Technical Report

Introduction to NetApp EF50 array

Feature overview with SANtricity

Alonso DeVega, NetApp

March 2026 | TR-5018

Abstract

The NetApp® EF50 NVMe (NVM Express) all-flash arrays deliver optimal performance without compromising on the Reliability, Availability, and Serviceability (RAS) features that deliver up to 99.9999% availability. This document provides detailed information about the hardware and software features of the EF50 all-flash array and new NetApp SANtricity® features.

TABLE OF CONTENTS

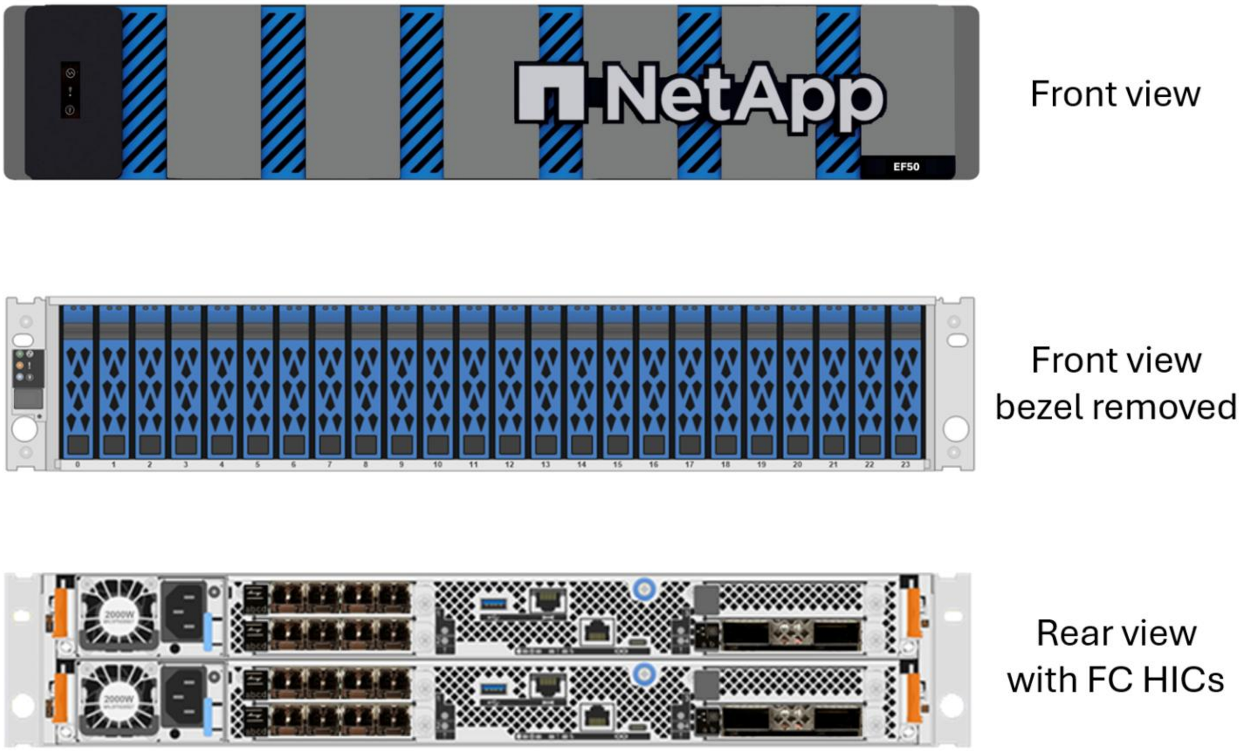
LIST OF TABLES

LIST OF FIGURES

Introduction

NetApp® EF50 all-flash array has a modern look, as shown in Figure 1, uses end-to-end NVMe NE224 drive shelves, supports up to 24 NVMe SSDs, and is managed by the secure web-based NetApp SANtricity® System Manager UI. The array's performance capabilities enable enterprise databases, analytics, and artificial intelligence (AI) workloads to run faster.

Figure 1) New generation EF50 all-flash array.



In one powerful all-flash array package, the EF50 array delivers optimal performance for both random workloads and large sequential workloads. The EF50 array can deliver consistent response times for up to 1.7 million 4KB random read IOPS. The same configuration can deliver about 42GBps large sequential read throughput and about 16GBps cache-mirrored large sequential write throughput. When your workload meets the criteria of the built-in full stripe write acceleration feature, you can accelerate write performance up to 26GBps. Performance numbers based on using NVMe/FC host protocol in lab environment.

The EF50 supports the SCSI over Fibre Channel protocol (FCP) and the NVMe over Fibre Channel (NVMe/FC) protocol on the 64-Gb FC host interface card (HIC).

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

- Entry-level 3.8TB SSDs for small fast, random workloads
- Fast, large-capacity 7.6TB and 15.3TB SSDs to support higher-capacity sequential workloads, random workloads, or mixed workloads
- High density 30TB and 60TB SSDs for large capacity needs

For entry-level and large-capacity SSDs, an EF50 system can be ordered with a minimum of 6 drives. For high-density drives an EF50 can be ordered with a minimum of 12 drives.

EF-Series products have a documented history of delivering up to 99.9999% availability when systems are properly sized, deployed, and maintained with NetApp Support agreements. EF-Series products also include NetApp Active IQ® technology to enhance your ongoing product experience.

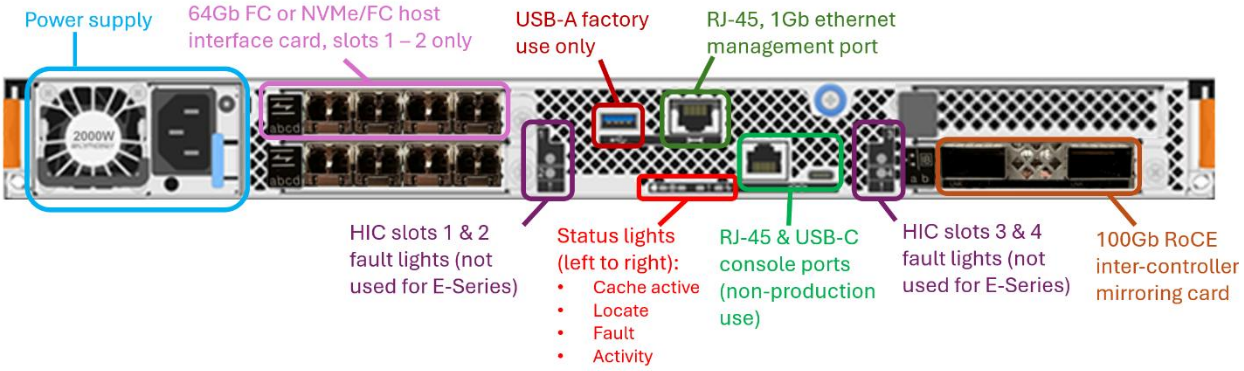
Each EF50 controller provides a single Ethernet management port for out-of-band management, in-band management not supported. The EF50 array also introduces new, faster host interface option that fits the needs of the world's most demanding storage environments. These options are in one easy-to-install and easy-to-maintain hardware and integrated management software package.

Currently this package only allows either one or two 4-port 64Gb FC or NVMe/FC (OM4 fiber required) HICs for host connectivity.

Note: Changing the host protocol between the various available protocols on each HIC can be done through System Manager.

Figure 2 identifies the various interface ports on the EF50 controller.

Figure 2) EF50 controller with ports identified.


Power supply
64Gb FC or NVMe/FC host interface card, slots 1 – 2 only
USB-A factory use only
RJ-45, 1Gb ethernet management port
2000W
abcd
abcd
a b
HIC slots 1 & 2 fault lights (not used for E-Series)
Status lights (left to right):
• Cache active
• Locate
• Fault
• Activity
RJ-45 & USB-C console ports (non-production use)
HIC slots 3 & 4 fault lights (not used for E-Series)
100Gb RoCE inter-controller mirroring card

Note: Type-A USB port for factory use only and is disabled if SANtricity OS is running.

For optical connections, you must order appropriate SFP modules for your specific implementation. Consult the NetApp Hardware Universe for a full listing of available host interface equipment.

The EF50 continues the E-Series legacy of providing fast, simple, reliable, and flexible SAN storage regardless of the workload. NetApp EF50 all-flash arrays can support the workload if the following conditions are met:

- Hosts are qualified with EF-Series arrays.
- Hosts use SAN access to the storage, whether directly connected or fabric connected.
- Storage is managed at the host or file system level.

In fact, some of the world's most demanding online transactional workloads run on EF-Series arrays because these arrays are blazing fast, simple to install and operate, and extremely reliable, providing up to 99.9999% data availability. You can apply these highly flexible SAN building blocks when you need them and plug them into your current application environment on demand without disrupting your primary storage management strategy. EF-Series arrays can operate in a space as small as 2U, seamlessly integrate with many software layers, and still deliver consistently low-latency performance. These capabilities make EF-Series arrays an optimal SAN building block for any size enterprise that needs to support demanding online or database-reliant workloads.

Whether you are running Oracle Automatic Storage Management (ASM), Microsoft SQL Server, Splunk real-time analytics, or specialty applications with demanding response-time requirements, the EF50 array maintains its performance profile. To fully maximize performance, only minor setting changes are required when you create disk pools, volume groups, or volumes to switch between high-IOPS configurations and high-throughput configurations. This characteristic makes EF-Series arrays easy to deploy regardless of your workload.

EF50 arrays use the web-based SANtricity System Manager GUI to manage individual arrays, and SANtricity Unified Manager enables you to organize and manage multiple new-generation E-Series and EF-Series arrays from a central management application. The built-in web services API integration or the management client-based web services package makes the EF-Series product line easier than ever to integrate with your standard API-driven environment.

The following sections provide broad product information, including technical details about some newer SANtricity features. Some familiarity with basic configuration concepts such as volumes, Dynamic Disk Pools (DDP) and RAID volume groups (VGs) is assumed.

SANtricity management features

NetApp E-Series and EF-Series arrays have a rock-solid reputation for reliability, availability, simplicity, and security.   The new-generation E-Series and EF-Series arrays running the latest SANtricity OS are Common Criteria certified (NDcPP v2 certification).

Deployment

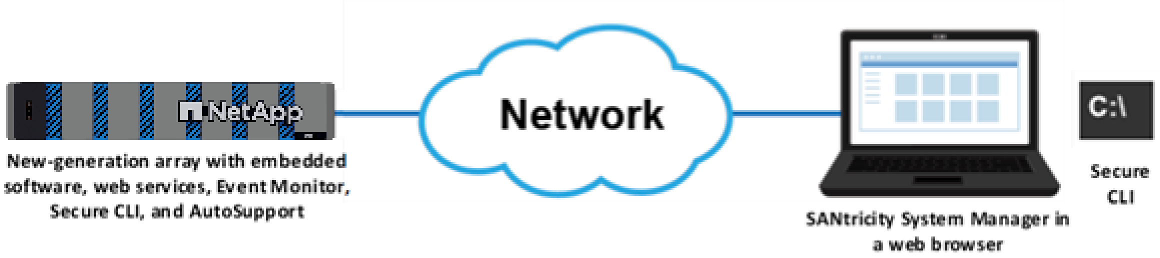
Deciding which components to install on an EF50-based storage array depends on if you want to manage single storage arrays individually or if you are managing multiple arrays.

Managing storage arrays individually

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

Note: EF50 does not support asynchronous or synchronous mirroring. It is recommended to use replication (mirroring) and erasure coding features available in modern applications.

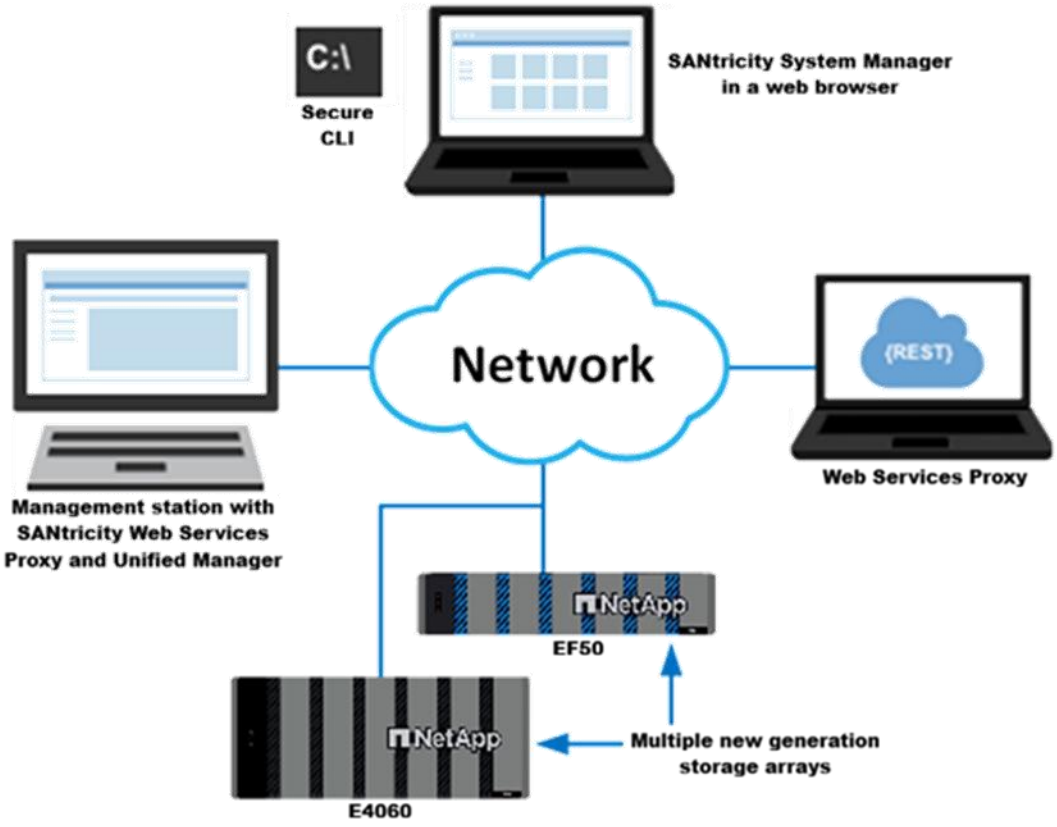
Figure 3) Managing a single EF50 with SANtricity System Manager.


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

Multiple storage arrays management

If you have one or more storage arrays, you can install the 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 4.

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


C:\
Secure CLI
SANtricity System Manager in a web browser
Network
Management station with SANtricity Web Services Proxy and Unified Manager
(REST)
Web Services Proxy
NetApp
EF50
NetApp
E4060
Multiple new generation storage arrays

SANtricity Unified Manager

SANtricity Unified Manager is a web-based central management interface that replaces the legacy SANtricity Storage Manager Enterprise Management Window (EMW) for managing the new-generation 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 adds the following time-saving features:

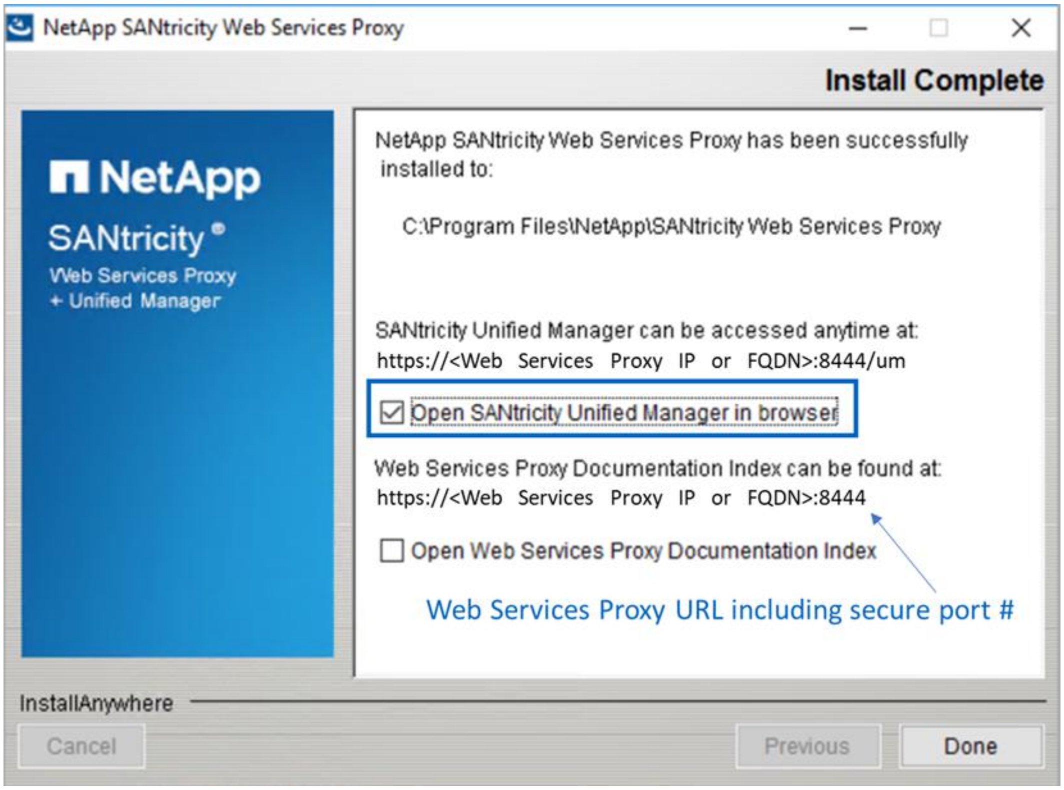
- Upgrades multiple arrays with the same type of controller at one time.
- Supports Lightweight Directory Access Protocol (LDAP) and role-based access control (RBAC) just like SANtricity System Manager. It includes a simplified certificate management workflow to manage the Unified Manager or Web Services 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. You save time by not duplicating setup steps for each array.
- Supports synchronous and asynchronous mirroring for all new generation arrays through the secure SSL interface.

Note: EF50 does not support asynchronous or synchronous mirroring. It is recommended to use replication (mirroring) and erasure coding features available in modern applications.

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

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

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



NetApp SANtricity Web Services Proxy

Install Complete

NetApp SANtricity Web Services Proxy has been successfully installed to:

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

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

☑ Open SANtricity Unified Manager in browser

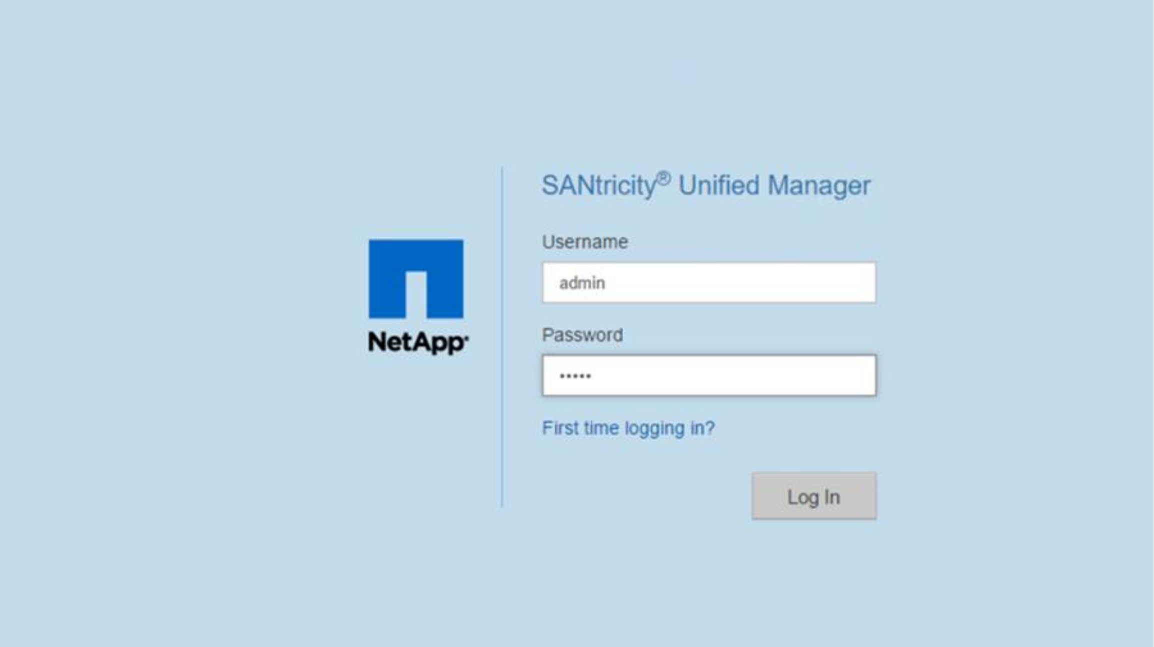
Web Services Proxy Documentation Index can be found at:
https://<Web Services Proxy IP or FQDN>:8444

□ Open Web Services Proxy Documentation Index

Web Services Proxy URL including secure port #

If you want to open the Unified Manager UI after the Web Services Proxy installation, open a browser, 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 6) by adding `/um` to the URL—for example, `https://<proxy-FQDN>:<port #>/um`.

Figure 6) SANtricity Unified Manager login page.



