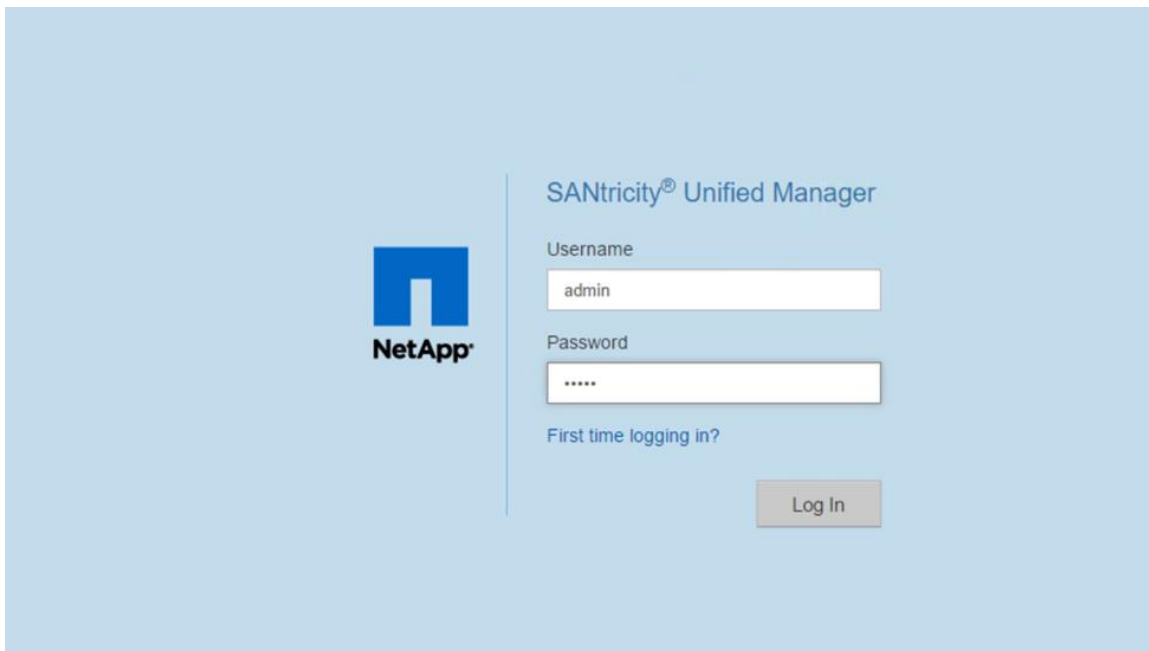
After the installation wizard completes, you can open Unified Manager, or you can directly access the SANtricity Web Services Proxy as shown in Figure 7.

Figure 7) 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 and 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 8) by adding `/um` to the URL. For example, `https://<proxy-FQDN>:<port #>/um`.

Figure 8) SANtricity Unified Manager login page.

The image shows the login page for SANtricity Unified Manager. On the left is the NetApp logo, which consists of a blue square with a white 'N' and the word 'NetApp' below it. To the right of the logo, the text 'SANtricity® Unified Manager' is displayed. Below this, there are two input fields: 'Username' with the text 'admin' and 'Password' with masked characters '*****'. A link 'First time logging in?' is positioned below the password field. At the bottom right, there is a 'Log In' button.

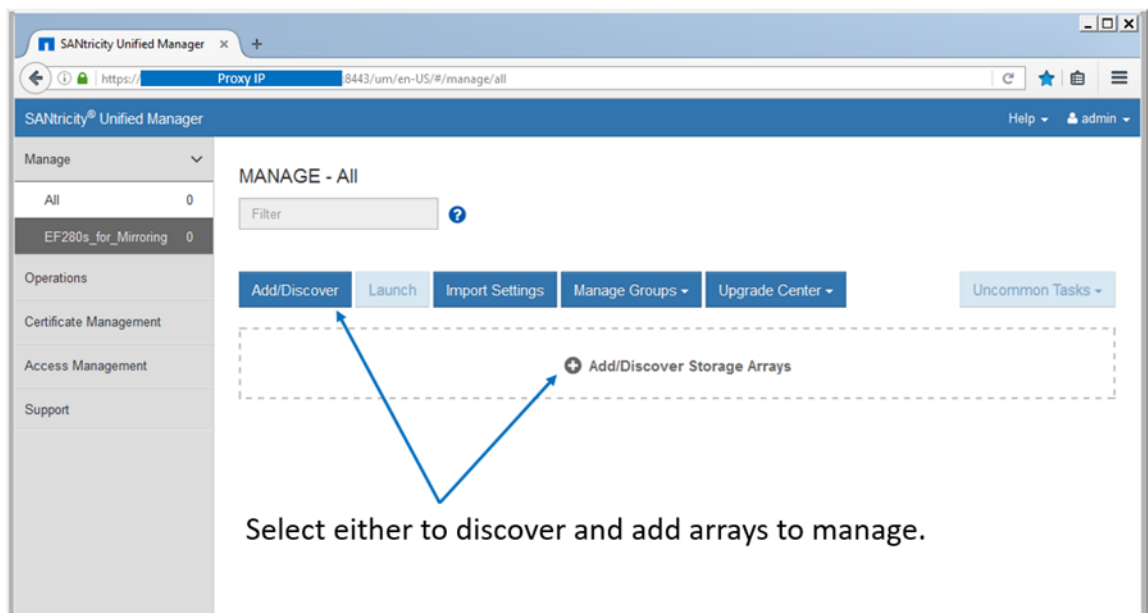
2.3 SANtricity Unified Manager Navigation

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

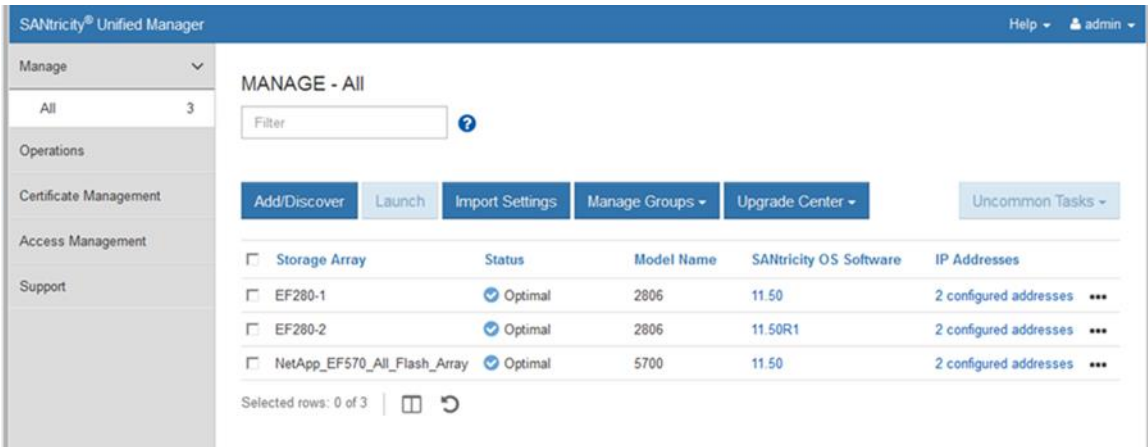
Like the SANtricity EMW, SANtricity Unified Manager must discover arrays to manage, and like the EMW, you can discover a single array or scan a range of IP addresses to discover multiple arrays simultaneously. Select the tab or link shown in Figure 9 to open the Add/Discover wizard. After discovering arrays, you then choose to manage them with Unified Manager.

Figure 9) New 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 10).

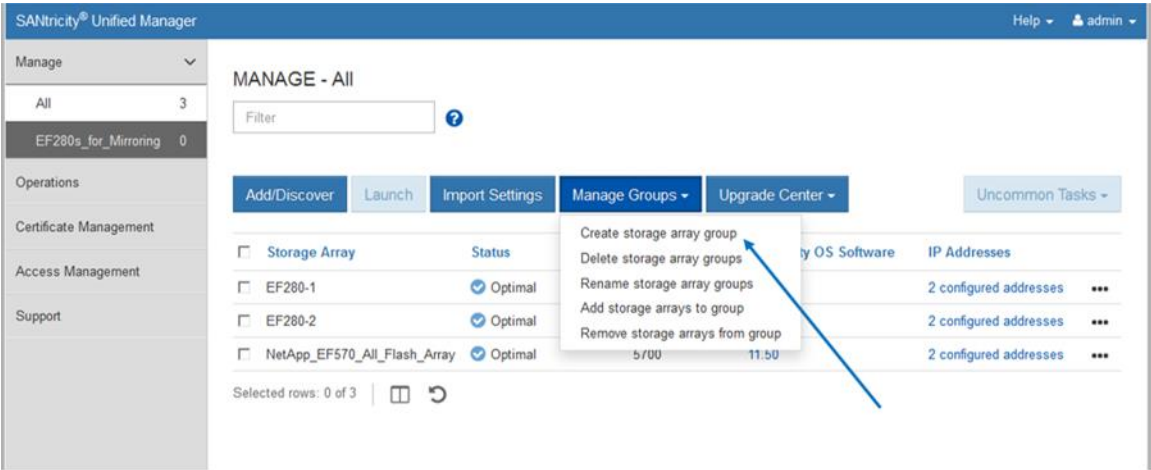
Figure 10) SANtricity Unified Manager landing page.



Organizing Arrays by Group

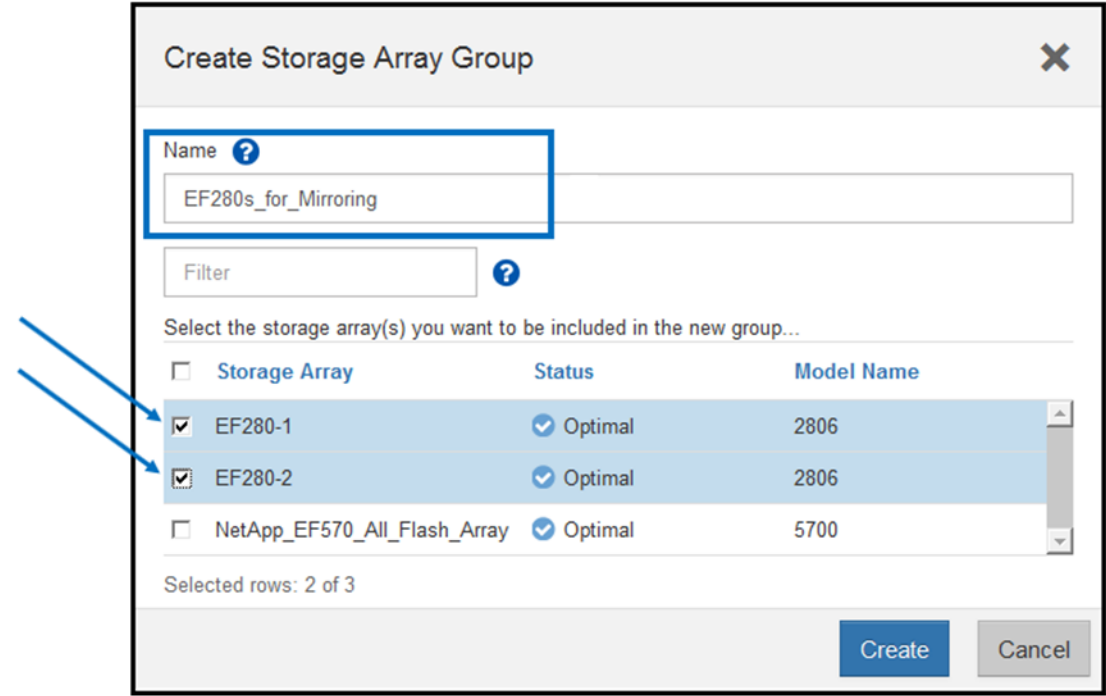
After you add arrays to Unified Manager, you can group them to organize your array management environment. Figure 11 shows EF280 arrays added to a group. This capability is available for all new generation E-Series and EF-Series arrays.

Figure 11) Creating a group to organize arrays in SANtricity Unified Manager.



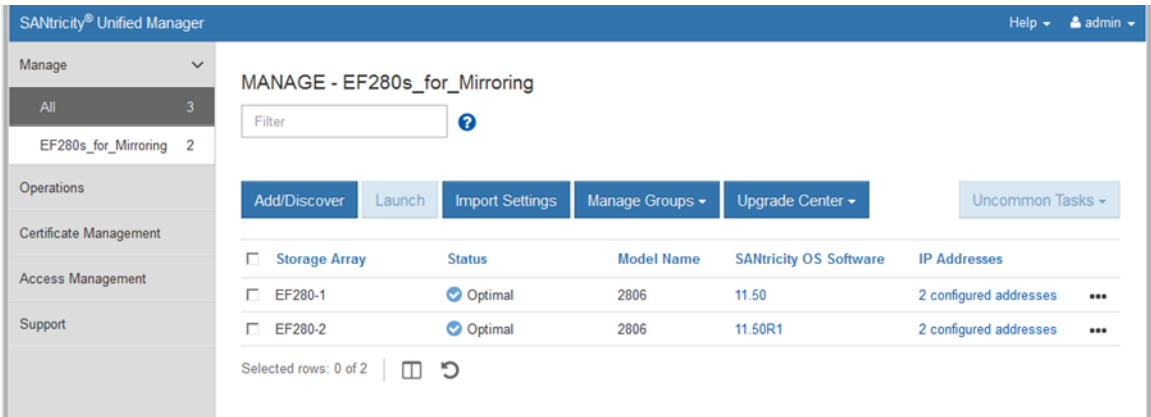
The built-in wizard makes adding arrays to groups quick and easy, as shown in Figure 12.

Figure 12) Creating a group in Unified Manager.



SANtricity Unified Manager allows you to see just the subset of arrays in the new group, as is shown in Figure 13.

Figure 13) SANtricity Unified Manager showing a newly created group.

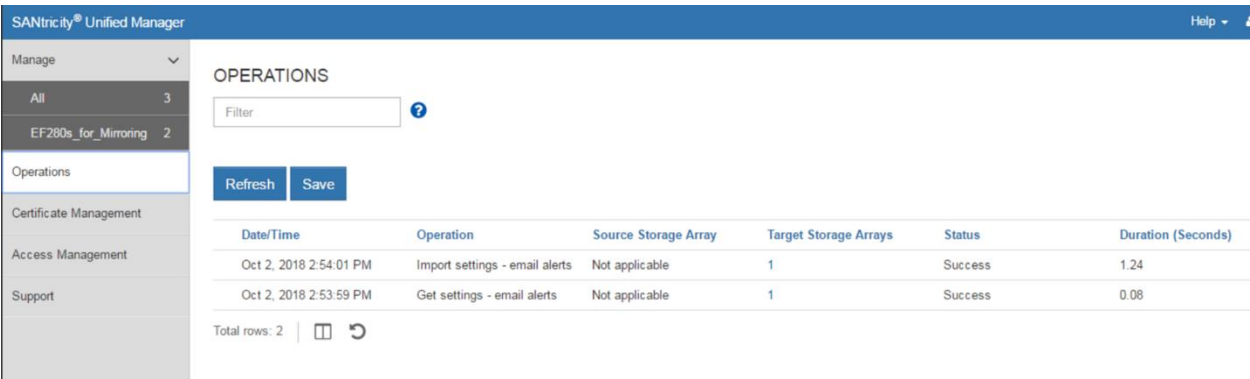


Import Settings and Viewing Operations

Other features in SANtricity Unified Manager require the ability to view operations that take some time to complete. One example is importing settings from one storage array to another. This feature is especially helpful and time saving when you install a new array in an environment that already contains E-Series or EF-Series arrays running SANtricity 11.50 or later. For example, if you want the same alerting and NetApp AutoSupport® settings on all systems, use the Import Settings wizard to select the setting category, the array to copy from, and the array to import to and click Finish. The operation to copy the settings is displayed in the Operations view, as shown Figure 14.

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.

