Technical Report

Introduction to NetApp EF-Series EF280

Feature Overview with SANtricity OS 11.40.2

Mitch Blackburn, NetApp
May 2018 | TR-4685

Abstract

The new NetApp® EF280 all-flash array delivers high performance in an entry-level EF-Series array. This report provides detailed information about the multiple system configuration options of NetApp SANtricity® OS 11.40.xx, including an overview of the embedded management software, SANtricity System Manager. It is also a great starting point to introduce EF280 system details to sales engineers, partners, service providers, and customers.

NetApp®

TABLE OF CONTENTS

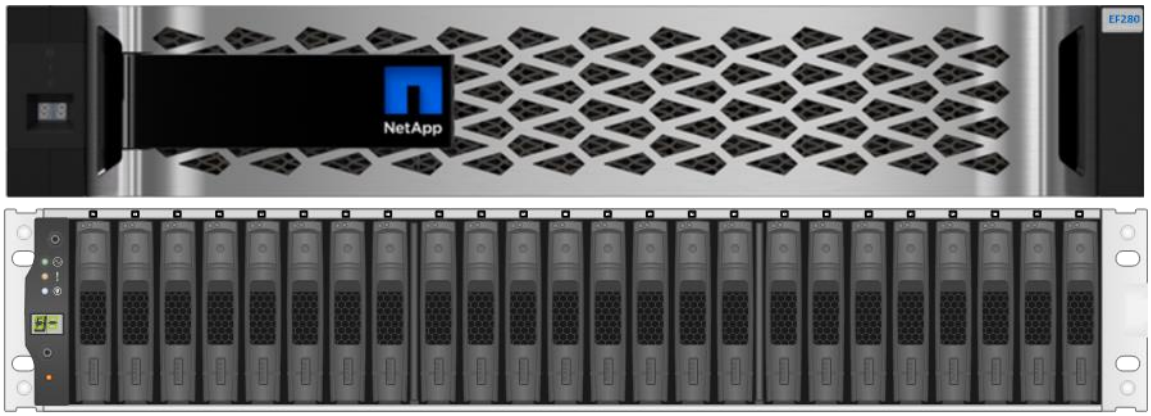
LIST OF TABLES

LIST OF FIGURES

1 Introduction

The NetApp EF280 has the same modern look as the new EF570, leverages the new 12Gbps DE224C drive shelves (Figure 1), and supports a more secure UI. In one powerful all-flash array package, it delivers exceptional performance for both mixed random workloads and large sequential workloads.

Figure 1) New-generation NetApp EF280 all-flash array with bezel on and off.



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

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

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

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

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

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

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

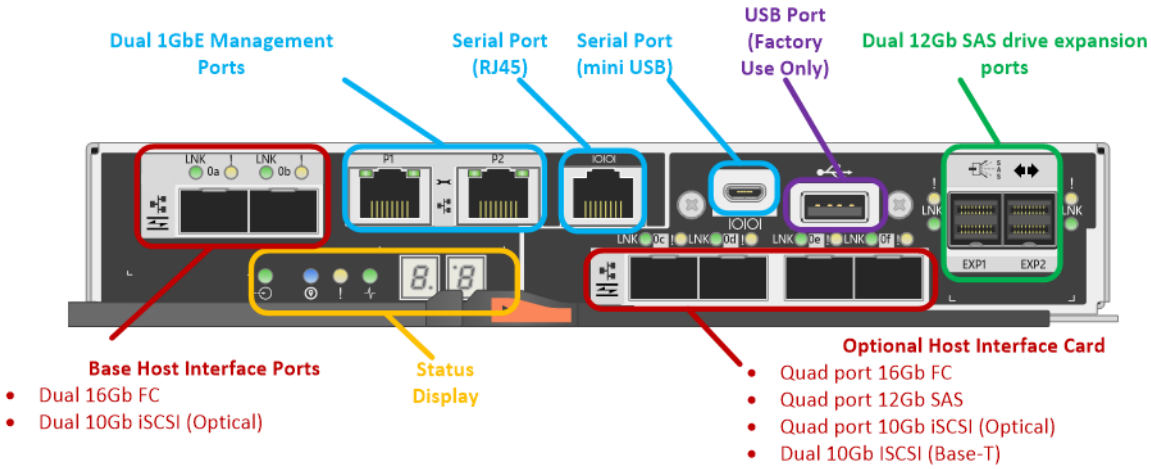
Note: A software feature pack can be applied in the field to change the host protocol of the optical baseboard ports and the optical HIC ports from FC to iSCSI or from iSCSI to FC.