SANtricity® Unified Manager

Username: admin

Password: •••••

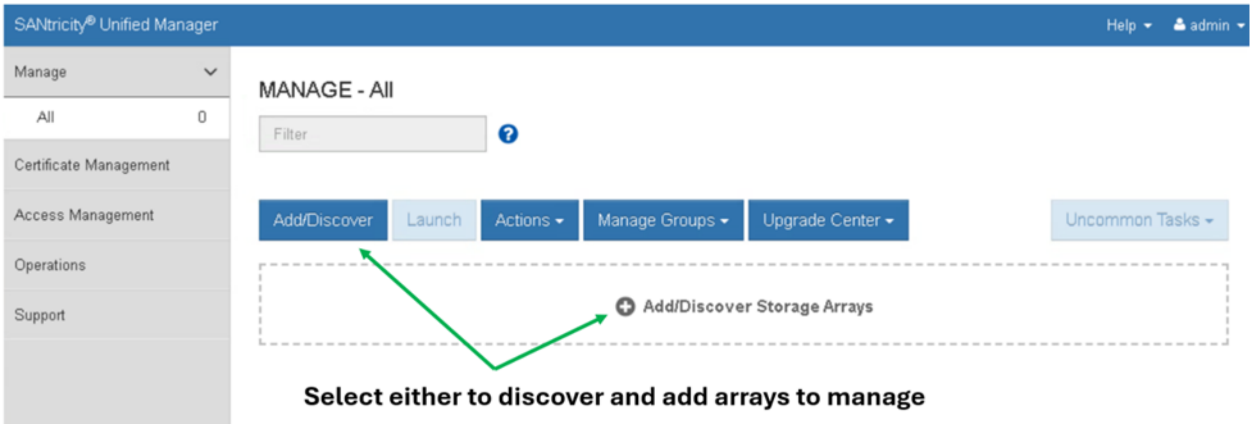
SANtricity Unified Manager navigation

The login page for SANtricity Unified Manager has a similar appearance to SANtricity System Manager and requires administrators to set the array admin password as part of the initial login. SANtricity Unified Manager has a factory default admin account: `admin`. There is also a `monitor` account that allows read-only access if needed.

Discovering and adding storage arrays

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

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

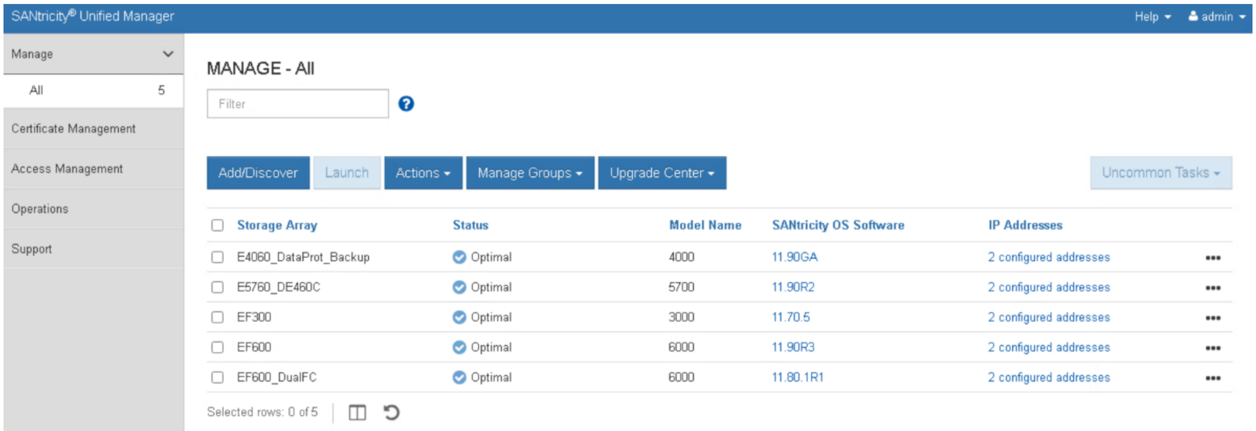


MANAGE - All

Select either to discover and add arrays to manage

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

Figure 8) SANtricity Unified Manager landing page.



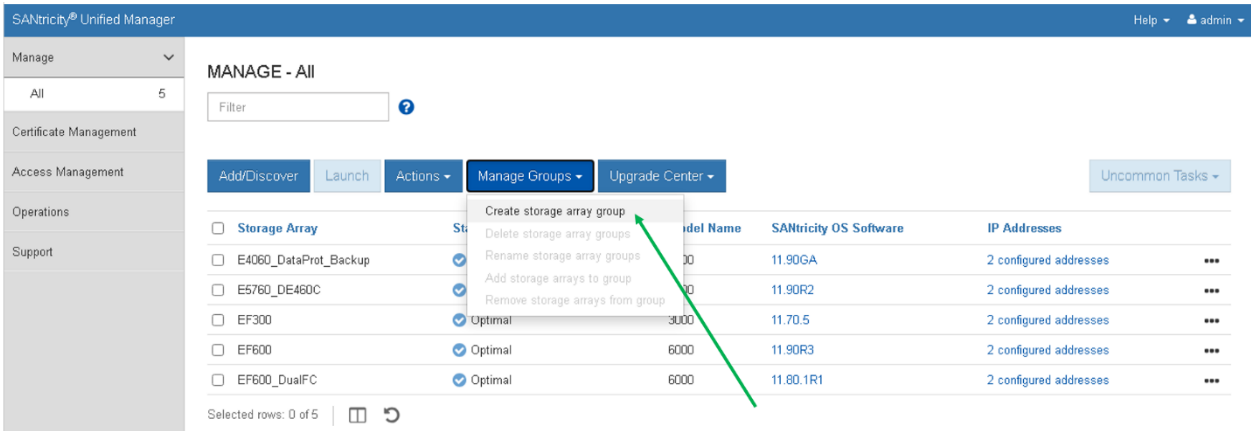
□	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses	
□	E4060_DataProt_Backup	Optimal	4000	11.90GA	2 configured addresses	•••
□	E5760_DE460C	Optimal	5700	11.90R2	2 configured addresses	•••
□	EF300	Optimal	3000	11.70.5	2 configured addresses	•••
□	EF600	Optimal	6000	11.90R3	2 configured addresses	•••
□	EF600_DualFC	Optimal	6000	11.80.1R1	2 configured addresses	•••

Selected rows: 0 of 5

Organize arrays by group

After you add arrays to Unified Manager, you can group them to organize your array management environment. Figure 9 shows the EF600 arrays added to a group. This capability is available for all new-generation E-Series and EF-Series arrays.

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

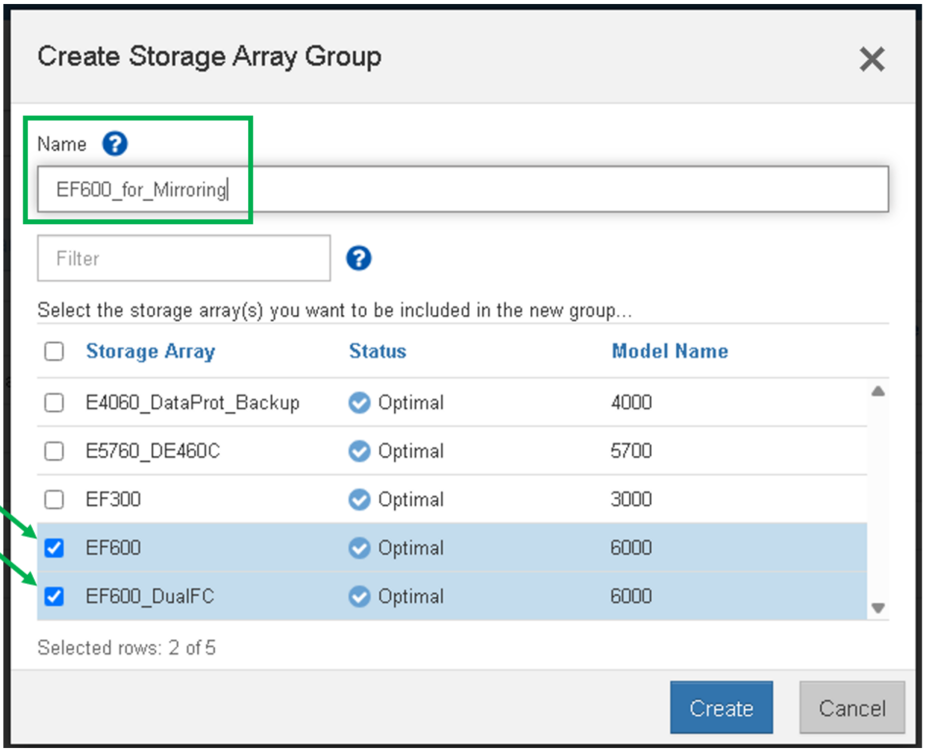

SANtricity® Unified Manager
Help
admin
Manage
All 5
Certificate Management
Access Management
Operations
Support
MANAGE - All
Filter
Add/Discover
Launch
Actions
Manage Groups
Upgrade Center
Uncommon Tasks
Create storage array group
Delete storage array groups
Rename storage array groups
Add storage arrays to group
Remove storage arrays from group

□	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses	
□	E4060_DataProt_Backup			11.90GA	2 configured addresses	•••
□	E5760_DE460C			11.90R2	2 configured addresses	•••
□	EF300	Optimal	3000	11.70.5	2 configured addresses	•••
□	EF600	Optimal	6000	11.90R3	2 configured addresses	•••
□	EF600_DualFC	Optimal	6000	11.80.1R1	2 configured addresses	•••

Selected rows: 0 of 5

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

Figure 10) Creating a group in Unified Manager.



Create Storage Array Group

Name

EF600_for_Mirroring

Filter

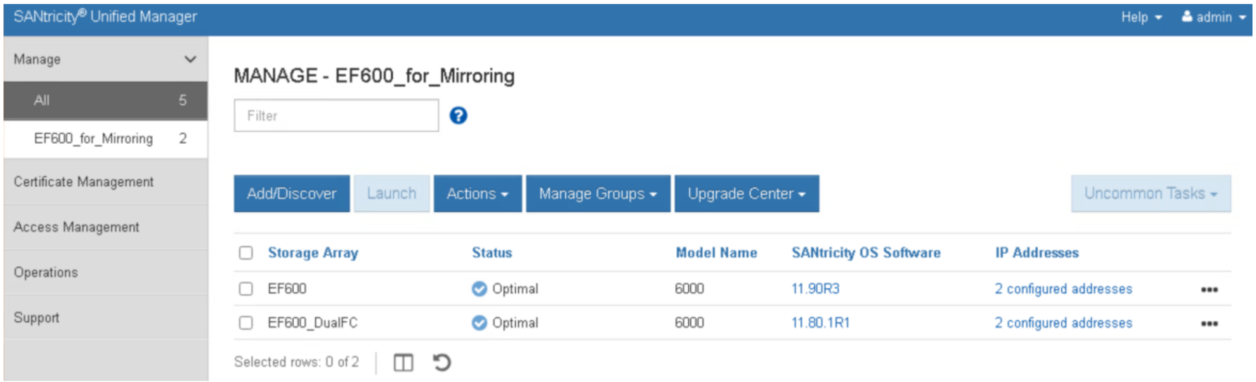
Select the storage array(s) you want to be included in the new group...

☐	Storage Array	Status	Model Name
☐	E4060_DataProt_Backup	Optimal	4000
☐	E5760_DE460C	Optimal	5700
☐	EF300	Optimal	3000
☑	EF600	Optimal	6000
☑	EF600_DualFC	Optimal	6000

Selected rows: 2 of 5

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

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



MANAGE - EF600_for_Mirroring

Filter

☐	Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses
☐	EF600	Optimal	6000	11.90R3	2 configured addresses
☐	EF600_DualFC	Optimal	6000	11.80.1R1	2 configured addresses

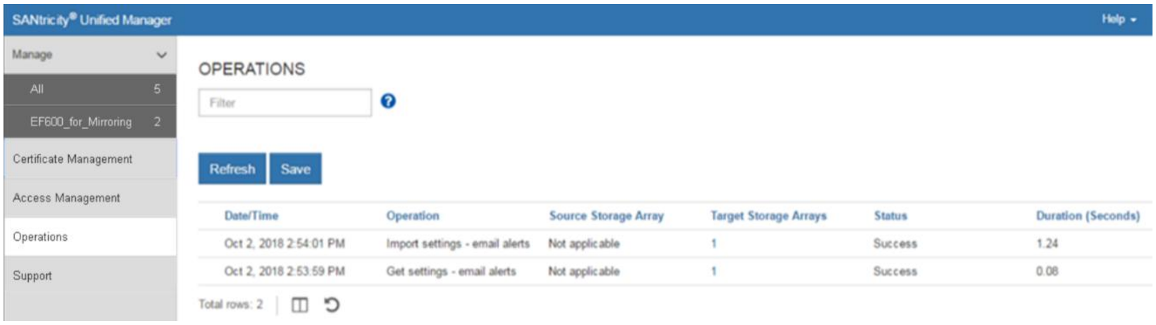
Selected rows: 0 of 2

Import settings and view 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 systems. For example, if you want the same alerting and NetApp AutoSupport settings on all systems, use the Import Settings wizard to select the setting category, the array to copy from, and the array to import to, and click Finish. The operation to copy the settings is displayed in the Operations view, as shown in Figure 12.

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

Figure 12) SANtricity Unified Manager Operations view.

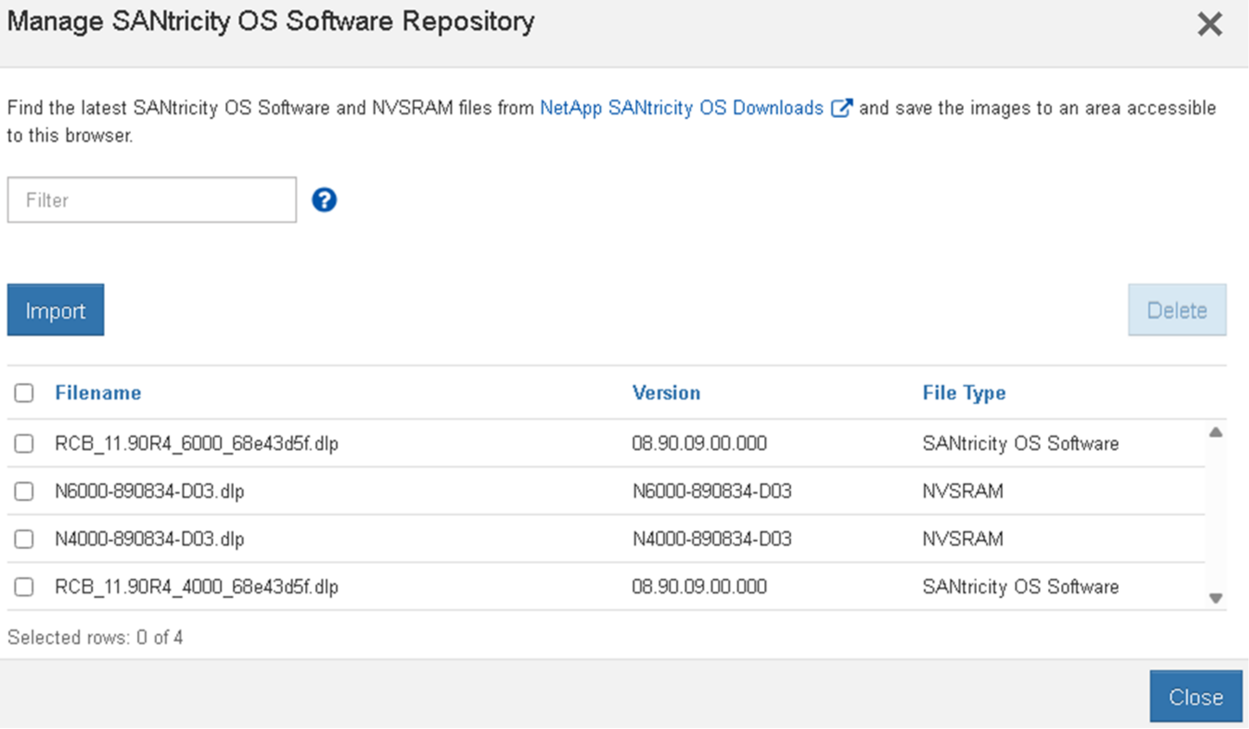


Date/Time	Operation	Source Storage Array	Target Storage Arrays	Status	Duration (Seconds)
Oct 2, 2018 2:54:01 PM	Import settings - email alerts	Not applicable	1	Success	1.24
Oct 2, 2018 2:53:59 PM	Get settings - email alerts	Not applicable	1	Success	0.08

Update SANtricity OS through Unified Manager

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

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



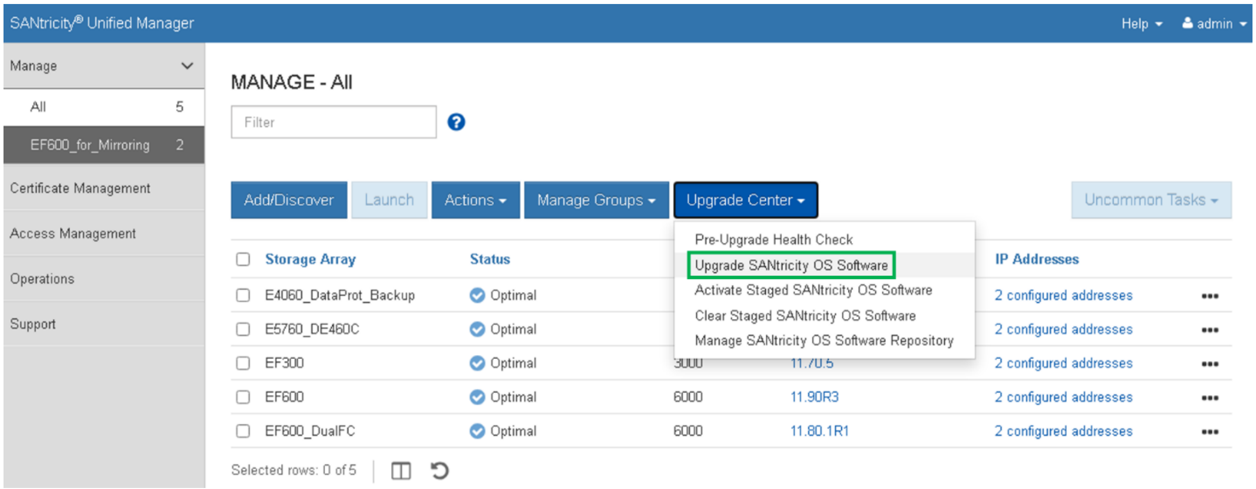
Manage SANtricity OS Software Repository

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

□	Filename	Version	File Type
□	RCB_11.90R4_6000_68e43d5f.dlp	08.90.09.00.000	SANtricity OS Software
□	N6000-890834-D03.dlp	N6000-890834-D03	NVSRAM
□	N4000-890834-D03.dlp	N4000-890834-D03	NVSRAM
□	RCB_11.90R4_4000_68e43d5f.dlp	08.90.09.00.000	SANtricity OS Software

Selected rows: 0 of 4

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

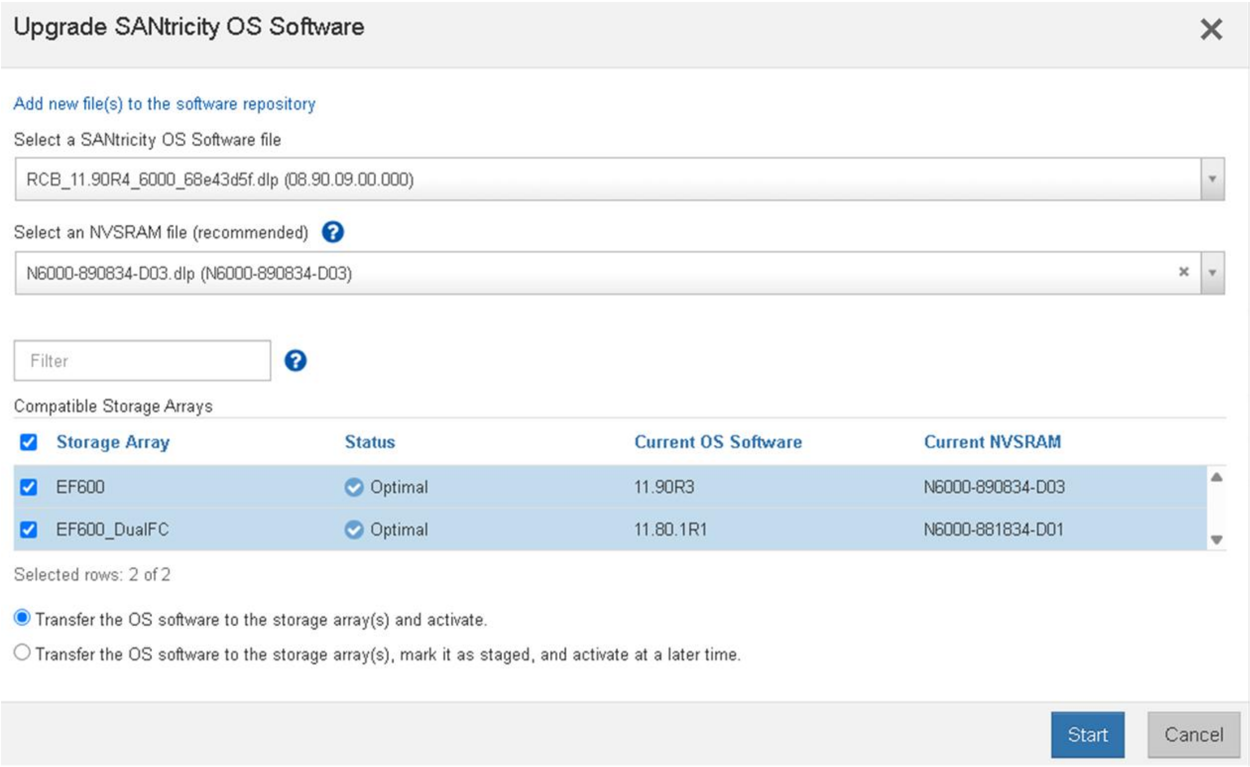


MANAGE - All

□	Storage Array	Status			IP Addresses	
□	E4060_DataProt_Backup	Optimal			2 configured addresses	•••
□	E5760_DE460C	Optimal			2 configured addresses	•••
□	EF300	Optimal	3000	11.70.5	2 configured addresses	•••
□	EF600	Optimal	6000	11.90R3	2 configured addresses	•••
□	EF600_DualFC	Optimal	6000	11.80.1R1	2 configured addresses	•••

Selected rows: 0 of 5

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



Upgrade SANtricity OS Software

Select a SANtricity OS Software file: RCB_11.90R4_6000_68e43d5f.dlp (08.90.09.00.000)

Select an NVSRAM file (recommended): N6000-890834-D03.dlp (N6000-890834-D03)

Compatible Storage Arrays

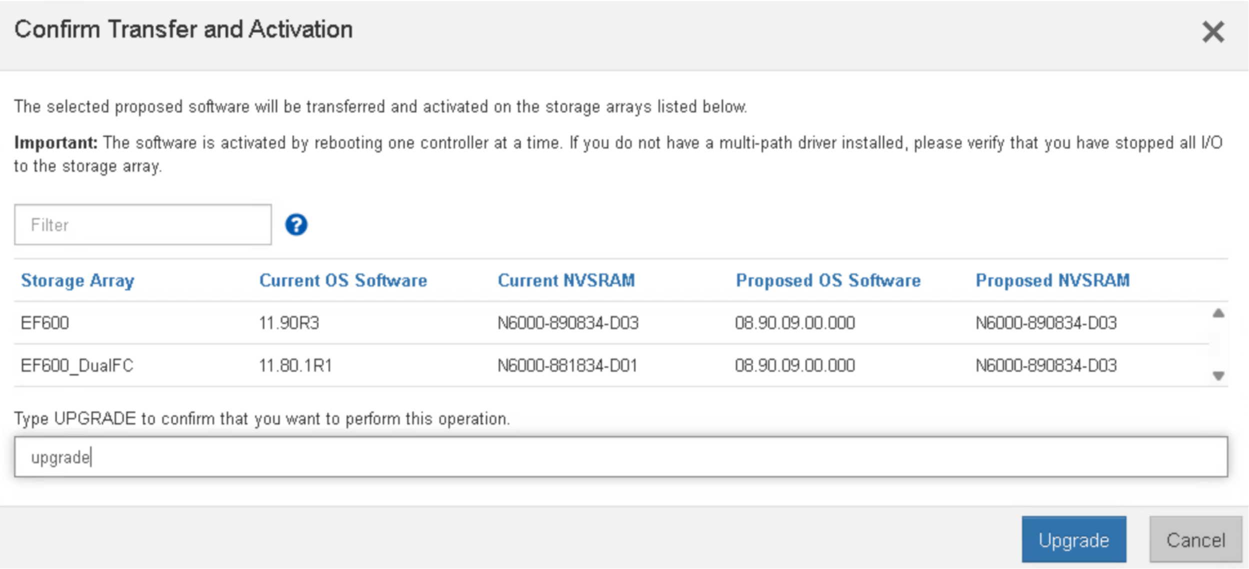
☑	Storage Array	Status	Current OS Software	Current NVSRAM
☑	EF600	Optimal	11.90R3	N6000-890834-D03
☑	EF600_DualFC	Optimal	11.80.1R1	N6000-881834-D01

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.