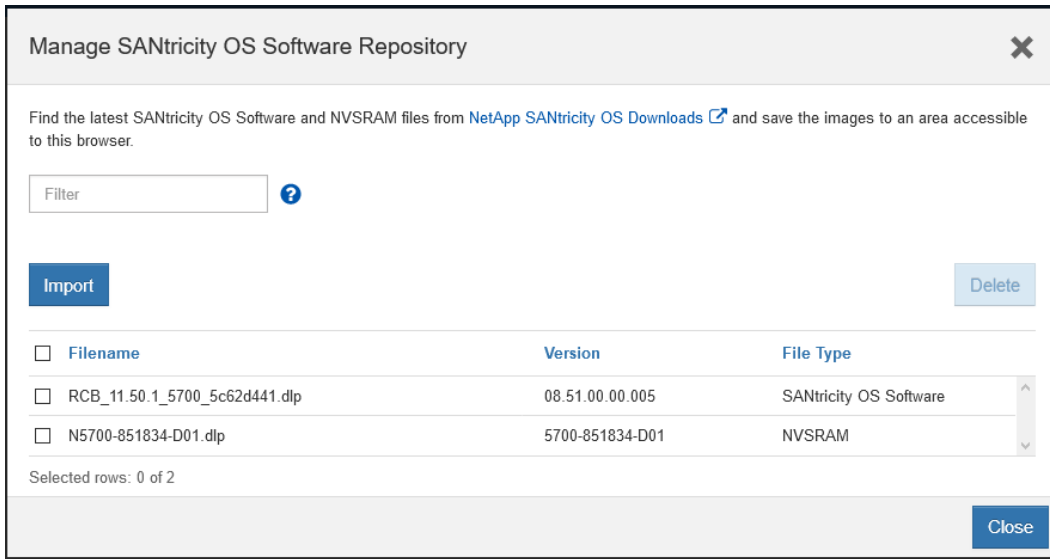
Figure 14) SANtricity Unified Manager Operations view.



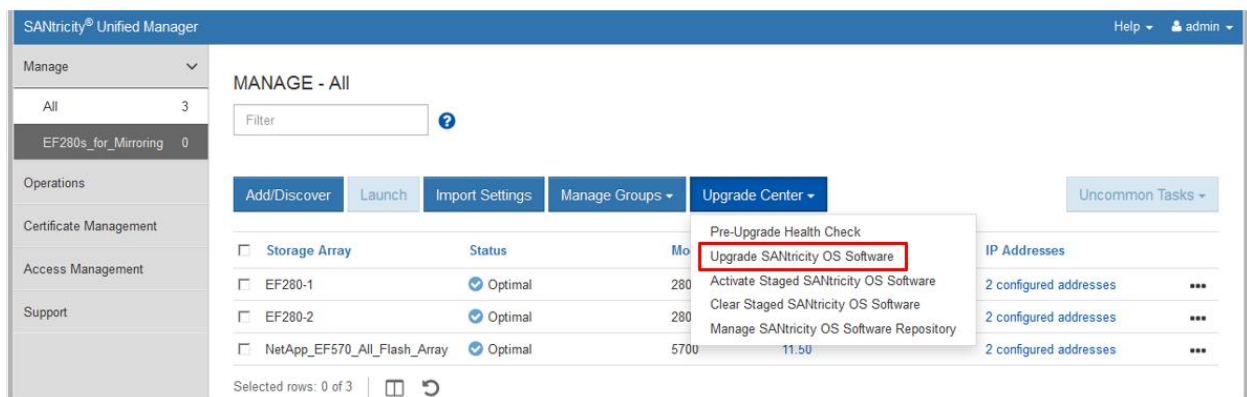
Updating SANtricity OS Through Unified Manager

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 Manage SANtricity OS Software Repository dialog under Upgrade Center on the landing page.



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



- 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
- Click Start to continue.

Upgrade SANtricity OS Software

Add new file(s) to the software repository

Select a SANtricity OS Software file

RCB_11.50.1_5700_5c62d441.dlp (08.51.00.00.005)

Select an NVSRAM file (recommended)

N5700-851834-D01.dlp (5700-851834-D01)

Filter

Compatible Storage Arrays

<input checked="" type="checkbox"/> Storage Array	Status	Current OS Software	Current NVSRAM
<input checked="" type="checkbox"/> EF570	Optimal	11.50	N5700-850834-D02
<input checked="" type="checkbox"/> NetApp_EF570_All_Flash_Array	Optimal	08.50.00.03.000	N5700-850834-D02

Selected rows: 2 of 2

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

Start

Cancel

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

Confirm Transfer and Activation

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

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

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

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			
<div>Filter</div>			
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			
<div>Filter</div>			
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.

SANtricity® Unified Manager					
<div> <div>Manage</div> <div>MANAGE - All</div> <div>Filter</div> <div> <div>Add/Discover</div> <div>Launch</div> <div>Import Settings</div> <div>Manage Groups</div> <div>Upgrade Center</div> </div> <div>Uncommon Tasks</div> </div>					
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	...
Selected rows: 0 of 4					

SANtricity Unified Manager Security

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

Remote Mirroring with SANtricity Unified Manager

With Unified Manager, you can set up remote mirroring between two E2800/EF280 and/or E5700/EF570 arrays. Starting with SANtricity 11.62, Unified Manager is used to create the mirror relationship. 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.

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).

2.4 SANtricity System Manager

Overview

SANtricity System Manager provides embedded management software, web services, event monitoring, secure CLI, and AutoSupport for EF280 arrays. Previous arrays that use EF560 or other legacy controllers do not have this embedded functionality or the new security features introduced with SANtricity System Manager 11.40 and later versions. There are various management options if you have a mixed environment with a new EF570 and older E-Series storage arrays. Table 2 provides an overview of management use cases.

Table 2) Management use cases.

Task	Mixed environment	E5700/EF570/E2800/EF280 only
Manage and Discover		
Discover an array in your management domain	EMW	SANtricity Unified Manager
Add an array to or remove an array from your management domain	EMW SANtricity storage management CLI (SMcli)	SANtricity Unified Manager
Launch SANtricity System Manager	N/A	SANtricity Unified Manager Directly from browser
Launch the AMW	EMW	N/A
AutoSupport and Legacy Support Bundle Collection		
Enable or disable AutoSupport, AutoSupport OnDemand, and AutoSupport remote diagnostics features	EMW SMcli	System Manager SANtricity Unified Manager SANtricity Web Services Proxy (REST) System Manager Secure CLI
Show AutoSupport logs for all arrays or a select storage array	EMW SMcli	System Manager REST Secure CLI
Enable or disable legacy support bundle collection for a select storage array	EMW SMcli	N/A

Task	Mixed environment	E5700/EF570/E2800/EF280 only
Specify the support bundle collection schedule	EMW SMcli	N/A
Configuration and Status		
Display information (other than alert settings) about configured arrays	AMW SANtricity Web Services Proxy (REST) SMcli	System Manager REST Secure CLI
Show the IP address of each array	AMW REST SMcli	SANtricity Unified Manager System Manager REST Secure CLI
Show the WWN of each array	AMW REST SMcli	System Manager REST Secure CLI
Show the status of each array	EMW/AMW REST SMcli	SANtricity Unified Manager System Manager REST Secure CLI
Set up remote volume mirroring groups and pairs	EMW/AMW REST SMcli	SANtricity Unified Manager and System Manager
Show array-level configuration, provisioning, and tuning	AMW REST SMcli	System Manager REST Secure CLI
Alert and SNMP Configuration		
Show or configure global alert settings	EMW REST SMcli	N/A REST
Configure email server or SNMP settings for an array	EMW REST SMcli	System Manager REST
Send a test email based on global alert settings	EMW REST SMcli	N/A REST
Certificate handling: view SSL information, get a certificate signing request (CSR), import a new certificate	N/A	System Manager REST
More convenient syslog configuration	N/A	System Manager REST

Task	Mixed environment	E5700/EF570/E2800/EF280 only
Save up to 30 days of historical statistical I/O data	N/A	System Manager REST
Apply application tags to volumes	N/A	System Manager REST

EF280 storage systems are shipped preloaded with SANtricity 11.60.x, which includes SANtricity System Manager 11.60 or later. To discover EF280 storage systems running SANtricity 11.60.x from a central view, download the latest version of the Web Services Proxy, which includes the latest version of SANtricity Unified Manager. To manage a mixed legacy and new generation environment, download the latest version of SANtricity Storage Manager 11.6x from the NetApp Support site to a management server that has IP access to the storage systems.

Note: The x in the SANtricity Storage Manager version number must be greater than or equal to the x in the SANtricity 11.60.x version number.

Previous versions of SANtricity Storage Manager (the EMW) cannot discover EF280 arrays running SANtricity 11.60.x. However, SANtricity Storage Manager 11.6x can discover new EF280 arrays and all previous E-Series array software versions from the last five years.

Following are reasons to download and install at least some portions of the SANtricity Storage Manager software package:

- You have multiple legacy and new generation E-Series or EF-Series arrays and want the enterprise view from the EMW.
- You plan to use synchronous or asynchronous remote mirroring from older-generation arrays and new-generation arrays.
- You need to use SMcli in legacy mode.
- You need the Host Utilities package (SMutils) for legacy arrays. The host package is loaded on I/O generating hosts.
- You need to install the Microsoft Windows device-specific module (DSM) on a Windows host for multipath failover (delivered as part of the Windows host package).

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 the SANtricity EMW or SANtricity Unified Manager to discover and manage your E-Series arrays, you do not need to download and install the legacy SANtricity Storage Manager or 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 from the NetApp Support site at <https://mysupport.netapp.com/eseries>.

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 Highlighted on the bottom-right corner is a Storage Hierarchy view of your array that includes the ability to provision the storage.

Figure 15.

- 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, and 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 15) SANtricity System Manager home page.

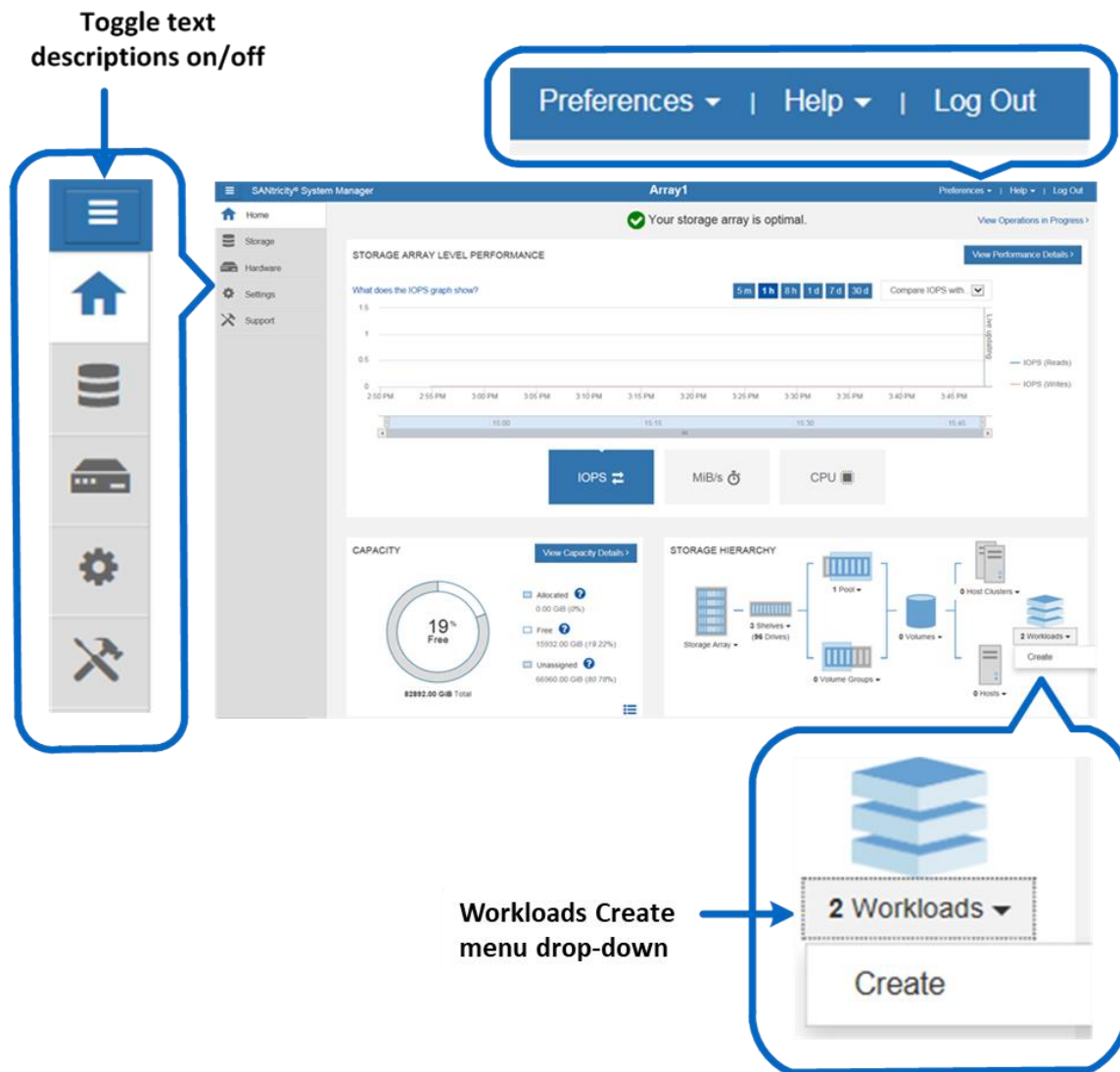


Figure 16, Figure 17, Figure 18, and Figure 19 show the other four main pages used in SANtricity System Manager that are accessible from anywhere in the application.

Figure 16) System Manager Storage page.



Figure 17) System Manager Hardware page.

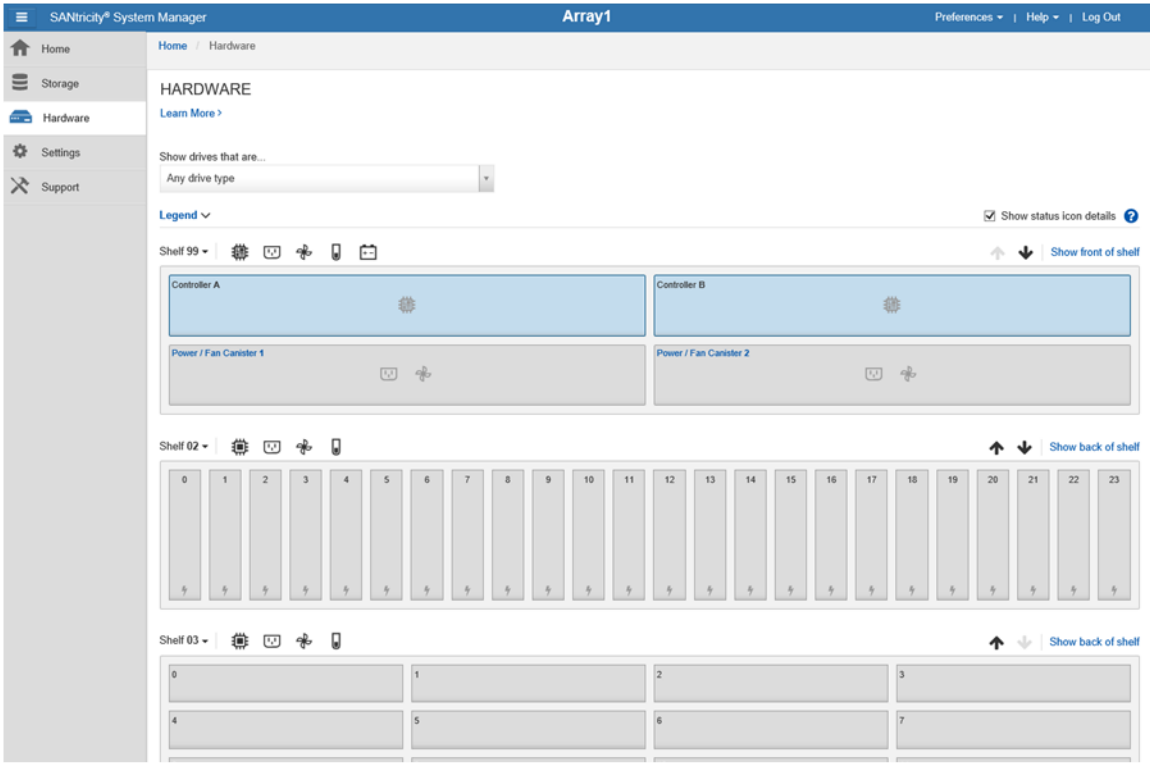


Figure 18) System Manager Settings page with new security tiles.



Note: Figure 18 shows the view for an administrator or security administrator. Other users with a lower access permission level see only the Alerts and System tiles.

Figure 19) System Manager Support page.