- 2-port 10Gb iSCSI (Cat6e/Cat7 RJ-45)

Note: If the base ports on the controller are configured with 10Gb iSCSI RJ-45, then the only HIC option supported is the 2-port 10Gb iSCSI (Cat6e/Cat7 RJ-45).

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

Figure 2) EF280 controller with ports identified.



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

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

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

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

In fact, some of the world's largest online transactional workloads run on EF-Series arrays because these arrays are blazing fast, simple to install and operate, and extremely reliable (99.9999% data availability). These highly flexible SAN building blocks can be applied when you need them and can be plugged into your current application environment on demand. EF-Series arrays can operate in a space as small as 2 rack units (RU), seamlessly integrate with many software layers, and still deliver consistent low-latency performance. These capabilities make EF-Series an optimal SAN building block for any size enterprise that supports demanding online customer transactions.

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 EF280 maintains its performance profile as systems scale up to 96 SSDs or four total shelves. 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, making EF-Series arrays easy to deploy regardless of your workload.

EF280 arrays use the new-generation, web-based SANtricity System Manager GUI that is bundled with SANtricity OS 11.40/11.40.2. 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 custom API-driven environment. For individual array management, the onboard web services API is an optimal way to configure an array as a bundled appliance in a third-party solution package.

The following sections provide broad product information about the new SANtricity OS 11.40/11.40.2 features that improve operational security and SSD wear-life monitoring. They also describe the new host path management capabilities that improve the overall operation and stability of the storage system.

2 SANtricity OS Features

EF280 arrays are new with the NetApp SANtricity OS 11.40.2 release, but there are also significant software enhancements in the release that apply to all the new-generation E-Series arrays, including the E2800, E5700, and EF570 arrays. An onboard web-based GUI manages these arrays: SANtricity System Manager.

2.1 SANtricity OS 11.40 Feature Additions and Changes

- Support for directory services using Lightweight Directory Access Protocol (LDAP)
- Support for role-based access control (RBAC): five standard roles defined with varying permission levels
- Support for certification authority (CA) and Secure Sockets Layer (SSL) certificates
- Implemented a secure CLI: secure when the certificates are installed
- Added support for an external encryption key manager in addition to the legacy E-Series drive security onboard encryption key manager
- Security enhancements 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 using API, the new security features can be disabled by the admin user when the storage system is initially set up.

In addition to LDAP and RBAC, there are also enhancements to our most used host multipath functionality that were released in previous SANtricity OS maintenance releases and are now part of the SANtricity OS 11.40 GA release.

2.2 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. These definitions in turn are used by many devices in a network infrastructure to identify and to authenticate users who are 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. The combination of authenticating a user with your LDAP server, then having specific permissions on the array side, enables SANtricity OS 11.40/11.40.1 to provide the management access granularity our customers require.

Setting Up the Directory Server and Roles

Directory servers, like most data center devices, are complex and designed to fulfill many use cases, but the E-Series LDAP/RBAC implementation focuses on authentication and two main elements: users and groups. Like most applications, there are several acronyms to understand and conventions that must be followed to set up communications between the E-Series array and the directory server. The most critical acronyms to understand include:

- CN: `commonName` used to identify group names as defined by the directory server tree structure
- DC: the network `domainComponent` where user and groups exist (for example, netapp.com)

- DN: `distinguishedName`: the fully qualified domain name made up of one or more common names separated by commas followed by one or more domain components that are also comma separated (for example, CN=functional_group_name, CN=users, DC=netapp, DC=com)