5. On the Confirm Transfer and Activation page, type `upgrade` and then click Upgrade button to begin the SANtricity OS files transfer.



Confirm Transfer and Activation

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

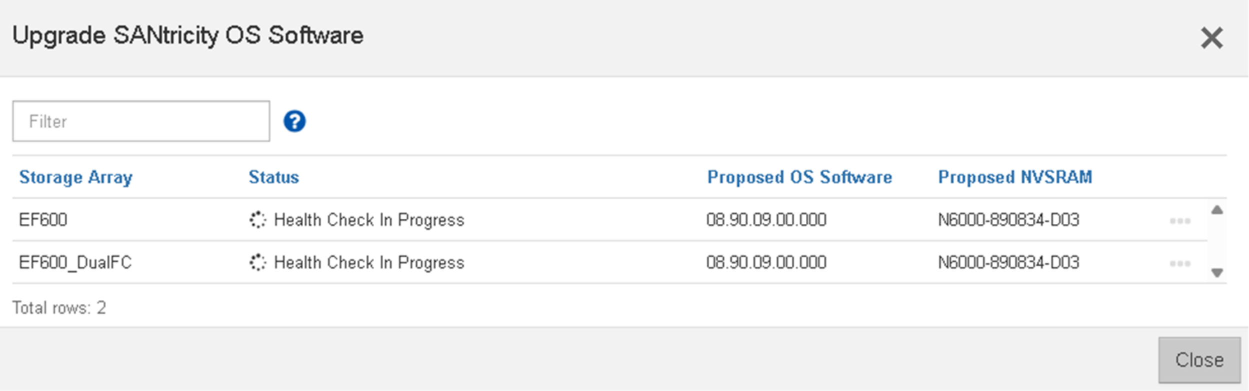
Important: The software is activated by rebooting one controller at a time. If you do not have a multi-path driver installed, please verify that you have stopped all I/O to the storage array.

Storage Array	Current OS Software	Current NVSRAM	Proposed OS Software	Proposed NVSRAM
EF600	11.90R3	N6000-890834-D03	08.90.09.00.000	N6000-890834-D03
EF600_DualFC	11.80.1R1	N6000-881834-D01	08.90.09.00.000	N6000-890834-D03

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

upgrade

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



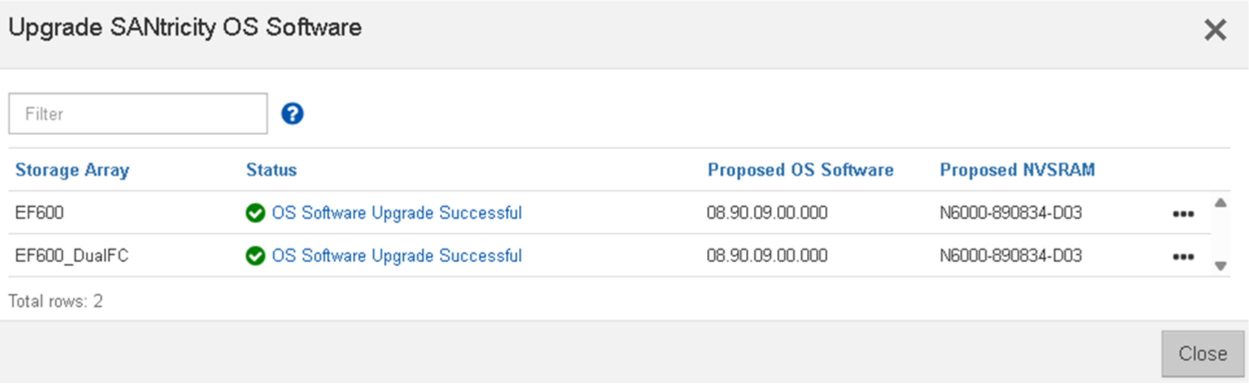
Upgrade SANtricity OS Software

Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF600	Health Check In Progress	08.90.09.00.000	N6000-890834-D03
EF600_DualFC	Health Check In Progress	08.90.09.00.000	N6000-890834-D03

Total rows: 2

7. After the files have been transferred and the controllers have completed rebooting, the status changes to OS Software Upgrade Successful. The Upgrade SANtricity OS Software window can now be closed.

Note: To have volumes failback to preferred controller, from Volumes screen in System Manager click on 3 vertical dots next to “Create” button and select Redistribute volumes from drop-down menu.

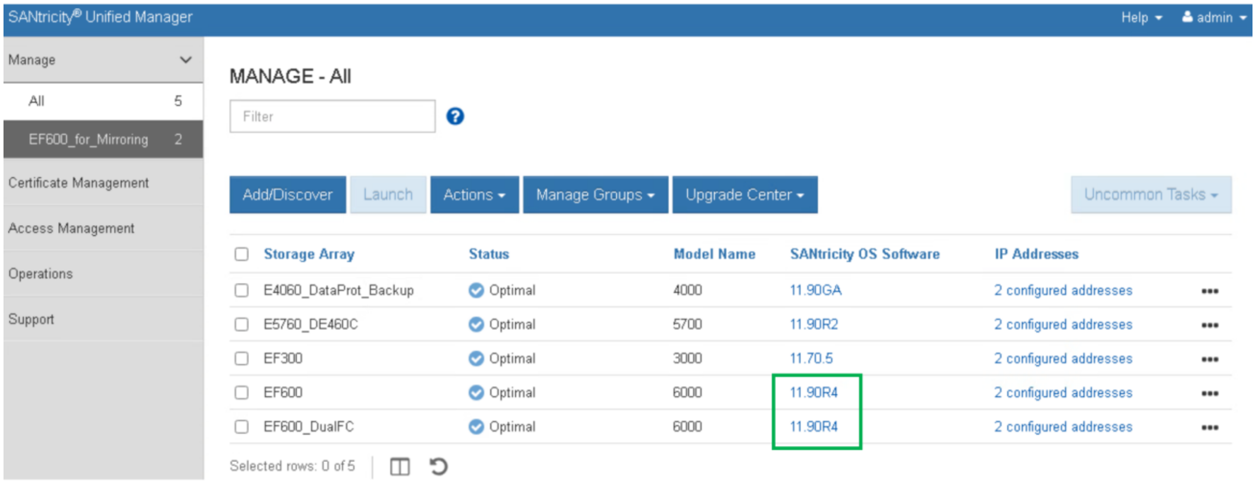


Upgrade SANtricity OS Software

Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF600	✓ OS Software Upgrade Successful	08.90.09.00.000	N6000-890834-D03
EF600_DualFC	✓ OS Software Upgrade Successful	08.90.09.00.000	N6000-890834-D03

Total rows: 2

8. On the Unified Manager landing page, the SANtricity OS Software version reflects the newly installed SANtricity OS version.



Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses
E4060_DataProt_Backup	Optimal	4000	11.90GA	2 configured addresses
E5760_DE460C	Optimal	5700	11.90R2	2 configured addresses
EF300	Optimal	3000	11.70.5	2 configured addresses
EF600	Optimal	6000	11.90R4	2 configured addresses
EF600_DualFC	Optimal	6000	11.90R4	2 configured addresses

SANtricity Unified Manager security

SANtricity Unified Manager supports the same secure management features as SANtricity System Manager, including LDAP, RBAC, and SSL certificates. For complete details and workflow examples, see TR-4712: NetApp SANtricity Management Security Feature Details and Configuration Guide, TR-4855: Security Hardening Guide for NetApp SANtricity, and TR-4813: Managing Certificates for NetApp E-Series Storage Systems.

SANtricity System Manager

SANtricity System Manager provides embedded management software, web services, event monitoring, secure CLI, and AutoSupport for EF50 arrays.

EF50 storage systems support and are shipped preloaded with the newest version of SANtricity OS available at the time of shipping, which includes SANtricity System Manager. To discover multiple EF50 storage systems running SANtricity OS from a central view, download the latest version of the Web Services Proxy, which includes the latest version of SANtricity Unified Manager.

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

Note: Host packages are not required for NVMe-oF installations. See the appropriate OS Express Guide for host setup requirements, instructions, and references. The guides are available from the NetApp Support Site at https://docs.netapp.com/us-en/e-series/index.html.

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

System Manager navigation

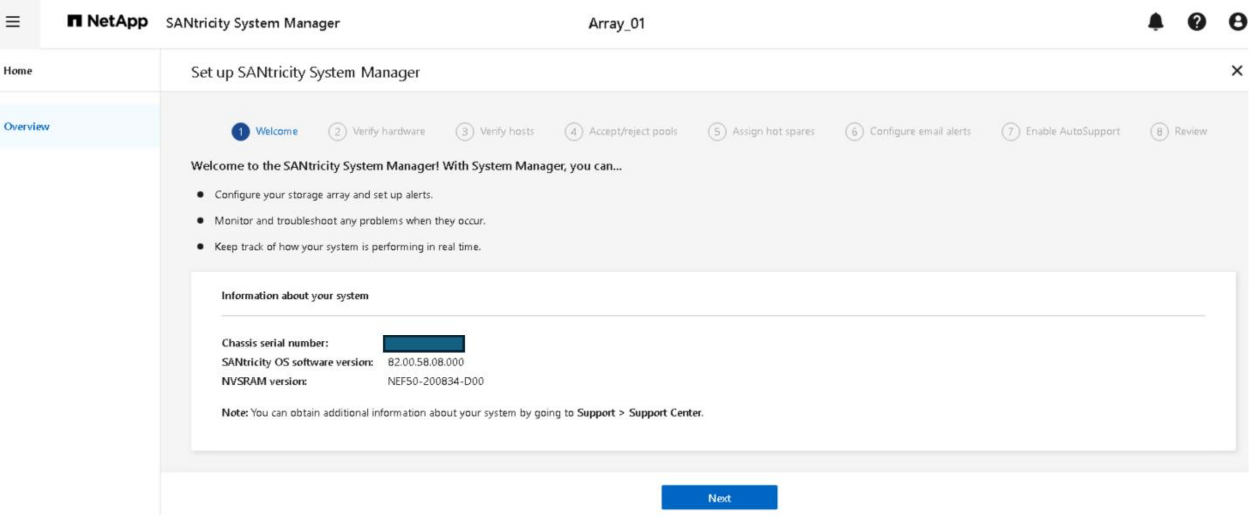
After you log in to SANtricity System Manager, if it's the first time logging in, or if at least one of the following is true:

- no pools or volume groups detected

- no workloads are detected
- no notifications are configured

Then the set-up wizard is displayed, see Figure 19.

Figure 13) SANtricity System Manager set up wizard.



Welcome to the SANtricity System Manager! With System Manager, you can...

- Configure your storage array and set up alerts.
- Monitor and troubleshoot any problems when they occur.
- Keep track of how your system is performing in real time.

Information about your system

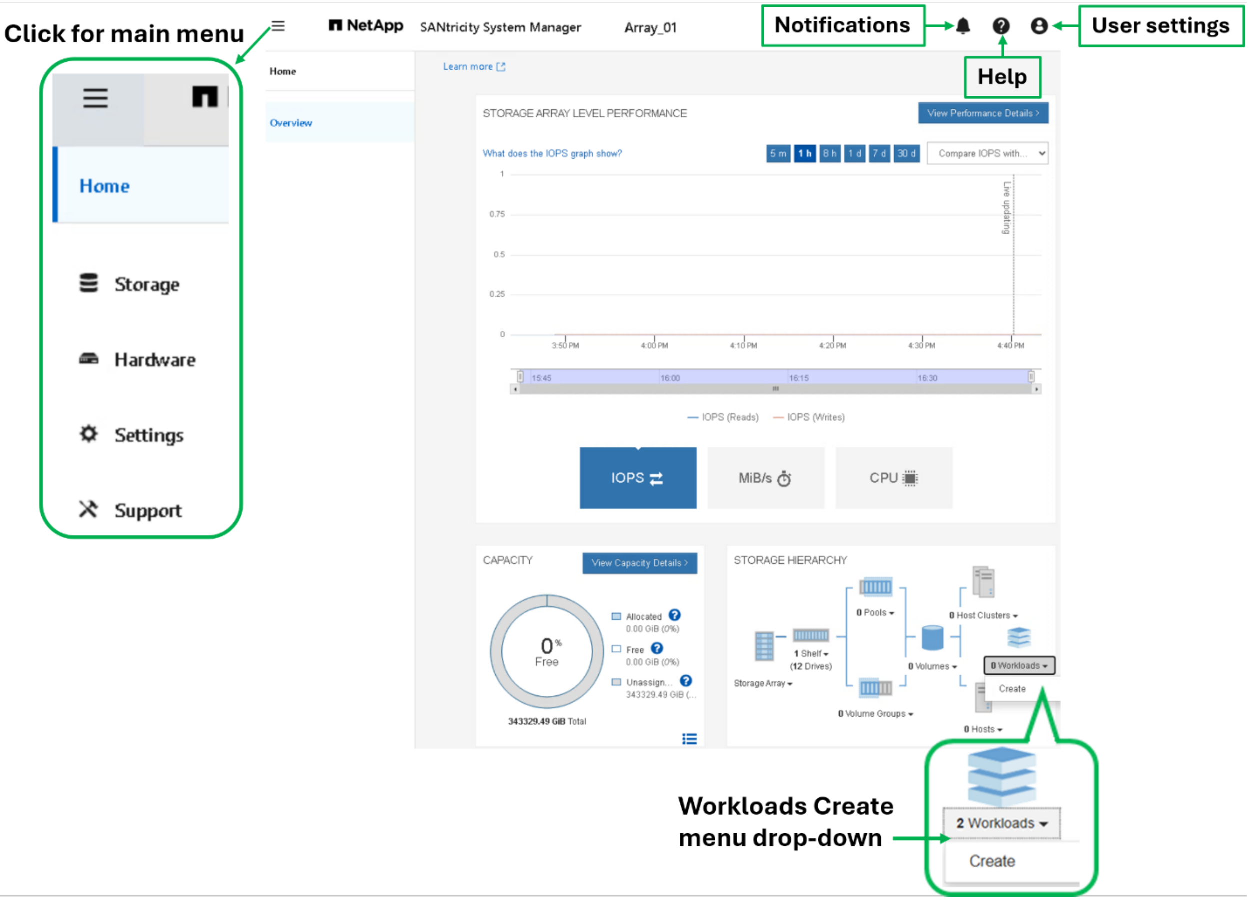
Chassis serial number: [redacted]
SANtricity OS software version: 82.00.58.08.000
NVSRAM version: NEF50-200834-D00

Note: You can obtain additional information about your system by going to **Support** > **Support Center**.

Once the set-up wizard has been closed, or when one of the conditions listed above has been met, the home page is displayed, as shown in Figure 14.

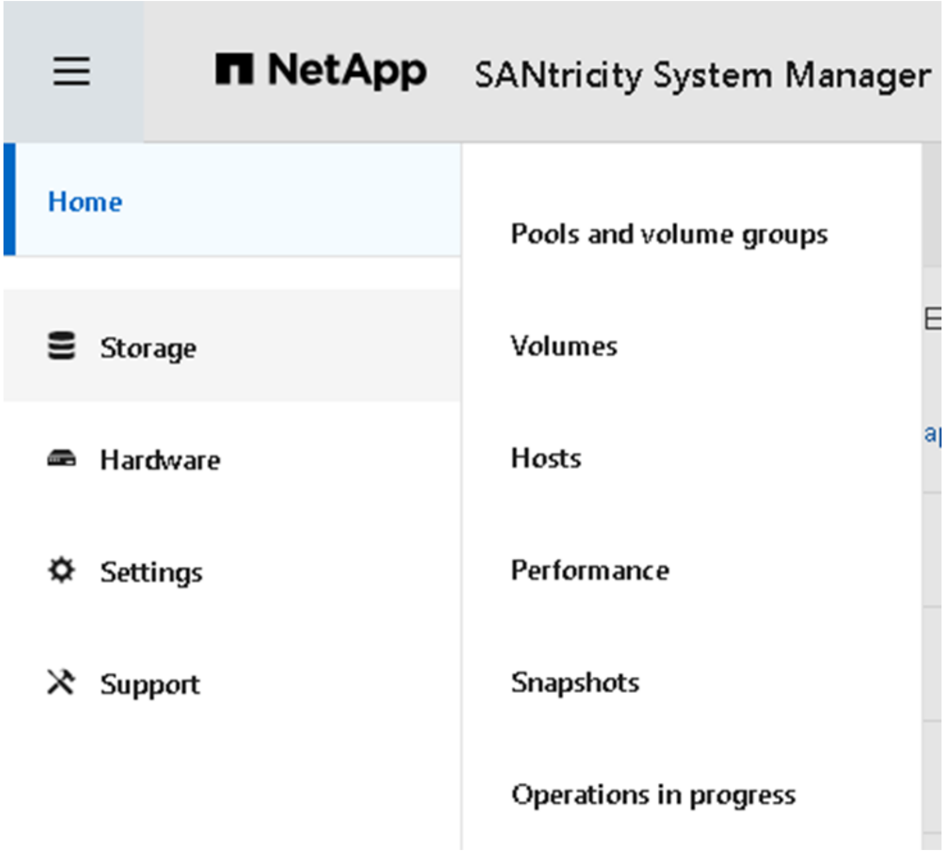
- The icons on the left let you navigate through the System Manager pages and are available on all pages. The text can be toggled on and off.
- The items on the top right (Preferences, Help, Log Out) are also available from any location in System Manager.
- At the bottom-right corner is an architectural view of your array that lets you provision the storage.

Figure 14) SANtricity System Manager home page.



Displaying the main menu allows the user to select one of the four main pages used in SANtricity System Manager: Storage, see Figure 15; Hardware, see Figure 16; Settings, see Figure 17; and Support, see Figure 18.

Figure 15) System Manager Storage options.



NetApp SANtricity System Manager

Home

Storage

Hardware

Settings

Support

Pools and volume groups

Volumes

Hosts

Performance

Snapshots

Operations in progress

Figure 16) System Manager Hardware options.

