



Technical Report

Introduction to NetApp EF300C array

Feature overview with SANtricity

Mitch Blackburn, NetApp
February 2025 | TR-5004

Abstract

The NetApp® EF300C NVMe high-density all-flash array delivers a performant high-density flash solution for customers that is also affordable and reliable. This document provides detailed information about the hardware and software features of the EF300C all-flash array and NetApp SANtricity® OS features.

TABLE OF CONTENTS

Introduction	5
SANtricity management features	8
Deployment	8
SANtricity Unified Manager.....	9
SANtricity Unified Manager navigation	11
SANtricity System Manager.....	18
SANtricity storage features	29
Drive encryption.....	29
SANtricity host and path management features	29
SANtricity reliability features	30
SANtricity storage management features	31
SANtricity Remote Storage Volumes.....	31
SANtricity copy services features	32
SANtricity management integration	33
SANtricity Storage Plugin for vCenter.....	37
SANtricity OS specifications for EF300C hardware	37
EF300C hardware configurations.....	38
Controller shelf configurations	38
Controller host interface features.....	40
Hardware LED definitions	41
Drive LED definitions	45
Drive loading for maximum performance	46
E-Series product support.....	47
Controller shelf serial number.....	47
License keys.....	49
Conclusion	50
Where to find additional information	51
Version history.....	51

LIST OF TABLES

Table 1) Built-in roles and associated permissions.	22
--	----

Table 2) LDAP/RBAC required fields and definitions.	23
Table 3) SANtricity host types and associated failover behavior.	30
Table 4) SANtricity features for long-term reliability.	30
Table 5) Standard features that are included with SANtricity.	31
Table 6) SANtricity copy services features.	32
Table 7) SANtricity APIs and toolkits.	33
Table 8) Third platform plug-ins that use the SANtricity Web Services Proxy.	33
Table 9) SANtricity OS boundaries for EF300C-based storage systems.	37
Table 10) EF300C technical specifications.	39
Table 11) Available feature pack submodel IDs (FP-SMIDs) for EF300C controllers.	40
Table 12) Host interface protocols and supported speeds.	40
Table 13) EF300C controller shelf LED definitions (front panel).	42
Table 14) EF300C with 4-port 32Gb FC HIC LED definitions.	44
Table 15) NVMe drive LED definitions.	46

LIST OF FIGURES

Figure 1) High-density EF300C all-flash array.	6
Figure 2) EF300C controller with ports identified.	7
Figure 3) Managing a single EF300C with SANtricity System Manager.	8
Figure 4) Managing multiple E-Series with SANtricity Unified Manager and SANtricity System Manager.	9
Figure 5) Final dialog box in the Web Services Proxy installation wizard.	10
Figure 6) SANtricity Unified Manager login page.	11
Figure 7) SANtricity Unified Manager landing page—discover and add arrays.	12
Figure 8) SANtricity Unified Manager landing page.	12
Figure 9) Creating a group to organize arrays in SANtricity Unified Manager.	13
Figure 10) Creating a group in Unified Manager.	13
Figure 11) SANtricity Unified Manager showing a newly created group.	14
Figure 12) SANtricity Unified Manager Operations view.	14
Figure 13) SANtricity System Manager home page.	19
Figure 14) System Manager Storage page.	20
Figure 15) System Manager Hardware page.	20
Figure 16) System Manager Settings page with new security tiles.	20
Figure 17) System Manager Support page.	21
Figure 18) System Manager Support Center.	21
Figure 19) SANtricity System Manager directory server setup wizard.	24
Figure 20) Role Mapping tab in the directory server settings wizard.	25
Figure 21) SANtricity System Manager views change according to user permission level.	26
Figure 22) Initial step required to set up web server certificates.	27
Figure 23) Expanded SANtricity System Manager Certificates tile.	27

Figure 24) Remote storage volumes solution architecture overview.	32
Figure 25) Opening the API documentation.	34
Figure 26) Example of expanding the Device-ASUP endpoint.	34
Figure 27) REST API documentation sample.....	35
Figure 28) Sample output from the Try It Out button.	35
Figure 29) Device-ASUP endpoint possible response codes and details.	36
Figure 30) Opening the CLI Command Reference.	37
Figure 31) EF300C front view with bezel.....	39
Figure 32) EF300C front view (open).	39
Figure 33) EF300C rear view.	39
Figure 34) EF300C controller HIC options.....	41
Figure 35) ODP on front panel of EF300C controller shelf.	42
Figure 36) Setting the shelf ID by using SANtricity System Manager.	43
Figure 37) Viewing system status information by using SANtricity System Manager.	44
Figure 38) LEDs on the EF300C with 4-port HIC.	44
Figure 39) NVMe drive carrier LEDs.	45
Figure 40) Loading drives from the inside drive slots outward.....	46
Figure 41) Loading drives from the outside drive slots inward.....	46
Figure 42) Example DDP using 12 drives.....	47
Figure 43) Controller shelf SN.	48
Figure 44) SANtricity System Manager Support Center tile showing chassis serial number.	48
Figure 45) Changing the feature pack from Settings > System view.	49
Figure 46) Change Feature Pack option.....	50

Introduction

With the release of SANtricity OS 11.90R1, NetApp EF-Series is expanding with two new capacity flash systems with the introduction of EF300C and EF600C. These core block storage systems provide the fast, affordable high-performance and high-capacity options required for demanding block workloads such as media and entertainment, HPC/AI, and high-performance databases.

With high performance and ultra-high throughput, the new EF-Series systems will improve operational efficiency, help accelerate the transition from E-Series HDD-based systems to flash and meet increasing capacity needs without compromising performance or reliability. NetApp EF-Series delivers all of this at a wide range of low-cost, performance and capacity options.

What you already know about the EF300 will still be valid for the EF300C, except for the following:

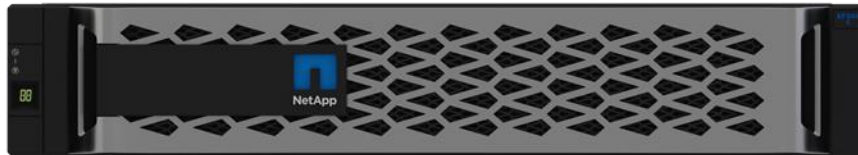
- Only supports NVMe QLC drives (mixing of QLC and TLC drives is not allowed).
- Available with a minimum of 12x up to a maximum of 24x QLC NVMe SSDs.
- The only drives supported will be 30TB or 60TB NVMe QLC drives.
- Expansion shelves are not supported.
- Default configuration is a single Dynamic Disk Pool (DDP) which is automatically created using all available drives for simplicity in management. If a new drive is inserted, Dynamic Capacity Expansion (DCE) will start automatically to incorporate the new drive into the existing DDP.
- If the default configuration is used, drive capacities cannot be mixed in the storage array.
- Standard RAID (5,6,10) volume groups are not supported.
- IOP and latency performance of EF300C is reduced using QLC drives.

Note: The default configuration can be deleted. This allows for manual creation of one or two pools and the use of both 30TB and 60TB drives in the same array.

NetApp® EF300C all-flash arrays have a new badge, as shown in Figure 1, use end-to-end NVMe NE224 drive shelves and are managed by the secure web-based NetApp SANtricity® System Manager UI.

Figure 1) High-density EF300C all-flash array.

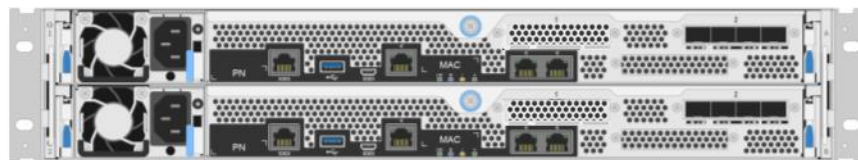
EF300C with FC host interface shown



Front View



Front View
(open)



Rear View

In one powerful all-flash array package, the EF300C array delivers optimal performance for both random workloads and large sequential workloads. The array can deliver consistent response times for up to 350,000 4KB random read IOPS with as few as 24 NVMe SSDs. The same configuration can deliver up to 20GBps large sequential read throughput and about 7GBps cache-mirrored large sequential write throughput.

The array supports the SCSI over FC protocol and the NVMe over Fibre Channel (NVMe/FC) protocol on the 32-Gb FC host interface card (HIC). The iSCSI protocol is supported on the 25Gb iSCSI HIC. NVMe over InfiniBand (NVMe/IB), NVMe over RoCE (NVMe/RoCE), SRP/IB, and iSER/IB are supported on the 100Gb HIC.

This versatility is enhanced by the large capacity SSD choices of either 30TB or 60TB QLC drives to achieve the price/performance combination that fits your business need.

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 EF300C controller provides a single Ethernet management port for out-of-band management. The EF300C array also introduces new, faster host interface options that fit 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.

This package includes your choice of the following HICs:

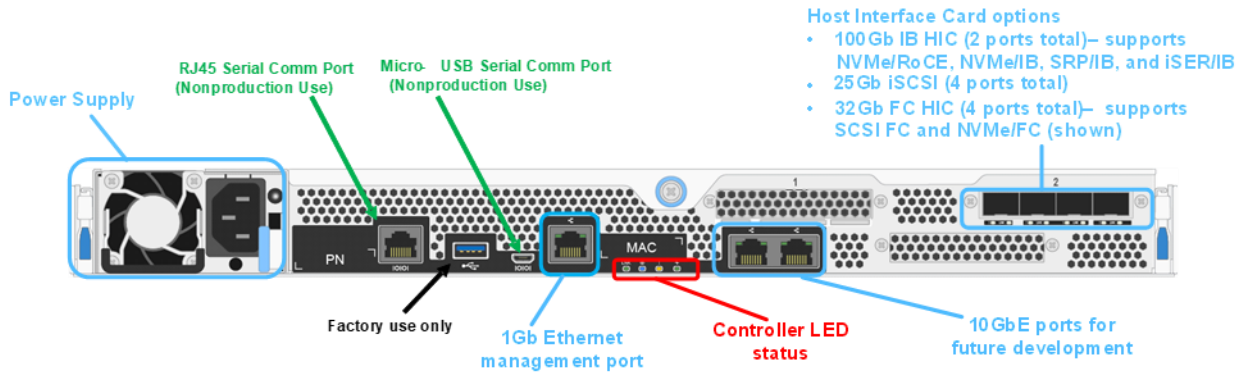
- One four-port 25Gb iSCSI
- One four-port 32Gb FC (OM4 fiber required)

- One two-port 100Gb IB (requires 100Gb-capable cables and host channel adapters [HCAs])

Note: You can download and install a software feature pack in the field to change the host protocol between the various available protocols on each HIC.

Figure 2 identifies the various interface ports on the EF300C controller.

Figure 2) EF300C controller with ports identified.



Note: No mixing of host protocols

Note: Type-A USB port for factory use only is disabled if using SANtricity OS 11.80 or newer.

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.

For detailed instructions about how to change host protocols, go to [E-Series documentation](#) page and search 'change host protocol'.

The EF300C continues the E-Series legacy of providing fast, simple, reliable, and flexible SAN storage regardless of the workload. NetApp EF300C 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 consistent 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 EF300C 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.

EF300C 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 NetApp SANtricity 11.70 release builds on that legacy with the addition of 512e, which allows for general support of the iSCSI host interface as well as support for VMware for FC, iSCSI, and NVMe/FC hosts for NVMe-based platforms.

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 EF300C-based storage array depends on if you want to manage single storage arrays individually or if you are managing multiple arrays.

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

Managing storage arrays individually

If you are not using 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.