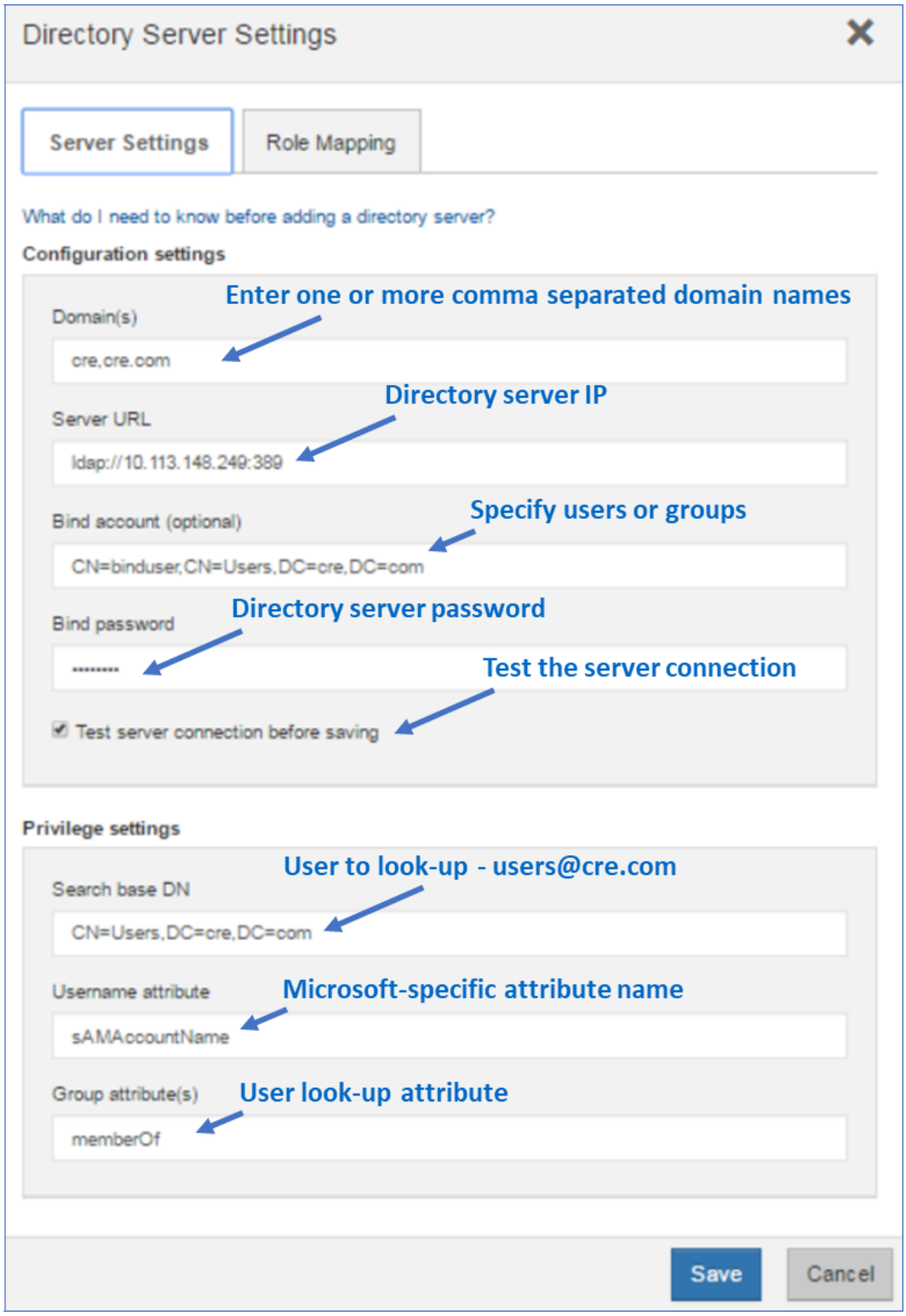
Given that E-Series follows a very standard web server implementation on the controllers, all the general directory services setup knowledge is well documented in many articles on the web. As a result, setting up the service on E-Series is relatively easy and only requires a few pieces of information, as shown in Table 1.