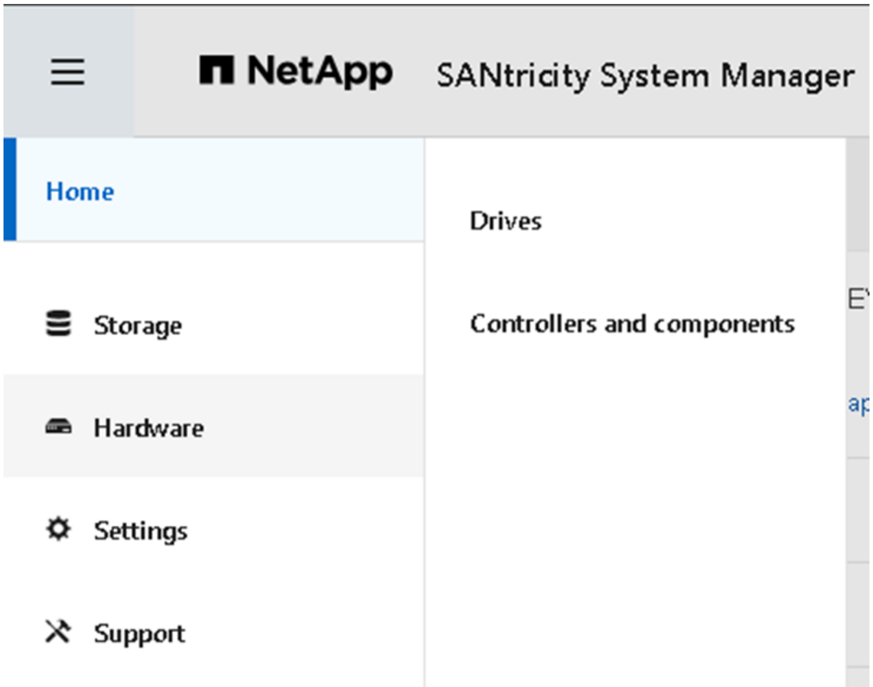
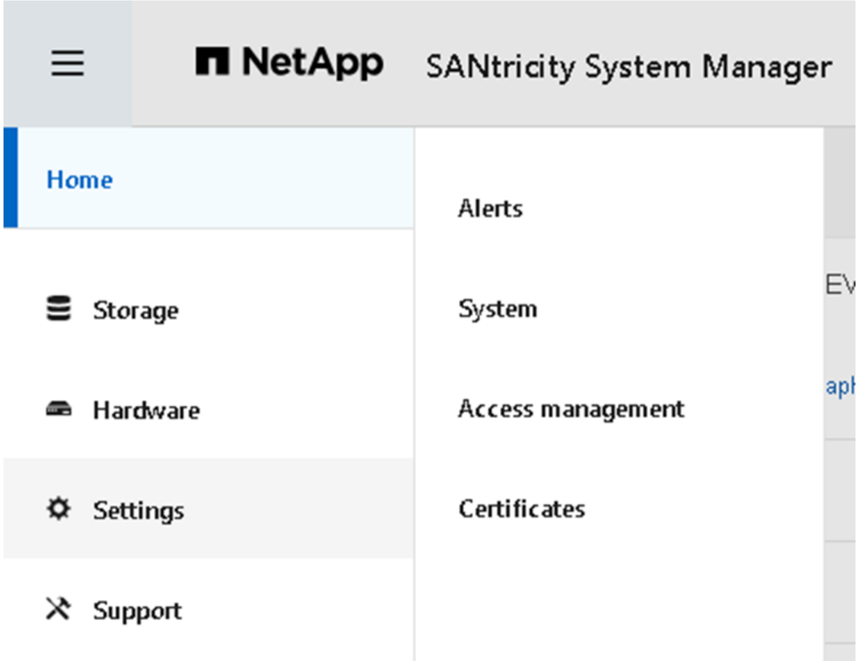


Figure 17) System Manager Settings options.



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

Figure 18) System Manager Support page with new "Script editor" option.

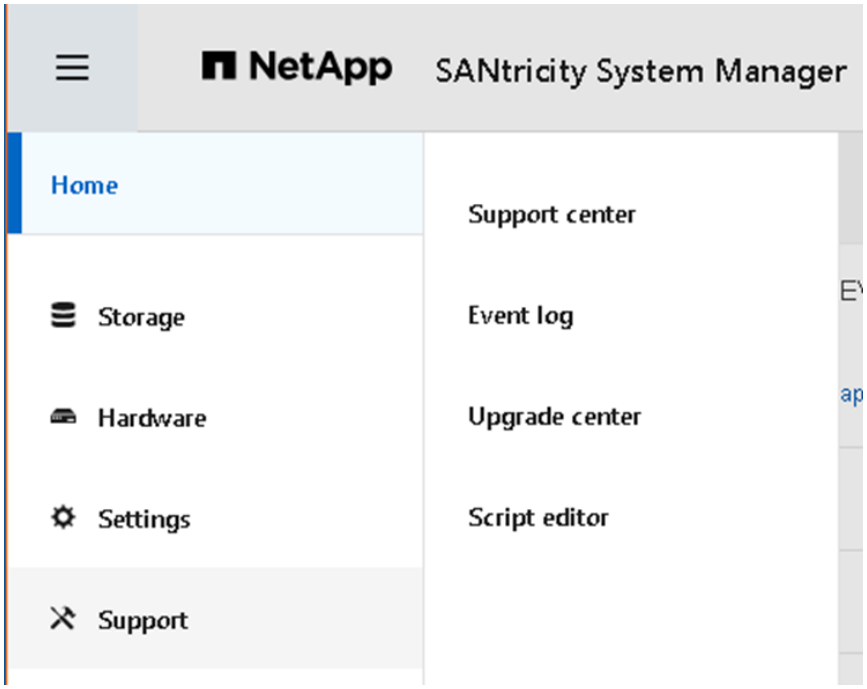
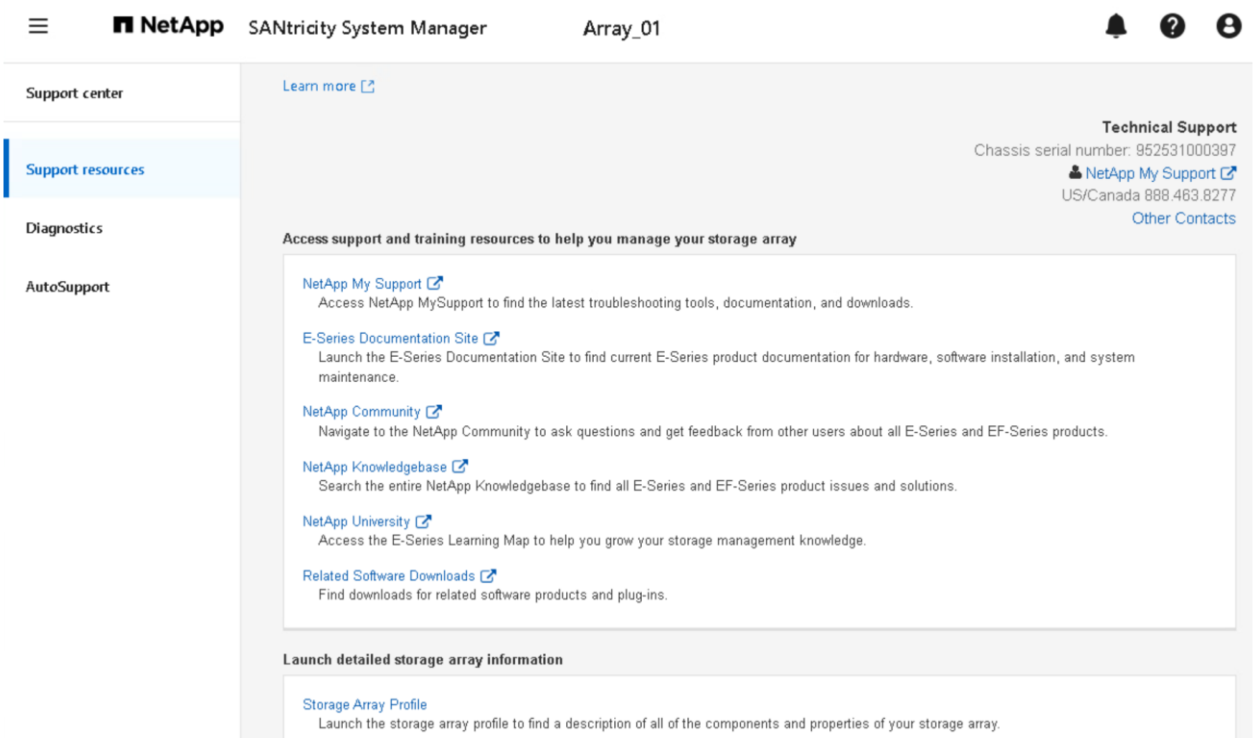


Figure 19 displays the Support Center, which you can reach by selecting Support Center from the Support main menu option. When Support Center is selected, Support resources is the first option selected from which support topics can be selected.

Figure 19) System Manager Support Center.



Technical Support
Chassis serial number: 952531000397
NetApp My Support
US/Canada 888.463.8277
Other Contacts

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

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

E-Series Documentation Site
Launch the E-Series Documentation Site to find current E-Series product documentation for hardware, software installation, and system maintenance.

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

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

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

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

Launch detailed storage array information

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

SANtricity System Manager security

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

- Support for directory services through 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 trusted certificates are installed on the host. Syntax and invocation are similar, but new security related parameters must be supplied to make a connection to the storage array.
- Security enhancements that extend to the onboard web services API, where user account passwords are now required.

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. The directory service is used by many devices in a network infrastructure to identify and authenticate users seeking access to devices in the network.

RBAC is software on the E-Series array that defines standard user levels, each with a well-defined set of access permissions. A user is authenticated as a member of a group, and specific permissions are set on the array side to define the type of access that user or group is allowed. This approach enables SANtricity to provide the granularity of access that customers require.

The permission level with each role is defined in Table 1.

Table 1) Built-in roles and associated permissions.

Role name (Log in as)	Access permissions
Root Admin (admin)	This role allows you to change the passwords of any local users and execute any command supported by the array. The admin password is set at initial login or any time after.
Security Admin (security)	This role allows you to modify security configuration settings on the array. It allows you to view audit logs; configure secure syslog server, LDAP, or LDAP over SSL (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, event log/audit log, and controller firmware (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 will not be able 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 as follows:

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

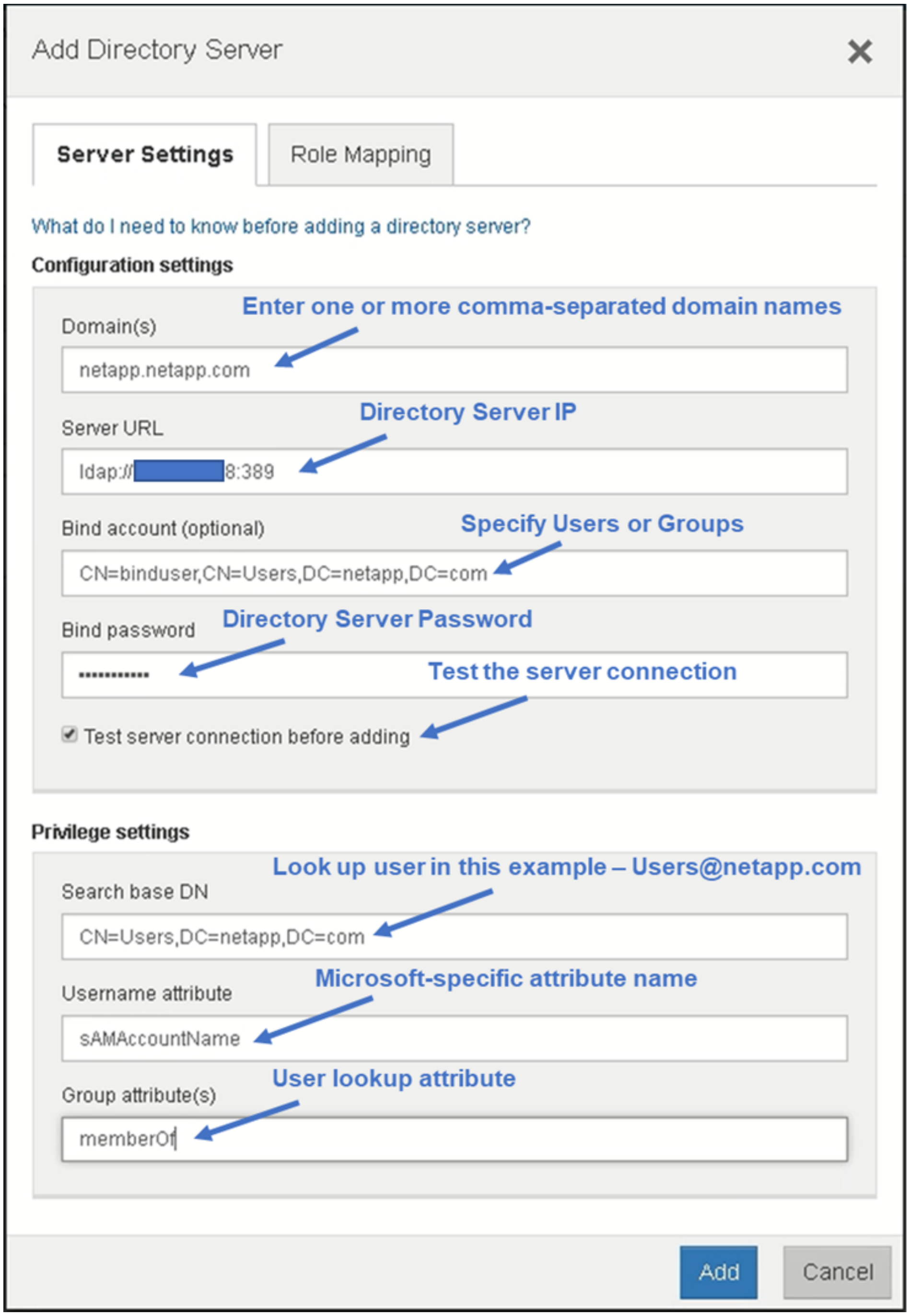
E-Series systems follow a standard web server implementation on the controllers, and information about the general directory services setup is available on the web. As a result, setting up the service on E-Series systems only requires some fields, which are listed in Table 2.

Table 2) LDAP/RBAC required fields and definitions.

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

Figure 20 shows an example Active Directory server integration with SANtricity System Manager. The entries are all examples except for username attributes and group attributes in the privileges section. Those items are standard entries for Windows and are not likely to change for most implementations.

Figure 20) SANtricity System Manager directory server setup wizard.



Add Directory Server ✕

Server Settings | Role Mapping

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

Configuration settings

Enter one or more comma-separated domain names

Domain(s): netapp.netapp.com

Directory Server IP

Server URL: ldap://[redacted]8:389

Specify Users or Groups

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

Directory Server Password

Bind password: •••••••••••

Test the server connection

☑ Test server connection before adding

Privilege settings

Look up user in this example – Users@netapp.com

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

Microsoft-specific attribute name

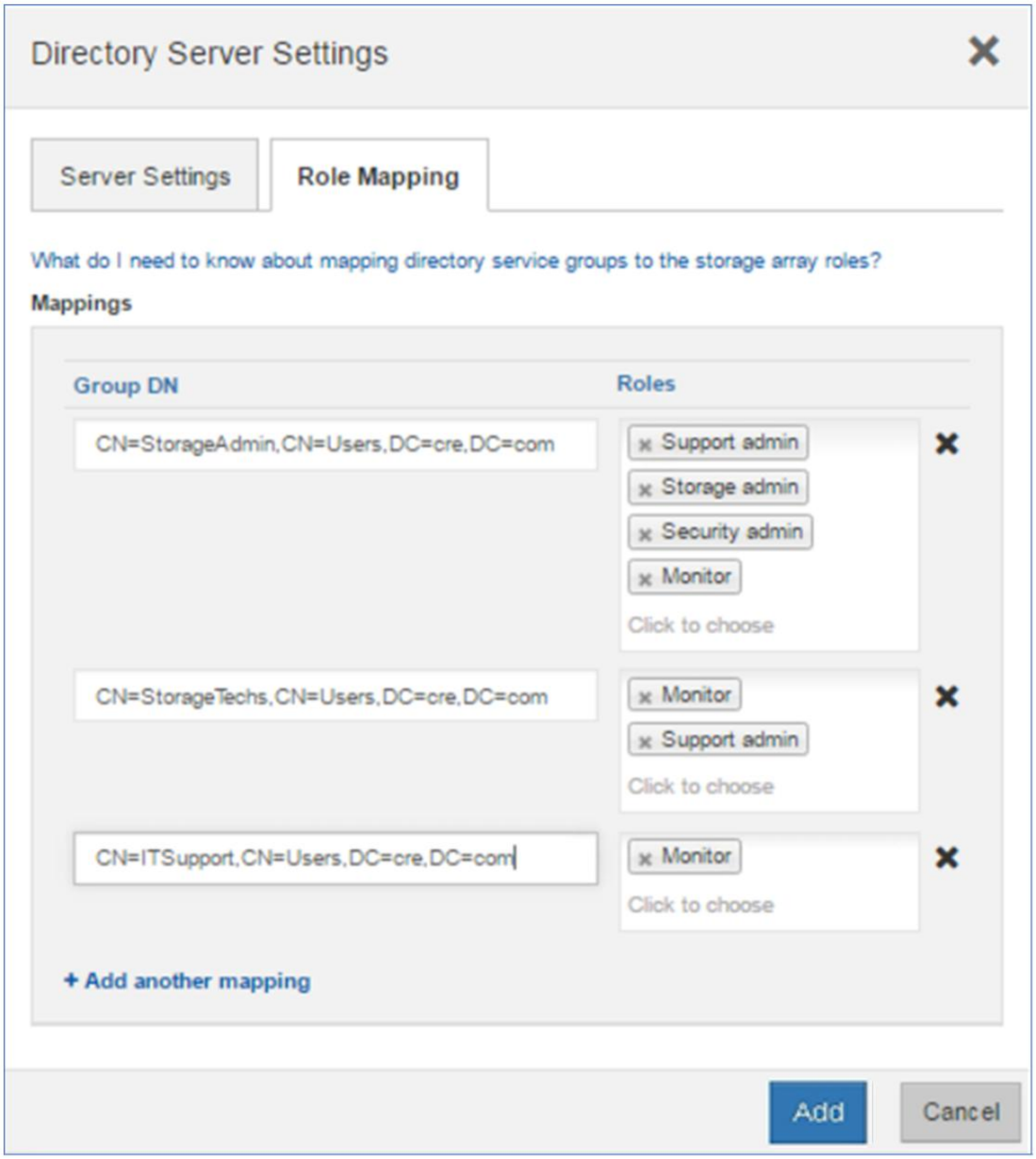
Username attribute: sAMAccountName

User lookup attribute

Group attribute(s): memberOf

The array roles for the specified user groups are set in the Role Mapping tab. As shown in Figure 21, users who are members of the StorageAdmin, StorageTechs, and ITSupport groups are authenticated as branches of the Users group `@cre.com`. When users in one of those groups log in to the array, they are allowed access to certain views and functions in the management interface according to the permissions granted.

Figure 21) Role Mapping tab in the directory server settings wizard.



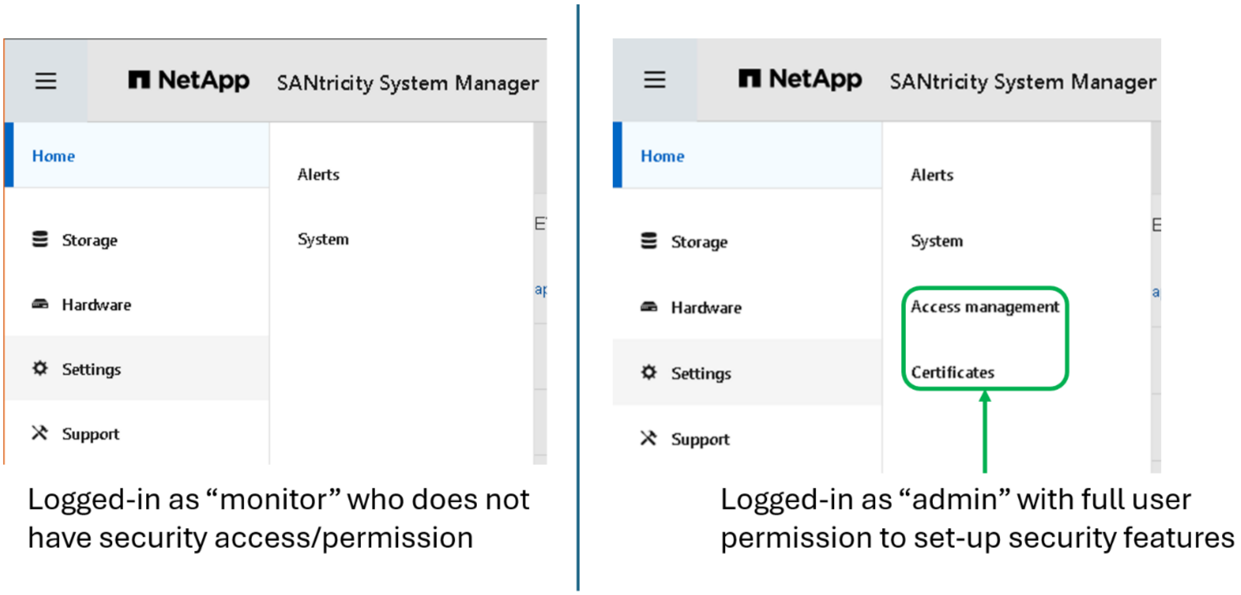
Directory Server Settings
Server Settings
Role Mapping
What do I need to know about mapping directory service groups to the storage array roles?
Mappings
Click to choose
+ Add another mapping
Add
Cancel

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

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

Multiple groups can be defined and mapped to specific roles that meet individual business requirements. Figure 22 shows the difference in user views and access to features according to access permission level. The login on the left provides monitor and support access, but it does not provide security access like the admin login on the right.

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



Logged-in as "monitor" who does not have security access/permission

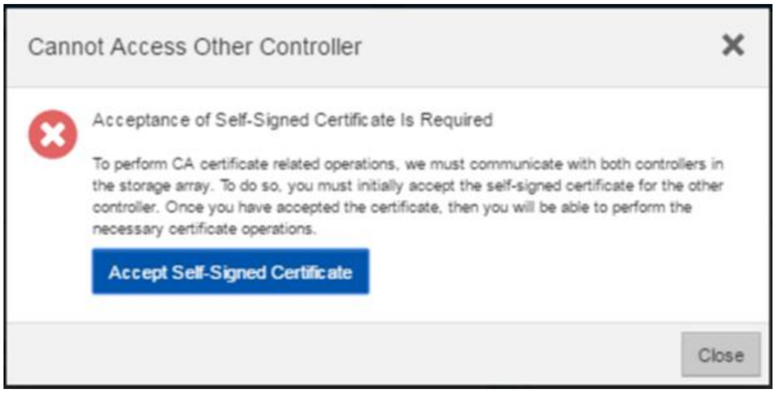
Logged-in as "admin" with full user permission to set-up security features

SANtricity web server security certificates

In addition to authentication and access control, SANtricity System Manager supports standard CA certificates. This support enables secure communications (SSL/TLS) between browser clients and the E-Series built-in web servers on the controllers. On EF50 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.