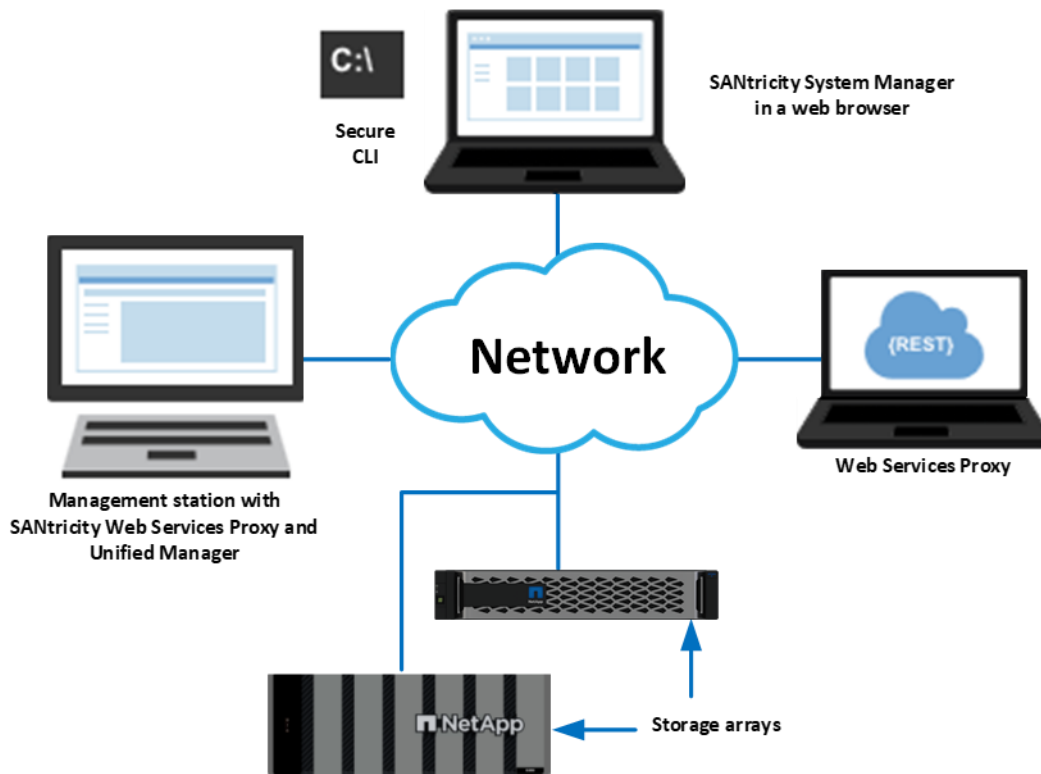
Figure 3) Managing a single EF300C with SANtricity System Manager.



Multiple storage arrays

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 E-Series with SANtricity Unified Manager and SANtricity System Manager.



SANtricity Unified Manager

SANtricity Unified Manager is a web-based central management interface that replaces the legacy SANtricity Storage Manager Enterprise Management Window (EMW) for managing 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:

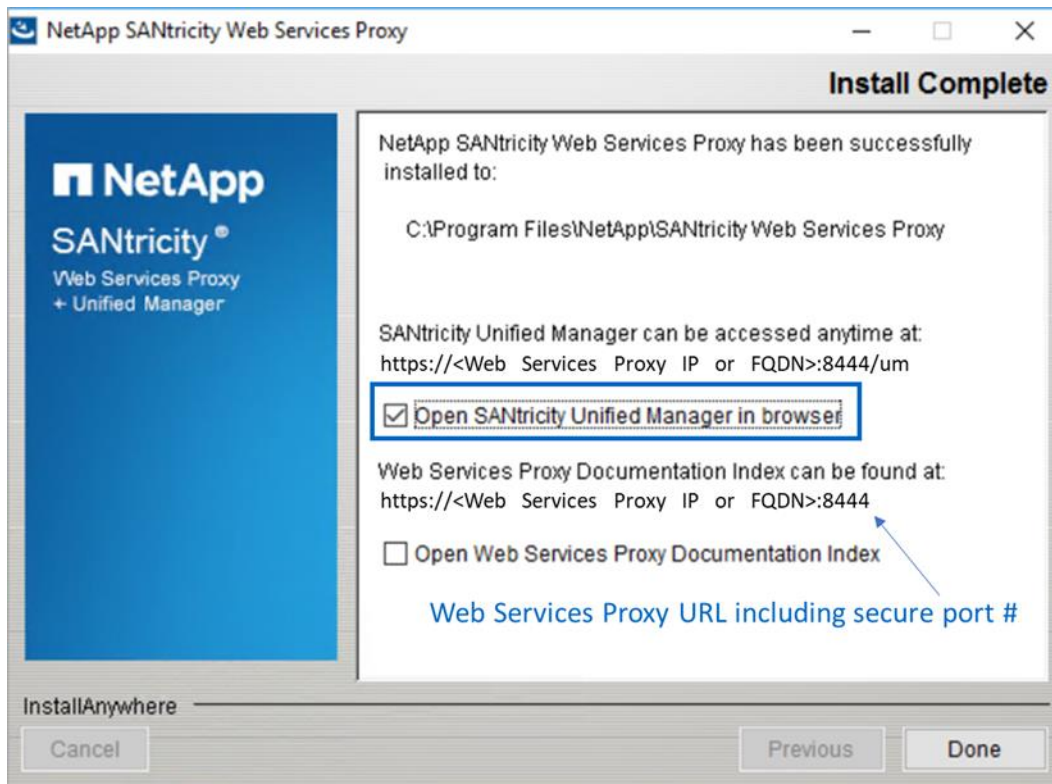
- Upgrades multiple arrays with the same type of controller at one time.
- Supports Lightweight Directory Access Protocol (LDAP) and role-based access control (RBAC) just like SANtricity System Manager. It includes a simplified certificate management workflow to manage the Unified Manager or Web Services 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 arrays through the secure SSL interface.

Note: There is no synchronous mirroring support for EF300C systems.

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.

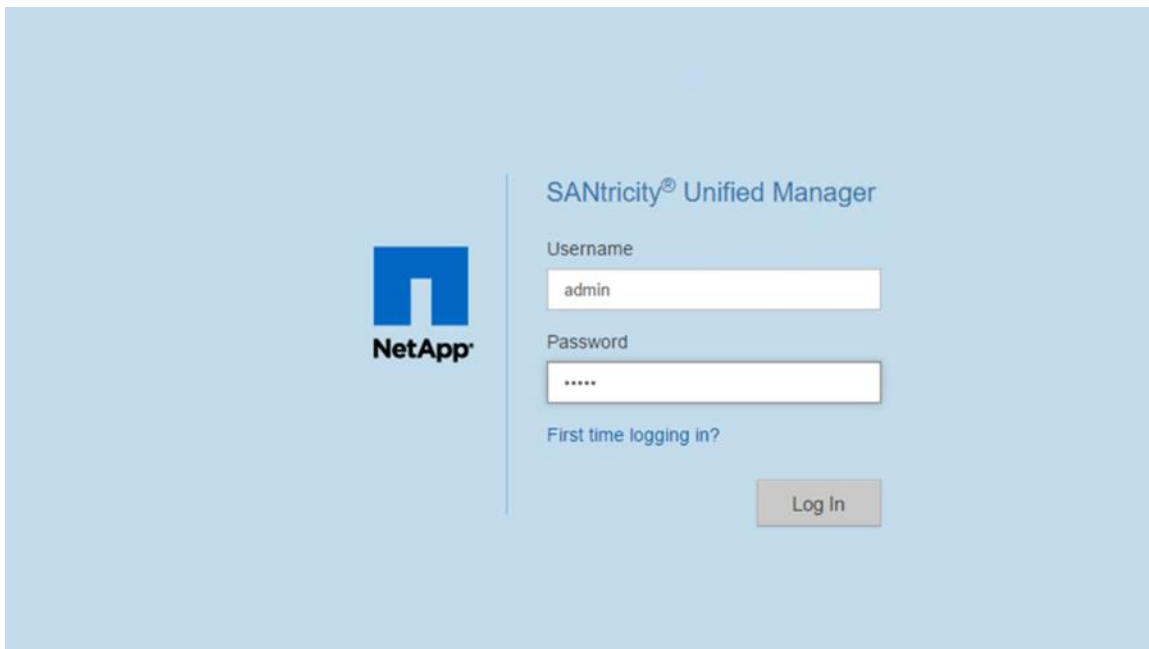
After the installation wizard completes, you can open Unified Manager, or you can directly access the SANtricity Web Services Proxy as shown in Figure 5.

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



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.

The image shows the login page for SANtricity Unified Manager. On the left is the NetApp logo. To its right, the title "SANtricity® Unified Manager" is displayed. Below the title are two input fields: "Username" with the text "admin" and "Password" with masked characters "*****". A link "First time logging in?" is positioned below the password field. A "Log In" button is located at the bottom right of the form area.

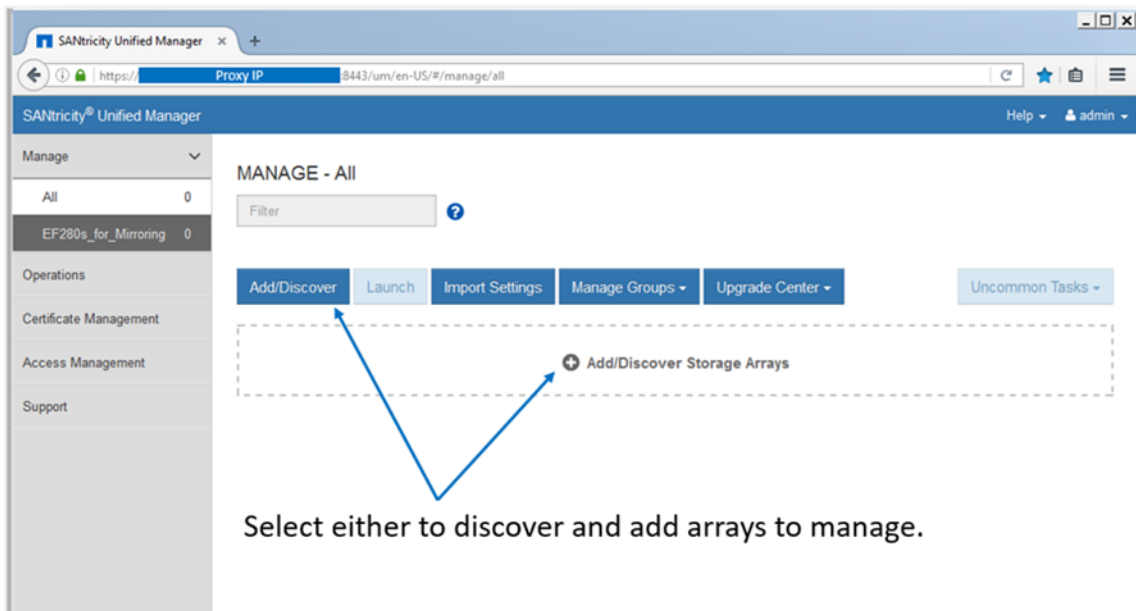
SANtricity Unified Manager navigation

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

Discovering and adding storage arrays

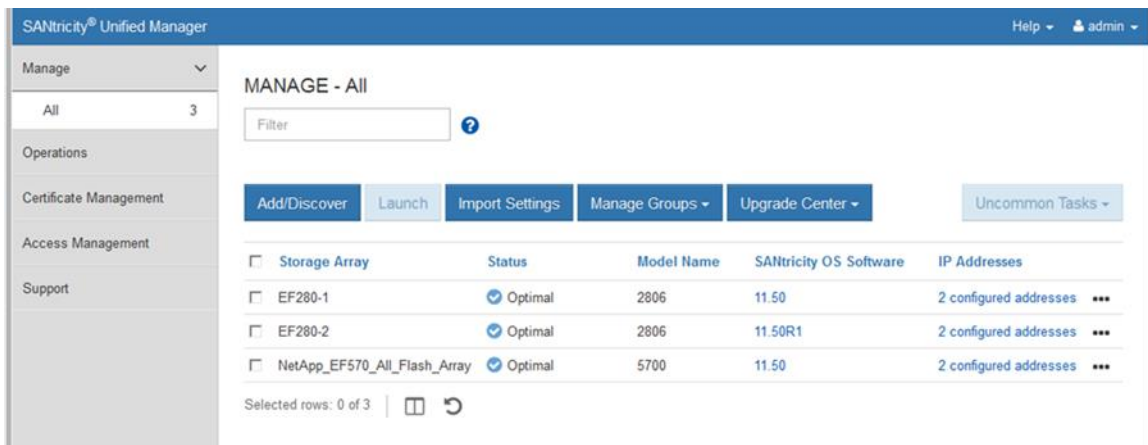
SANtricity Unified Manager must discover arrays to manage. You can discover a single array or scan a range of IP addresses to discover multiple arrays simultaneously. Select the tab or link shown in Figure 7 to open the Add/Discover wizard. After discovering arrays, you then choose to add them to be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

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



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

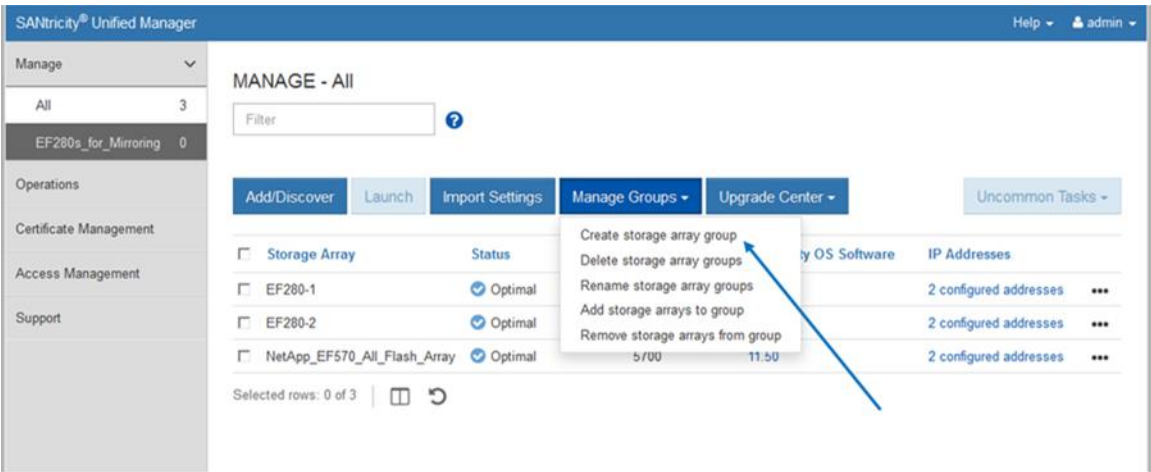
Figure 8) SANtricity Unified Manager landing page.