Table 1) SANtricity OS 11.40 LDAP/RBAC required fields and definitions.

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

Figure 3 shows an example Microsoft Active Directory (AD) server integration with SANtricity System Manager 11.40. The entries shown are all examples, except user name attributes and group attributes in the privileges section. Those items are standard entries for Windows and not likely to change for most implementations.

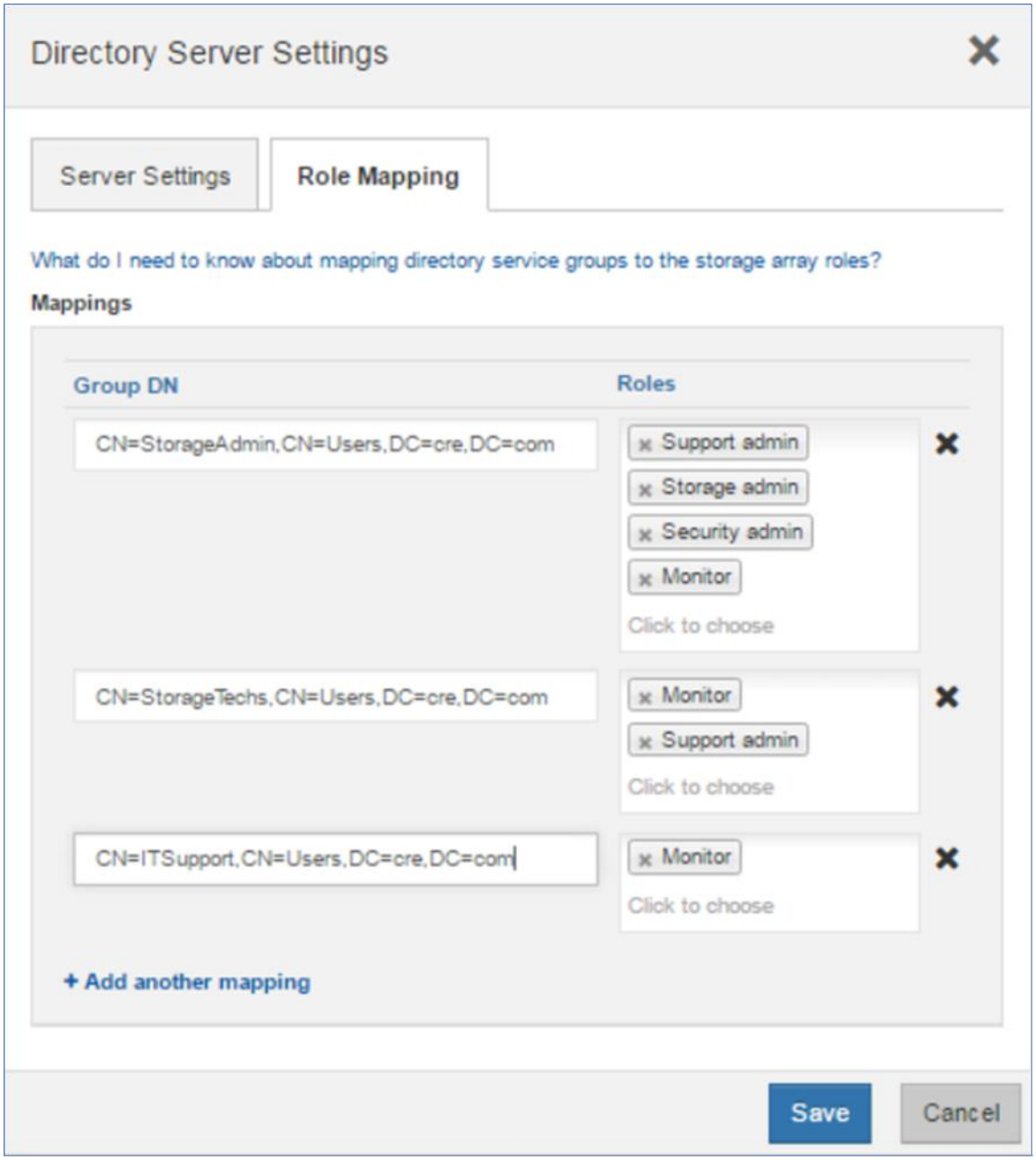
Figure 3) SANtricity System Manager Directory Server Settings wizard.