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 option. Figure 23 shows the dialog box that is displayed the first time the option is opened.

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



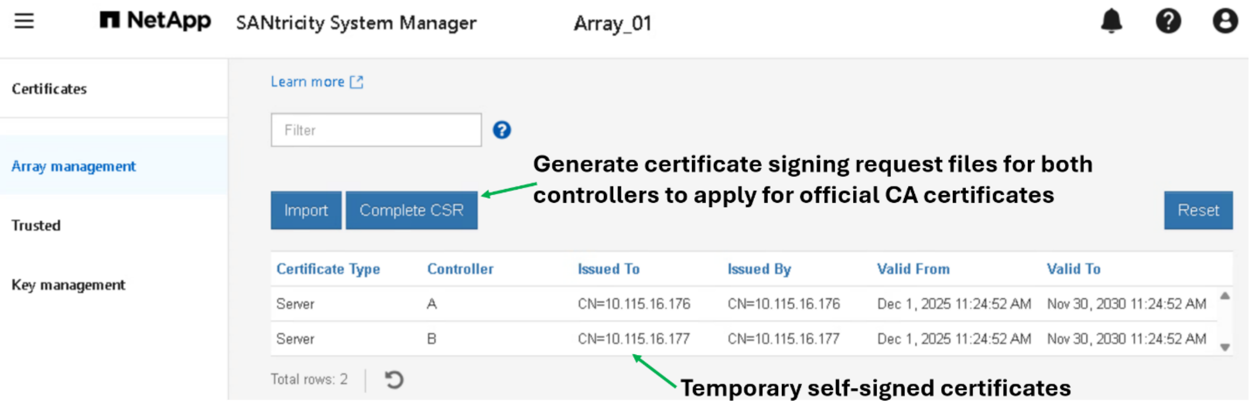
Cannot Access Other Controller

Acceptance of Self-Signed Certificate Is Required

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

You must accept the self-signed certificate to continue setting up certificates. The process takes you to another webpage, where the certificate is created in the background. Follow the prompts to complete the process. When the process is complete, the array requires the admin user or a user with security permissions to log in again. Both controllers are then displayed with valid local host certificates, as shown in Figure 24.

Figure 24) Selected SANtricity System Manager Certificates option.



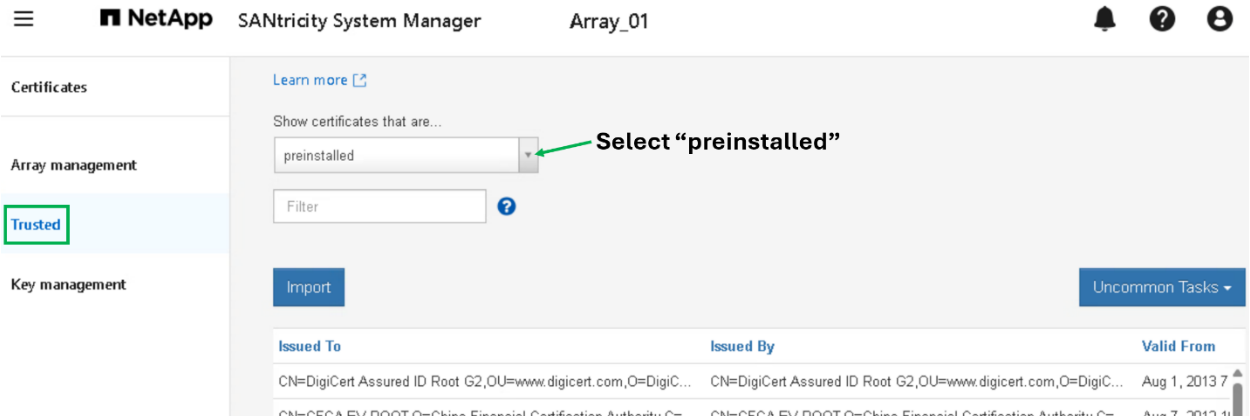
Generate certificate signing request files for both controllers to apply for official CA certificates

Certificate Type	Controller	Issued To	Issued By	Valid From	Valid To
Server	A	CN=10.115.16.176	CN=10.115.16.176	Dec 1, 2025 11:24:52 AM	Nov 30, 2030 11:24:52 AM
Server	B	CN=10.115.16.177	CN=10.115.16.177	Dec 1, 2025 11:24:52 AM	Nov 30, 2030 11:24:52 AM

Temporary self-signed certificates

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 that fully support TLS 1.2 and 1.3. For more information on TLS support see TR-4855 Security hardening guide for NetApp SANtricity. To view the standard root certificates, select the Trusted menu option in the Certificates window and then select ”preinstalled” from the drop-down menu, as shown in Figure 25.

Figure 25) View preinstalled certificates.



Show certificates that are... preinstalled

Select “preinstalled”

Issued To	Issued By	Valid From
CN=DigiCert Assured ID Root G2,OU=www.digicert.com,O=DigiC...	CN=DigiCert Assured ID Root G2,OU=www.digicert.com,O=DigiC...	Aug 1, 2013 7
CN=CFCA EV ROOT,O=China Financial Certification Authority,C=...	CN=CFCA EV ROOT,O=China Financial Certification Authority,C=...	Aug 7, 2012 1(

Multifactor authentication

Feature overview

Multifactor authentication (MFA) includes several functional areas on EF50 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 for a download to succeed. If you attempt to download unsigned firmware during the controller upgrade process, an error is displayed, and the download is aborted.

- **Certificate revocation checking by using Online Certificate Status Protocol (OCSP).** Certificate management includes certificate revocation checking through an OCSP server. The OCSP server determines whether the 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, 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 one or more syslog servers to archive audit logs. After configuration, all new audit logs are sent to the syslog server; however, previous logs are not transferred. Configuration tasks are available from Settings > Access Management and require security admin permissions.

How MFA works

MFA is provided through the industry standard SAML protocol. SAML does not directly provide the MFA functionality; instead, it allows the web service to send a request to an external system known as the Identity Provider (IdP). The IdP 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, the IdP provides all authentication activity. The IdP can be configured to require any amount and types of user authentication factors.

SAML identifies two distinct entities that cooperate to provide authentication of users:

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

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

Note: When SAML is enabled, SANtricity System Manager is the only management access point. There is therefore no access through the SANtricity CLI, the SANtricity Web Services REST API.

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.

SANtricity storage features

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

Drive encryption

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

SANtricity host and path management features

When considering the elements of E-Series multipath functionality, you must understand two concepts. The first is controller-to-volume ownership and how path failover between controllers is managed through asymmetrical logical unit access (ALUA) for SCSI hosts or asymmetric namespace access (ANA) for NVMe-oF hosts. 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 for SCSI hosts, or ANA for NVMe-oF hosts) to spread I/O across the interfaces and maximize performance. For steps on configuring NVMe specific multipath settings, see the Linux Express Guide or VMWare Express Guide, depending on which operating system is being used.

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 with the following characteristics:

- Volume ownership alternates as volumes are provisioned.
- Write I/O is by default 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 volumes and continues to process I/O.

These attributes allow host multipath drivers to spread I/O across each controller's ports that are associated with the volumes owned by that controller. 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 to the controller that owns the volumes. In parallel, a volume-ownership 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 volume I/O.

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

Table 3) SANtricity host types and associated failover behavior.

Host type	ALUA/AVT status	Implicit failover	Implicit failback	Automatic load balance
Linux DM-Multipath (kernel 3.10 or later)*	Enabled	Supported	Supported	Supported
VMware	Enabled	Supported	Supported	Supported
Windows	Enabled	Supported	Supported	Supported
Windows cluster	Enabled	Supported	Supported	Supported
ATTO cluster (all operating systems)	Enabled	Supported	Not supported	Not supported
*For NVMe-oF host protocols ANA is used for MPIO				

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

SANtricity reliability features

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

Table 4) SANtricity features for long-term reliability.

Reliability features with SANtricity
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, 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. You can perform these tasks by using global hot spare drives for standard RAID and spare pool capacity for 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. **Note:** Parallel drive firmware upgrades are supported offline to upgrade multiple drives more quickly during a maintenance window.
Automatic load balancing. This feature provides automated I/O workload balancing and confirms that incoming I/O traffic from hosts is dynamically managed and balanced across both controllers. The workload of each controller is continually monitored and analyzed in the background. When I/O on one controller significantly exceeds the I/O on the other controller for a prolonged, predictable period, SANtricity can change volume 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 EF50 controller, SNMP is supported natively. The embedded SNMP agent complies with RFC 1213 (MIB-II) and the SNMP V2C and V3 standards, but only one version of SNMP can

be used at a time. 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 Storage Manager 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 storage management features

E-Series EF50 systems ship with significant storage management features that can be activated from SANtricity System Manager. Table 5 lists standard features included with SANtricity OS.

Table 5) Standard features that are included with SANtricity.

Standard features with SANtricity
SANtricity System Manager (embedded single-array management). The browser-based, on-box SANtricity System Manager is used to manage individual new-generation storage arrays. • Access all array setup, storage provisioning, and array monitoring features from one UI. • System Manager includes an embedded RESTful API that can be used for management.
Volume workload tags. SANtricity System Manager provides a built-in volume tagging feature that allows administrators to organize the volumes in their arrays by workload type. The tag is only for organization purposes.
Storage partitions. Partitions can consist of an individual host without shared volumes, host groups with shared volumes, or a combination of both, with each applied to different volumes. This concept has been abstracted in the new System Manager, but you can view the partitions by using a CLI.
Changing host protocol. This capability is supported by accessing System Manager -> Settings -> System, then click on “Change Host I/O Protocol” under Additional Settings section.

DDP changes with high-density NVMe SSDs

In SANtricity 12 OS and for the new EF50 array there are some changes on how DDP works when using the high-density 30TB/60TB drives.

Mixing of 30TB/60TB drives with either 3.8TB, 7.6TB or 15.3TB drives in the same array is not supported.

If an array is populated with 30TB/60TB drives, a single pool using all available drives will be created automatically at boot-up, no legacy RAID options available. If 20 or more drives are in a pool, then the system will use 16+2 stripes instead of the traditional 8+2 stripes to lower RAID 6 parity overhead (11.1% vs. 20%).

If needed, two smaller pools of 12 drives each can be created. The default pool can be deleted using either System Manager, SMcli or REST api, but only SMcli or REST api can be used to create the two smaller pools. Creating a pool in System Manager will only allow one pool using all available drives to be created.

The 30TB/60TB drives have lower write bandwidth so don’t assume same write throughput using 30TB/60TB drives that can be achieved using the lower capacity NVMe SSDs.

SANtricity copy services features

Table 6 lists standard copy services features with EF50 storage arrays.

Table 6) SANtricity copy services features.

Copy services features with SANtricity
SANtricity Snapshot copies. Point-in-time NetApp Snapshot™ copies.
Volume copy. Used to clone volumes for testing/development or analytics purposes.

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

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

Note: EF50 does not support asynchronous mirroring or synchronous mirroring. It is recommended to use replication (mirroring) and erasure coding features available in modern applications

Note: EF50 does not support remote storage volumes (RSVs).

SANtricity management integration

Table 7 shows the SANtricity APIs and toolkits that can be used for scripting and custom integration into other management tools and appliance architectures. To download the latest version of the E-Series SANtricity Web Services (REST API) visit 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).

Table 7) SANtricity APIs and toolkits.

APIs and toolkits	Description
SANtricity Web Services Proxy **Note:** You can use either the proxy or the embedded REST API for new-generation 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.
SANtricity Secure CLI	SANtricity Secure CLI (SMcli) can be downloaded from System Manager. New for SANtricity 12.00 is built-in script editor in System Manager.

Table 8 provides a list of third platform plug-ins that use E-Series storage systems as building blocks. Usually, the listed plug-ins 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 8) Third platform plug-ins that use the SANtricity Web Services Proxy.

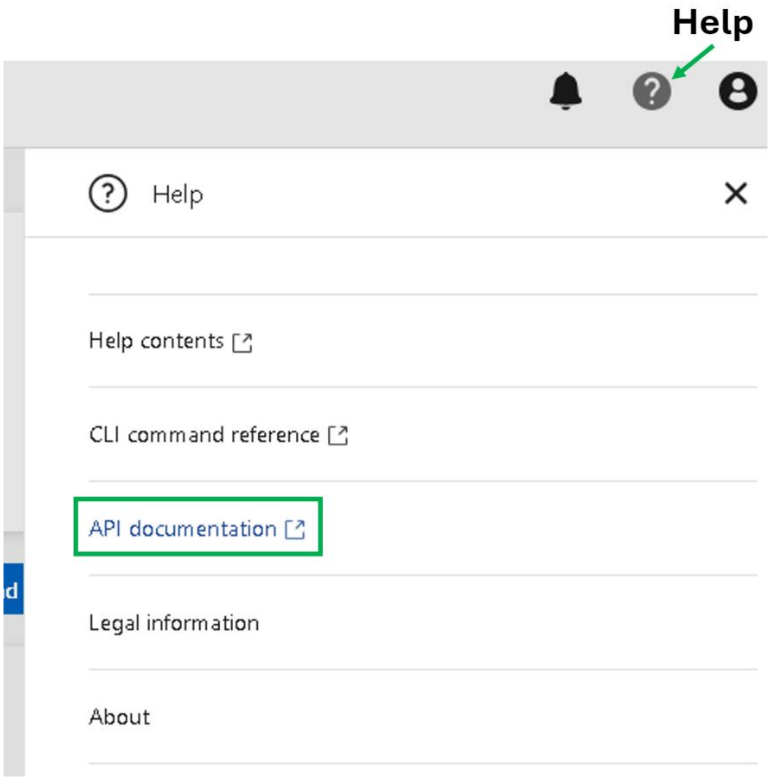
Software package	Use
NetApp SANtricity Performance App for Splunk Enterprise https://splunkbase.splunk.com/app/1932/ Technology Add-On for NetApp SANtricity https://splunkbase.splunk.com/app/1933/	A display and monitor tool to report configuration and performance details of multiple E-Series systems 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.

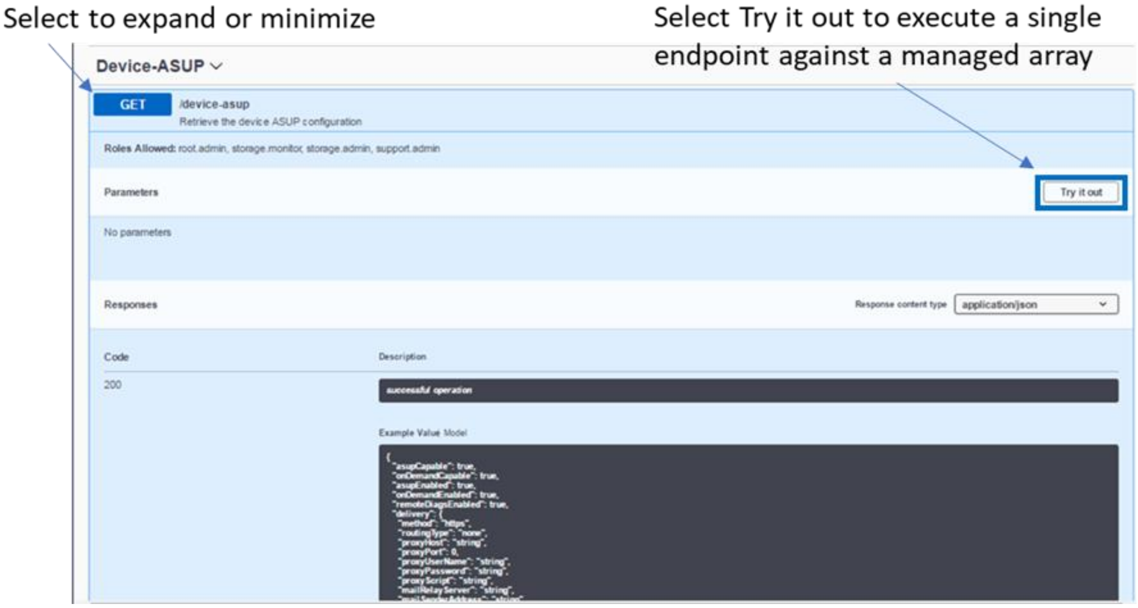
Figure 26) Opening the API documentation.



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 of 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
Retrieve the device ASUP configuration

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

Parameters

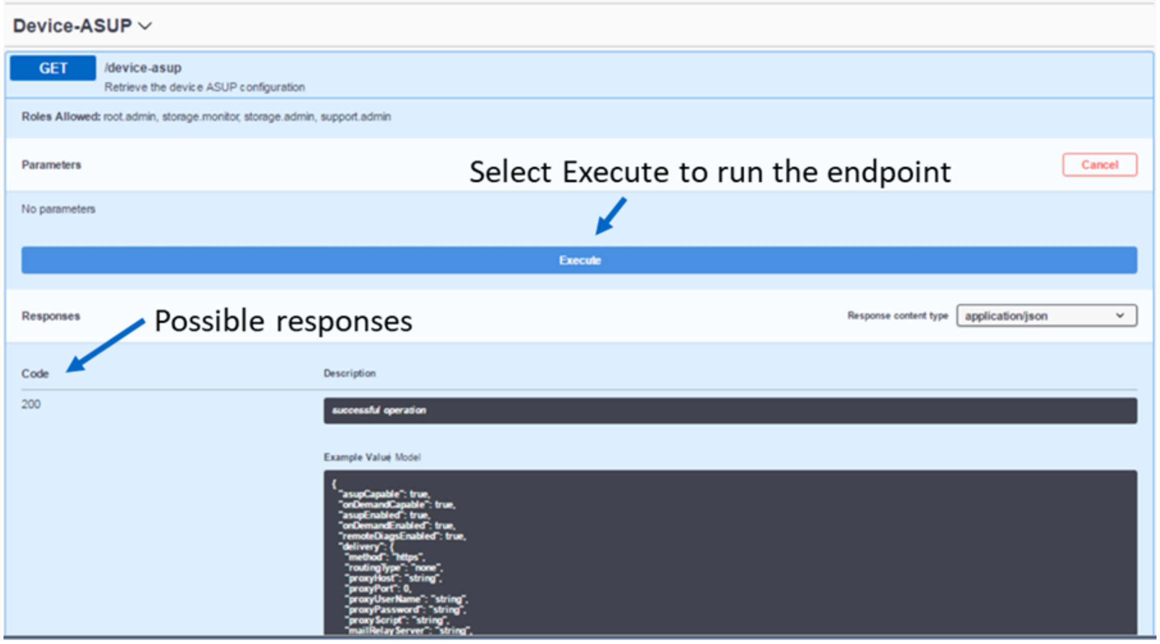
No parameters

Responses

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",
    "mailSenderAddress": "string",
```

Figure 28) REST API documentation sample.



Select Execute to run the endpoint

Possible responses

/device-asup
Retrieve the device ASUP configuration

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

Parameters

No parameters

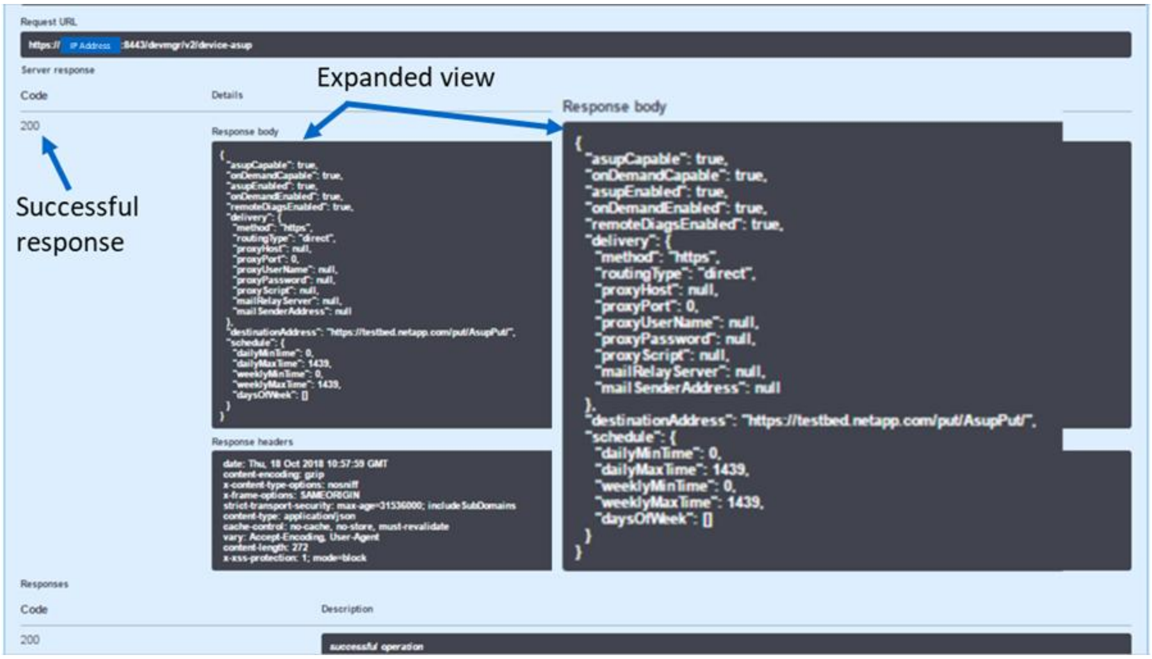
Responses

Code	Description
200	successful operation Example Value Model

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

The corresponding output for the GET device-asup verb is shown in Figure 29 and Figure 30.

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



Request URL