Organize arrays by group

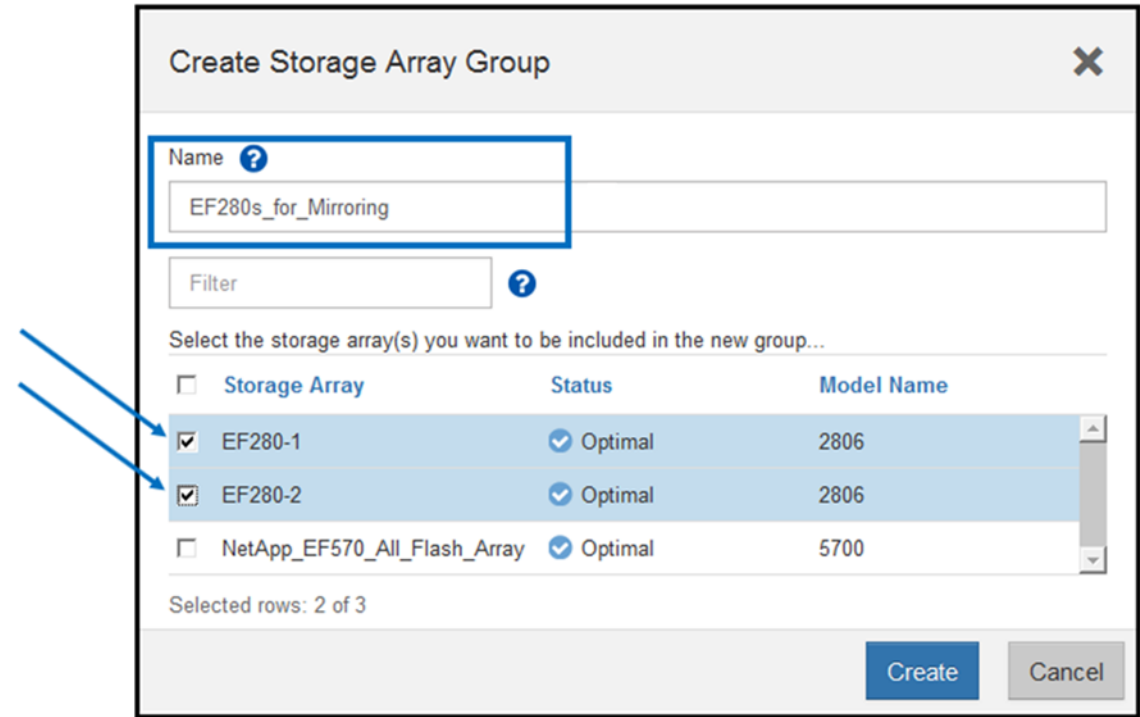
After you add arrays to Unified Manager, you can group them to organize your array management environment. Figure 9 shows the EF280 arrays added to a group. This capability is available for all new-generation E-Series and EF-Series arrays.

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



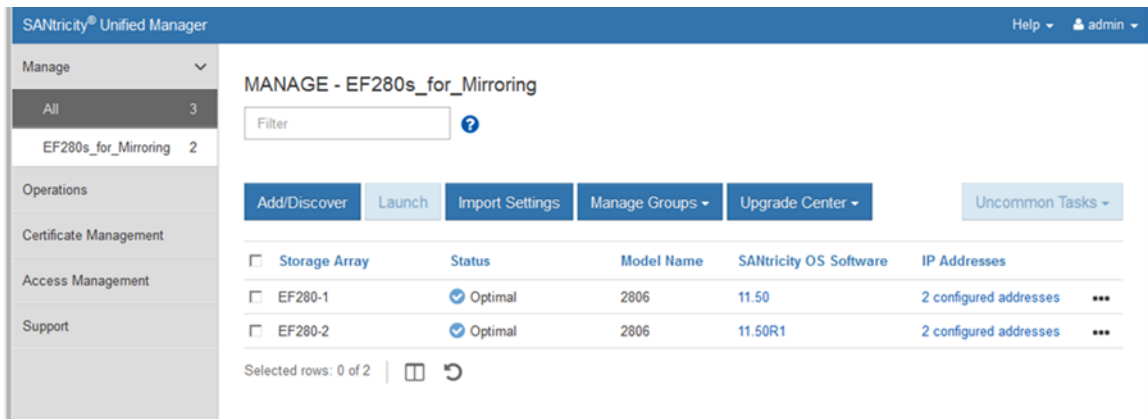
The built-in wizard makes adding arrays to groups quick and easy, as shown in Figure 10.

Figure 10) Creating a group in Unified Manager.



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.



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 or EF-Series arrays running SANtricity 11.60 or later. For example, if you want the same alerting and NetApp AutoSupport settings on all systems, use the Import Settings wizard to select the setting category, the array to copy from, and the array to import to, and click Finish. The operation to copy the settings is displayed in the Operations view, as shown in Figure 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.

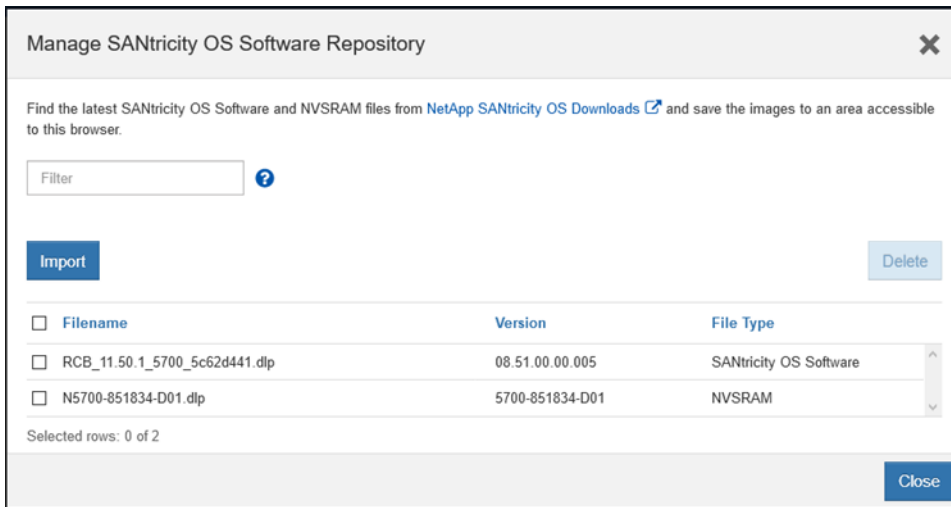
Figure 12) SANtricity Unified Manager Operations view.



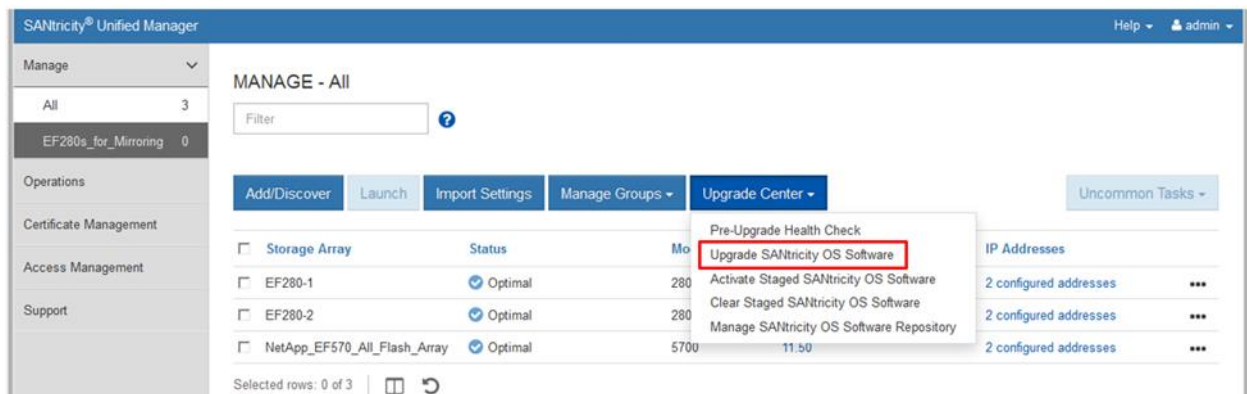
Update SANtricity OS through Unified Manager

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.



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



- 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
- Click Start to continue.

Upgrade SANtricity OS Software

Add new file(s) to the software repository

Select a SANtricity OS Software file

RCB_11.50.1_5700_5c62d441.dlp (08.51.00.00.005)

Select an NVSRAM file (recommended)

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

Filter

Compatible Storage Arrays

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

Selected rows: 2 of 2

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

Start

Cancel

- On the Confirm Transfer and Activation page, 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.

Filter

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

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

upgrade

Upgrade

Cancel

- After 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			
<div>Filter</div>			
Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF570	Health Check In Progress	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	Health Check In Progress	08.51.00.00.005	5700-851834-D01
Total rows: 2			
Close			

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

Upgrade SANtricity OS Software			
<div>Filter</div>			
Storage Array	Status	Proposed OS Software	Proposed NVSRAM
EF570	OS Software Upgrade Successful	08.51.00.00.005	5700-851834-D01
NetApp_EF570_All_Flash_Array	OS Software Upgrade Successful	08.51.00.00.005	5700-851834-D01
Total rows: 2			
Close			

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

SANtricity Unified Manager					
<div> <div>Manage</div> <div>MANAGE - All</div> <div>Filter</div> <div> <div>Add/Discover</div> <div>Launch</div> <div>Import Settings</div> <div>Manage Groups</div> <div>Upgrade Center</div> </div> <div>Uncommon Tasks</div> </div>					
Storage Array	Status	Model Name	SANtricity OS Software	IP Addresses	
<input type="checkbox"/> E2860	Optimal	2806	11.50R1	2 configured addresses	...
<input type="checkbox"/> EF280-1	Optimal	2806	11.50R1	2 configured addresses	...
<input type="checkbox"/> EF570	Optimal	5700	11.50.1	2 configured addresses	...
<input type="checkbox"/> NetApp_EF570_All_Flash_Array	Optimal	5700	11.50.1	2 configured addresses	...
Selected rows: 0 of 4					

SANtricity Unified Manager security

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

Remote mirroring with SANtricity Unified Manager

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

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

Note: EF300C does not support synchronous mirroring.

Prior to SANtricity 11.62, for a description of mirroring between two new generation E-Series arrays or between a new generation E-Series array and a legacy E-Series array, see [SANtricity Synchronous and Asynchronous Mirroring \(11.61 and below\)](#).

SANtricity System Manager

SANtricity System Manager provides embedded management software, web services, event monitoring, secure CLI, and AutoSupport for EF300C arrays.

EF300C storage systems are shipped preloaded with SANtricity OS, which includes SANtricity System Manager. To discover multiple EF300C 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 and SANtricity documentation resources 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://mysupport.netapp.com/eseries>.

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, the home page is displayed, as shown in Figure 13.

- 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 13) SANtricity System Manager home page.



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

Figure 14) System Manager Storage page.