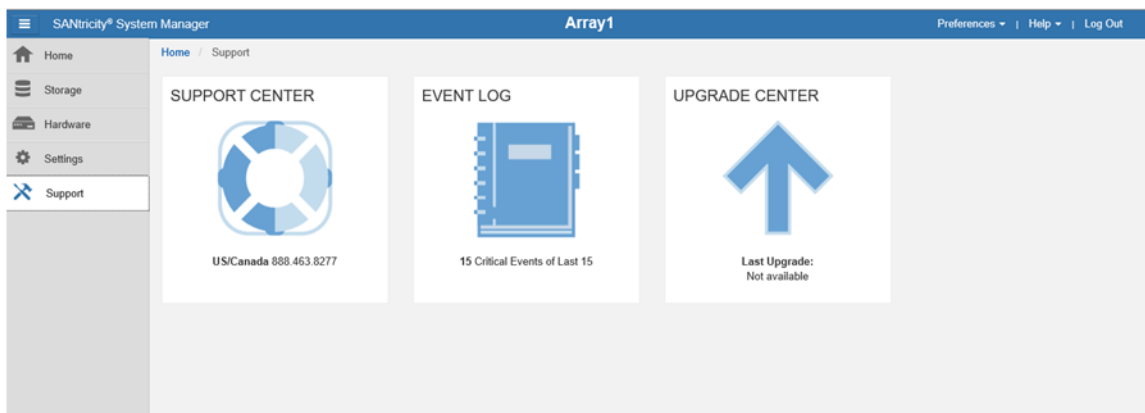
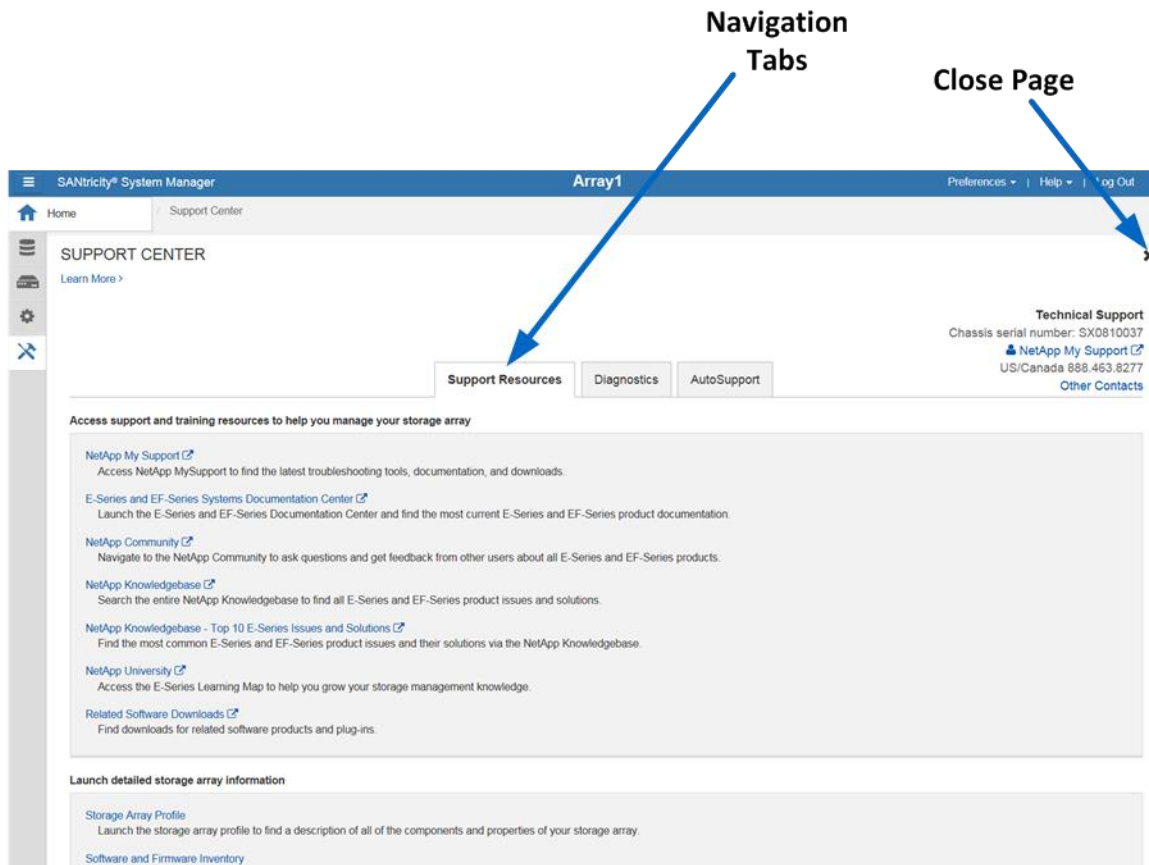


Figure 20 displays the Support Center, which you can reach by selecting the Support Center tile on the Support page. From the Support Center, use navigation tabs to reach support topics.

Figure 20) 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, for which user account passwords are now required.

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

LDAP and RBAC

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

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

Table 3 defines the permission level with each role.

Table 3) Built-in roles and associated permissions.

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

Setting Up the Directory Server and Roles

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

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

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

Table 4) LDAP/RBAC required fields and definitions.

Field Name	Definitions
Domain (for example, <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> .

Field Name	Definitions
Bind account password	Password for bind account user.
Search base DN	Format is CN=Users,DC=<some_name>,DC=com.
Username attribute	The LDAP attribute that defines the username. Example: <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 21 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 21) 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://[redacted]:389

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

Bind password Directory Server Password
[redacted]

☒ 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 22, 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 22) Role Mapping tab in the directory server settings wizard.

Directory Server Settings

Server Settings Role Mapping

What do I need to know about mapping directory service groups to the storage array roles?

Mappings

Group DN	Roles
CN=StorageAdmin,CN=Users,DC=cre,DC=com	<input checked="" type="checkbox"/> Support admin <input checked="" type="checkbox"/> Storage admin <input checked="" type="checkbox"/> Security admin <input checked="" type="checkbox"/> Monitor Click to choose
CN=StorageTechs,CN=Users,DC=cre,DC=com	<input checked="" type="checkbox"/> Monitor <input checked="" type="checkbox"/> Support admin Click to choose
CN=ITSupport,CN=Users,DC=cre,DC=com	<input checked="" type="checkbox"/> Monitor Click to choose

+ Add another mapping

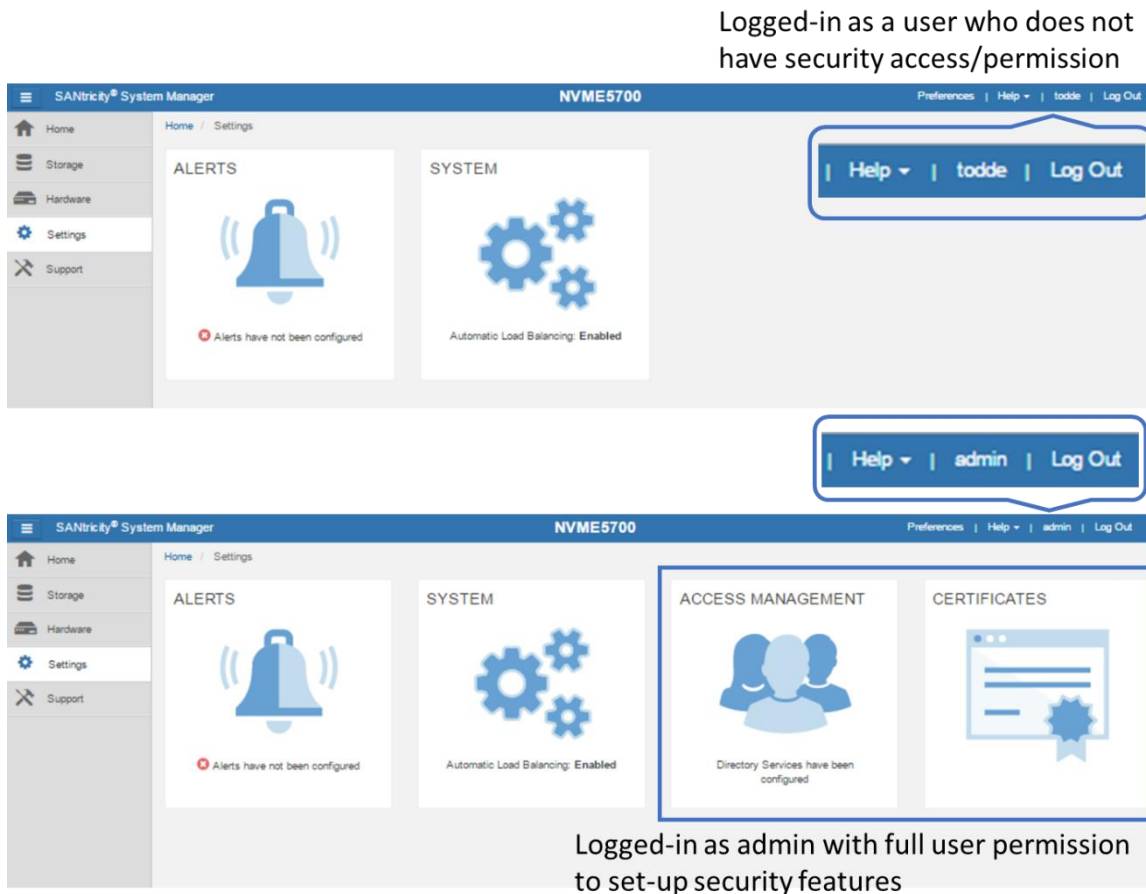
Save Cancel

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

You can define and map multiple groups to specific roles that meet individual business requirements. Figure 23 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 23.

Figure 23) SANtricity System Manager views change based on user permission level.

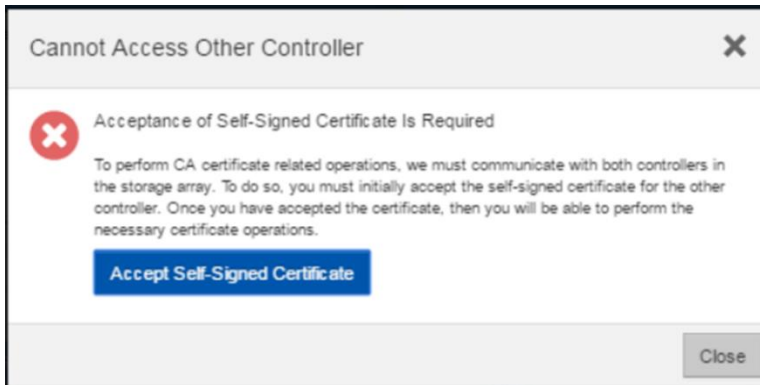


SANtricity Web Server Security Certificates

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 EF280 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 EF280 array is performed through the midplane in the shelf.

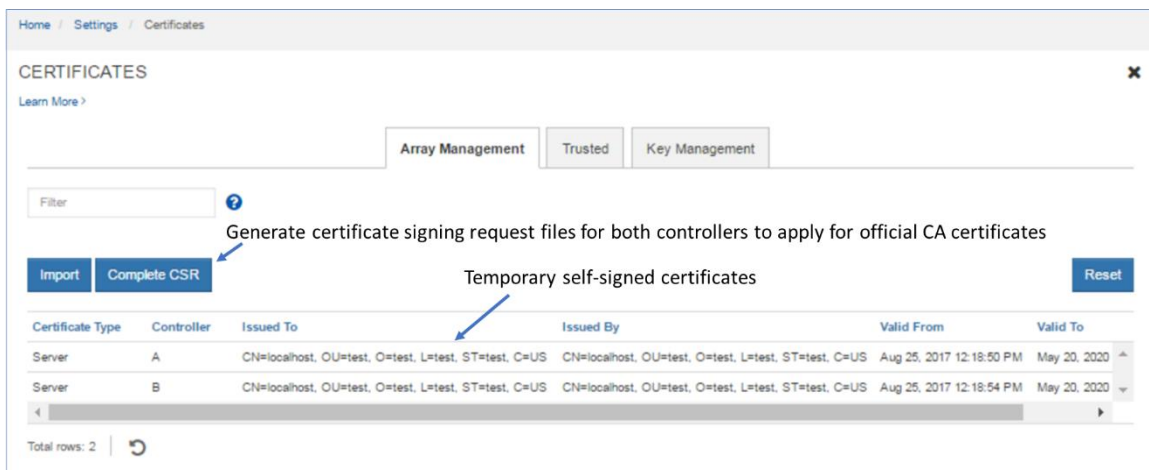
Because you can log in to either of the controllers through the web browser, both controllers must run a web server instance. For proper communication, both controllers must present a self-signed certificate to each other. This process happens automatically when the admin or security user logs in to each controller and opens the Certificates tile. Figure 24 shows the dialog box that is displayed the first time the tile is opened.

Figure 24) 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 25.

Figure 25) SANtricity System Manager Certificates tile expanded.



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 25 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 EF280 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 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 number and type of user authentication factor.

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

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

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

Note that when SAML is enabled, SANtricity System Manager is the only management access point. Therefore, there is no access through the SANtricity CLI, the SANtricity Web Services REST API, in-band management (the I/O path that uses a host agent), or a 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 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](#).

2.5 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 provide 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: NetApp SANtricity Drive Security - Feature Details Using SANtricity OS 11.60](#).

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 that have the following characteristics:

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

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

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

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

Table 5) SANtricity host types and associated failover behavior in SANtricity 11.60.x.

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	Enabled	Supported	Supported	Supported
Windows cluster	Enabled	Supported	Supported	Supported
ATTO cluster (all operating systems)	Enabled	Supported	Not supported	Not supported

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

Reliability Features

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

Table 6) SANtricity 11.60.x features for long-term reliability.

EF280 Reliability Features with SANtricity 11.60.x
<p>Dynamic Disk Pools (DDPs). NetApp patented technology that allows administrators to group a set of drives on the array to form a specialized RAID configuration. The configuration uses an 8+2 RAID 6-like algorithm to stripe I/O across all drives in the pool. The technology provides consistent performance, but it excels when a drive fails; rebuilds often take hours instead of days when the system uses large-capacity NL-SAS drives. For feature details, see TR-4652: SANtricity OS Dynamic Disk Pools - Feature Description and Best Practices.</p>
<p>DDP capacity limits. As of SANtricity 11.50, the total allowable capacity associated to the DDP feature on an E2800/EF280 array is 6PiB. The maximum single volume size is 4PiB.</p> <p>Note: The current maximum volume capacity for a thin-provisioned volume is 256TiB.</p>
<p>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.</p> <p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>

EF280 Reliability Features with SANtricity 11.60.x

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.

Online drive firmware upgrade. This feature upgrades one drive at a time and tracks writes to the affected drives during the upgrade window; it should be used only during low write I/O periods. Parallel drive firmware upgrades are supported offline to upgrade multiple drives more quickly during a maintenance window.

Automatic load balancing. This feature provides automated I/O workload balancing and confirms that incoming I/O traffic from hosts is dynamically managed and balanced across both controllers. The workload of each controller is continually monitored and analyzed in the background. When I/O on one controller significantly exceeds the I/O on the other controller for a prolonged and predictable period, SANtricity can change LUN ownership from the busy controller to the less busy controller. The feature does not react to short-term changes in I/O patterns. However, when a change of ownership is needed, SANtricity interacts with the affected host multipath driver to initiate an implicit path failover. Most current server operating systems and associated multipath drivers support implicit failover. For more information, search for "What is automatic load balancing?" in the System Manager online help.

Embedded SNMP agent. For the EF280 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 EF280 systems ship with significant storage management features that can be activated from SANtricity System Manager. Table 7 lists the EF280 features that are standard with SANtricity 11.60.x.

Table 7) EF280 standard features that are included with SANtricity 11.60.x.

EF280 Data Management Features with SANtricity 11.60.x
<p>SANtricity System Manager (embedded single-array management). Browser-based, on-box SANtricity System Manager is used to manage individual E5700/EF570 and E2800/EF280 storage arrays.</p> <ul style="list-style-type: none"> • Access all array setup, storage provisioning, and array monitoring features from one UI. • Includes an embedded RESTful API that can be used for management.
<p>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.</p>
<p>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.</p>
<p>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.</p> <p>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.</p>
<p>SSD read cache. This feature enables you to accelerate 85% or higher random read workloads by using a few SSDs.</p> <p>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.</p>
<p>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.</p> <p>Note: If drive security is enabled and the SSD is secure capable, the SSD read cache can be secured only when you create it.</p>
<p>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 11 Resources page (Upgrading > Hardware Upgrade).</p>

SANtricity Copy Services Features

Table 8 lists standard copy services features with EF280 storage arrays.

Table 8) SANtricity 11.60.x copy services features.

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

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 the mirror relationship. 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.

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).

2.6 SANtricity Management Integration

Starting with SANtricity 11.40 and continuing with SANtricity 11.60.x, the E-Series SANtricity integration model changed focus. To support today's modernized data center operations and partner appliances, NetApp is de-emphasizing legacy plug-ins and emphasizing API integration.

Table 9 shows the SANtricity APIs and toolkits that can be used for scripting and custom integration into other management tools and appliance architectures. To download the latest version of the E-Series SANtricity Web Services (REST API) visit NetApp support at <http://mysupport.netapp.com/>. Information for how to use Ansible with E-Series for managing your storage can be in [TR-4574: Deploying NetApp E-Series with Ansible \(Automating E-Series\)](#). For the Windows PowerShell toolkit, go to the [NetApp PowerShell Toolkit](#) page of the NetApp Support site.