```
https:// IP Address :8443/devmgr/v2/device-asup
```

Server response

Code | Details

200

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

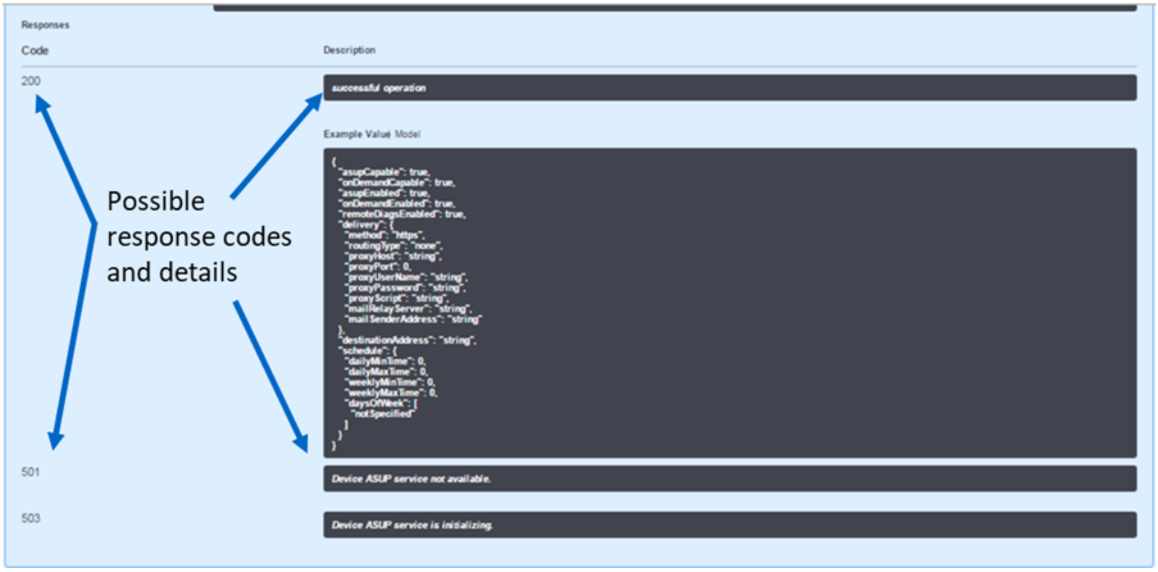
Response body

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

Responses

Code	Description
200	*successful operation*

Figure 30) Device-ASUP endpoint possible response codes and details.



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 simply 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 command line interface (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.

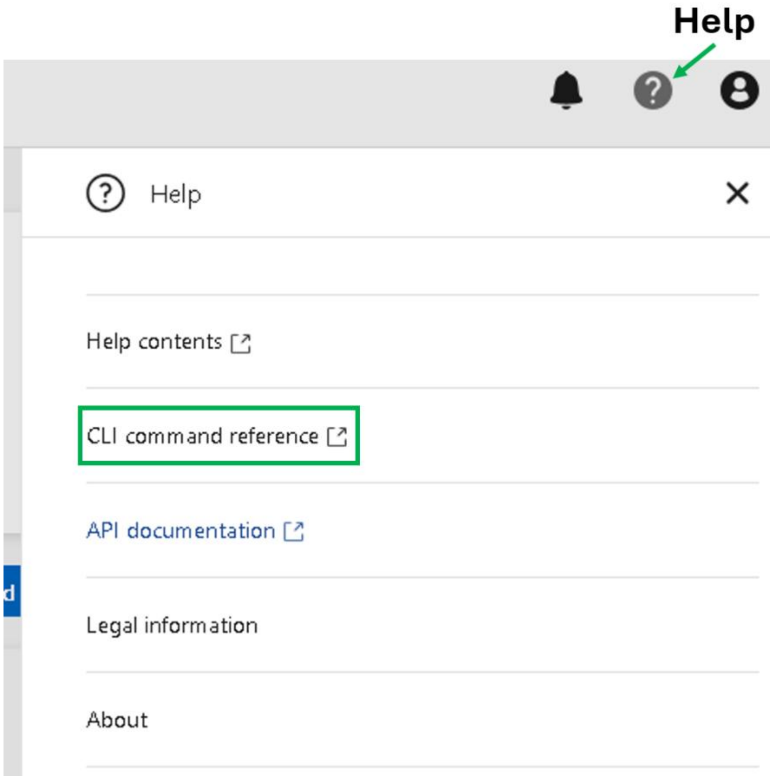
Downloading the CLI

- 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 Windows command prompt.

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

Figure 31) Opening the CLI Command Reference.



Script editor

New for SANtricity OS 12 is the Script editor that allows CLI scripts to be run from within System Manager.

To access Script editor, open System Manager, click on the three horizontal bars near upper left corner to access the options drop-down menu, click on Support then click on Script editor, as seen in Figure 32.

Figure 32) Opening the Script editor.

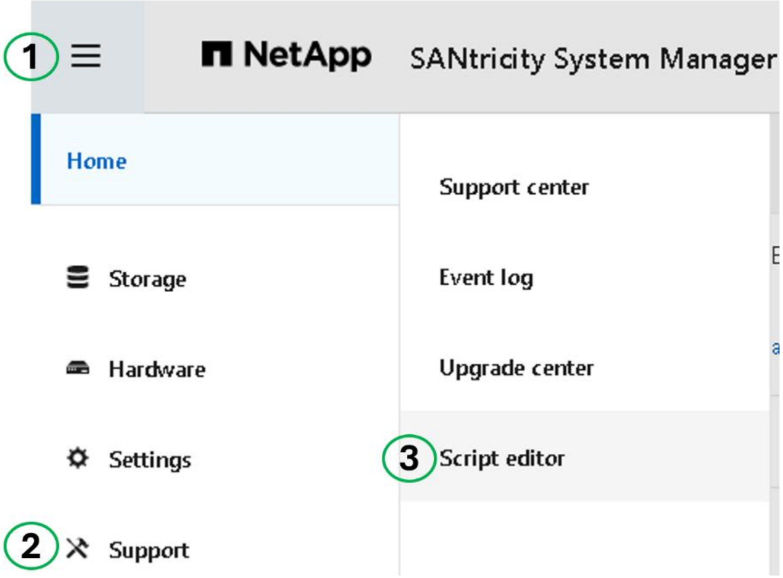
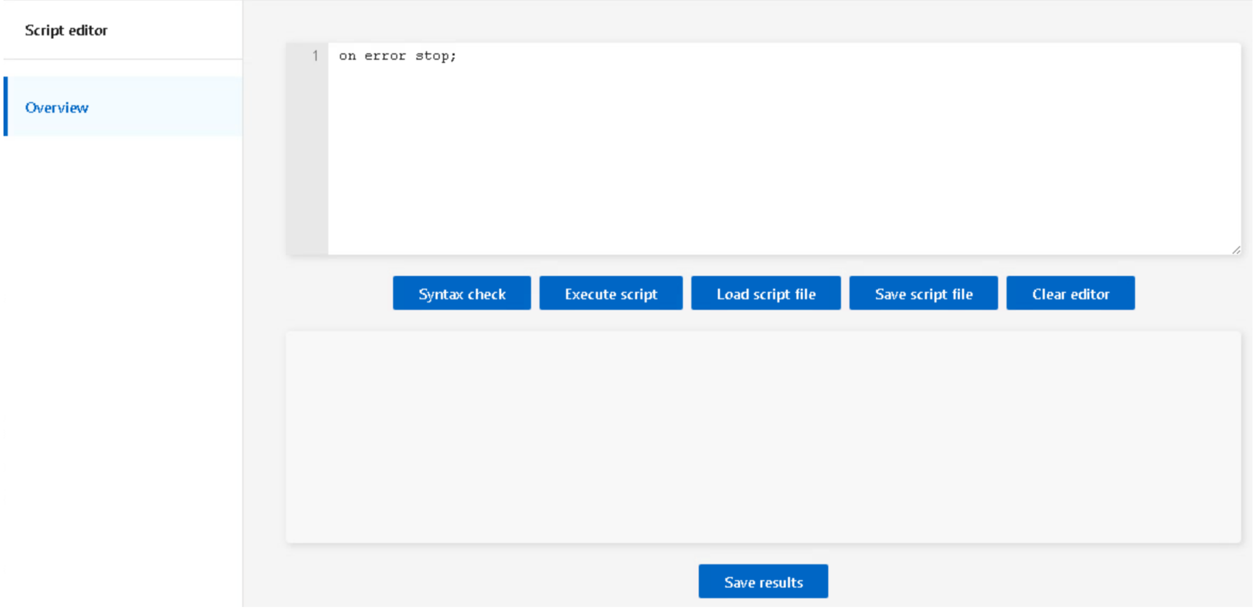


Figure 33 shows the Script editor start page.

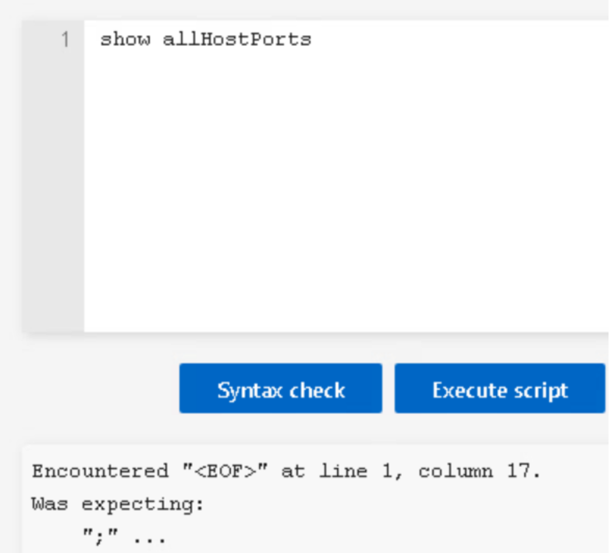
Figure 33) Script editor start page.



```
on error stop;
```

Multiple CLI commands can be entered in the top box, each command must end with a semicolon or a syntax error will be reported. To verify syntax prior to executing the script, click on Syntax check button, any errors will be reported in lower box, see Figure 34.

Figure 34) Script editor syntax check.

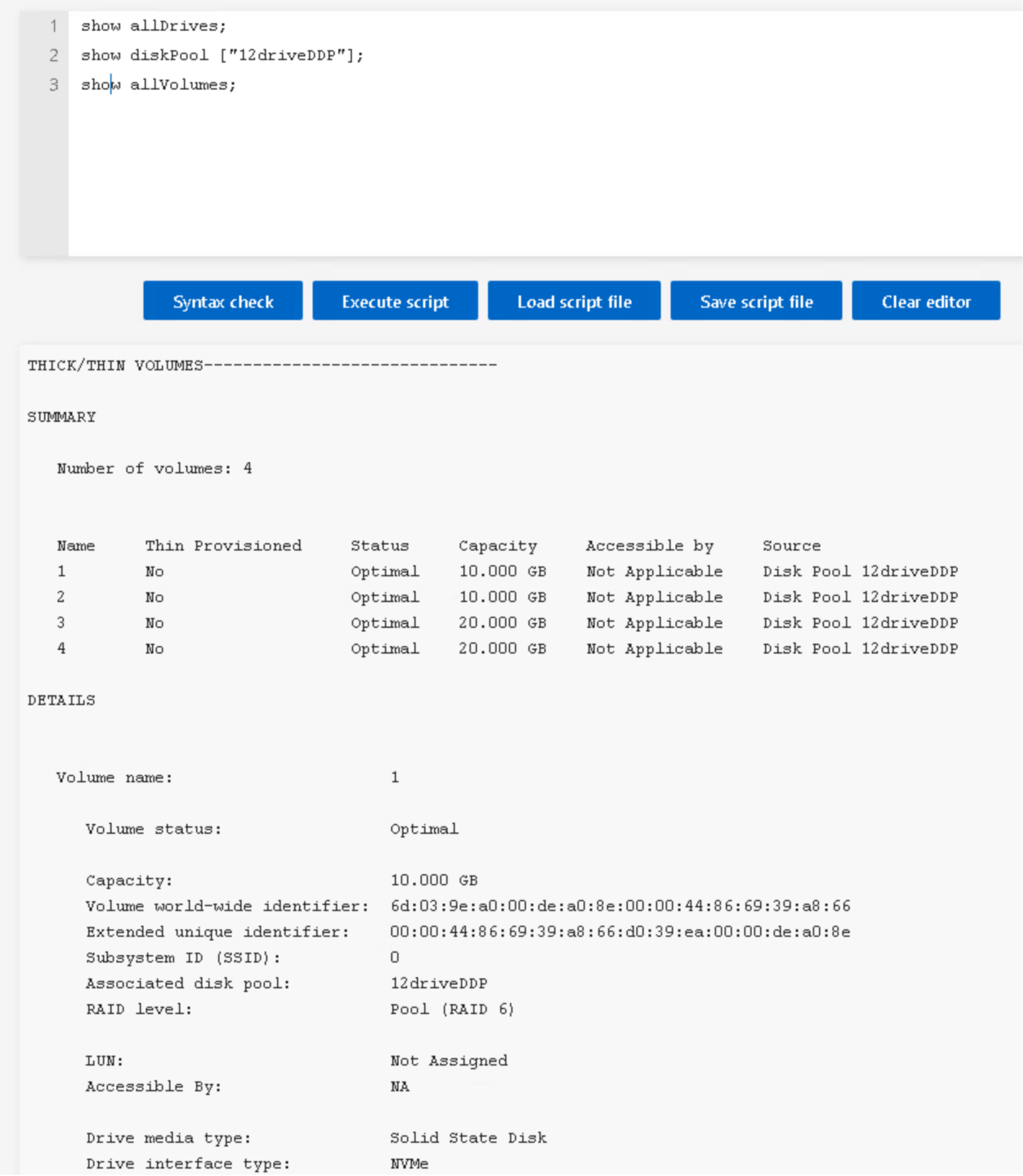


```
show allHostPorts
```

```
Encountered "<EOF>" at line 1, column 17.
Was expecting:
    ";" ...
```

To execute a script, click on Execute script button. First a syntax check will be performed, if any syntax errors are found the errors will be reported in the lower box and execution will fail. If no syntax errors are found the script will then execute automatically and the lower box will report the results, see Figure 35.

Figure 35) Script editor execution output.



```
show allDrives;
show diskPool ["12driveDDP"];
show allVolumes;
```

```
THICK/THIN VOLUMES------------------------------

SUMMARY

   Number of volumes: 4


   Name      Thin Provisioned     Status     Capacity     Accessible by      Source
   1         No                   Optimal    10.000 GB    Not Applicable     Disk Pool 12driveDDP
   2         No                   Optimal    10.000 GB    Not Applicable     Disk Pool 12driveDDP
   3         No                   Optimal    20.000 GB    Not Applicable     Disk Pool 12driveDDP
   4         No                   Optimal    20.000 GB    Not Applicable     Disk Pool 12driveDDP

DETAILS


   Volume name:                       1

      Volume status:                  Optimal

      Capacity:                       10.000 GB
      Volume world-wide identifier:   6d:03:9e:a0:00:de:a0:8e:00:00:44:86:69:39:a8:66
      Extended unique identifier:     00:00:44:86:69:39:a8:66:d0:39:ea:00:00:de:a0:8e
      Subsystem ID (SSID):            0
      Associated disk pool:           12driveDDP
      RAID level:                     Pool (RAID 6)

      LUN:                            Not Assigned
      Accessible By:                  NA