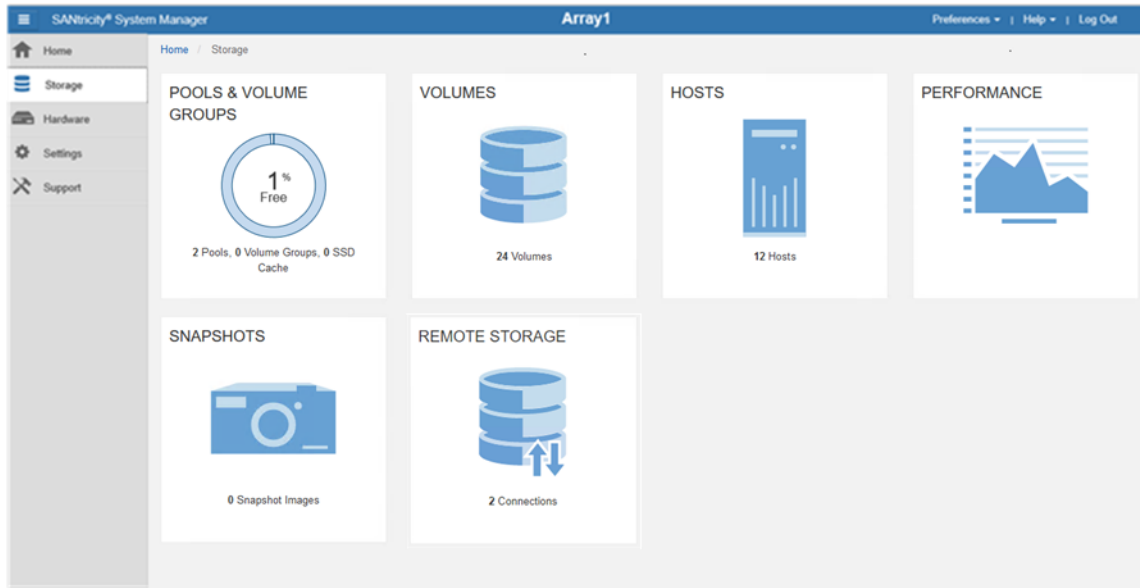


Figure 15) System Manager Hardware page.



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



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

Figure 17) System Manager Support page.

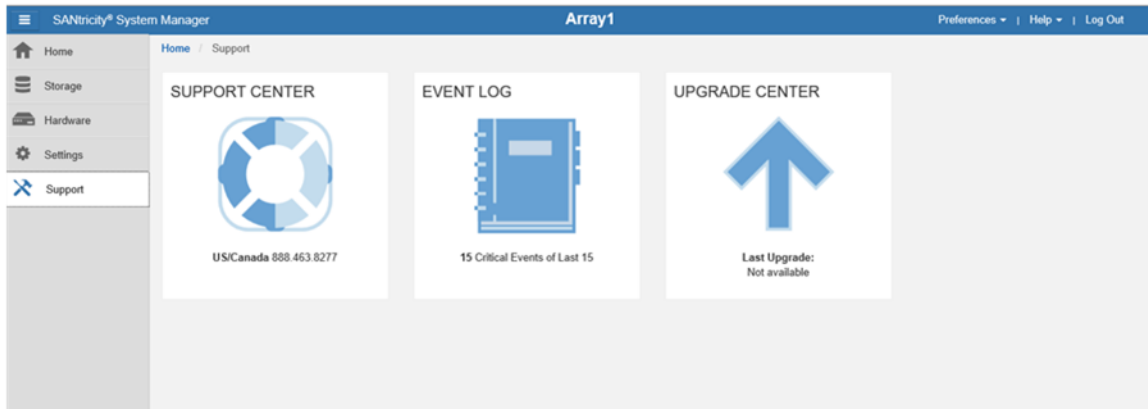
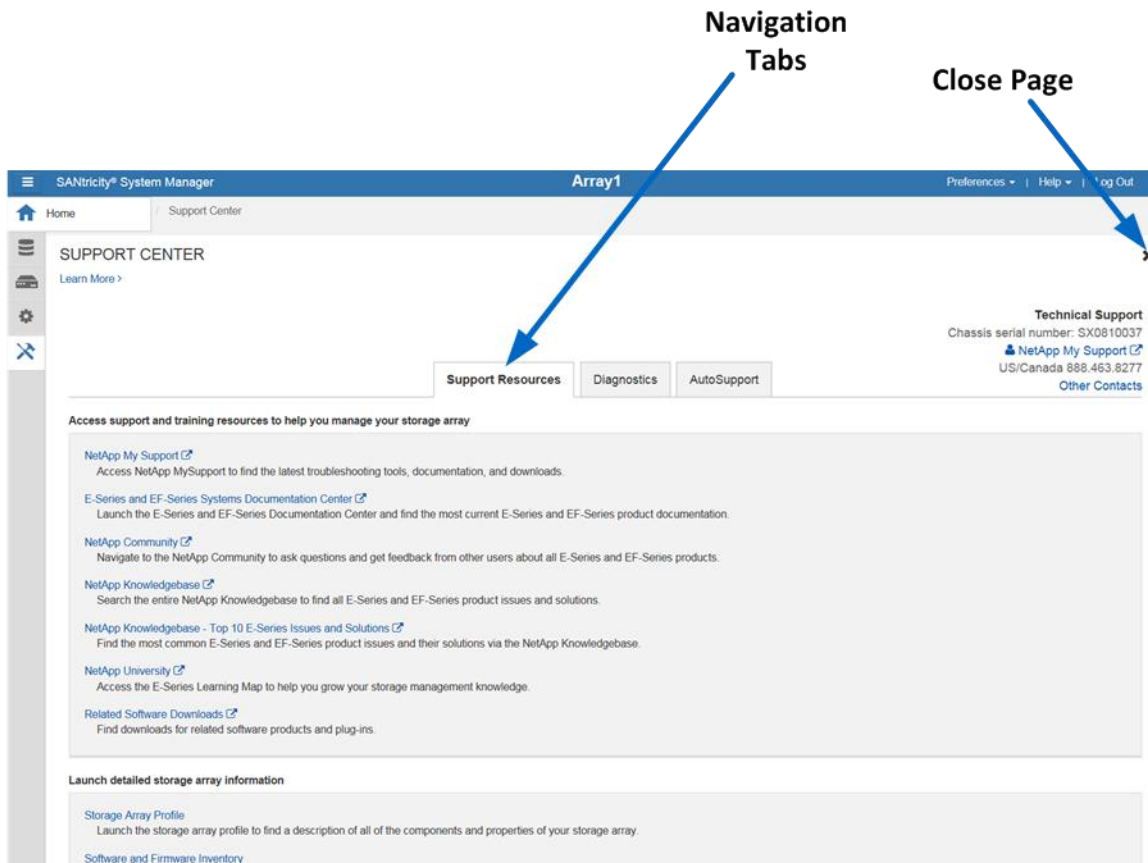


Figure 18 displays the Support Center, which you can reach by selecting the Support Center tile on the Support page. From the Support Center, use navigation tabs to reach support topics.

Figure 18) System Manager Support Center.



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 the certificates are installed. Syntax and invocation are the same as in the legacy CLI, but additional security parameters are supplied.
- Security enhancements that extend to the onboard web services API, where user account passwords are now required.

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

LDAP and RBAC

LDAP is a commonly used communication protocol that enables directory servers such as Microsoft Active Directory to provide centralized identity control over user and group definitions. 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 11.40 and later versions 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, <code>netapp.com</code>)	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 <code>ldap://<IP:port_number></code> (port 389 or port 636 for LDAPS).
Bind account	Format is <code>CN=binduser,CN=Users,DC=<some_name>,DC=com</code> .
Bind account password	Password for bind account user.
Search base DN	Format is <code>CN=Users,DC=<some_name>,DC=com</code> .
Username attribute	The LDAP attribute that defines the username. Example: <code>sAMAccountName</code> : 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: <code>memberOf</code> is a standard attribute.

Figure 19 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 19) 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

Domain(s) **Enter one or more comma-separated domain names**
netapp.netapp.com

Server URL **Directory Server IP**
ldap://[redacted]:389

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

Bind password **Directory Server 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

Add **Cancel**

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

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

Directory Server Settings

Server Settings Role Mapping

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

Mappings

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

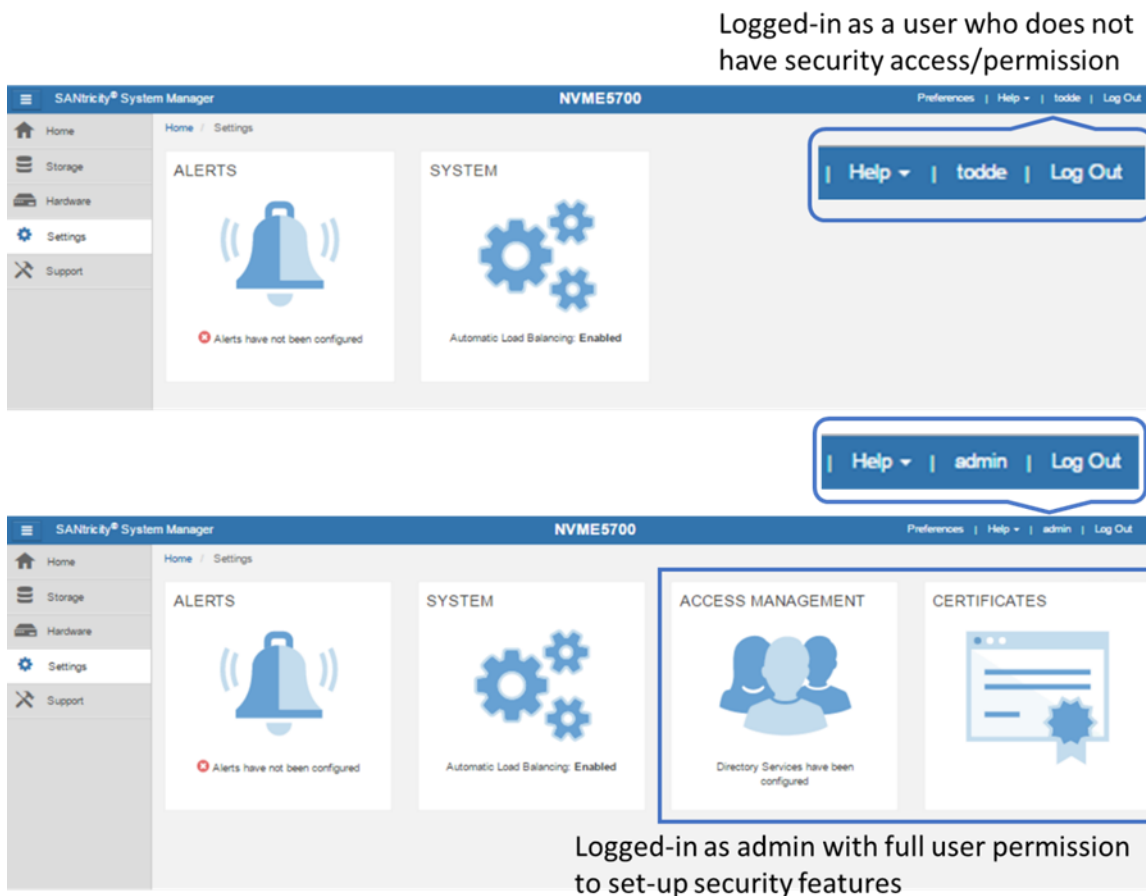
+ Add another mapping

Save Cancel

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

Multiple groups can be defined and mapped to specific roles that meet individual business requirements. Figure 21 shows the difference in user views and access to features according to access permission level. The login on top provides monitor and support access, but it does not provide security access like the admin login below it.

Figure 21) SANtricity System Manager views change according to user permission level.

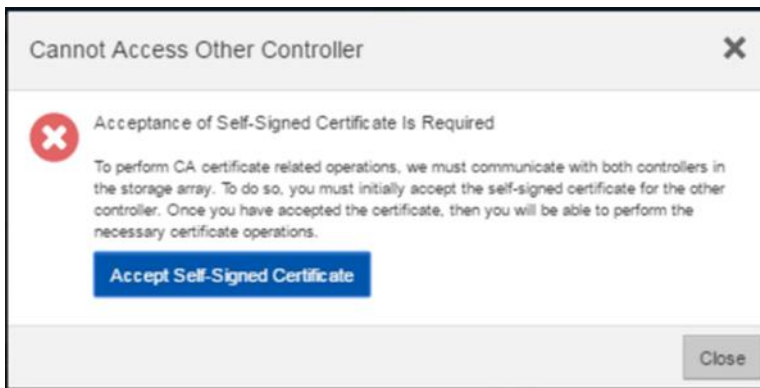


SANtricity web server security certificates

In addition to authentication and access control, SANtricity System Manager supports standard CA certificates. This support enables secure communications (SSL/TLS) between browser clients and the E-Series built-in web servers on the controllers. On EF300C arrays, the SANtricity System Manager UI is accessed through one of the two controllers. (In the legacy SANtricity Storage Manager application, access was through both controllers simultaneously.) As a result, all communication to the other controller in the EF300C array is performed through the midplane in the shelf.