The array roles for the specified user groups are set in the Role Mapping tab. For the example shown in Figure 4, users who are members of the StorageAdmin, StorageTech, 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 based on the permissions granted.

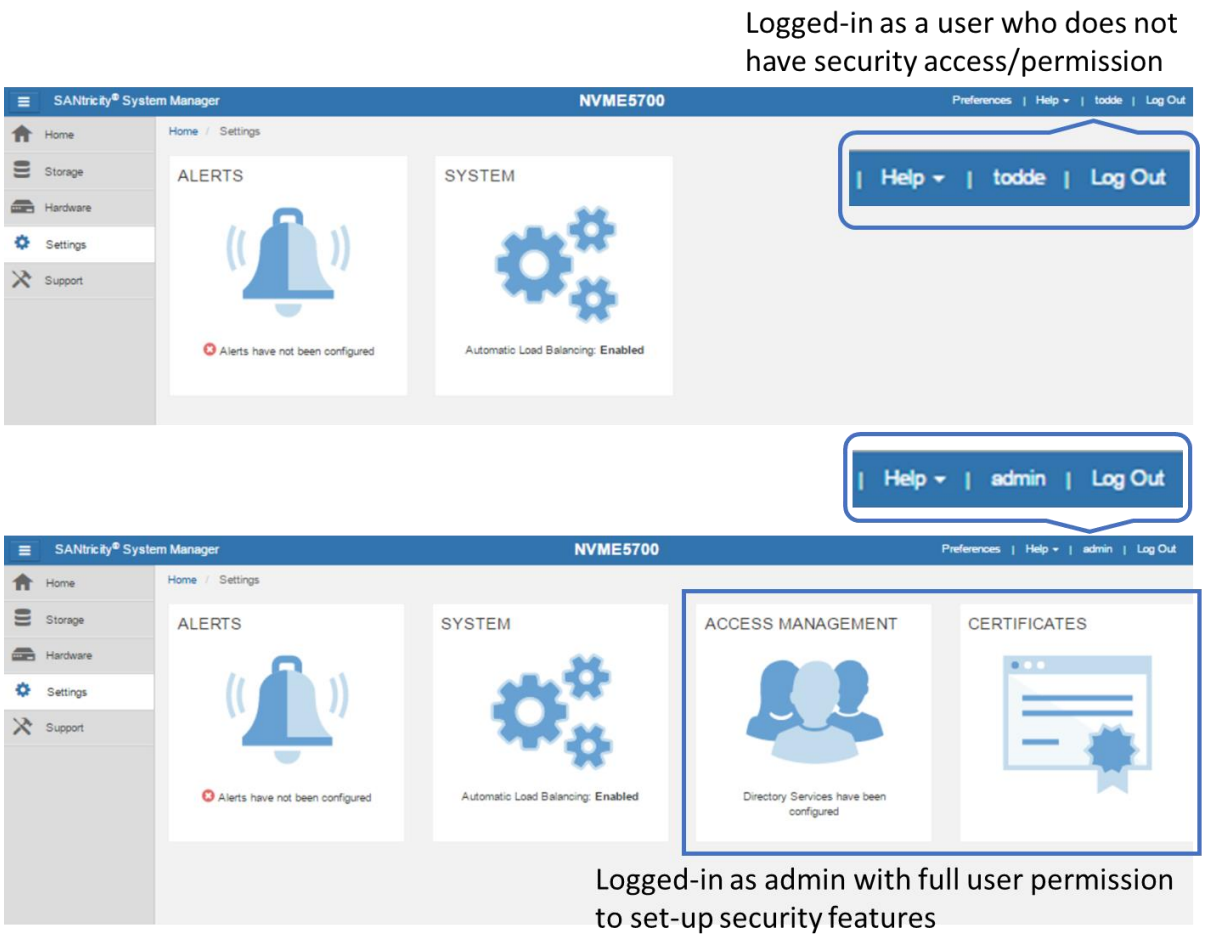
Figure 4) Role Mapping tab in the Directory Server Settings wizard.