      Drive media type:               Solid State Disk
      Drive interface type:           NVMe
```

SANtricity Storage Plugin for vCenter

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

- View and manage discovered storage arrays in the network.
- Perform batch operations on groups of multiple storage arrays.
- Perform upgrades on the software operating system.
- Import settings from one storage array to another.

- Configure volumes, SSD cache, hosts, host clusters, pools, and volume groups.
- Launch the System Manager interface for additional management tasks on an array.

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

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

You can download the plugin from the NetApp Support site, NetApp Support Site - Downloads - All Downloads.

You can find installation and configuration documentation on the NetApp Documentation site, E-Series and SANtricity Documentation Center.

SANtricity software specifications for EF50 hardware

Table 9 lists the NetApp SANtricity software specifications for NetApp EF50-based storage systems.

Table 9) SANtricity software boundaries for EF50-based storage systems.

Components	Maximum
Storage hardware components	
Shelves (controller and expansion)	1
Max supported drives - drive slot count	24 NVMe SSDs
Logical Components	
Hosts per partition	512
Volumes per partition	256
Volumes per system	1,024
Disk pools per system	20 (test limit)
Volumes per disk pool	1,024
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)	12PiB maximum DDP capacity per EF50 array
Maximum DDP single volume capacity	4PiB
Maximum disks per volume group	• 24 (NVMe SSDs) for RAID 0 and RAID 1 • 24 (NVMe SSDs) all other RAID levels
Maximum single volume capacity for standard RAID	4PiB
Maximum standard RAID volumes per volume group	256
Consistency groups	
Volumes per consistency groups	64
Consistency groups per system	32
Snapshot copies	
Per Snapshot group	32
Per volume	128
Per storage system	1,024
Snapshot volumes	
Per Snapshot copy	4

Per system	512
Snapshot groups	
Per volume	4
Per system	512

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

Note: EF50 does not support remote storage volumes (RSVs).

Note: EF50 does not support thin provisioning.

Note: EF50 does not support asynchronous or synchronous mirroring. It is recommended to use replication (mirroring) and erasure coding features available in modern applications.

EF50 hardware configurations

NetApp EF50 storage systems, like all NetApp E-Series arrays, use a modular approach to hardware configuration. This approach can meet most customer SAN storage requirements for flexible host interfaces and versatile drive choices without sacrificing supportability, ease of implementation, and long-term stability. The E-Series has a proven record of accomplishment for reliability and scalability to satisfy requirements in remote dedicated environments or primary data centers that provide mission-critical infrastructure.

Controller shelf configurations

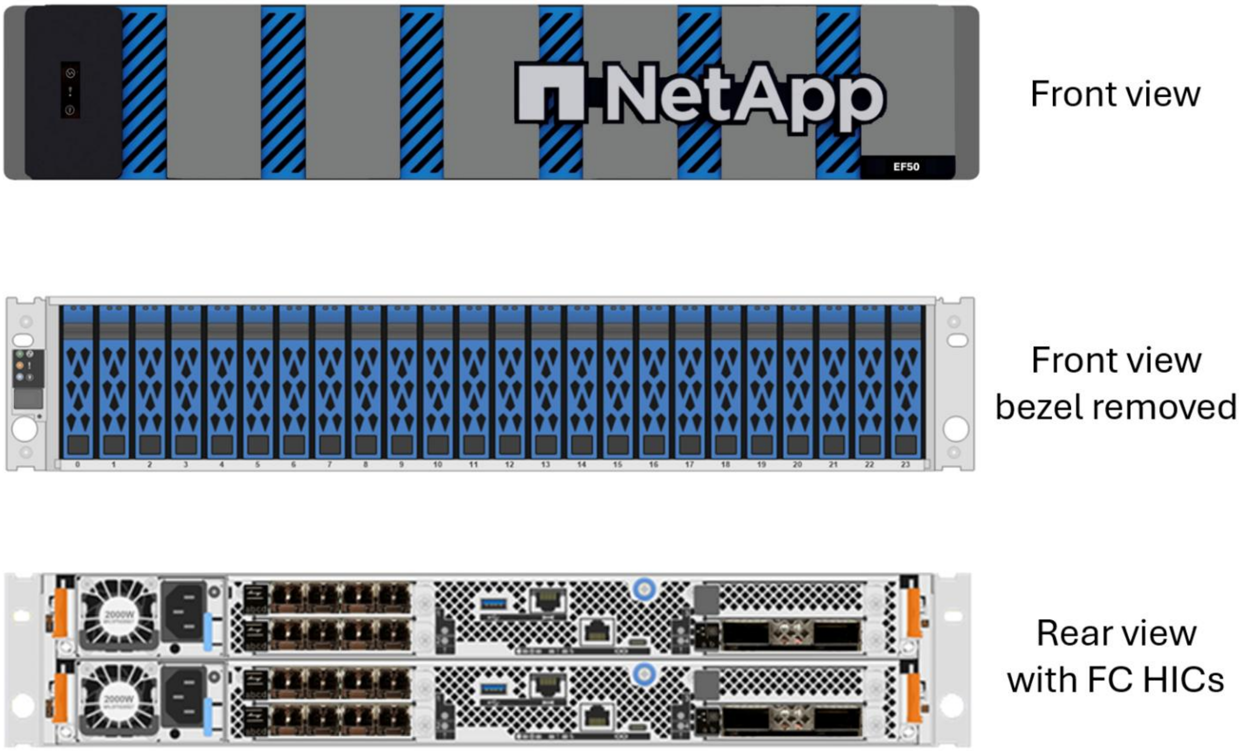
The following sections provide detailed information about the EF50 shelf configuration.

EF50 controller shelf

The EF50 controllers are paired with the NE224 shelf. It is a two-rack-unit-high (2U) shelf that holds up to twenty-four 2.5" NVMe SSDs. It features two RAID controllers and two ENERGY STAR Titanium certified high-efficiency power supplies (2000W) with integrated fans.

Figure 36 shows the front and rear views of the EF50 controller shelf. In the example, the EF50 controllers each have two 4-port 64Gb FC HICs installed in slots 1 and 2 and one RoCE inter-controller mirroring card in slot 4.

Figure 36) EF50 front and rear views.



The EF50 controller has the following base hardware features:

- Ethernet port for management-related activities
- RJ-45 and USB-C ports for serial console connections
- Type-A USB port for factory use only and is disabled if SANtricity OS is running

Table 10 lists the technical specifications for the EF50-based storage systems.

Table 10) EF50 technical specifications.

Specification	EF50
Maximum raw system capacity (assumes 24 NVMe SSDs)	1,473TB (24 x 61.4TB SSDs)
Maximum number of drives per system	24 NVMe SSDs
NE224 shelf form factor	2U, 24 drives
Memory	32GB per controller
	64GB per duplex system
• Either 1 or 2 HICs per controller (slots 1 – 2) • Controllers must match. • Cannot mix host protocols. • Use System Manager to convert between host protocols. See “Controller host interface features” for details.	• 64Gb FC HIC (from 4 up to 12 ports per controller) – supports traditional FC or NVMe/FC – all ports on array must be same protocol

Inter-controller mirroring card (required)	• Installed in HIC slot 4 of controller • 2-port 100Gb RoCE card
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 DDP **Note:** If 30TB or 60TB drives installed, default will be one DDP using all available drives with ability to delete DDP and create new DDPs. **Note:** It is only possible to create RAID 3 volumes through the CLI. For more information, see online documentation for Create volume group CLI command.
	Redundant, hot-swappable storage controllers, disks, and power supplies. Fans require that you remove the controller to do a replacement.
	Mirrored data cache with battery-backed destage to flash

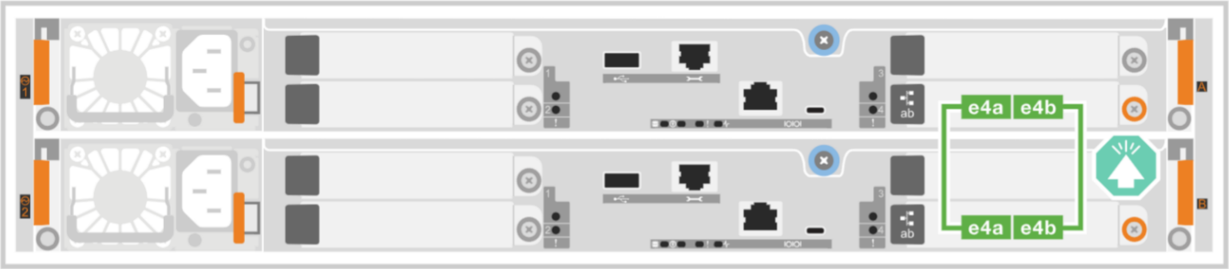
Note: For current supported drive availability information and encryption capability by drive capacity (full disk encryption [FDE] and FIPS), see the Hardware Universe.

Inter-controller mirroring card and cables

A unique feature of the new EF-Series arrays is the inclusion of the inter-controller mirroring card, which is required in each controller. The inter-controller mirroring card is used for RDMA mirroring between controllers. The EF50 supports a 100Gbps mirroring card that can provide approximately 14GBps write bandwidth.

Each port of the inter-controller mirroring card needs to be connected to the equivalent port of the alternate controller, see Figure 37.

Figure 37) Inter-controller mirroring card port connections.



It is important that the mirroring cables stay connected on a live system. If a controller needs to be removed for whatever reason, fail the controller prior to unplugging the mirroring cables.

Both cables shipped with a system will be a 200Gb rated 0.5-meter cable that will run at 100Gb RoCE.

Ethernet management

By default, the EF50 controller includes an Ethernet management port that provides out-of-band system management access.

Note: EF50 does not support in-band management.

The management port defaults to the Dynamic Host Configuration Protocol (DHCP). If you want to use static addresses to manage the EF50, simply leave the management ports disconnected for approximately 5 minutes after powering up, to allow the DHCP feature to time out. Then, you can connect with a local PC to the default IP addresses:

- Controller A Management port = 169.254.128.101
- Controller B Management port = 169.254.128.102

Controller host interface features

Table 11 lists the supported host protocol speeds for the FC HIC.

Table 11) Host interface protocol and supported speeds.

HIC Protocol	Supported speeds
64Gbps FC	64Gbps, 32Gbps, 16Gbps
64Gbps NVMe/FC	64Gbps, 32Gbps, 16Gbps

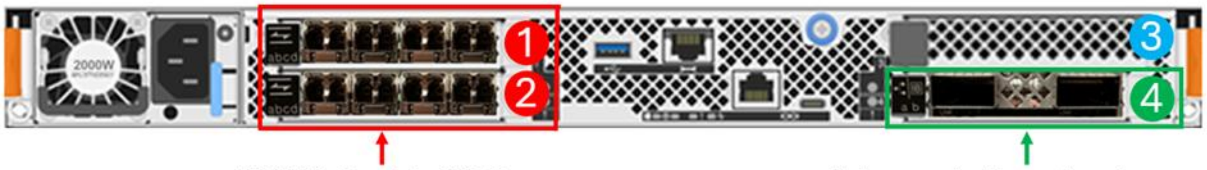
Note: 16Gbps SFPs are not supported, but 32Gbps or 64Gbps SFPs will auto-negotiate to 16Gbps speed.

Note: For optical connections, the appropriate SFPs must be ordered for the specific implementation. Consult the Hardware Universe for a full listing of available host interface equipment. All EF50 optical connections use the OM4 optical cable.

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

The HIC options are shown in Figure 38.

Figure 38) EF50 controller HIC options.



FC HICs in slots 1 & 2

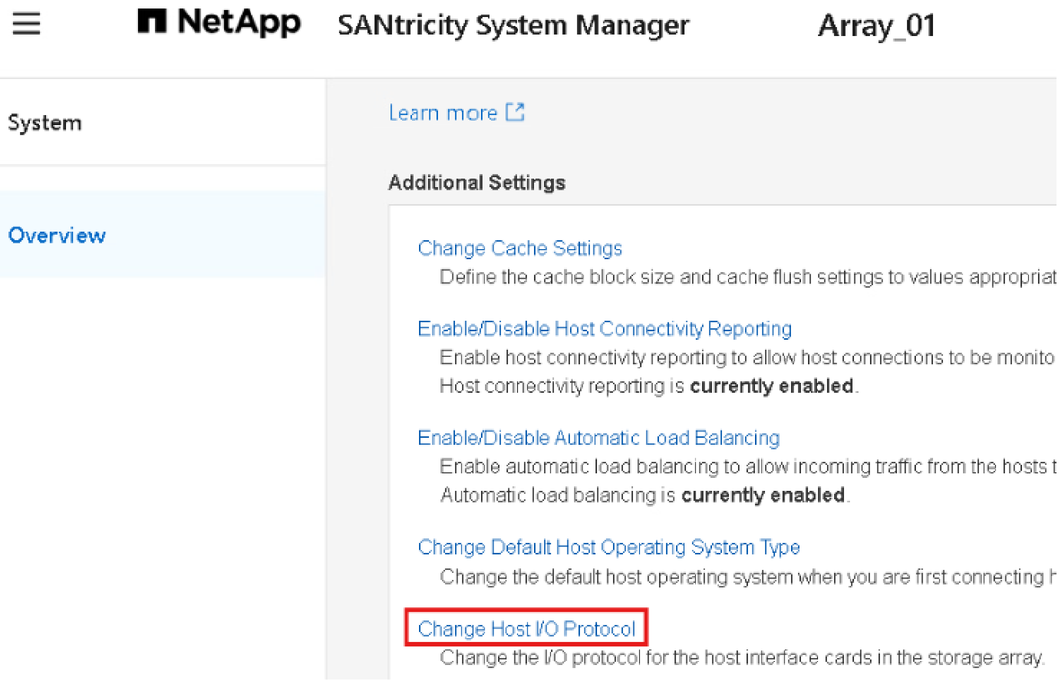
- 4-port 64Gb FC or NVMe/FC
- Minimum installed HIC is 1, maximum is 2
- HICs installed in order of HIC slot

Inter-controller mirroring card in slot 4 (required)

- 2-port 100Gb RoCE
- No host connectivity allowed

Another new feature in SANtricity 12.00 for EF50 is the ability to change HIC host protocols through System Manager. For HICs that support multiple host protocols, the current protocol can be changed by using the Change Host I/O Protocol feature on the System Manager, Settings, System screen under Additional Settings, see Figure 39.

Figure 39) Changing HIC protocol through System Manager.



NetApp SANtricity System Manager Array_01

System

Overview

Learn more

Additional Settings

Change Cache Settings
Define the cache block size and cache flush settings to values appropriat

Enable/Disable Host Connectivity Reporting
Enable host connectivity reporting to allow host connections to be monito
Host connectivity reporting is **currently enabled**.

Enable/Disable Automatic Load Balancing
Enable automatic load balancing to allow incoming traffic from the hosts t
Automatic load balancing is **currently enabled**.

Change Default Host Operating System Type
Change the default host operating system when you are first connecting h

Change Host I/O Protocol
Change the I/O protocol for the host interface cards in the storage array.

Drive loading for maximum performance

With the NE224 shelf, the order in which drives slots are populated has changed. When inserting fewer than 24 drives into an NE224 shelf, you must alternate between the two halves of the drive shelf. You must load drives evenly either from the middle drive slots (11,12) outward, Figure 40, or from the outside drive slots (0, 23) inward, Figure 41.

Figure 40) Loading drives from the inside drive slots outward.

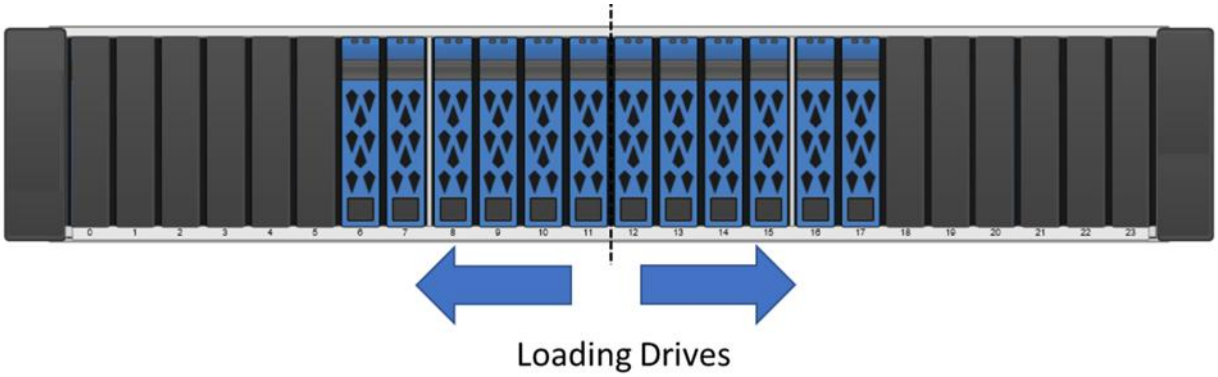
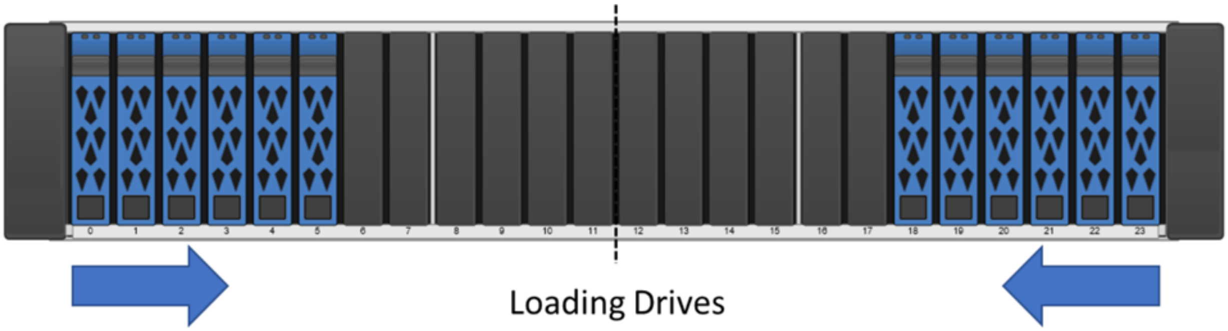


Figure 41) Loading drives from the outside drive slots inward.