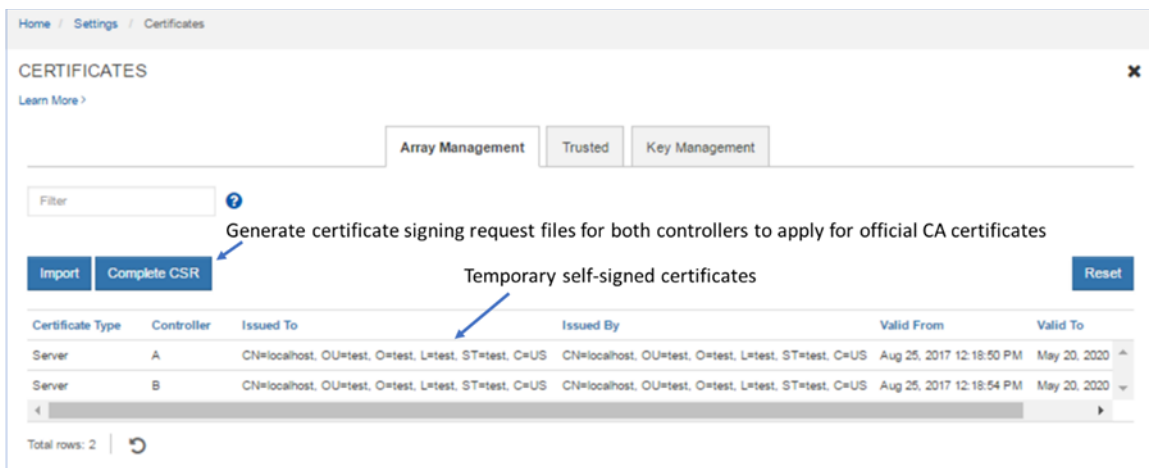
Because you can log in to either of the controllers through the web browser, both controllers must run a web server instance. For proper communication, both controllers must present a self-signed certificate to each other. This process happens automatically when the admin or security user logs in to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

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



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

Figure 23) Expanded SANtricity System Manager Certificates tile.



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

Multifactor authentication

Feature overview

Multifactor authentication (MFA) includes several functional areas on EF300C arrays:

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

- **Digitally signed firmware.** The controller firmware verifies the authenticity of any downloadable SANtricity firmware. Digitally signed firmware is required in controller firmware version 8.42 (SANtricity 11.40.2) and later. If you attempt to download unsigned firmware during the controller upgrade process, an error is displayed, and the download is aborted.
- **Certificate revocation checking 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 a syslog server to archive audit logs. After configuration, all new audit logs are sent to the syslog server; however, previous logs are not transferred. Configuration tasks are available from Settings > Access Management and require security admin permissions.

How MFA works

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

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

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

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

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

For more information about MFA, see the E-Series online help center and the [E-Series 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 the Settings tile, use the Key Management tab 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 tab to enable secure communication between the E-Series controllers and the external key management server. For more information about the SANtricity drive security feature, see the E-Series online help center and [TR-4474: SANtricity Drive Security](#).

SANtricity host and path management features

When considering the elements of E-Series multipath functionality, you must understand two concepts. The first is controller-to-volume ownership and how path failover between controllers is managed through asymmetrical logical unit access (ALUA) 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 a deep explanation of E-Series multipath behavior, see [TR-4604: Clustered File Systems with E-Series Products: BPG for Media](#).

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

- Volume ownership alternates as volumes are provisioned.
- Write I/O is mirrored to the peer controller.
- Both controllers have access to every volume on the array.
- Both controllers have multiple host ports.
- If one E-Series controller fails, the other controller takes control of all the 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 to 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 across the shelf midplane 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 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 fallback	Automatic load balance
Linux DM-Multipath (kernel 3.10 or later)	Enabled	Supported	Supported	Supported
VMware	Enabled	Supported	Supported	Supported
Windows	Enabled	Supported	Supported	Supported
Windows cluster	Enabled	Supported	Supported	Supported
ATTO cluster (all operating systems)	Enabled	Supported	Not supported	Not supported

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

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
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>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.</p>
<p>Note: Parallel drive firmware upgrades are supported offline to upgrade multiple drives more quickly during a maintenance window.</p>
<p>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.</p>
<p>Embedded SNMP agent. For the EF300C controller, SNMP is supported natively. The embedded SNMP agent complies with the SNMP V2C standard and RFC 1213 (MIB-II). For more information, search for "manage SNMP alerts" in the System Manager online help.</p>

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 EF300C 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. Usually, the tag is only for organization purposes. In some cases, the Volume Creation wizard provides suggested configuration or volume segment size settings associated with the workload type. You do not have to accept the recommendations. The configurations are suggestions for saving time when you provision volumes for common applications.

Storage partitions. Partitions can consist of an individual host without shared volumes, host groups with shared volumes, or a combination of both. This concept has been abstracted in the new System Manager, but you can view the partitions by using a CLI.

Changing host protocol. This capability is supported through new feature pack keys. To obtain free activation codes and detailed instructions for each starting and ending protocol, go to the [E-Series and SANtricity 11 Resources](#) page (Upgrading > Hardware Upgrade).

SANtricity Remote Storage Volumes

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

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

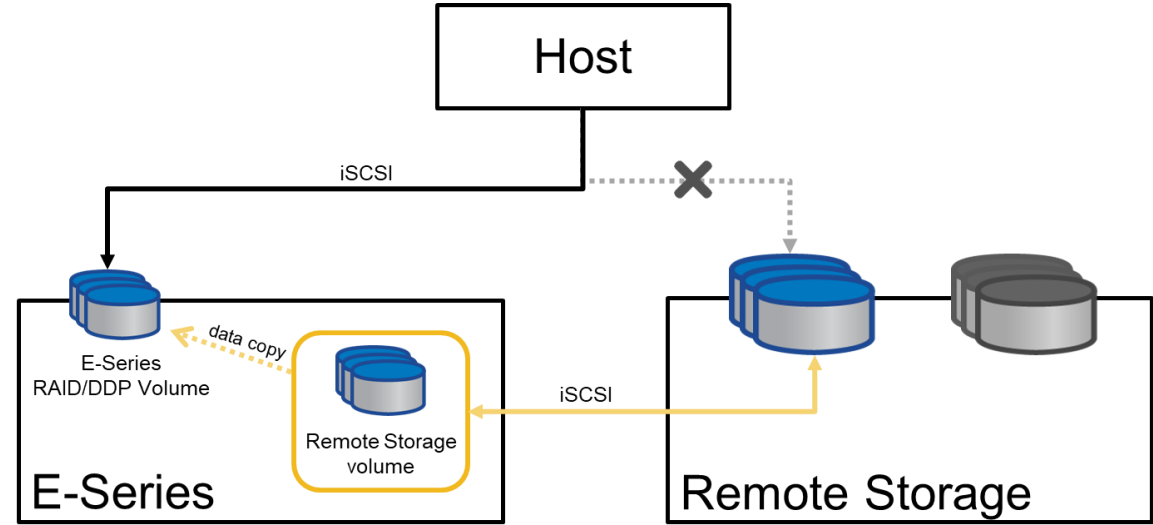
With the iSCSI connection in place, you can then map the remote storage device to the E-Series system. After the mapping is in place, you can then use SANtricity System Manager or REST API commands for the E-Series system to initiate and manage the import operation.

During the import operation, you can set up the target volume to process the I/O operations that the remote storage device was originally processing. Any I/O operations going to the target volume are then

propagated back to the remote storage device until the import operation has completed and the import has been disconnected.

Figure 24 shows the technical components of the solution.

Figure 24) Remote storage volumes solution architecture overview.



Information that you must provide to initiate the import operation includes:

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

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

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

For more information about remote storage volumes, see [TR-4893-DEPLOY: SANtricity Remote Storage Volumes](#).

SANtricity copy services features

Table 6 lists standard copy services features with EF300C storage arrays.

Table 6) SANtricity copy services features.

Copy services features with SANtricity
SANtricity Snapshot copies. Point-in-time NetApp Snapshot™ copies.
Asynchronous mirroring. Mirroring to a remote site where RPO = 0 is not a requirement.
Volume copy. Used to clone volumes for testing/development or analytics purposes.

For additional details and use case information about SANtricity copy services features, see [TR-4458: Deploying NetApp E-Series 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](#).

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

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

SANtricity management integration

To support today's modernized data center operations and partner appliances, NetApp is deemphasizing legacy plug-ins and emphasizing API integration.

Table 7 shows the SANtricity APIs and toolkits that can be used for scripting and custom integration into other management tools and appliance architectures. To download the latest version of the E-Series SANtricity Web Services (REST API) visit NetApp support at <http://mysupport.netapp.com/>. Information for how to use Ansible with E-Series for managing your storage can be in [TR-4574: Deploying NetApp E-Series with Ansible \(Automating E-Series\)](#). For the Windows PowerShell toolkit, go to the [NetApp PowerShell Toolkit](#) page of the NetApp Support site.

Table 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.
NetApp PowerShell Toolkit	The unified toolkit provides end-to-end automation and storage management across NetApp storage systems.
SANtricity Secure CLI	New in SANtricity 11.60.2 is the ability to download the SANtricity Secure CLI (SMcli) from System Manager.

Table 8 provides a list of third platform plug-ins that use E-Series storage systems as building blocks. Usually, the plug-ins listed are available on the various provider websites. For more information about third platform integration with EF-Series storage systems, contact your NetApp sales representative.

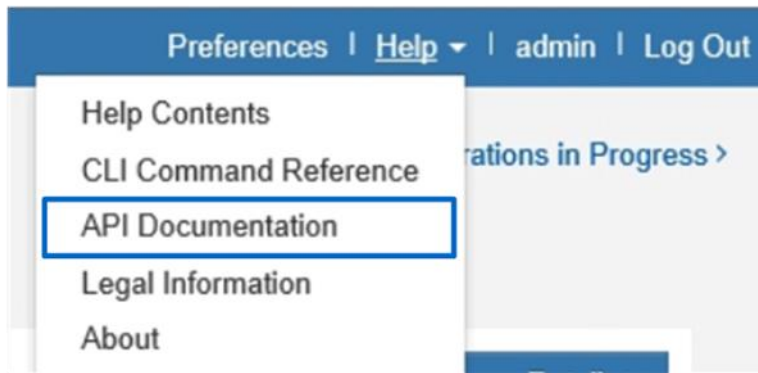
Table 8) Third platform plug-ins that use the SANtricity Web Services Proxy.

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 25.

Figure 25) Opening the API documentation.



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

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

Figure 26) Example of expanding the Device-ASUP endpoint.

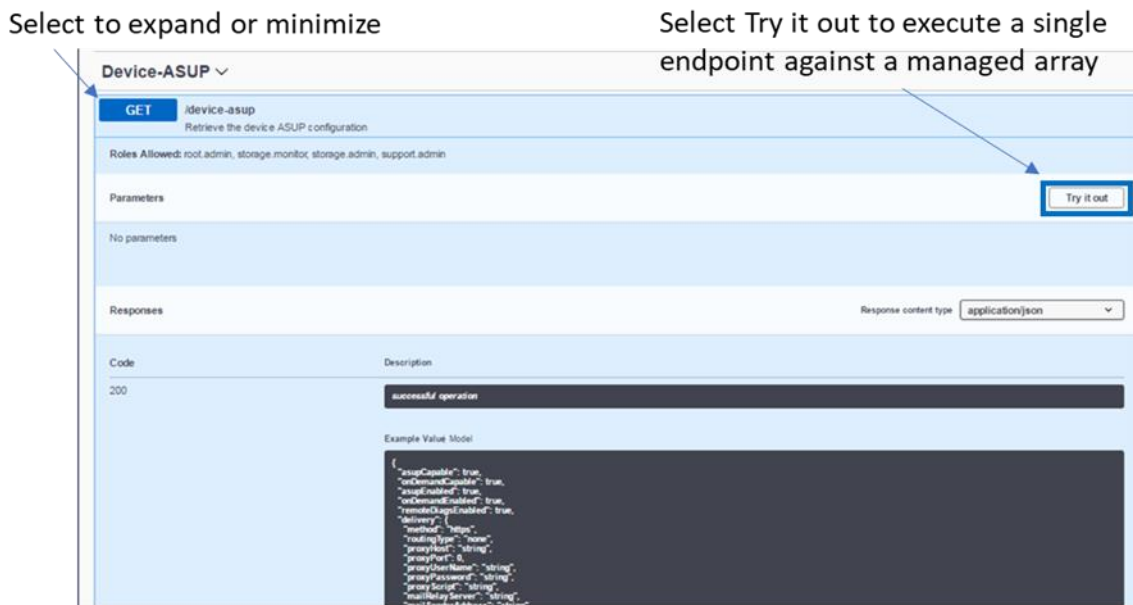
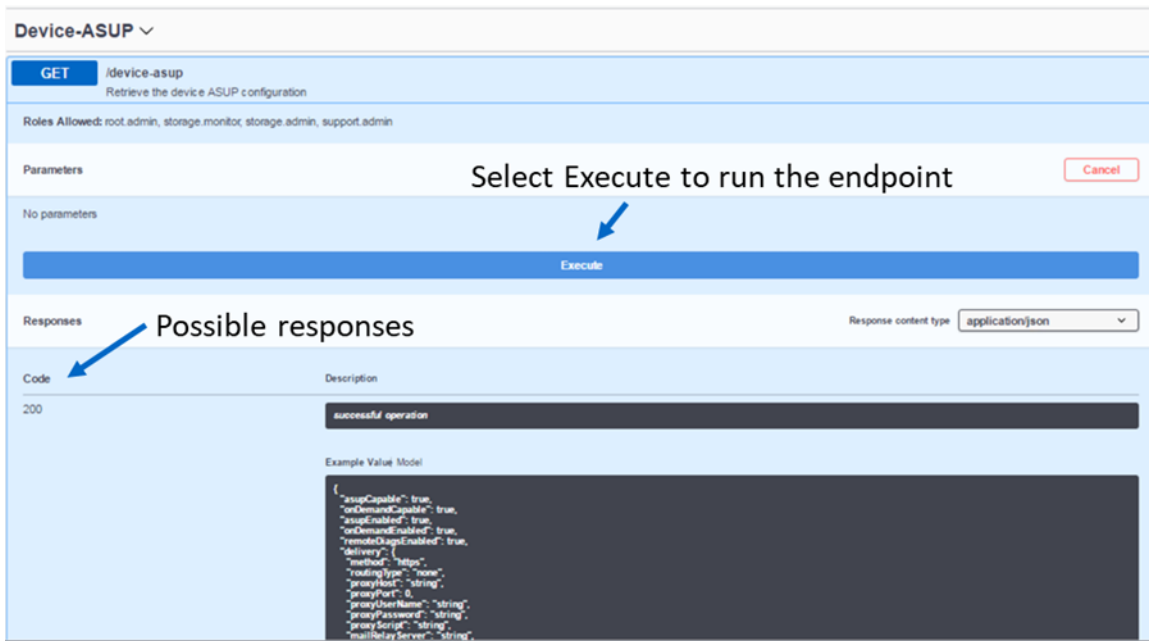