Table 9) SANtricity APIs and toolkits.

APIs and Toolkits	Description
SANtricity Web Services Proxy You can use either the proxy or the embedded REST API for E5700/EF570/E2800/EF280 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	New in SANtricity 11.60.2 is the ability to download the SANtricity Secure CLI (SMcli) from System Manager.

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

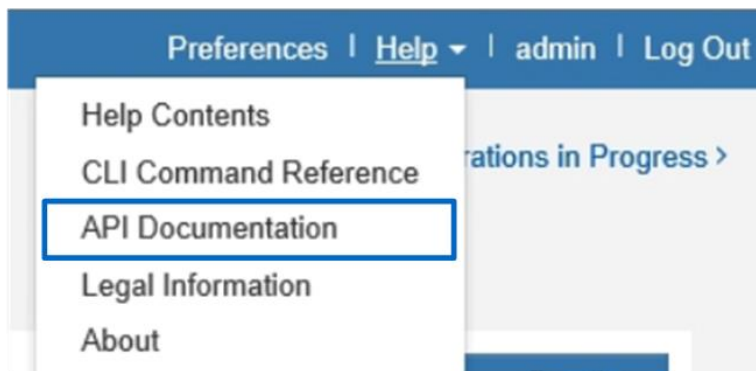
Table 10) Third platform plug-ins that use the SANtricity Web Services Proxy.

Software Package	Use
NetApp SANtricity Performance App for Splunk Enterprise https://splunkbase.splunk.com/app/1932/ Technology Add-On for NetApp SANtricity https://splunkbase.splunk.com/app/1933/	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.

Select to expand or minimize

Select Try it out to execute a single endpoint against a managed array

Device-ASUP ▾

GET /device-asup
Retrieve the device ASUP configuration

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

Parameters

No parameters

Responses

Response content type: application/json ▾

Code Description

200 successful operation

Example Value 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",
    "mailRelayPort": "string"
  }
}
```

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

Possible 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",
    "mailRelayPort": "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

Details: 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-ssr-protection: 1, mode=block
```