When configuring the storage array, each controller should have access to an equal number of drives in the first 12 slots and from the last 12 slots to use both drive-side PCIe buses effectively. After you create a pool or volume group, create an even number of volumes split equally across the two controllers. Figure 42 shows an example of creating a pool from the middle drives. For DDP creation, NetApp recommends using all drives in the storage array.

Figure 42) Example DDP using 12 drives.

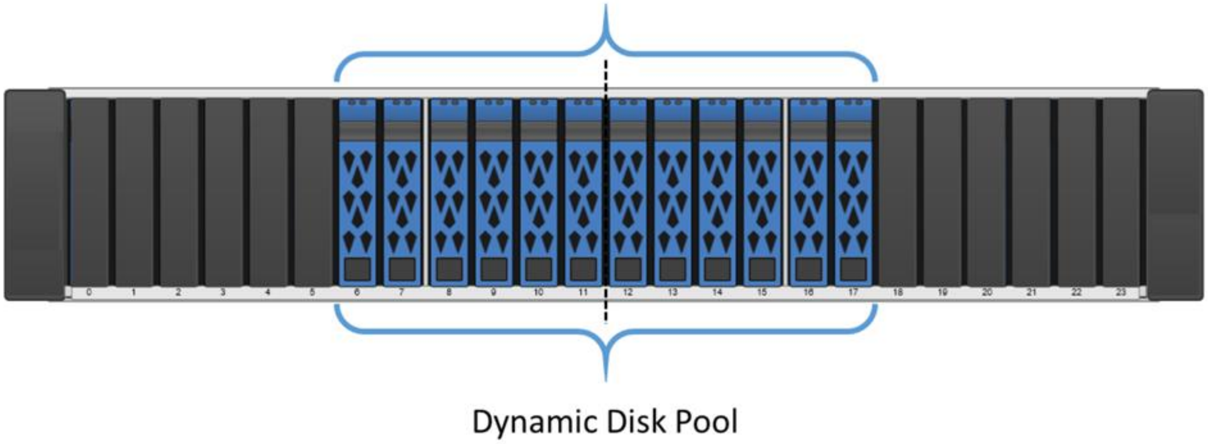
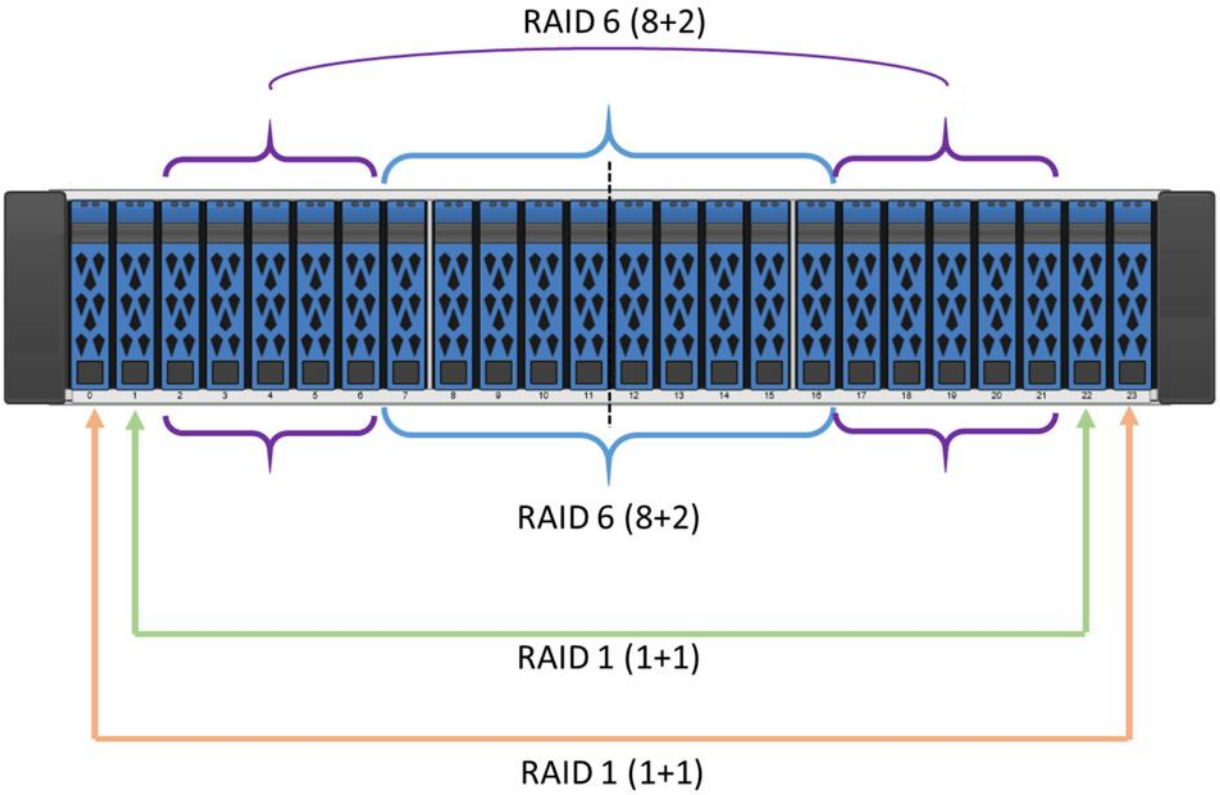


Figure 43 shows an example where RAID 6 volume groups are created from the middle drives, then from an outside set of drives, and finally two RAID 1 volume groups are built from the outside in. SANtricity currently allows drive selection under the Manually select drives (advanced) feature when creating a volume group.

Figure 43) Example of using all 24 drives in a configuration.



Hardware LED definitions

EF50 controller shelf LEDs

The EF50 controller shelf has LED status indicators on the front of the shelf, the operator display panel (ODP), the rear of the shelf, the power supply, and the controller canisters. The LEDs on the ODP indicate systemwide conditions, and the LEDs on the power-fan canisters and controller canisters indicate the status of the individual units.

Figure 44 shows the ODP of the EF50 controller shelf.

Figure 44) ODP on front panel of EF50 controller shelf.

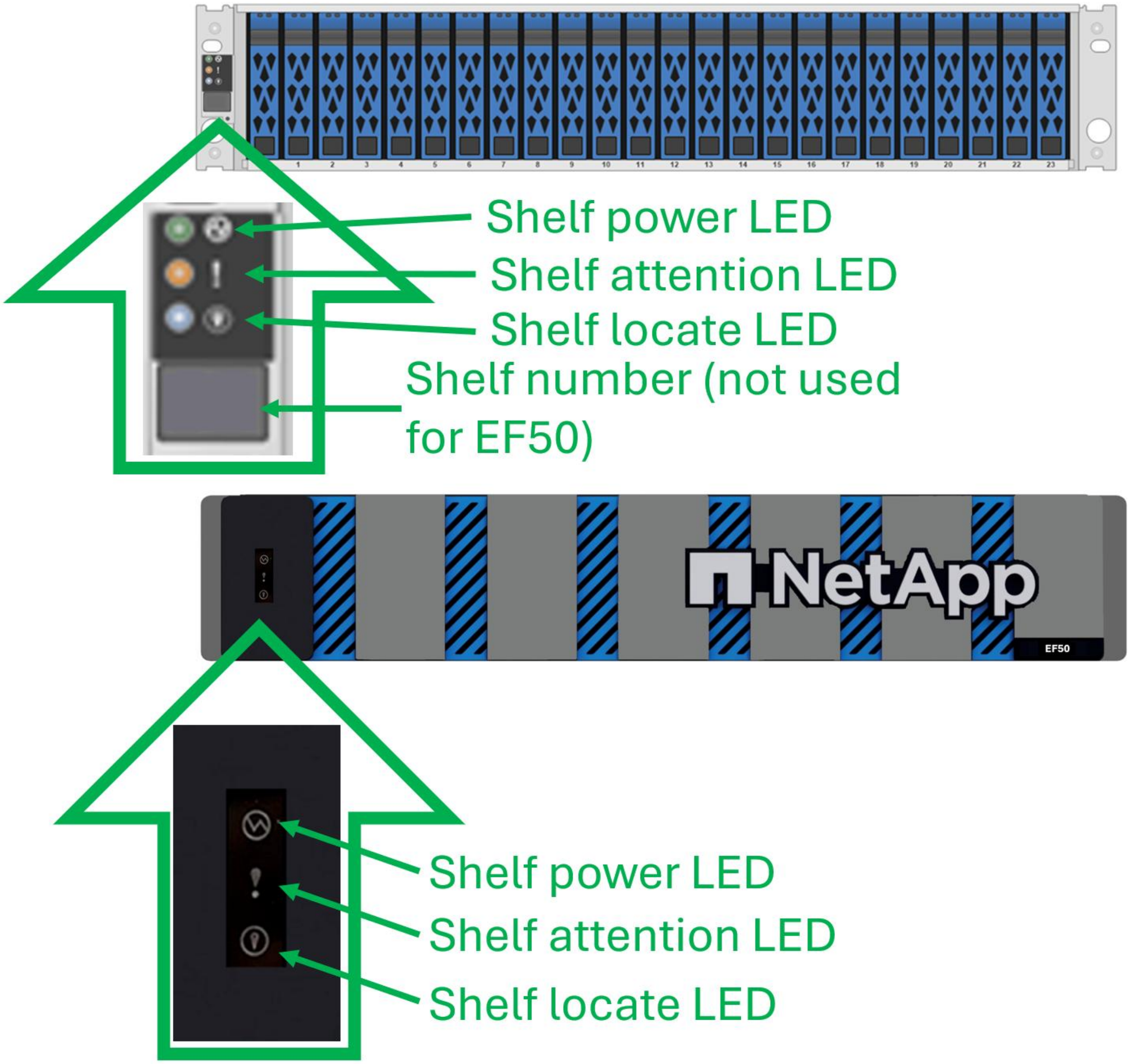


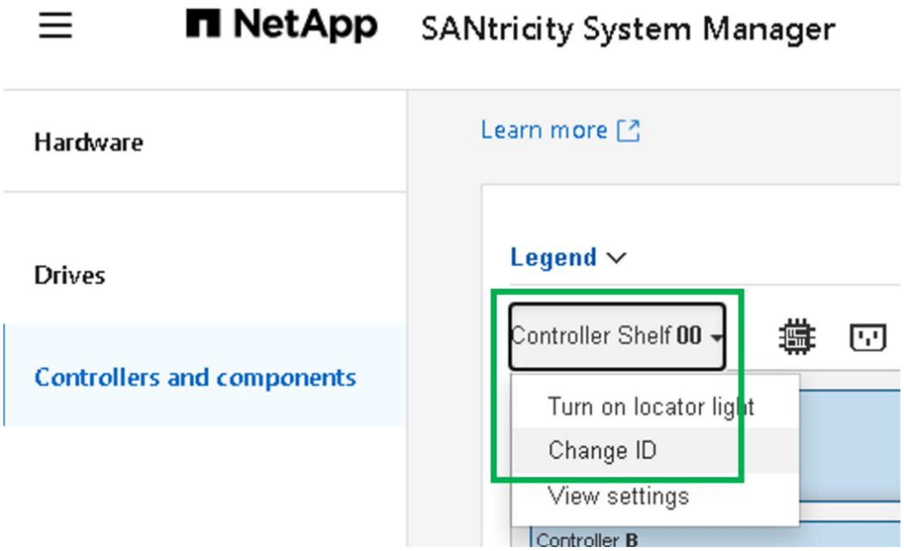
Table 12 defines the ODP LEDs on the EF50 controller shelf.

Table 12) EF50 controller ODP LED definitions.

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 dual seven-segment display in the ODP is not used for EF50 so it remains blank and is covered when front bezel is installed. A unique shelf ID using values from 00 to 99 can be set from the NetApp SANtricity System Manager Hardware option, Controller and components screen, as shown in Figure 45.

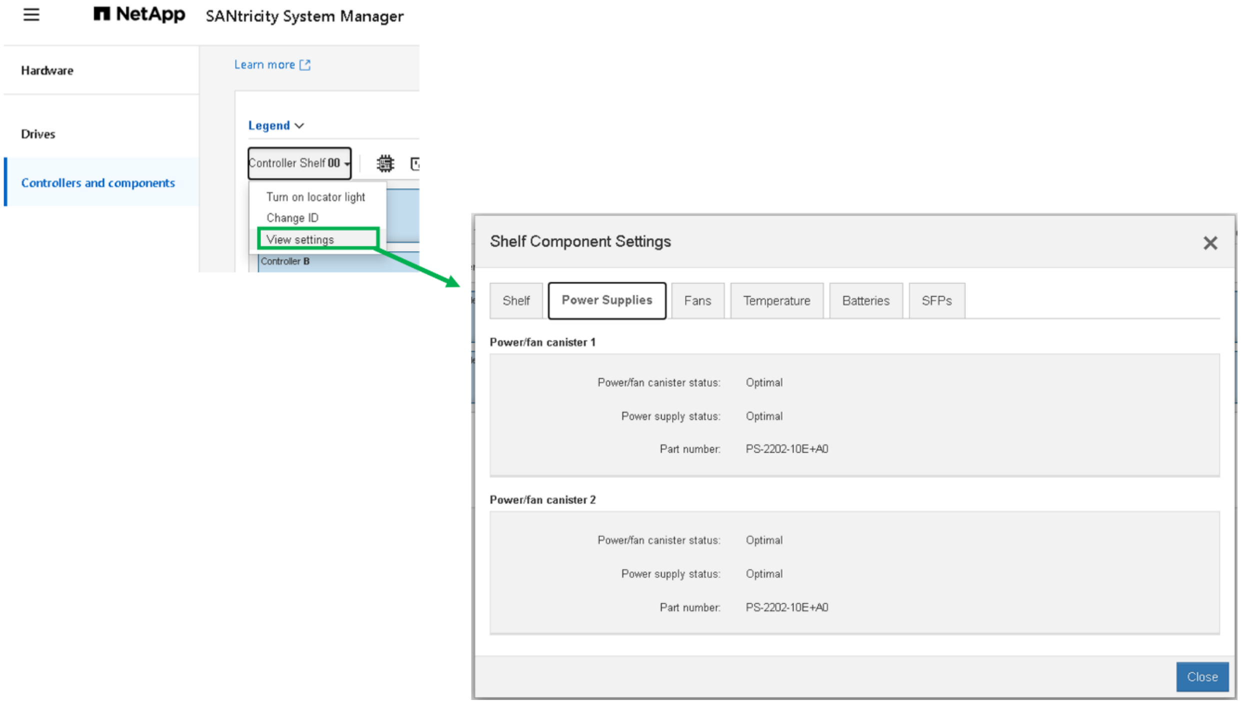
Figure 45) Setting the shelf ID by using SANtricity System Manager.



EF50 controller canister LEDs

The EF50 controller canister has several LED status indicators. You can verify host port status and other system-level status information by directly checking the port LEDs, see Figure 47, or by using the SANtricity System Manager GUI. For example, systemwide status information is displayed on the View Settings page, as shown in Figure 46.

Figure 46) Viewing system status information by using SANtricity System Manager.



Power/fan canister 1

Power/fan canister status: Optimal

Power supply status: Optimal

Part number: PS-2202-10E+A0

Power/fan canister 2

Power/fan canister status: Optimal

Power supply status: Optimal

Part number: PS-2202-10E+A0

LED definitions with HIC installed

The EF50 controller supports either one or two 4-port 64Gbps FC and NVMe/FC HICs. Figure 47 shows the LEDs for the FC HIC.

Figure 47) LEDs on the EF50 (4-port HIC).

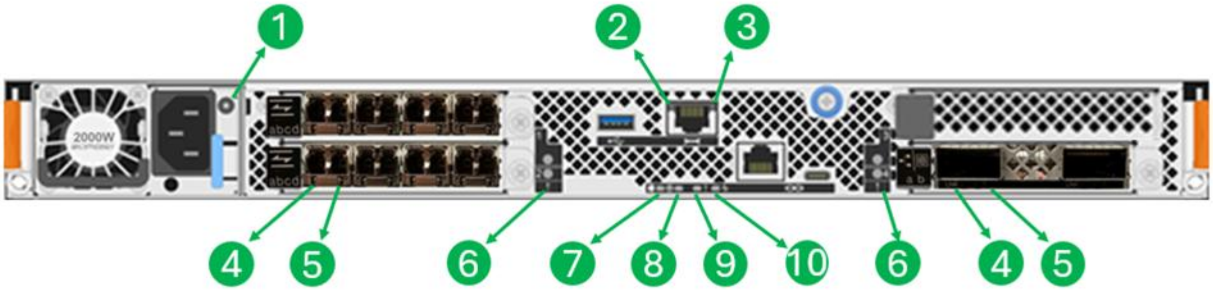


Table 13 defines the LEDs for the 4-port HIC.

Table 13) EF50 controller LEDs with 4-port HIC definitions.

Call-out	LED name	Color	LED description
1	PSU	Green/Red	• LED off: no AC power • Green: AC present and DC output OK • Red: AC cord unplugged or power supply failure
2	Management port activity LED	Green	• Blinking: indicates activity for the Ethernet port
3	Management port link LED	Green	• LED on: link up • LED off: link down
4	HIC port link LED	Green	• On: link up • Off: no link
5	HIC port attention LED	Amber	• On: a condition that requires attention • Off: no special conditions
6	Chassis HIC attention LEDs	N/A	Not used for E-Series
7	Cache activity LED	Green	• On: dirty data in write cache • Blinking: performing cache offload (destage) • Off: no dirty data in write cache
8	Locate LED	Blue	• On: identifies enclosure • Off: not locating enclosure
9	Fault LED	Amber	• On: a condition that requires attention • Off: no special conditions
10	Activity LED	Green	• Blinking: activity on controller • Off: no activity, controller powered off

For more information about the EF50 storage systems and related hardware, see the E-Series and SANtricity 12 Resources page.

Drive LED definitions

Figure 48 shows the LEDs on the drive carriers for the NVMe SSDs. The NE224 shelf in the EF50 architecture supports only 2.5-inch form-factor SSDs.

Figure 48) NVMe drive carrier LEDs.

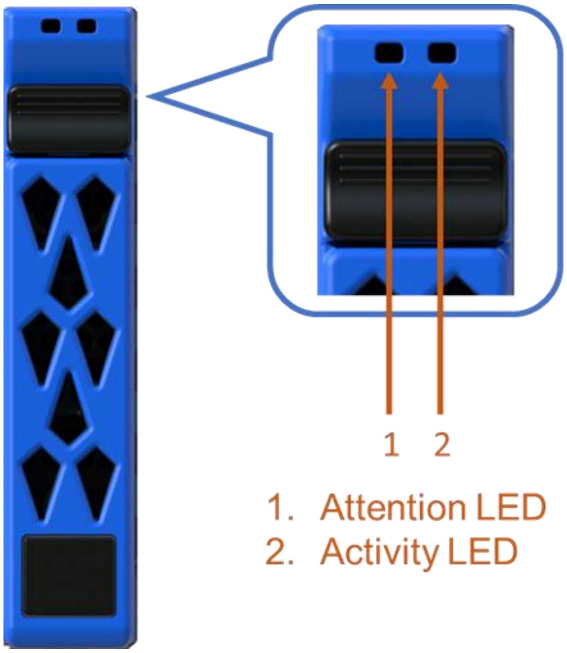


Table 14 defines the LEDs for the drives.

Table 14) NVMe 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

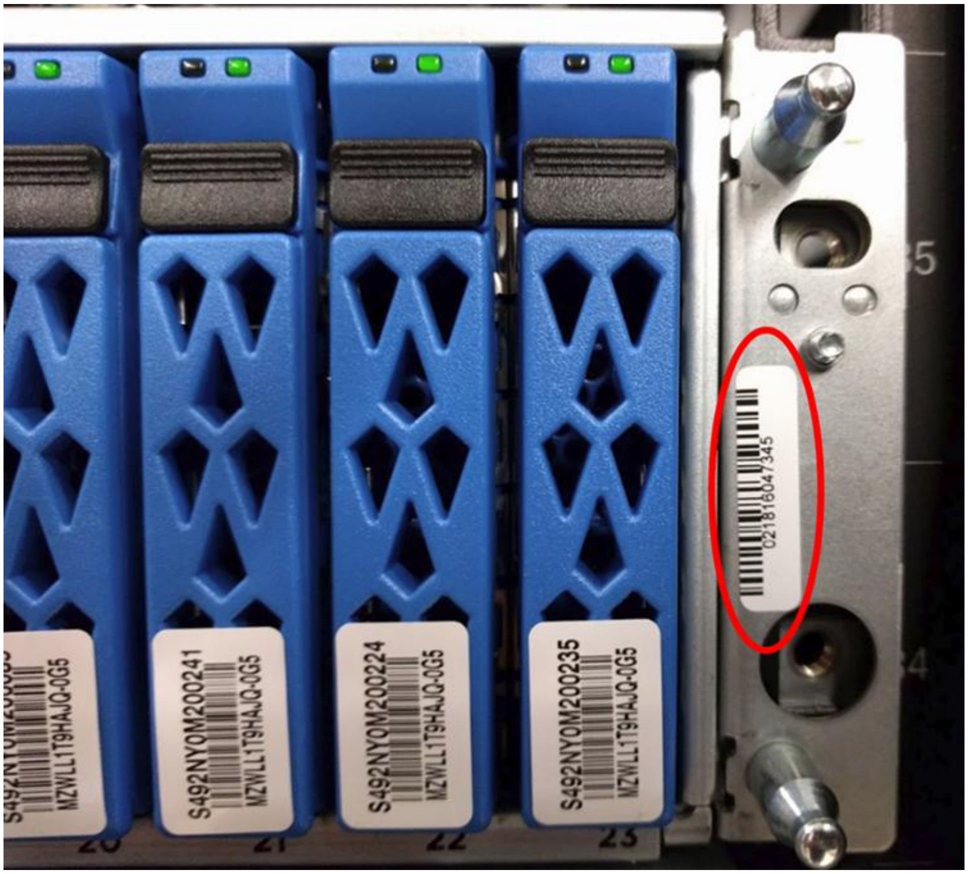
E-Series product support

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

Controller shelf serial number

NetApp EF50 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 that is affixed to the controller shelf behind the right end cap on the front of the chassis. The serial number is circled in red on Figure 49.

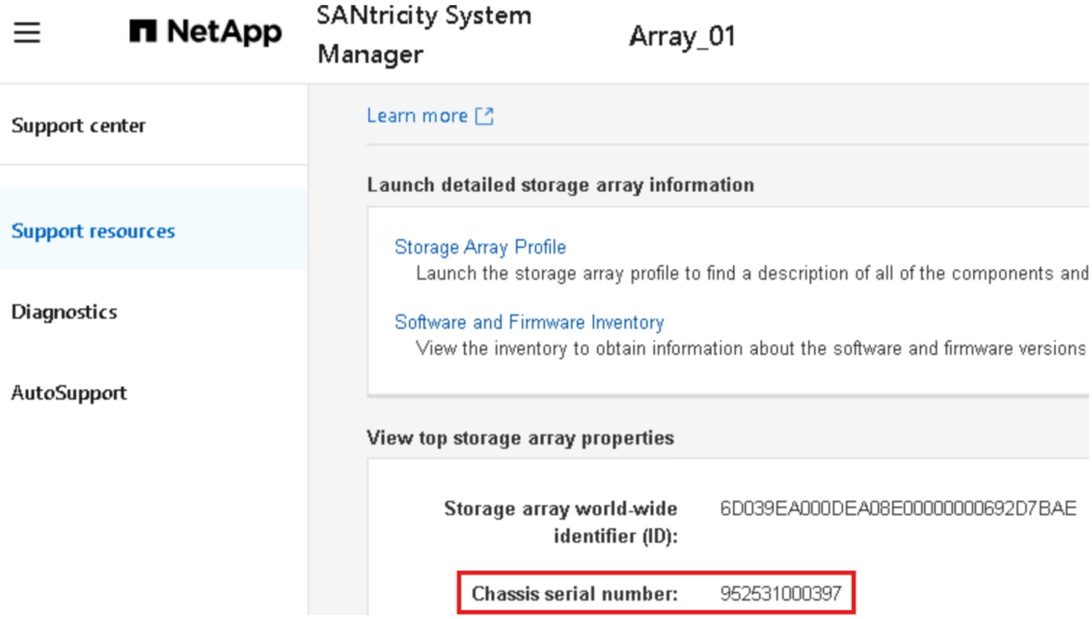
Figure 49) Controller shelf serial number.



The serial number 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, you can also find the chassis serial number through NetApp SANtricity System Manager by selecting Support from drop-down menu, then select Support Center and scroll down to View top storage array properties section in right pane, as shown in Figure 50.

Figure 50) SANtricity System Manager Support Center showing chassis serial number.



Launch detailed storage array information

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

Software and Firmware Inventory
View the inventory to obtain information about the software and firmware versions

View top storage array properties

Storage array world-wide identifier (ID): 6D039EA000DEA08E00000000692D7BAE

Chassis serial number: 952531000397

License keys

E-Series storage arrays use two types of license keys. One type of key file is for premium features, and the other type of key file is used to change the storage system feature pack (which enables or disables the port-to-lun (PTL) ability).

For the EF50 system, there are currently no premium features. All features are enabled out of the box.

The process of generating a new feature pack key for your storage array is almost the same as the process of generating a premium feature key. The difference is that the 11-digit key activation code for each package is available at no additional cost and is listed in the hardware upgrade instructions per controller type, available on the E-Series and SANtricity 12 Resources page.

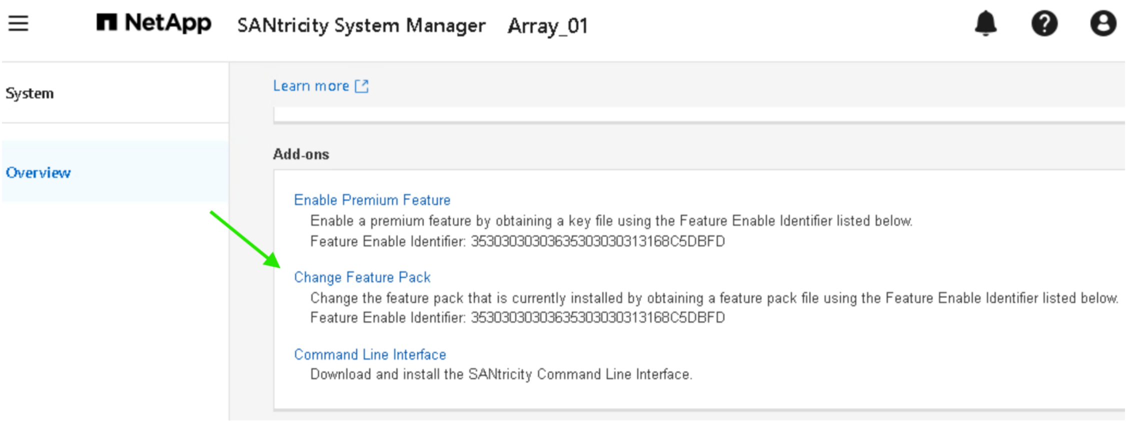
The following information is required to generate a feature pack key file:

- 11-digit key activation code
- Array serial number shown in System Manager by selecting Support, then Support Center

Select the feature enable identifier shown in System Manager by selecting Settings > System and then reference the identifier in the Add-Ons section.

After the feature pack file is downloaded to the host server, click Change Feature Pack, as shown in Figure 51. Follow the prompts, beginning with browsing to the feature pack file, as shown in Figure 52.

Figure 51) Changing the feature pack from Settings > System view.



Add-ons

Enable Premium Feature

Enable a premium feature by obtaining a key file using the Feature Enable Identifier listed below.

Feature Enable Identifier: 35303030303635303030313168C5DBFD

Change Feature Pack

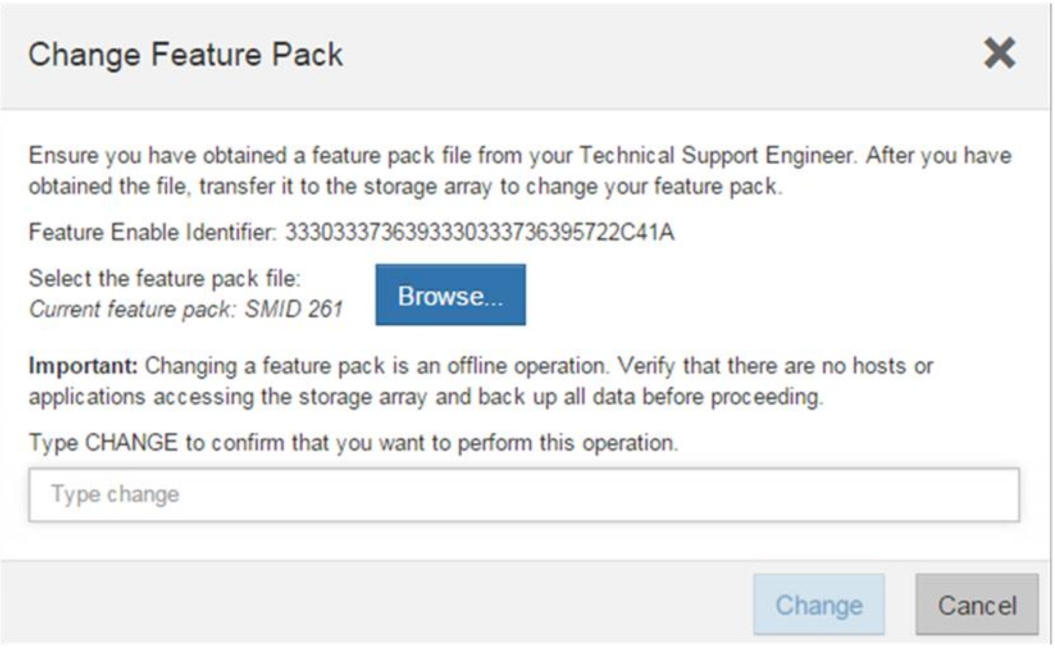
Change the feature pack that is currently installed by obtaining a feature pack file using the Feature Enable Identifier listed below.

Feature Enable Identifier: 35303030303635303030313168C5DBFD

Command Line Interface

Download and install the SANtricity Command Line Interface.

Figure 52) Change Feature Pack option.



Change Feature Pack

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

Feature Enable Identifier: 3330333736393330333736395722C41A

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

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

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

Note: Changing the feature pack causes the storage array to reboot. The new protocol will be active after the system is back online.

For issues with accessing license key files, open a support ticket with NetApp Support by using the serial number of the registered controller shelf for the associated storage system. This will require a NetApp Support login.

Conclusion

The EF50 storage systems provide extreme throughput performance with fast host interfaces and can offer up to 1.4PB of raw NVMe SSD capacity to support fast, large-capacity applications.

For high-random IOPS environments, the EF50 supports up to 1.7 million 4KB read IOPS. For high-bandwidth workloads, it supports approximately 16GBps cache-mirrored sequential writes and up to

42GBps sequential reads. When your workload meets the criteria of the built-in full stripe write acceleration feature, you can accelerate write performance up to 26GBps.

With its extreme versatility—including multiple host interface choices, multiple RAID choices, and a range of entry-level-capacity to enterprise-capacity drive choices—the EF50 is a modern, ready-to-work, NVMe all-flash storage system. The use of NVMe/FC makes the EF50 a truly new-generation NVMe all-flash array. The EF50 system delivers industry-leading price/performance, excellent interface and configuration flexibility, and the extended RAS value that enterprise customers can trust with their highest-value workloads.

Where to find additional information

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

- NetApp Product Documentation
  https://www.netapp.com/support-and-training/documentation/

Version history

Version	Date	Document version history
Version 1.0	March 2026	Initial release of EF50 array and SANtricity 12.00

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

Trademark information

TR-5018-0226