Figure 27) REST API documentation sample.



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

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

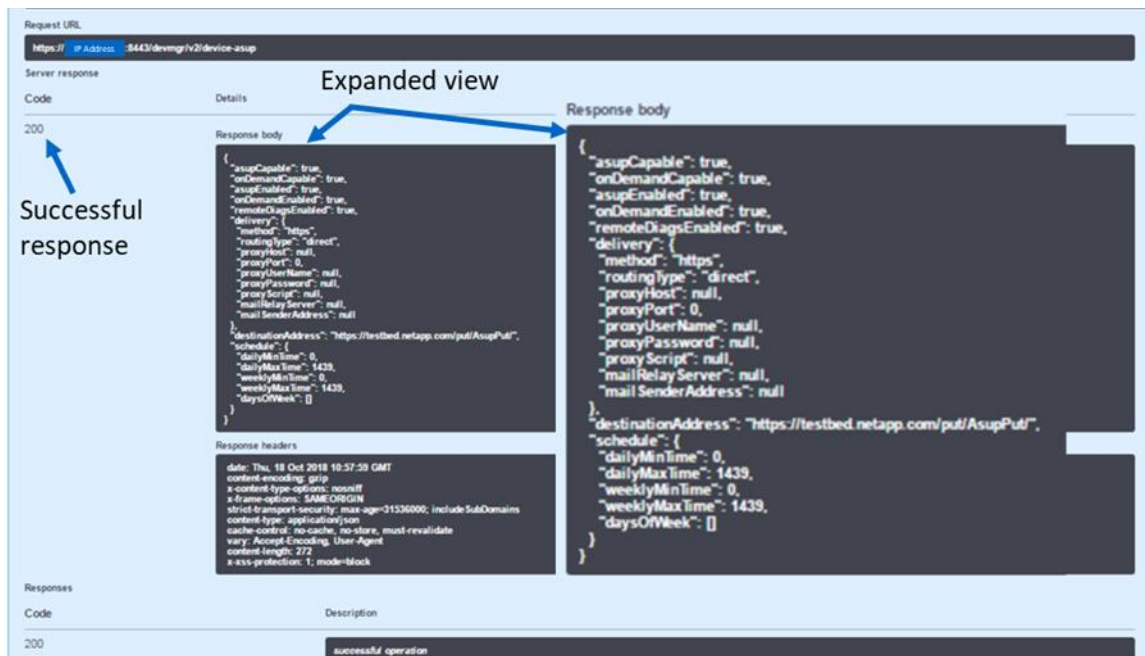


Figure 29) Device-ASUP endpoint possible response codes and details.

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,
  "remoteDebugEnabled": true,
  "delivery": {
    "method": "https",
    "routingType": "none",
    "proxyHost": "string",
    "proxyPort": 0,
    "proxyUser": "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.

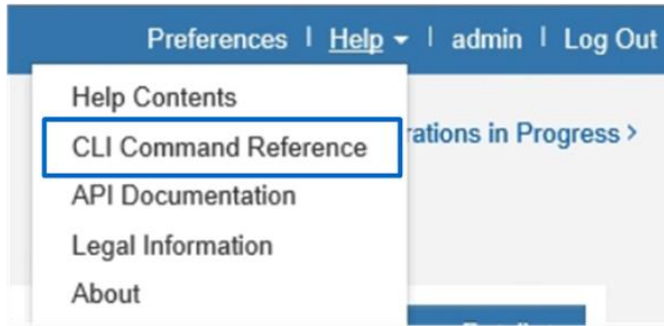
Downloading the CLI

- 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 DOS C: prompt.

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

Figure 30) Opening the CLI Command Reference.



SANtricity Storage Plugin for vCenter

The vSphere Client is a single management interface that you can use to manage the VMware infrastructure and all your day-to-day storage needs. The following functions are available in the 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 for performing certain storage administration tasks on a single array.

The plugin requires a VMware vCenter Server Appliance deployed in the VMware environment and an application host to install and run the plugin 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 OS specifications for EF300C hardware

Table 9 lists the NetApp SANtricity software specifications for NetApp EF300C-based storage systems.

Table 9) SANtricity OS boundaries for EF300C-based storage systems.

Components	Maximum
Storage hardware components	
Shelves	Only a single controller shelf is supported
Drives—drive slot count	24 QLC NVMe SSDs
Logical Components	
Host Partitions	256
Volumes per partition	256
Volumes per system	1,024
Disk pools per system	1

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 EF300C array
Maximum DDP single volume capacity	4PiB
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	1,024
Snapshot groups	
Per volume	4
Per system	1,024
Asynchronous mirrors	
Mirrors per system	64
Mirrors per volume	1
Mirrors per asynchronous mirror group	32
Asynchronous mirror groups per system	4

For additional software limits and specifications, see the [Hardware Universe](#).

Note: EF300C does not support thin provisioning.

Note: EF300C does not support synchronous mirroring.

EF300C hardware configurations

NetApp EF300C 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 EF300C shelf configuration.

EF300C controller shelf

The EF300C controllers are paired with the NE224 shelf. It is a two-rack-unit-high (2U) shelf that holds up to 24 2.5" NVMe SSDs. It features two RAID controllers, and two ENERGY STAR Platinum certified high-efficiency power supplies (1600W) with integrated fans.

Figure 31, Figure 32, and Figure 33 show the front and rear views of the EF300C controller shelf.

Figure 31) EF300C front view with bezel.

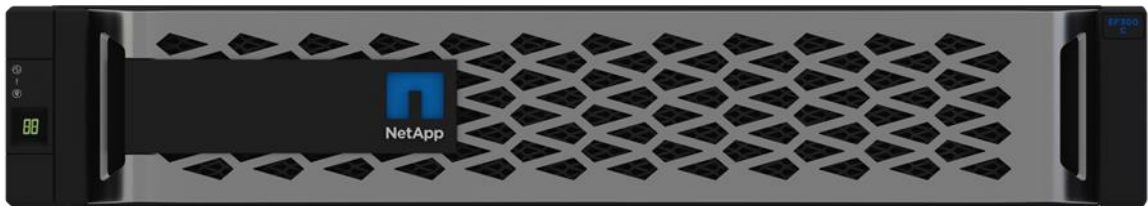


Figure 32) EF300C front view (open).



Figure 33) EF300C rear view.



EF300C hardware specifications

The EF300C controller has the following base hardware features:

- Ethernet port for management-related activities
- Dual 10GbE ports not used for E-Series
- Type-A USB port for factory use only is disabled

Table 10 lists the technical specifications for the EF300C-based storage systems.

Table 10) EF300C technical specifications.

Specification	EF300C
Maximum raw system capacity	1.474PB (24 x 61.4TB SSDs)
Maximum number of NVMe drives per system	24 NVMe SSDs
NE224 shelf form factor	2U, 24 drives
Memory	16GB per controller 32GB per duplex system
<ul style="list-style-type: none">• Single HIC per controller• Controllers must match.• Cannot mix host protocols.	<ul style="list-style-type: none">• 100Gb IB HIC (2 ports per controller) – supports NVMe/IB, NVMe/RoCE, SRP/IB, and iSER/IB• 25Gb iSCSI (4 ports per controller)

<ul style="list-style-type: none"> You can apply a software feature pack to convert between host protocols. See “Controller host interface features” for details. 	<ul style="list-style-type: none"> 32Gb FC HIC (4 ports per controller) – supports traditional FC as well as NVMe/FC
High-availability (HA) features	Dual active controllers with automated I/O path failover
	Support for DDP only
	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](#).

Controller host interface features

By default, the EF300C controller includes an Ethernet management port that provides out-of-band system management access.

The management port defaults to the Dynamic Host Configuration Protocol (DHCP). If you want to use static addresses to manage the EF300C, 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

Host interface ports can be added, as indicated in Table 11. Other than the 25Gb iSCSI HIC, each HIC supports multiple protocols.

Table 11) Available feature pack submodel IDs (FP-SMIDs) for EF300C controllers.

FP-SMID	HIC protocol
570	NVMe/FC, NVMe/RoCE or iSCSI
571	NVMe/FC or NVMe/IB
572	FC (not NVMe)
573	FC PTL (not NVMe)
574	iSER/IB
575	SRP/IB

For instructions on how to obtain and apply a software feature, see the [E-Series and EF-Series Systems Documentation Center](#). Go to the Upgrading → Hardware Upgrade section of the page, select Change or Add Host Protocols, and download the Converting EF300C Host Protocol document.

Table 12 provides port speed detail options.

Table 12) Host interface protocols and supported speeds.

HIC Protocol	Supported speeds
25Gbps iSCSI	25Gbps, 10Gbps
32Gbps FC	32Gbps, 16Gbps, 8Gbps
32Gbps NVMe/FC	32Gbps, 16Gbps, 8Gbps
100Gbps NVMe/IB	100Gbps, 56Gbps, 40Gbps

100Gbps NVMe/RoCE	100Gbps, 50Gbps, 40Gbps, 25Gbps, 10Gbps
100Gbps SRP/IB or iSER/IB	100Gbps, 56Gbps, 40Gbps

Note: NetApp does not sell IB cables; however, cables are readily available from suppliers such as NVIDIA Mellanox and QLogic.

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 EF300C 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 34.

Figure 34) EF300C controller HIC options.

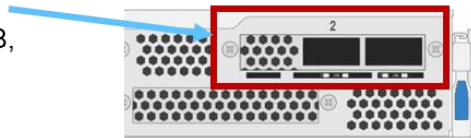
FC or iSCSI HIC – see icon

- 4-port 25Gb iSCSI
- 4-port 32Gb FC (use for NVMe/FC and traditional FC)



100Gb IB HIC

- 2-port 100Gb IB (use for NVMe/IB, NVMe/RoCE, SRP/IB, iSER/IB)



Hardware LED definitions

EF300C controller shelf LEDs

The EF300C 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 35 shows the ODP of the EF300C controller shelf.

Figure 35) ODP on front panel of EF300C controller shelf.