Responses

Code	Description
200	successful operation

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

Responses

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

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",
    "mailSenderAddress": "string"
  },
  "destinationAddress": "string",
  "schedule": {
    "dailyMinTime": 0,
    "dailyMaxTime": 0,
    "weeklyMinTime": 0,
    "weeklyMaxTime": 0,
    "daysOfWeek": [
      "notSpecified"
    ]
  }
}
```

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 the [E-Series Documentation Center](#).

SANtricity Secure CLI

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

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

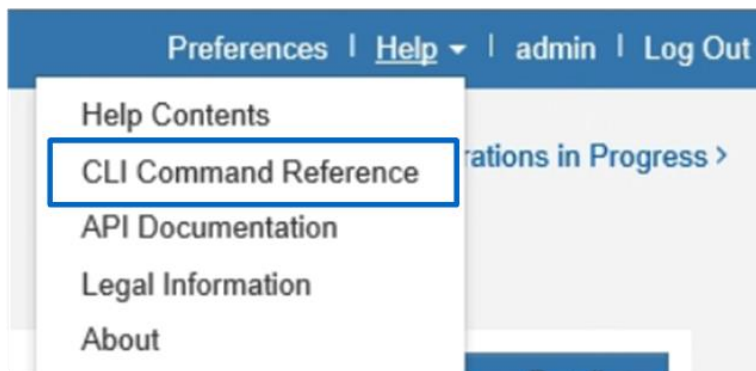
Downloading the CLI

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

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

To access the documentation, select CLI Command Reference in the Help drop-down menu from any page in the System Manager A CLI (Figure 31).

Figure 31) Opening the CLI Command Reference.



3 SANtricity Software Specifications for EF280 Hardware

Table 11 lists the software specifications for EF280-based storage systems.

Table 11) SANtricity software boundaries for EF280-based storage systems.

Components	Maximum
Storage Hardware Components	
Shelves (controller drive and expansion drive)	(1x controller + 3x expansion)
Max Drives - Drive Slot Count	96 SSDs
SSD cache capacity	N/A
Logical Components	
Host Partitions	128
Volumes per partition	256

Components	Maximum
Volumes	512
Disk pools per system	20
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
Maximum standard RAID capacity limits	Limits for standard RAID based on the maximum supported drives per RAID type: 30 drives with any supported capacity for RAID 5 and RAID 6 All drives with any supported capacity for RAID 10
Maximum DDP single volume capacity as of SANtricity 11.50 and later	4PiB
Maximum single-DDP thin volume capacity (SANtricity 11.30 and later)	256TB
Consistency Groups	
Volumes per consistency group	32
Consistency groups per system	16
Snapshot Copies	
Per Snapshot group	32
Per volume	128
Per storage system	512
Snapshot Volumes	
Per Snapshot copy	4
Per system	256
Snapshot Groups	
Per volume	4
Per system	256
Mirrors	
Mirrors per system	32
Mirrors per volume	1
Mirrors per asynchronous mirror group	32
Asynchronous mirror groups per system	4

See Hardware Universe for additional software limits and specifications.

4 EF280 Hardware Configurations

EF280 storage systems use a modular approach to hardware configuration. This approach can meet most customer SAN storage requirements for flexible host interfaces and versatile drive choices without sacrificing supportability, ease of implementation, and long-term stability. E-Series has a proven track record of reliability and scalability to satisfy requirements in remote dedicated environments or primary data centers.

4.1 Controller Shelf Configurations

EF570 controllers can only be paired with DE224C E-Series shelves. The following sections provide detailed information about the EF280 shelf configuration.

EF280 Controller Shelf

The EF280 is a 2RU shelf that holds up to 24 2.5" SSDs. It features two RAID controllers and two Energy Star Platinum-rated high-efficiency power supplies (913W) with integrated fans. EF280 all-flash arrays support a maximum of 96 SSDs in up to 4 DE224C shelves (one controller and three expansion drive shelves).

Figure 32, Figure 33, and Figure 34 show the front and rear views of the EF280 controller shelf. In the example, the EF280 controllers have two optical base ports and no HIC.

Figure 32) EF280 front view with bezel.

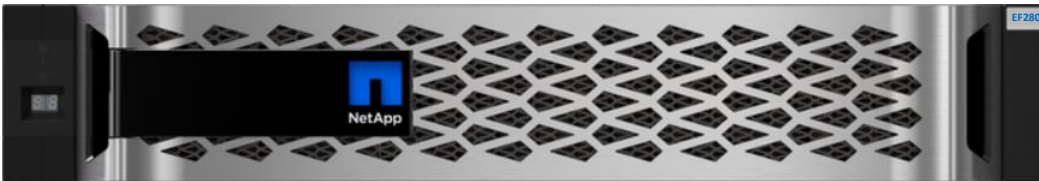


Figure 33) EF280 front view (open).



Figure 34) EF280 rear view.



EF280 Hardware Specifications

The EF280 controller has the following base hardware features:

- Dual Ethernet ports for management-related activities
- Dual optical 16Gbps FC or 10Gbps iSCSI baseboard ports for host connection

- Dual 12Gb SAS drive expansion ports to attach expansion drive shelves

Table 12 lists the technical specifications for the EF280-based storage systems.

Table 12) EF280 technical specifications.

Specification	EF280
Current maximum raw system capacity (assumes 120 SSDs)	1468TB (96 x 15.3TB SSDs)
Maximum number of drives per system (assumes not mixing shelf models)	96 SSDs maximum
Shelf form factor	2RU, 24 drives
Memory	8GB or 32GB per controller
	16GB or 64GB per duplex system
Onboard host interface	2-port 10Gb iSCSI (Base-T) per controller or 2-port 10Gb iSCSI (optical)/16Gb FC per controller. Note: Only one interface can be configured per system on the onboard host ports.
Optional host I/O (HIC) <ul style="list-style-type: none"> • Controllers must match • A software feature pack can be applied to convert the FC HIC ports to iSCSI or to convert iSCSI HIC ports to FC 	2-port 12Gb SAS (wide-port) per controller
	4-port 12Gb SAS (wide-port) per controller
	2-port 10Gb iSCSI (optical) or 16Gb FC per controller
	4-port 10Gb iSCSI (optical)/16Gb FC per controller
	4-port optical 32Gb FC per controller
	4-port optical 25Gb iSCSI
Drive shelves supported for expansion drive offerings	DE224C (2RU, 24 drives): 3 x SAS 3 12Gbps expansion shelves maximum
	DE5600 (2RU, 24 drives): 3 x expansion shelves maximum Note: Supports only SAS 2 (6Gbps) transfer speeds.
High-availability (HA) features	Dual active controllers with automated I/O path failover
	Support for RAID 0, 1 (10 for 4 drives or more), 5, 6, and DDPs technology 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

Specification	EF280
	Support for ALUA and TPGS with implicit path management for the most popular host types, including clustered host environments
	Proactive drive health monitoring with the drive evacuator feature to identify problem drives and begin removing data before hard failures occur
	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
	Mirrored data cache with battery-backed destage to flash
	Online controller firmware and NVSRAM upgrade