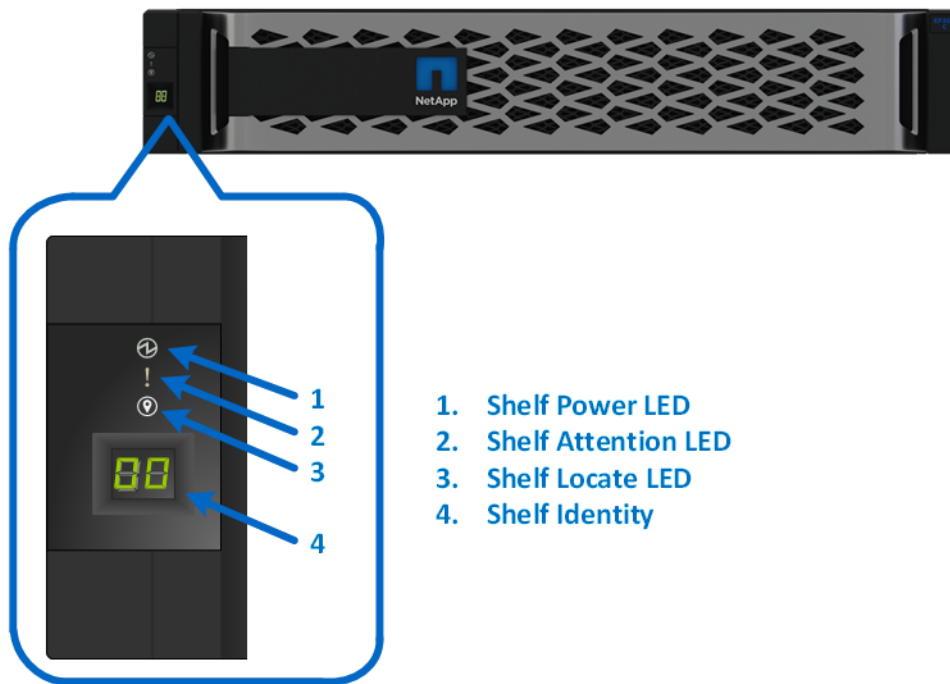


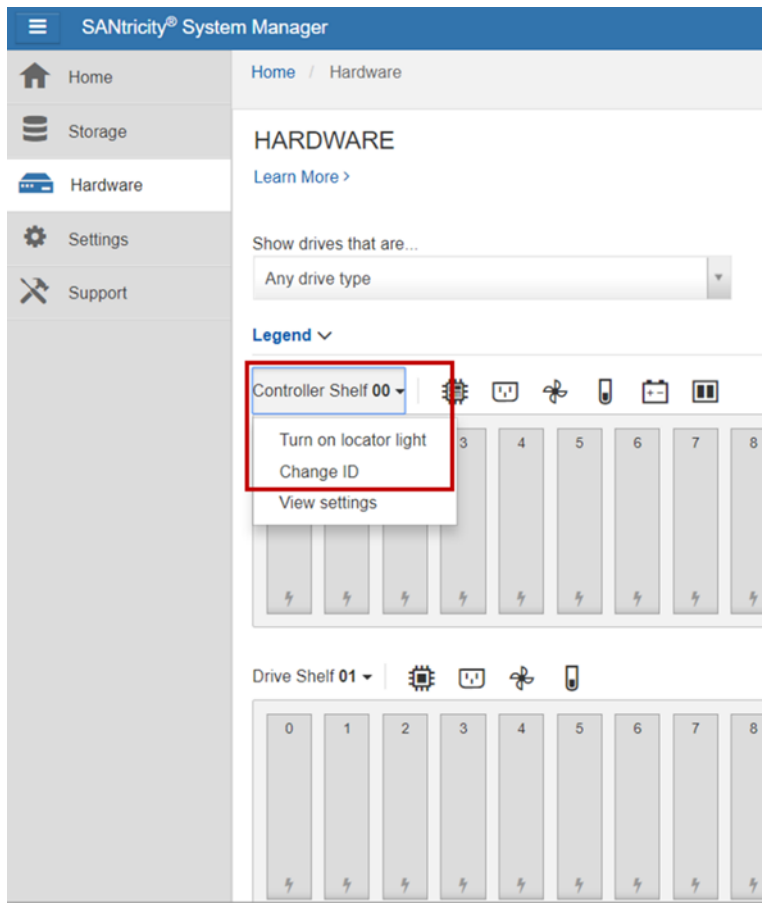
Table 13 defines the ODP LEDs on the EF300C controller shelf.

Table 13) EF300C controller shelf LED definitions (front panel).

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

The shelf-identity feature displays a numerical value to identify the shelf. The dual seven-segment display indicates values from 00 to 99 that can be set from the NetApp SANtricity System Manager Hardware tab shown in Figure 36.

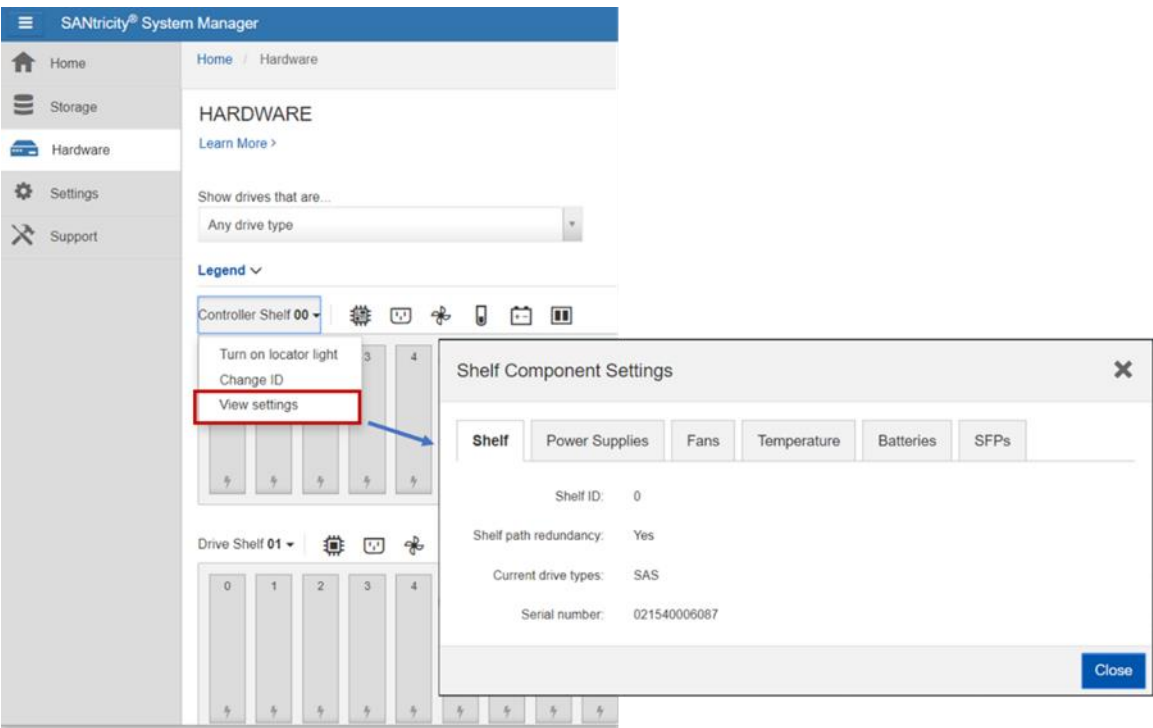
Figure 36) Setting the shelf ID by using SANtricity System Manager.



EF300C controller canister LEDs

The EF300C 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 or by using the SANtricity System Manager GUI. For example, systemwide status information is displayed on the View Settings page, as shown in Figure 37.

Figure 37) Viewing system status information by using SANtricity System Manager.



LED definitions with 4-port HIC installed

The EF300C controller supports an optical 4-port 25Gbps iSCSI HIC, an optical 4-port 32Gbps FC and NVMe/FC HIC, and a 2-port 100Gbps IB HIC for NVMe/IB, NVMe/RoCE, SRP/IB, and iSER/IB. Figure 38 shows the LEDs for the 4-port HIC option; the 2-port HIC option is similar.

Figure 38) LEDs on the EF300C with 4-port HIC.

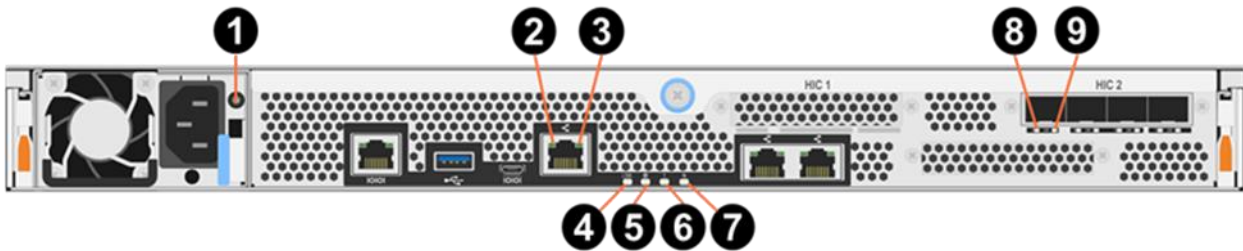


Table 14 defines the LEDs for the 4-port HIC.

Table 14) EF300C with 4-port 32Gb FC HIC LED definitions.

Call-out	LED name	Color	LED description
1	PSU	Green/Red	<ul style="list-style-type: none">LED off: no AC powerGreen: AC present and DC output OKRed: AC cord unplugged or power supply failure
2	Link	Green	<ul style="list-style-type: none">LED on: link upLED off: link down

3	Activity	Green	<ul style="list-style-type: none"> Blinking: indicates activity for the Ethernet port
4	NV LED	Green	Defaults to on at power-up. Software turns off this LED during boot. On indicates that battery backup has been enabled to support caching activity.
5	Locate LED	Blue	<ul style="list-style-type: none"> On: identifies enclosure Off: not locating enclosure <p>Note: During power-up, this LED is on initially, but it will turn off after boot-up process is complete</p>
6	Attention LED	Amber	<ul style="list-style-type: none"> On: direct attention to the controller for service event Off: no issues on controller <p>Note: During power-up, this LED is on initially, but it will turn off after boot-up process is complete (if no issues are indicated).</p>
7	Activity LED	Green	<ul style="list-style-type: none"> Blinking: activity on controller
8	Attention LED	Amber	<ul style="list-style-type: none"> On: a condition that requires attention Off: no special conditions
9	Link LED	Green	<ul style="list-style-type: none"> On: link up Off: no link

Note: LED definitions with alternate HIC options are similar.

For more information about the EF300C storage systems and related hardware, see the [E-Series and SANtricity 11 Resources page](#).

Drive LED definitions

Figure 39 shows the LEDs on the drive carriers for the NVMe SSDs. The NE224 shelf in the EF300C architecture supports only 2.5-inch form-factor SSDs.

Figure 39) NVMe drive carrier LEDs.

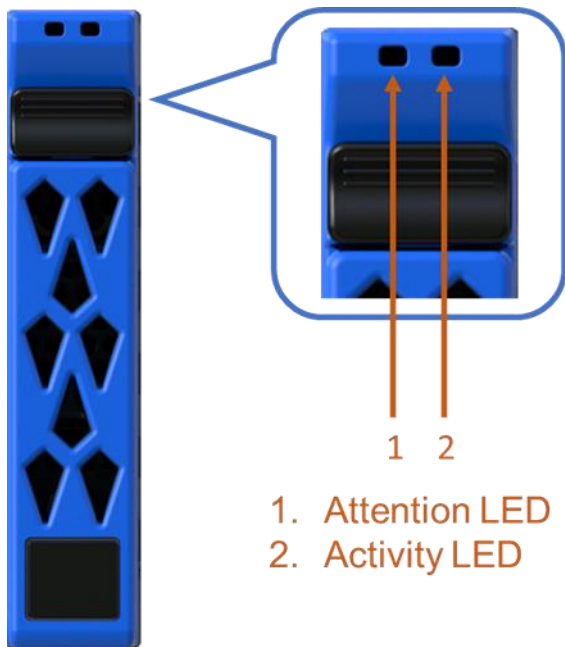


Table 15 defines the LEDs for the drives.

Table 15) 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

Drive loading for maximum performance

With the release of the NE224 shelf, the process by which drive slots are assigned to the PCIe bus has changed. In previous versions of EF-Series, alternate drive slots were assigned to a different PCIe bus. With the EF300C and EF600C arrays, the first PCIe bus is connected to the drive slots 0 through 11, the first 12 drive slots; and the second PCIe bus is connected to drive slots 12 through 23, the second 12 drive slots.

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

Note: Storage system performance can be significantly reduced if drives are not loaded such that both PCIe buses are employed.

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

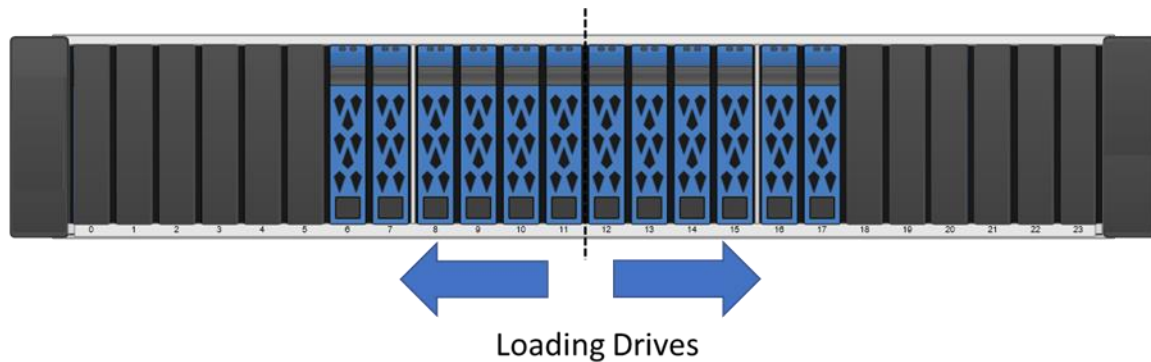
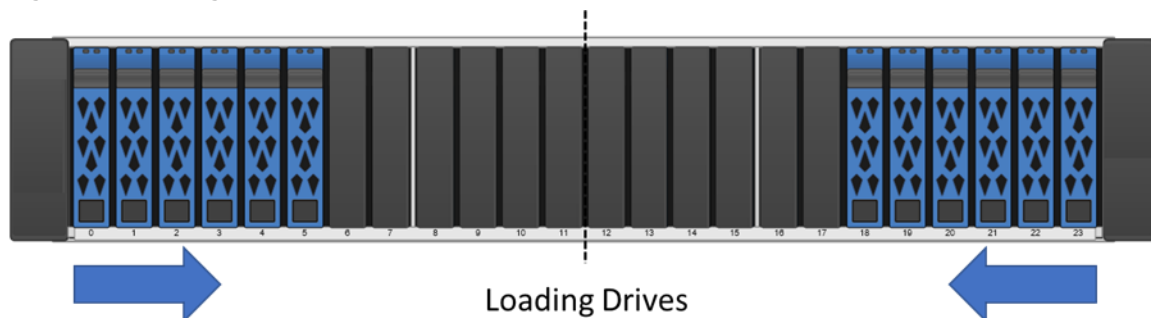
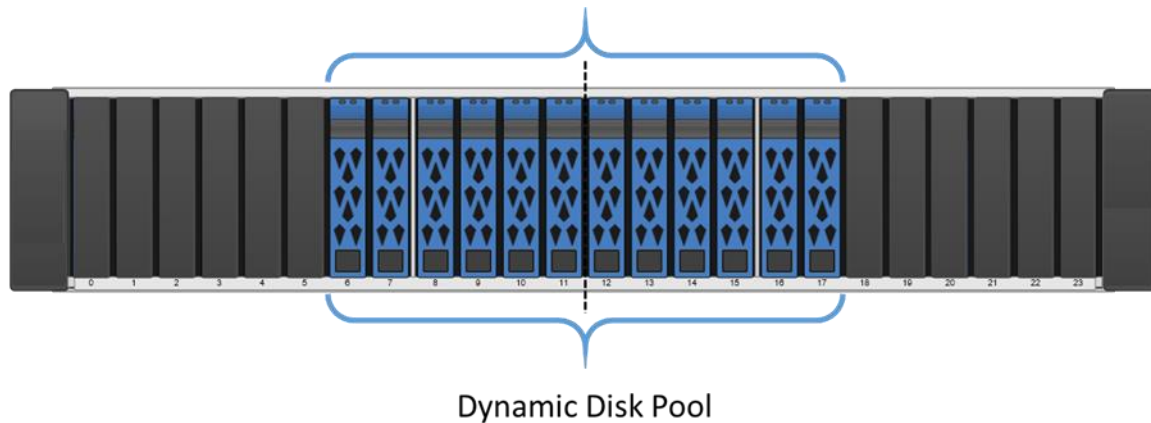


Figure 41) Loading drives from the outside drive slots inward.



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, 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.



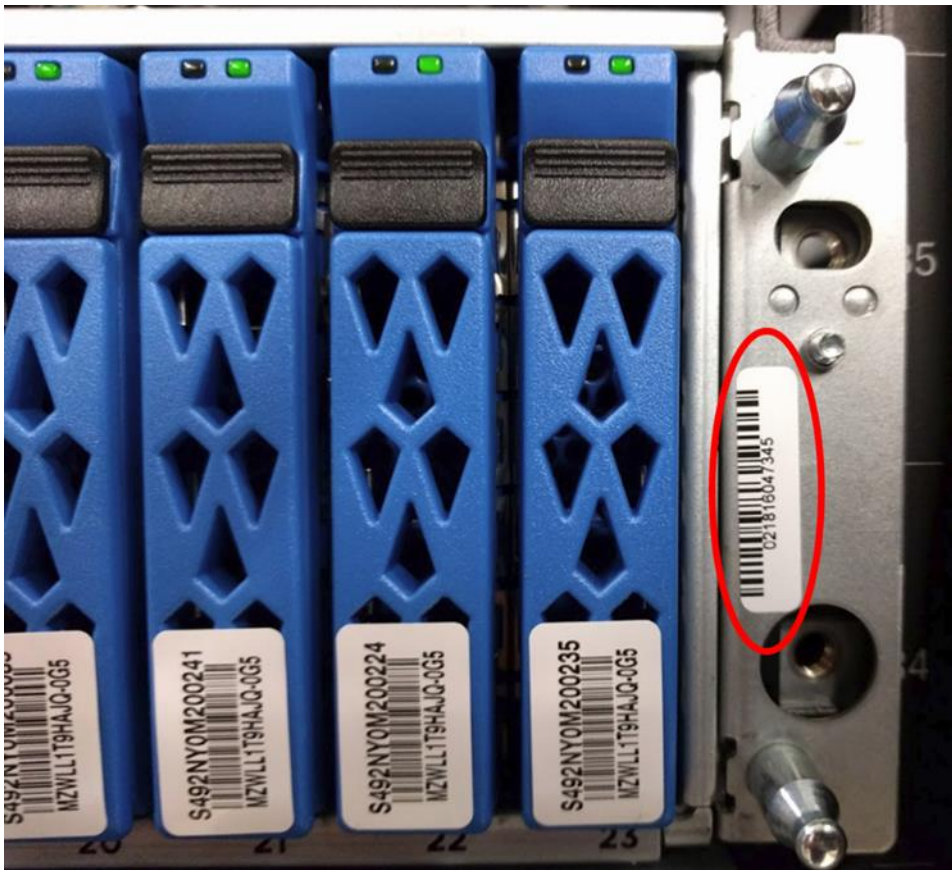
E-Series product support

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 EF300C 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 SN is circled in red on Figure 43.

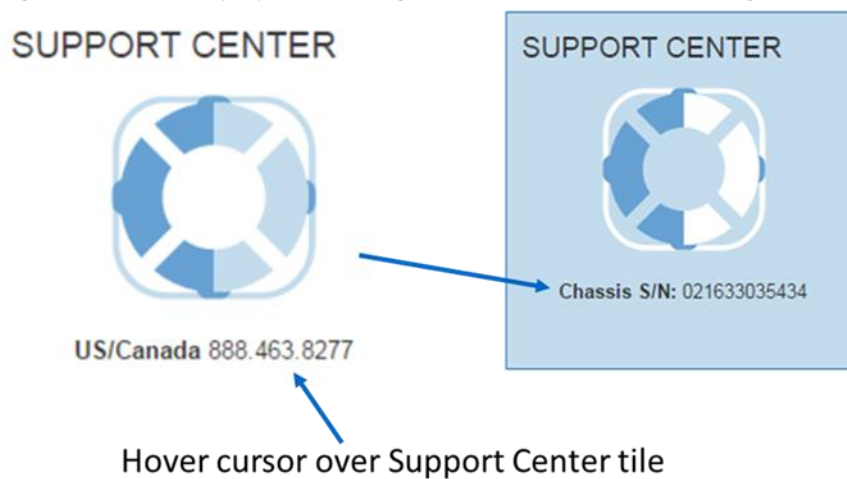
Figure 43) Controller shelf SN.



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

On a running storage system, you can also find the chassis serial number through NetApp SANtricity System Manager by selecting the Support tab and positioning your cursor over the Support Center tile, as shown in Figure 44.

Figure 44) SANtricity System Manager Support Center tile showing chassis serial number.



License keys

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

For the EF300C system, there are currently no premium features. All features are enabled out of the box.

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

The feature pack keys are used to change the protocol on IB HICs between NVMe/IB and NVMe/RoCE and between FC and NVMe/FC on FC HICs. The process to generate a new feature pack key for your storage array is almost the same as the process to generate 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 11 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 45. Follow the prompts, beginning with browsing to the feature pack file, as shown in Figure 46.

Figure 45) Changing the feature pack from Settings > System view.

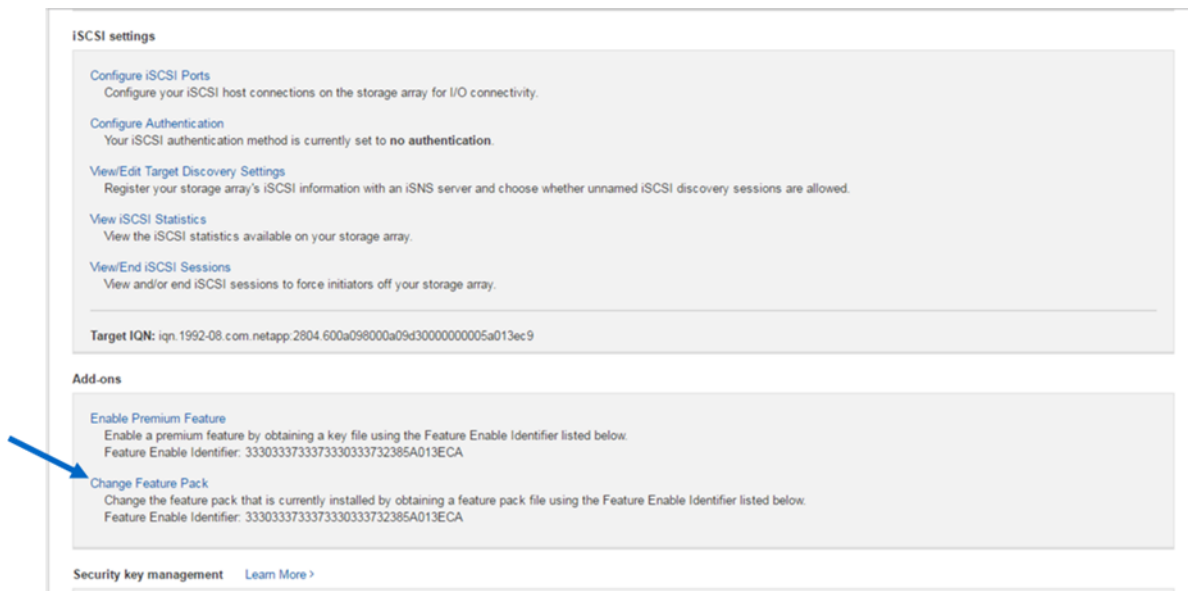


Figure 46) Change Feature Pack option.

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: [Browse...](#)

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.

Type change

[Change](#) [Cancel](#)

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

NetApp EF-Series with high-capacity flash drives broadens the abilities of the array to manage more use cases. The additional capacity enables the EF300C array to store an application backup or provide a cold tier for an application such as Splunk.

This core block storage system provides the fast, affordable high-performance and high-density options required for demanding block workloads such as media and entertainment, HPC/AI, and high-performance databases.

With high-capacity NVMe SSD drives, the newest EF-Series systems will improve operational efficiency, help accelerate the transition from E-Series HDD-based systems to high-capacity flash and meet increasing capacity needs without compromising performance or reliability.

The EF300C storage systems provide extreme throughput performance with fast host interfaces and can offer up to 1.5PB of raw NVMe SSD capacity in only 2U with 24 60TB drives to support fast, large-capacity applications. The EF300C is also available with 30TB NVMe drives.

For high-random IOPS environments, the EF300C supports up to 350,000 4KB read IOPS. For high-bandwidth workloads, it supports approximately 7GBps cache-mirrored sequential writes and up to 20GBps sequential reads.

With its extreme versatility—including multiple host interface choices—the EF300C is a modern, ready-to-work, NVMe all-flash storage system. The addition of NVMe/IB, NVMe/RoCE, and NVMe/FC makes the EF300C a truly new-generation NVMe all-flash array. The EF300C 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:

- EF-Series All-Flash Arrays
<https://www.netapp.com/data-storage/ef-series/>
- E-Series and SANtricity 11 Documentation Center
<https://docs.netapp.com/ess-11/index.jsp>
- SANtricity software documentation 11.90
<https://mysupport.netapp.com/info/web/ECMP1658252.html>

Version history

Version	Date	Document version history
Version 1.0	February 2025	Initial release of EF300C array.

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

Copyright information

Copyright © 2025 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data—Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

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

TR-5004-0125