	Online IOM12 firmware and drive firmware upgrade (consult CSD for guidance before performing ESM upgrades)
	Online drive firmware upgrades (consult CSD for guidance before performing drive firmware upgrades)
	SANtricity Event Monitor and AutoSupport, for making periodic copies of the storage system configuration
	Automatic load balancing and path connectivity monitoring
See the Hardware Universe for current supported drive availability information and encryption capability by drive capacity (FDE, FIPS).	

4.2 Controller Host Interface Features

By default, the EF280 controller includes two Ethernet management ports that provide out-of-band system management access and either two optical FC/iSCSI or two RJ-45 iSCSI baseboard ports for host connection. The E-Series EF280 controller also supports three HIC options, including the following:

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

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

For instructions to obtain and apply software feature packs to change baseboard and HIC protocol, go to the [E-Series and EF-Series Systems Documentation Center](#). Then locate the Upgrading > Hardware Upgrade section of the page, select Changing the Host Protocol, and download the “Converting EF280 Host Protocol” document.

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 13 provides details about the FC options.

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

HIC Protocol	32Gbps SFP	16Gbps SFP	8Gbps SFP
32Gbps FC	32Gbps/16Gbps	16Gbps/8Gbps	N/A
16Gbps FC base ports	N/A	16Gbps/8Gbps/4Gbps	8Gbps/4Gbps

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

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

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

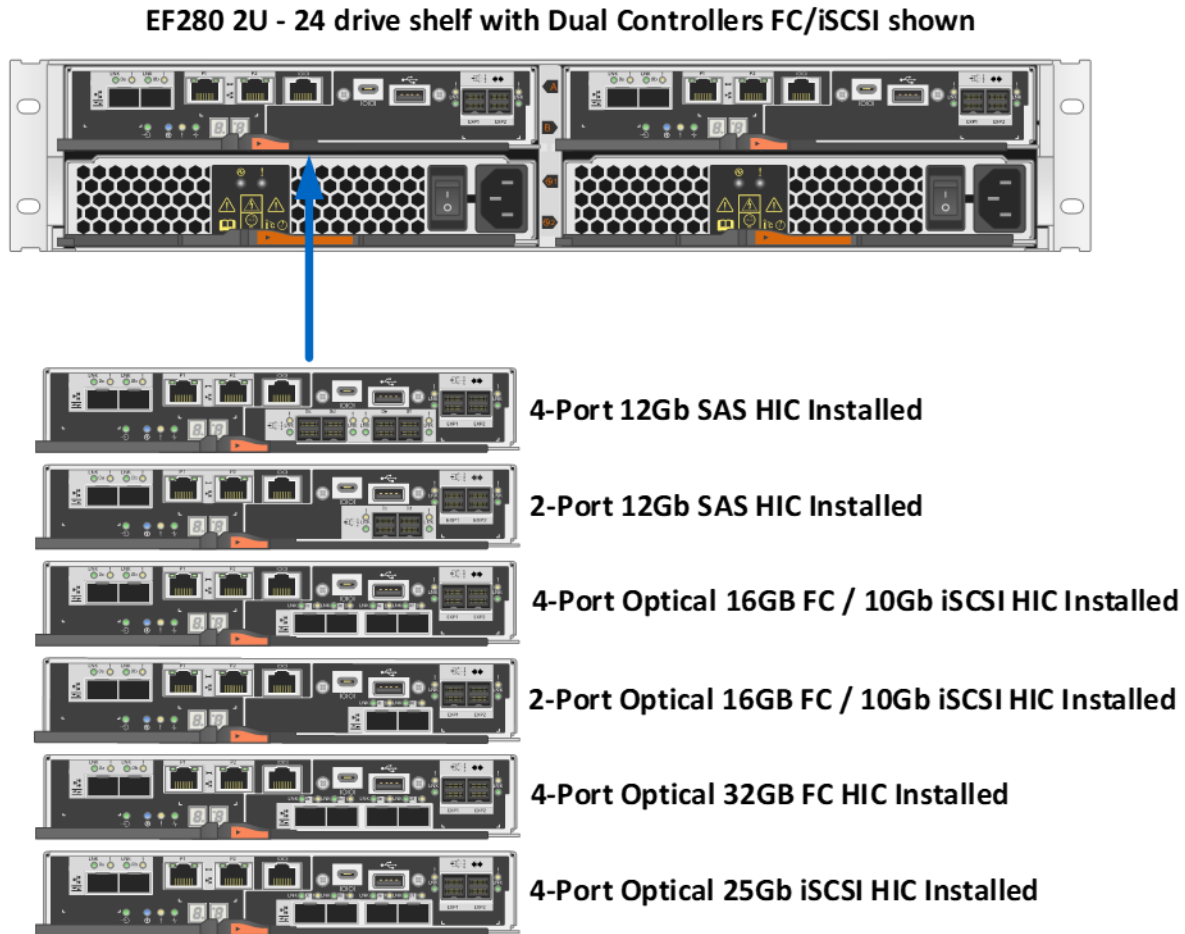
HIC Protocol	25Gbps SFP	10Gbps SFP (Unified SFP)	1Gbps SFP
25Gbps iSCSI	25Gbps/10Gbps*	N/A	N/A
10Gbps iSCSI base ports	N/A	10Gbps	1Gbps

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

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

Both controllers in a duplex configuration must be configured identically. The six HIC options are shown in Figure 35.

Figure 35) EF280 with optional HICs.



4.3 Hardware LED Definitions

EF280 Controller Shelf LEDs

The EF280 controller shelf has LED status indicators on the front of the shelf, the operator display panel (ODP), the rear of the shelf, the power fan canisters, and the controller canisters. The new EF280 shelf ODP also includes a dual seven-segment display to indicate the shelf identity. The LEDs on the ODP indicate system-wide conditions, and the LEDs on the power fan canisters and controller canisters indicate the status of the individual units.

Figure 36 shows the ODP of the EF280 controller shelf.

Figure 36) ODP on front panel of EF280 controller shelf.

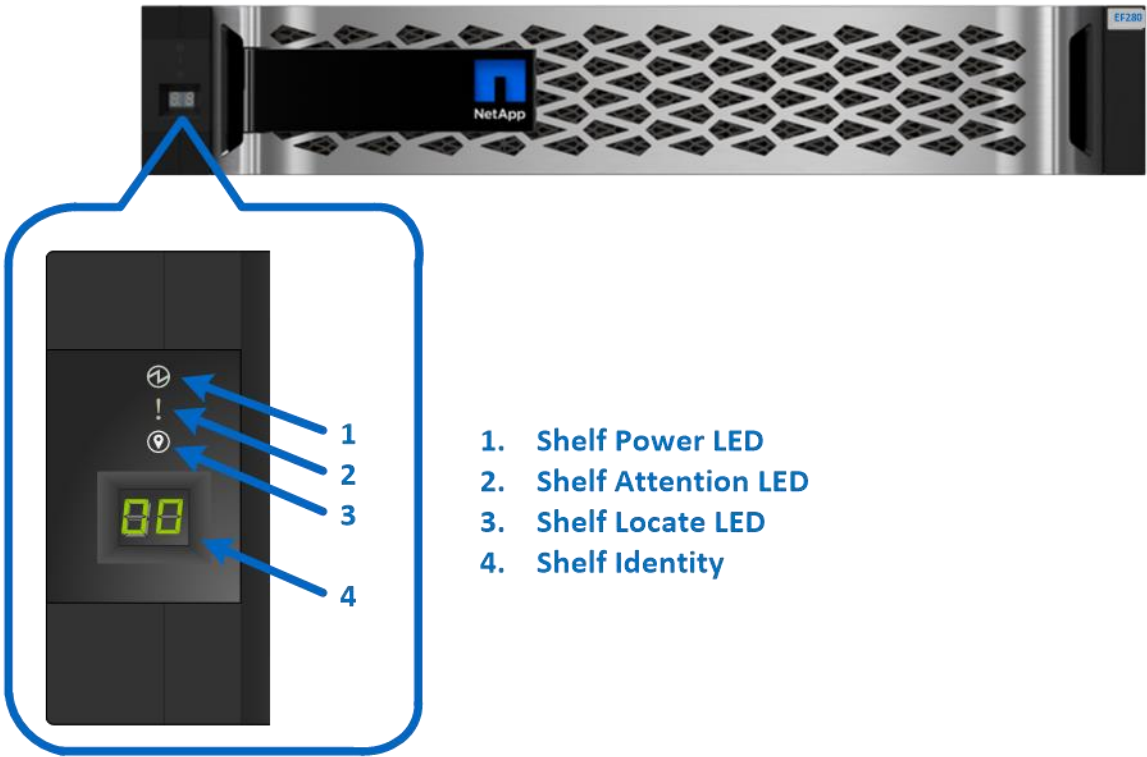


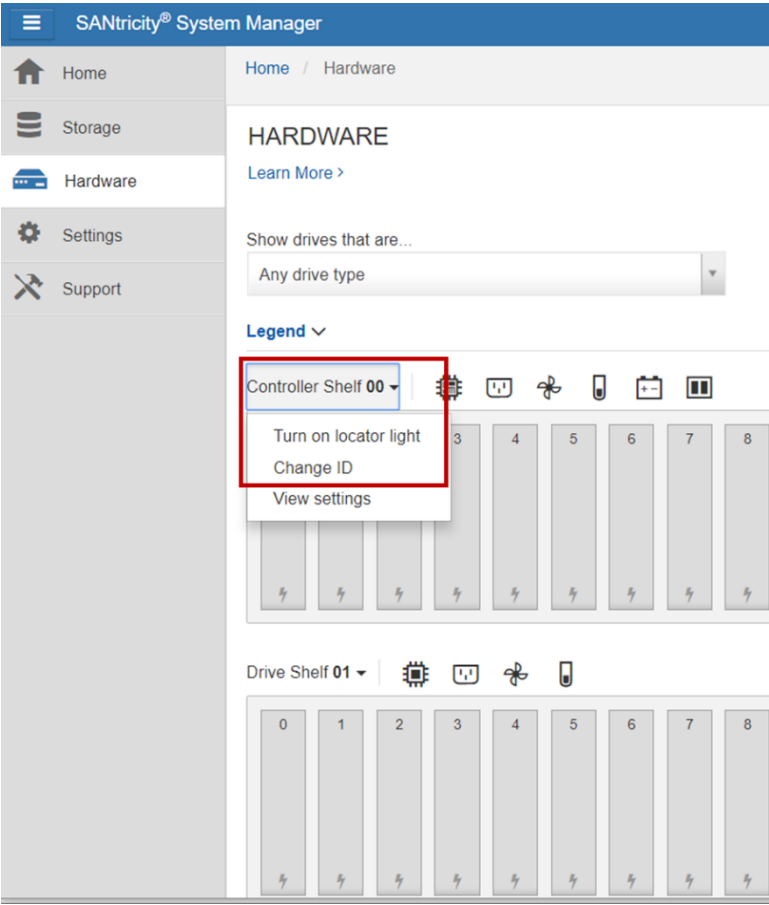
Table 15 defines the ODP LEDs on the EF280 controller shelf.

Table 15) EF280 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 shown in Figure 37.

Figure 37) Setting shelf ID by using SANtricity System Manager.



Power Fan Canister Status LEDs

The LEDs on the rear panel of the EF280 integrated power and fan canisters are shown in Figure 38 and are defined in Table 16.

Figure 38) LEDs on EF280 power fan canister (rear view).

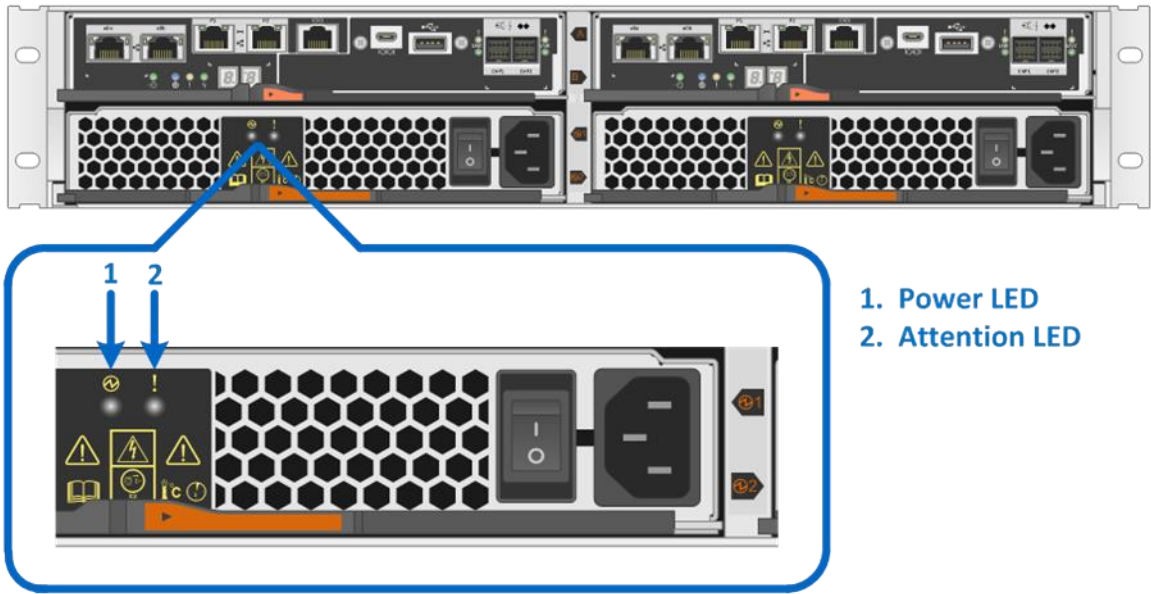


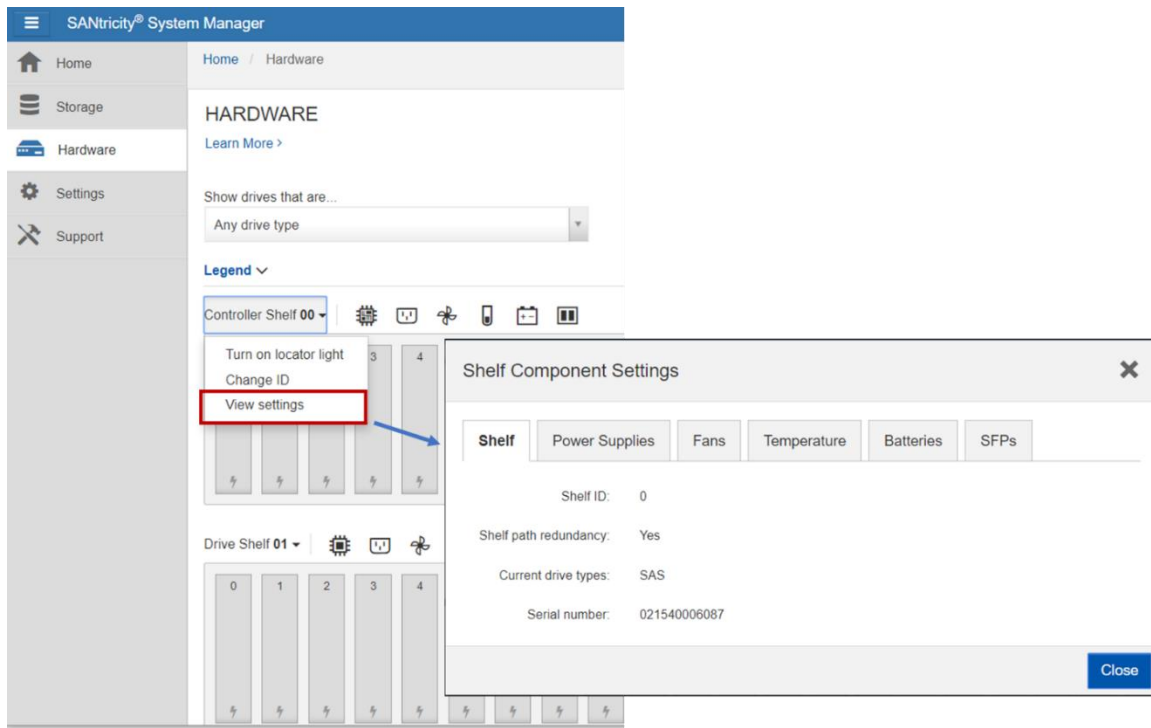
Table 16) EF280 controller shelf power and fan canister LED definitions.

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.

EF280 Controller Canister LEDs

The EF280 controller canister has several LED status indicators. Host port status and other system-level status information can be verified by directly checking the port LEDs or by using the SANtricity System Manager GUI. For example, systemwide status information is displayed in the view settings window shown in Figure 39.

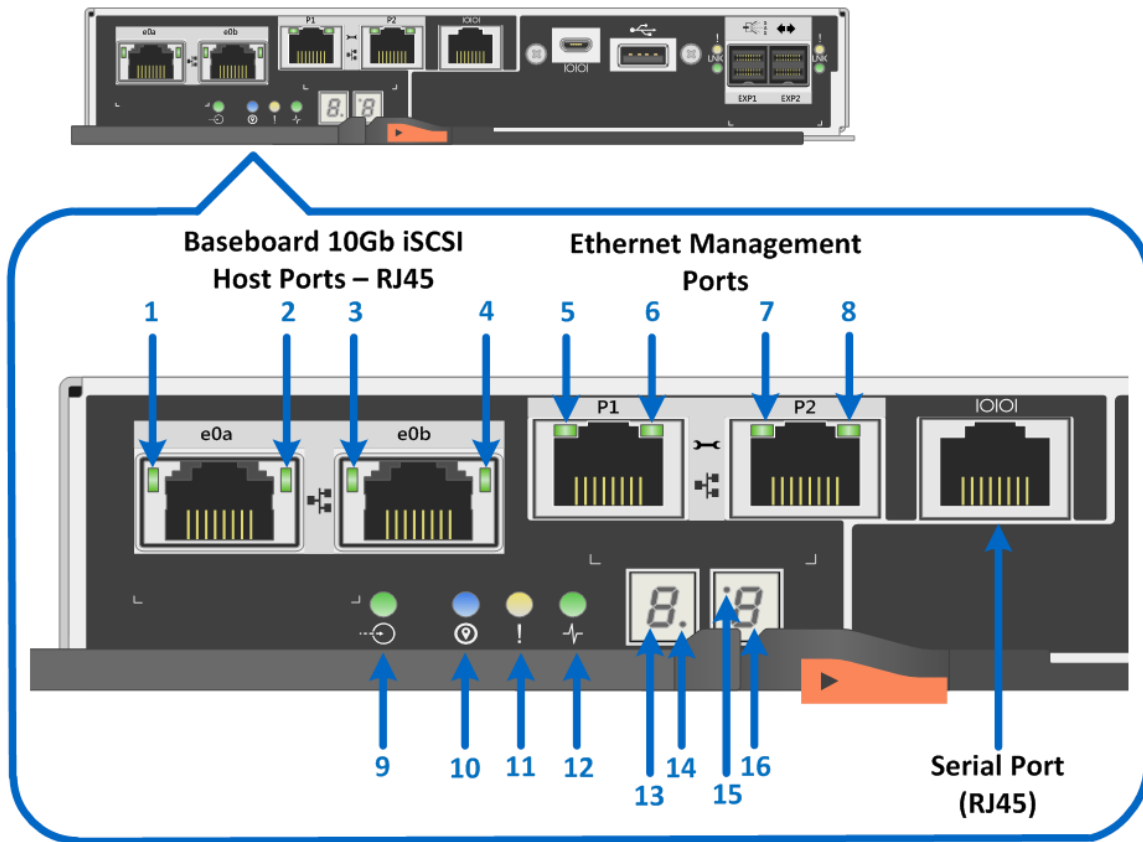
Figure 39) Viewing system status information by using SANtricity System Manager.



Controller Base Port Status LEDs

Figure 40 shows the onboard LED status indicators on the left side of the EF280 controller canister with the RJ-45 iSCSI baseboard host ports. Most of the LEDs are lit when a fault condition exists. However, the cache active LED is lit when the cache is active. The seven-segment LEDs provide status codes for both normal operation and fault conditions. The dot in the first seven-segment LED is the controller heartbeat indicator, which comes on when an intercontroller communication link has been established. The dot in the second seven-segment LED is on to indicate a diagnostic code. Otherwise, the display indicates the shelf ID.

Figure 40) LEDs on left side of EF280 controller canister with Base-T iSCSI host ports.



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

Table 17 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 40). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

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

LED Name	Color	LED On	LED Off
Host port link state (top left)	Green	Link is up.	Link is down.
Host port link activity (top right)	Green	Link activity.	No link activity.

Table 18 defines the Ethernet management port LEDs on the controller (LEDs 5 through 8 in Figure 40).

Table 18) Ethernet management port LED definitions.

LED Name	Color	LED On	LED Off
Ethernet management port link state (top left)	Green	Link is up.	Link is down.
Ethernet management port link activity (top right)	Green	Blinking: the link is up with activity.	No link activity.

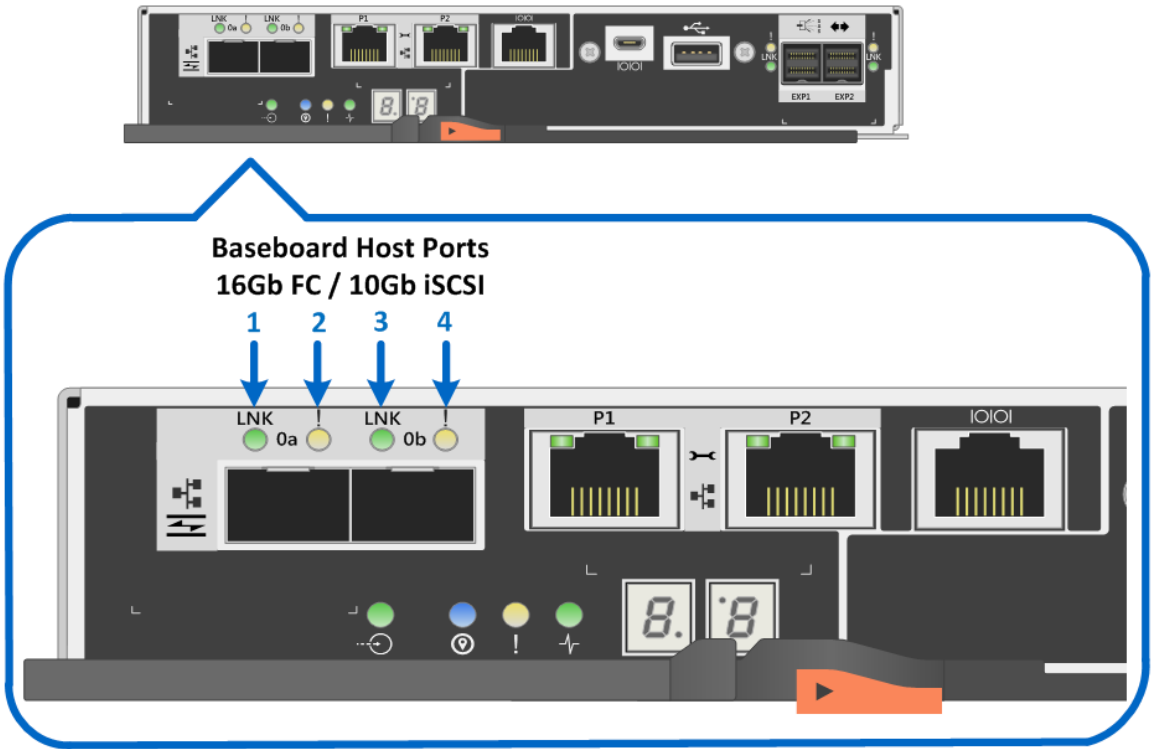
Table 19 defines the controller status LEDs (LEDs 9 through 15 in Figure 40).

Table 19) Controller base features LED definitions.

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

Figure 41 shows the onboard LED status indicators on the left side of the EF280 controller canister with the 16Gb FC/10Gb iSCSI baseboard host port LEDs indicated.

Figure 41) LEDs on left side of EF280 controller canister with 16Gb FC/10Gb optical iSCSI host ports.



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

Table 20 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 41). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

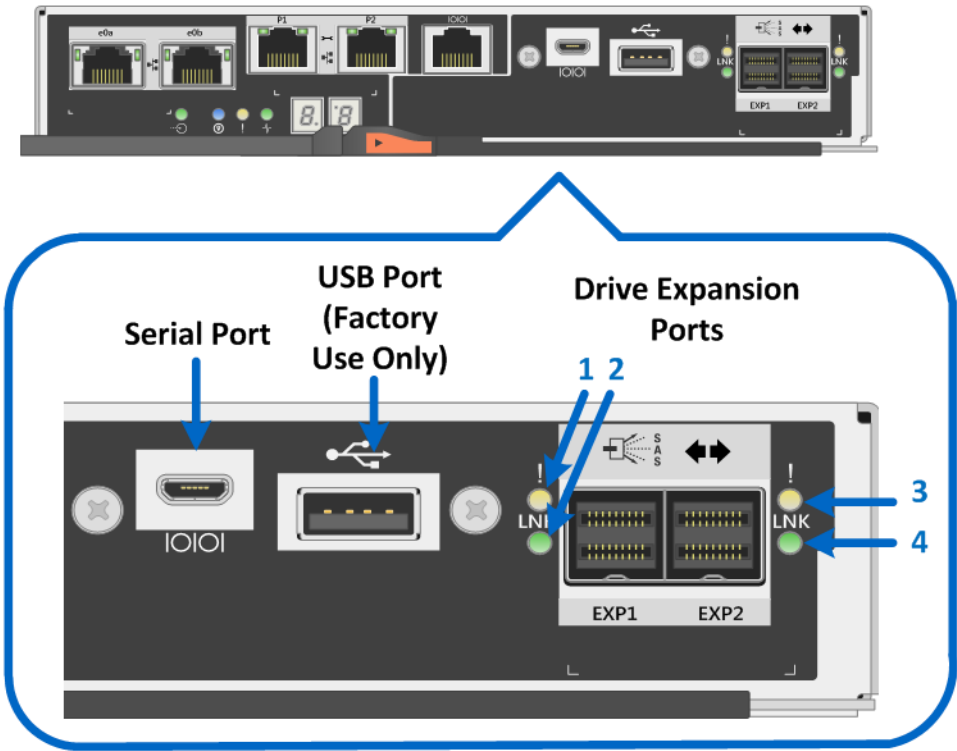
Table 20) 16Gb FC/10Gb iSCSI baseboard host port LED definitions.

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

Drive-Side SAS Expansion Port LEDs

The EF280 controller canister is equipped with two SAS expansion ports that are used to connect expansion drive shelves to the EF280 controller shelf. Figure 42 shows the SAS expansion port LEDs.

Figure 42) LEDs for drive expansion ports (no HIC installed).



- 1. Drive Expansion Port EXP1 Fault LED
- 2. Drive Expansion Port EXP1 Link LED
- 3. Drive Expansion Port EXP2 Fault LED
- 4. Drive Expansion Port EXP2 Link LED

Table 21 defines each drive-side LED (LEDs 1 through 4 in Figure 42).

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.

EF280 Optional Host Interface Cards

The EF280 supports several host interface expansion options, including SAS, FC, and iSCSI. This section provides the detailed LED status definitions for all the host interface card choices.

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

Figure 43 and Figure 44 show the LEDs for the 4-port and 2-port 12Gb SAS HICs. LEDs are called out for only the 4-port SAS HIC; the 2-port HIC LEDs are the same.

Figure 43) LEDs for 4-port 12Gb SAS HIC.

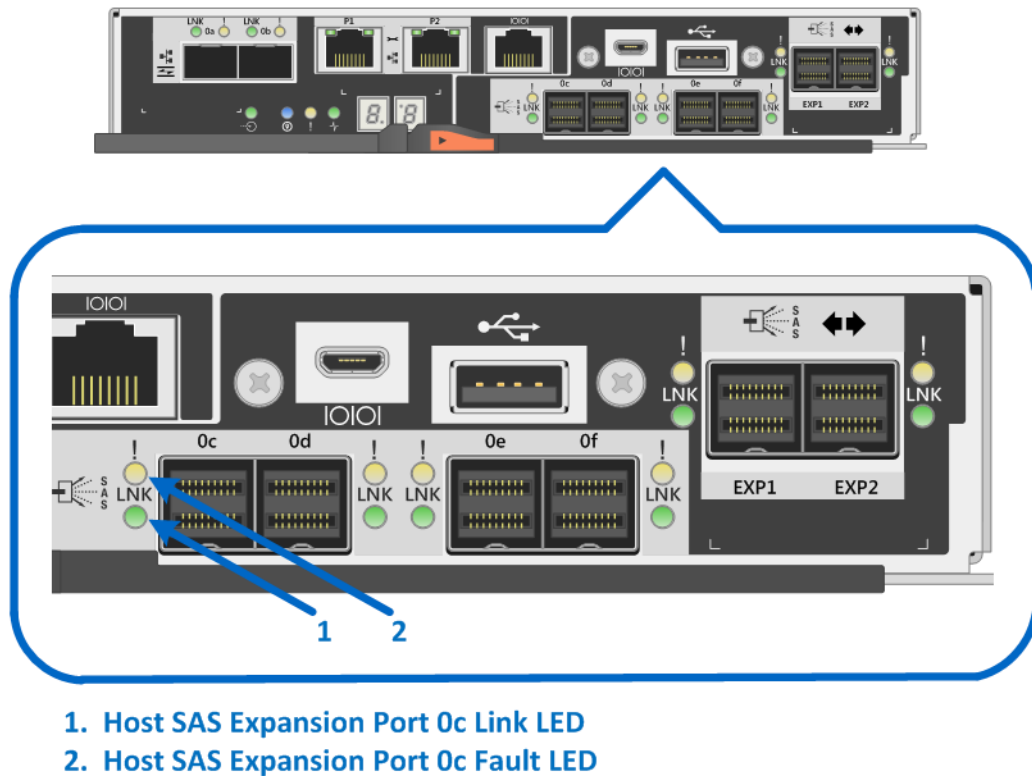


Figure 44) LEDs for 2-port 12Gb SAS HIC.

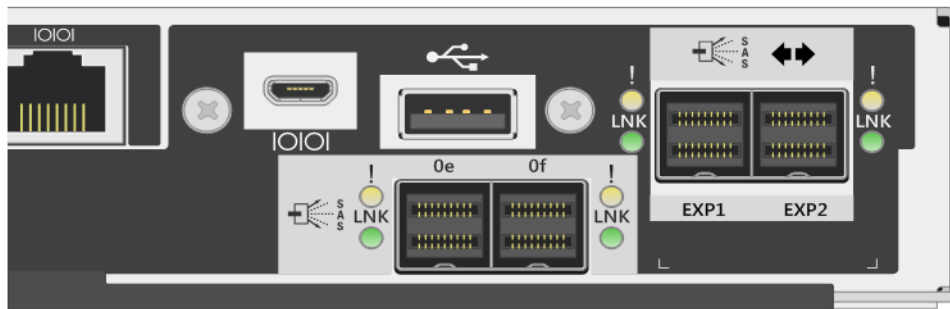


Table 22 defines the LEDs for the 12Gb SAS HICs.

Note: Table 21 defines the drive expansion port LEDs.

Table 22) 2-port and 4-port 12Gb SAS HIC LED definitions.

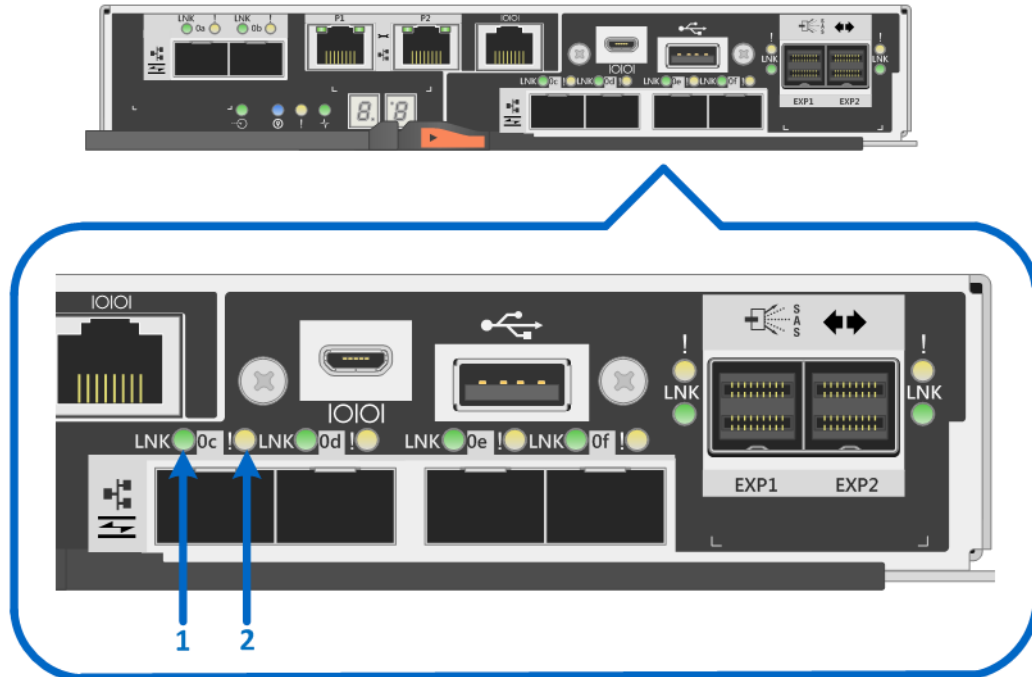
LED Name	Color	LED On	LED Off
Drive expansion link	Green	Link is up.	Link is down.
Drive expansion fault	Amber	At least one of the four PHYs in the output port is working, but another PHY cannot establish the same link to the expansion output connector.	Port is optimal (all PHYs in the port are up).

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

The EF280 controller supports a 2-port or 4-port optical HIC that offers 16Gb FC protocol or 10Gb iSCSI protocol. The 2-port HIC is functionally equivalent to the 4-port HIC. When using the 4-port HIC and dual controllers, the EF280 storage system provides a maximum of 12 16Gb FC or 12 10Gb iSCSI ports or a mixture of 16Gb FC and 10Gb iSCSI ports.

Figure 45 and Figure 46 show the LEDs for the 4-port and 2-port optical HIC. LEDs are called out for only the 4-port optical HIC; the 2-port HIC LEDs are the same.

Figure 45) LEDs for 4-port optical HIC (16Gb FC or 10Gb iSCSI).



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

Figure 46) LEDs for 2-port optical HIC (16Gb FC or 10Gb iSCSI).

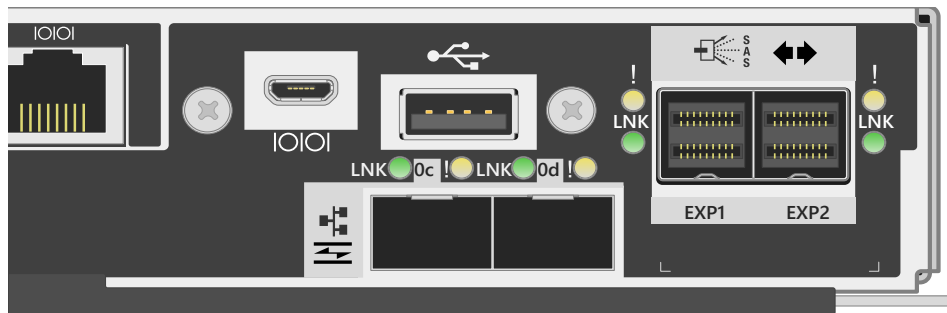


Table 23 defines the LEDs on the 2-port and 4-port optical HICs (16Gb FC or 10Gb iSCSI).

Table 21 defines the drive expansion port LEDs.

Table 23) 2-port and 4-port optical HIC (16Gb FC or 10Gb iSCSI) LED definitions.

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

4-Port 32Gb FC HIC LEDs

The EF280 controller supports a 4-port 32Gbps FC HIC that offers the ability to auto-negotiate down to 16Gbps using the 32Gbps SFP. The new 32Gbps FC HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 47 shows the LEDs for the 4-port 32Gbps FC HIC.

Figure 47) LEDs for 4-port 32Gb FC HIC.

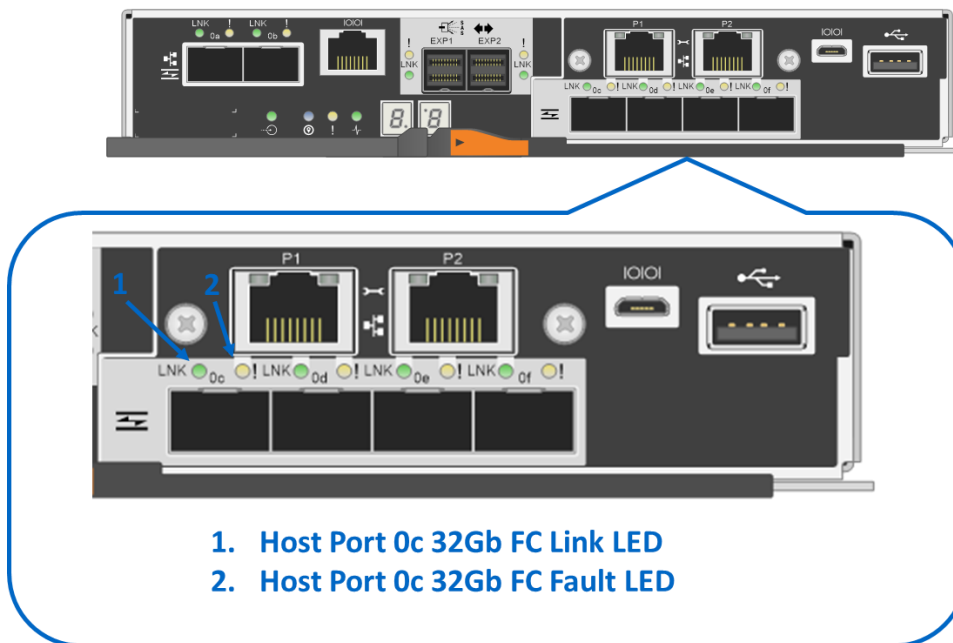


Table 24 defines the LEDs on the 4-port 32Gbps optical HIC.

Table 24) 4-port 32Gb FC HIC LED definitions.

LED Name	Color	LED On	LED Off
Host port link/activity	Green	<ul style="list-style-type: none"> • Solid: Link is up with no activity. • Blinking: Link is 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 EF280 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 new 25Gbps iSCSI HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 48 shows the LEDs for the 4-port 25Gbps iSCSI HIC.

Figure 48) LEDs for 4-port 25Gb iSCSI HIC.

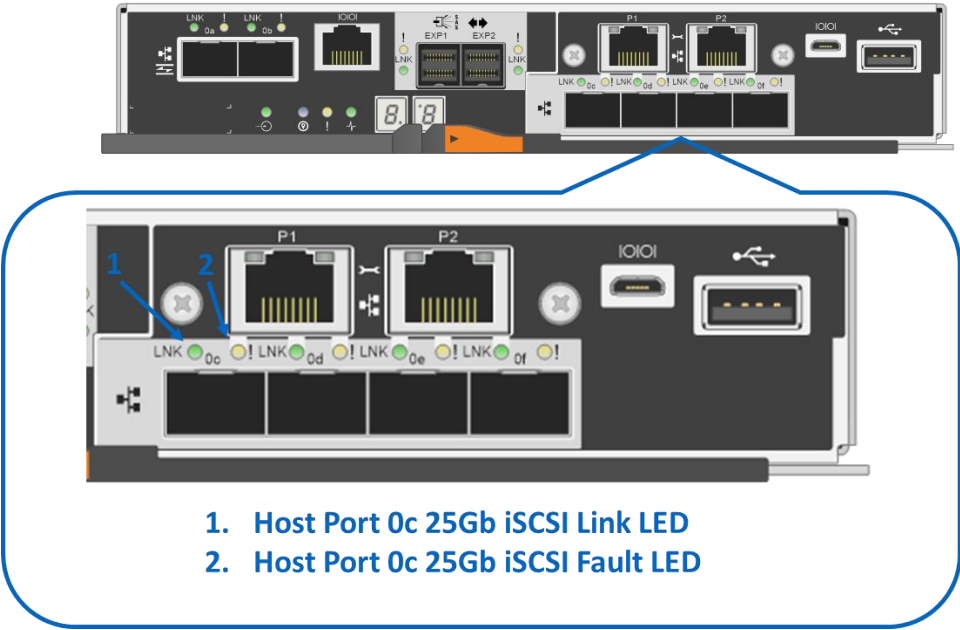


Table 25 provides the LED definitions for the 25Gbps iSCSI HIC.

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

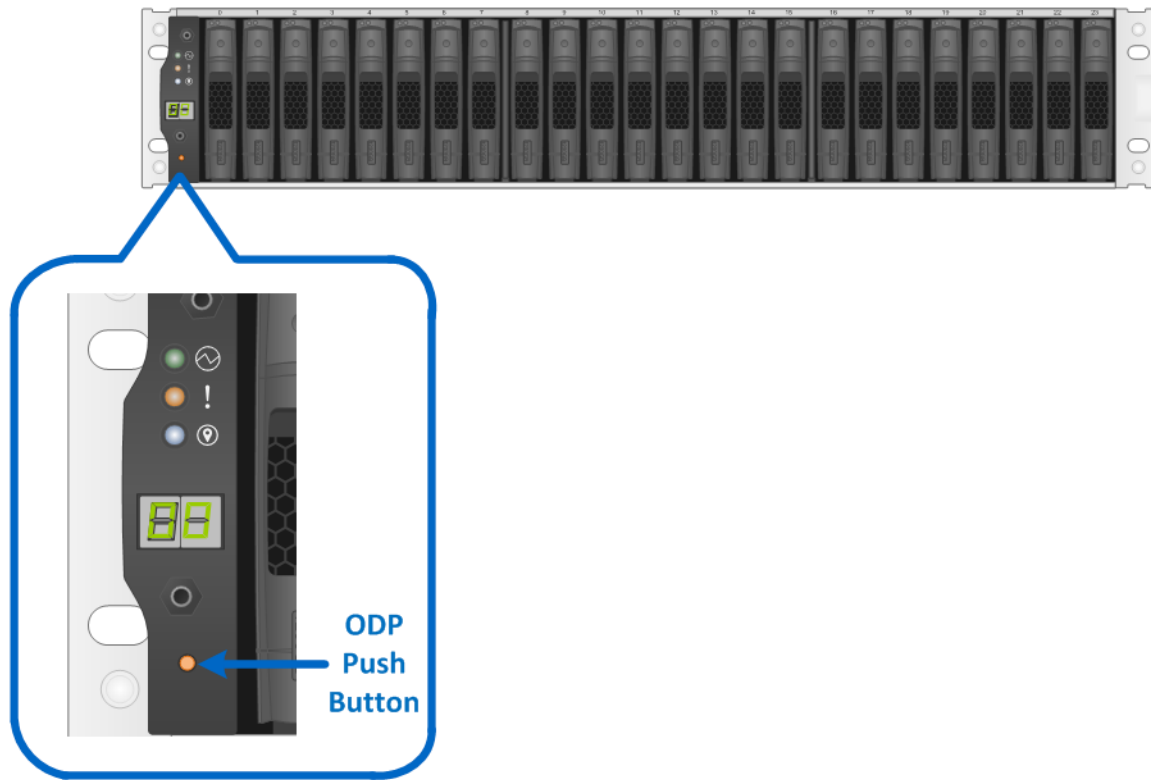
LED Speed (Left Side)	LED Activity (Right Side)	Link Rate	Color
On	On	Link operating at 25Gbps; no activity.	Green
	Blinking	Link operating at 25Gbps with active I/O in progress.	Green
Off	On	Link operating at 10Gbps; no activity.	Green
	Blinking	Link operating at 10Gbps with active I/O in progress.	Green
	Off	Link down.	N/A

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

4.4 Setting Shelf ID with ODP Pushbutton

The shelf ID for the controller shelves and drive shelves can be changed externally by using the ODP pushbutton, shown in Figure 49 for the EF280 (DE224C).

Figure 49) ODP on the DE224C (front bezel or end caps removed).



Follow these steps to modify the shelf ID:

6. Turn on the power to the shelf if it is not already on.
7. Remove either the front bezel or the left end cap to locate the ODP push button.
8. 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.
9. 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.
10. Press the button to advance the number until you reach the desired number from 0 to 9. The first number continues to blink.
11. 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.
12. Press the button to advance the number until you reach the desired number from 0 to 9. The second number continues to blink.
13. 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.
14. 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 EF280 storage systems and related hardware, see the EF280 documentation at <http://mysupport.netapp.com/eseries>.

5 Drive Shelves

The EF280 all-flash array consists of a controller drive shelf that supports 24 SSDs and up to 3 DE224C expansion drive shelves for a maximum of 96 SSDs.

The DE224C is a 2RU shelf that holds up to 24 2.5" drives. It features dual high-speed 12Gbps SAS 3 I/O modules (IOMs) and dual Energy Star Platinum-rated high-efficiency power supplies (913W) with integrated fans in a duplex system. It is fully redundant with hot-swappable components.

Figure 50, Figure 51, and Figure 52 show the front and rear views of the DE224C drive shelf.

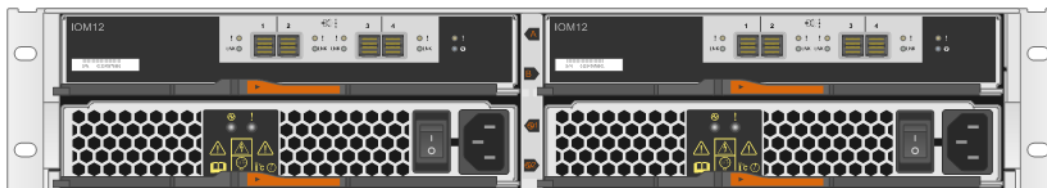
Figure 50) DE224C front view with end caps.



Figure 51) DE224C front view without end caps.



Figure 52) DE224C rear view.

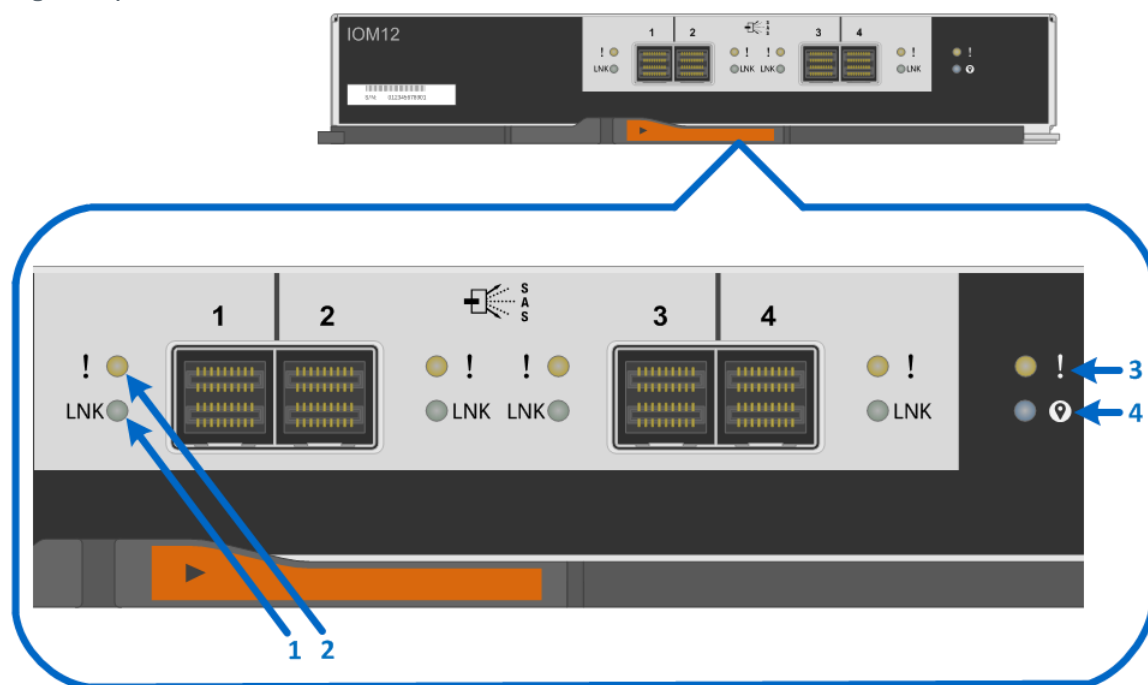


The modular design of the DE224C make the hardware easy to deploy and maintain over the life of the storage system.

5.1 IOM LED Definitions

Figure 53 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 53) LEDs for IOM.



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

Table 26 defines the LEDs for the IOM.

Table 26) 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.

5.2 Drive LED Definitions

Figure 54 shows the LEDs on the drive carriers for the EF280 SSDs. The DE224C shelf in the EF280 architecture supports only 2.5-inch form-factor SSDs.

Figure 54) EF280 drive carrier LEDs.

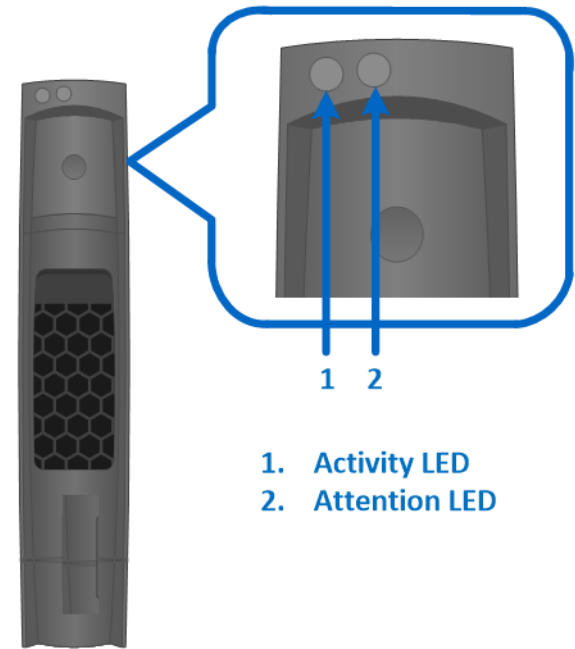


Table 27 defines the LEDs for the drives.

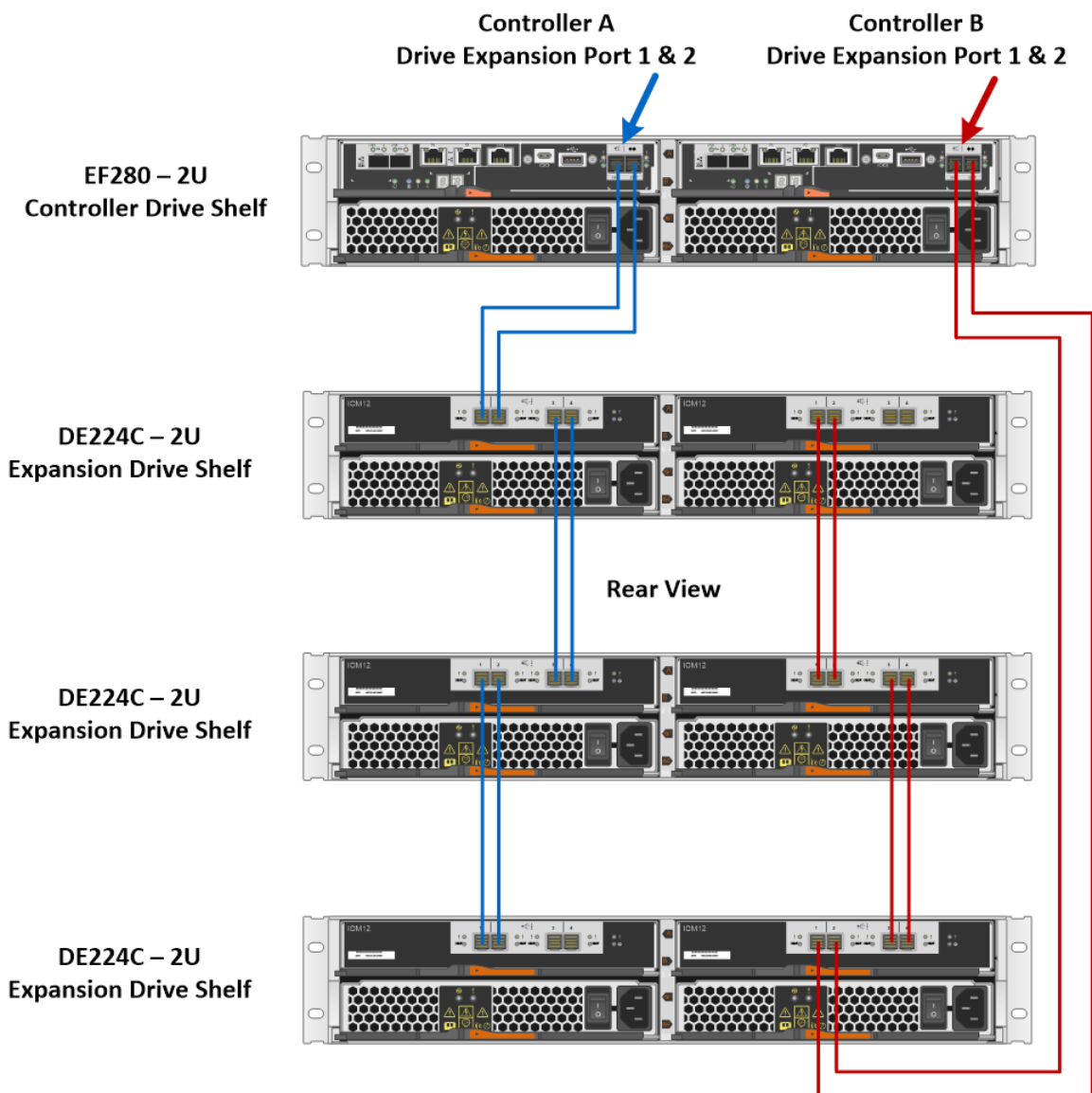
Table 27) EF280 drive LED definitions.

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.

5.3 Greenfield Installation

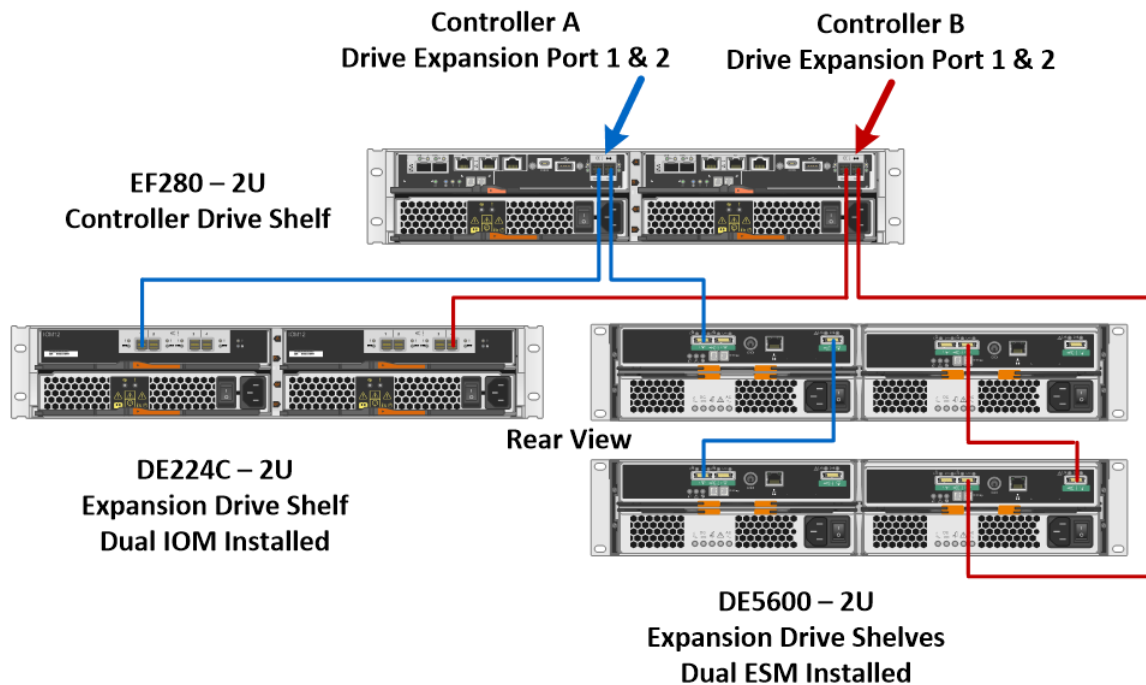
EF280 storage systems use a single-stack method where both controllers have a 12Gbps SAS path to both the expansion port 1 and expansion port 2 paths, as shown in Figure 55.

Figure 55) EF280 expansion drive shelf cabling example for maximum DE224C shelf configuration.



For optimal performance, SAS 2 and SAS 3 drive shelves should be isolated into different storage systems. If you decide to combine SAS 2 and SAS 3 shelves on the same EF280, use the double-stack cabling method shown in Figure 56.

Figure 56) EF280 with mixed 6Gbps and 12Gbps expansion shelves.



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

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.

5.4 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.

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 new volume groups and disk pools.

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

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

Figure 57 and Figure 58 show the hot-add connectivity when a drive shelf is added as the last shelf in the system.

Figure 57) Drive shelf hot-add controller expansion A-side cabling.

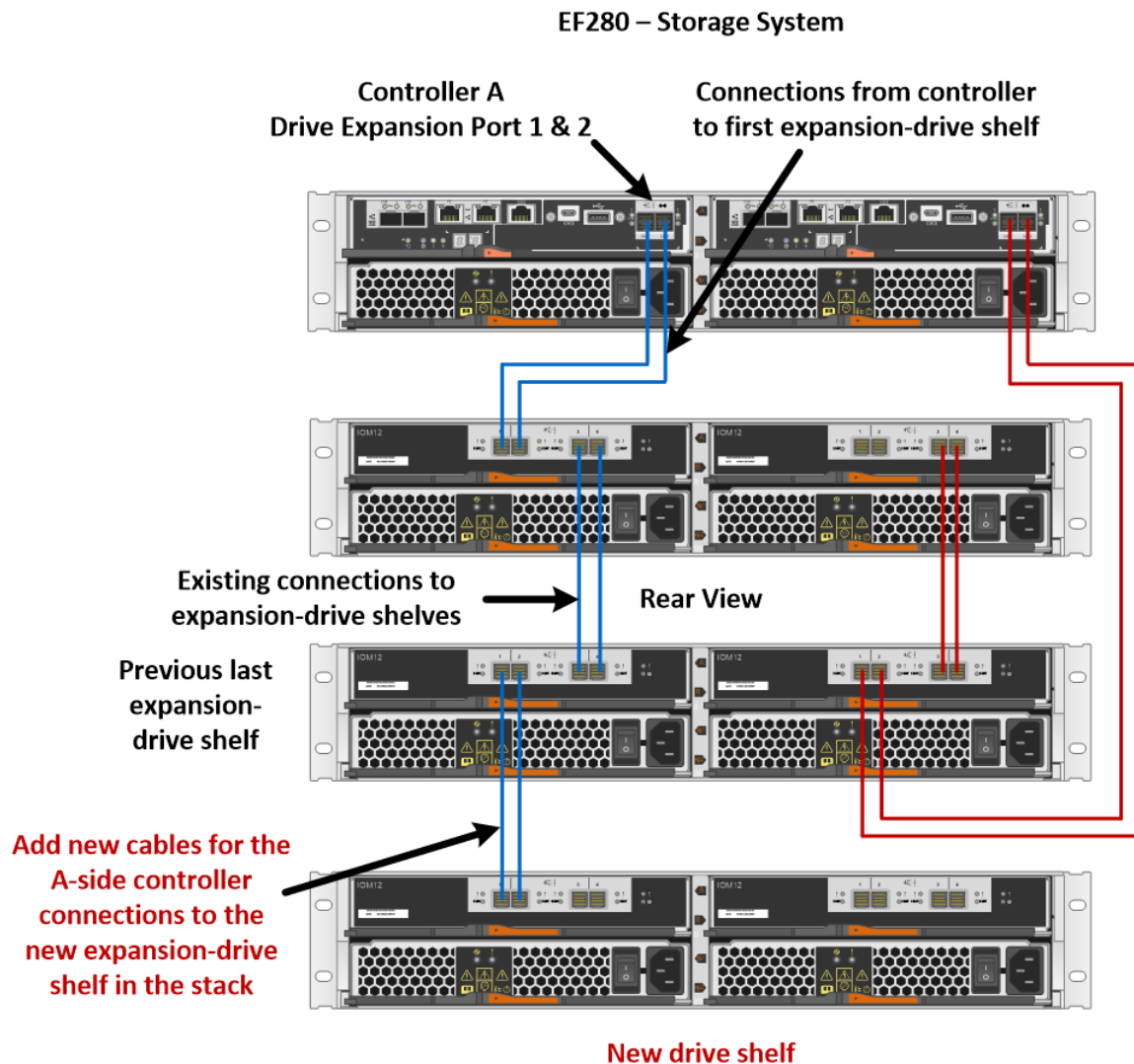
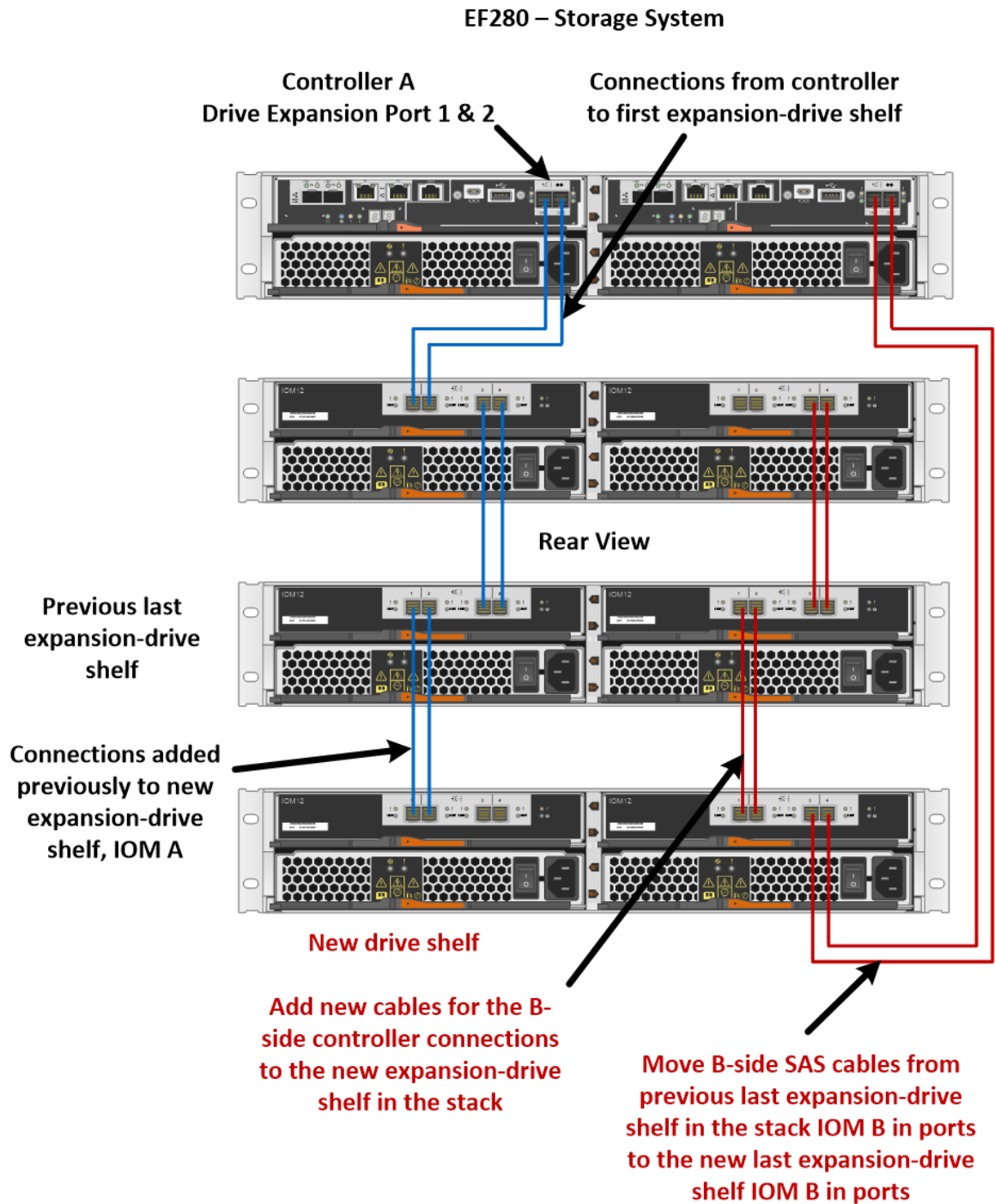


Figure 58) Drive shelf hot-add controller expansion B-side cabling.



Best Practice

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.
- The new expansion port 1 path is confirmed to be valid, and the new shelf is visible in the SANtricity management software before expansion path 2 is disconnected and moved to the new shelf.

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

6 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.

6.1 Controller Shelf Serial Number

The EF280 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 59.

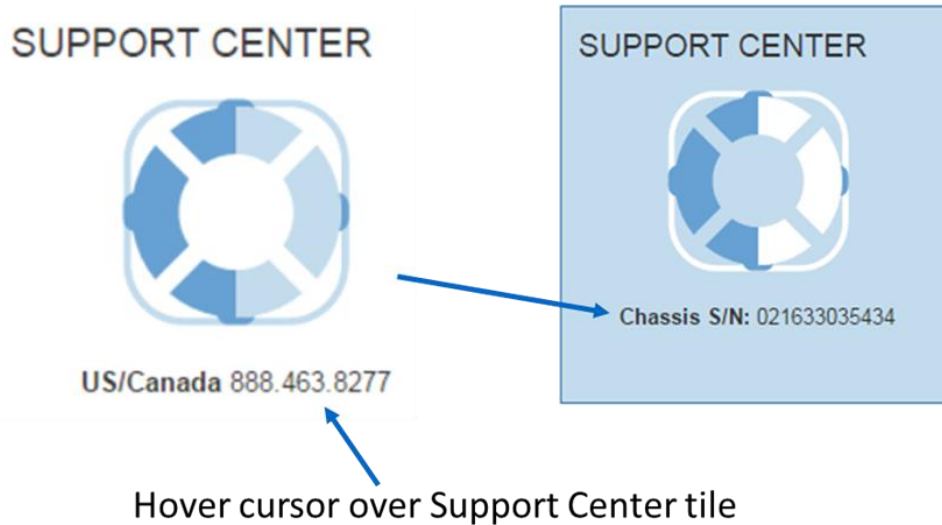
Figure 59) Controller shelf SN.



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 60.

Figure 60) SANtricity System Manager Support Center tile showing chassis serial number.



6.2 License Keys

E-Series and EF-Series storage arrays use two types of license keys. One type of key file is for premium features, and the other type of key file is used to change the storage system feature pack (changes the host interface protocol). For the EF280 arrays, all features are enabled out of the box.

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

When EF280 controllers are equipped with either the 2-port optical baseboard or the 2 or 4-port optical 16Gb FC or 10Gb iSCSI HIC, feature pack keys are used to change the host interface protocol from FC to iSCSI or from iSCSI to FC. The process to generate a new feature pack key for your storage array is the same as generating a premium feature key, except that the 11-digit key activation code for each package is available at no additional cost. This process is listed in the hardware upgrade instructions per controller type, at <https://mysupport.netapp.com/eseries>.

After the feature pack file is downloaded to the host server, click Change Feature Pack (Figure 61). Follow the prompts, beginning with browsing to the feature pack file (Figure 62).

Figure 61) Change feature pack from Settings > System view.

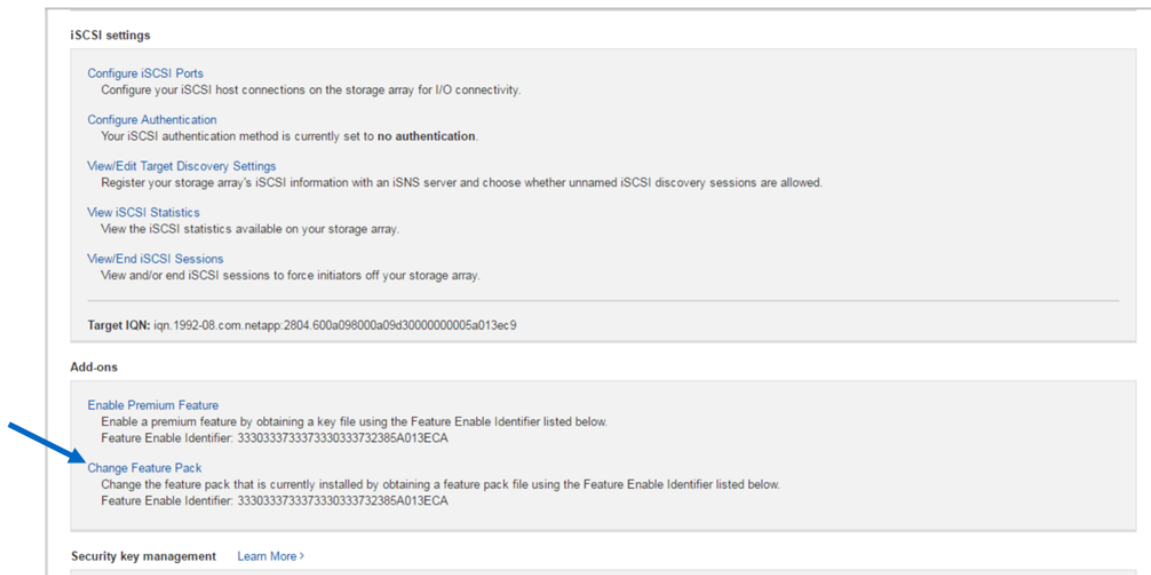
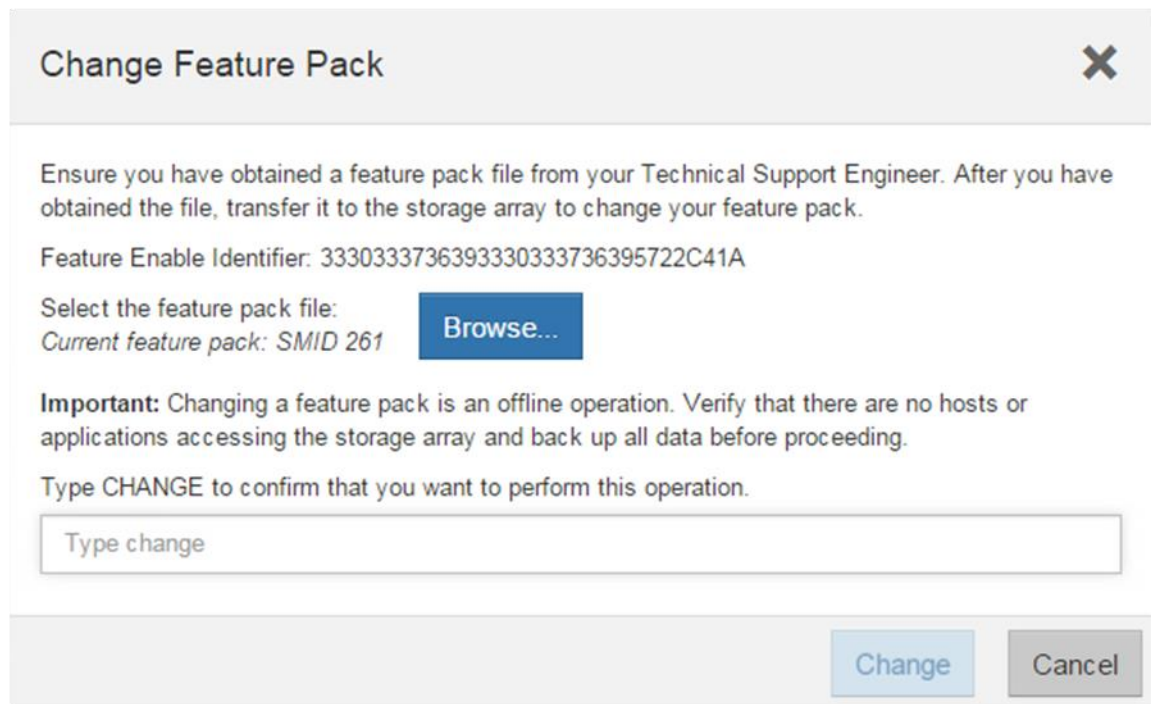


Figure 62) Change Feature Pack option.



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.

7 Conclusion

The NetApp EF280 all-flash storage system helps you cut operational costs with ultra-dense drive shelves for capacity-hungry applications while simplifying storage administration with the intuitive, easy-to-learn SANtricity System Manager and SANtricity Unified Manager web-based UIs. EF280 arrays are easily integrated with popular enterprise application software to accelerate workloads that use Oracle, Microsoft SQL Server, Splunk, and many other applications, especially in the small to medium enterprise space.

EF280 storage systems provide consistent performance and versatility, including multiple host interface choices, multiple RAID choices, and the ability to scale up to 1.4PB of raw, fast capacity. For high-random IOPS environments, the EF280 supports up to 300k 4KB read IOPS. For high-bandwidth workloads, the EF280 supports up to 10GBps sequential read workloads. This combination of entry-level packing with enterprise-grade scale out makes the EF280 an optimal solution for SMB performance challenges.

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 Documentation Center
<http://mysupport.netapp.com/eseries>
- NetApp Product Documentation
docs.netapp.com

Version History

Version	Date	Document Version History
Version 1.0	May 2018	Initial release
Version 1.1	March 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

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 © 2020 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-4727-0520