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 5 shows the difference in user views and access to features based on access permission level. The login on top provides monitor and support access, but it does not provide security access like the second group mapping in Figure 4.

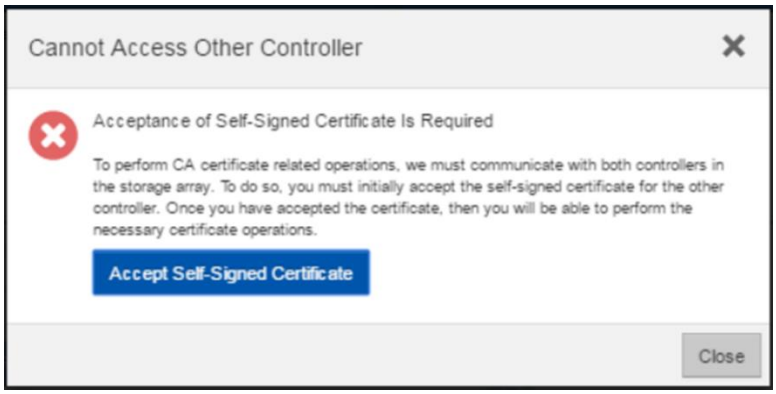
Figure 5) SANtricity System Manager views change based on the user permission level.



SANtricity Web Server Security Certificates

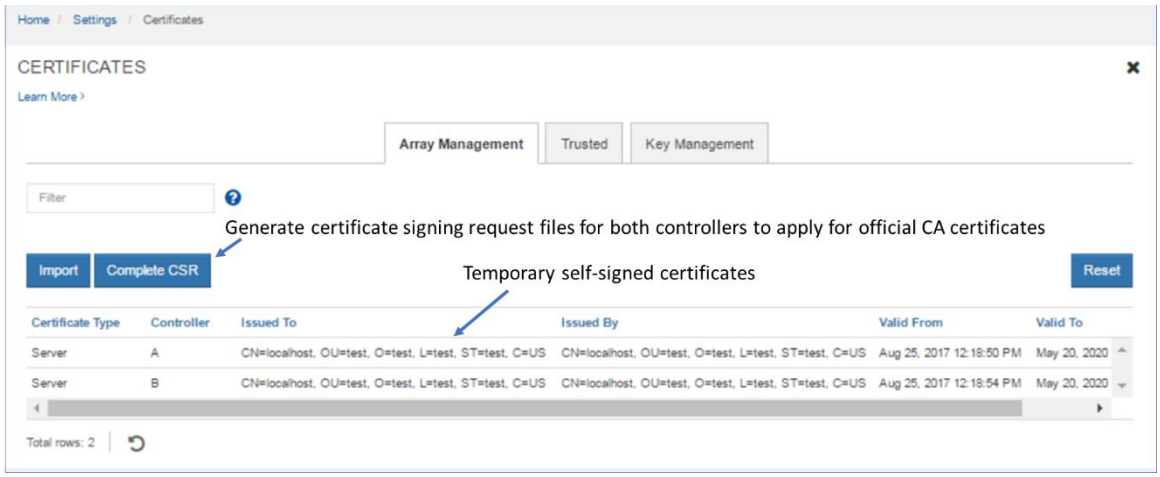
In addition to authentication and access control, SANtricity OS 11.40 supports standard CA certificates. This feature enables secure communications (SSL/TLS) between browser clients and the E-Series built-in web servers on the controllers. On new EF280 arrays, the SANtricity System Manager web-based GUI is accessed through one of the two controllers instead of both controllers simultaneously like the legacy SANtricity Storage Manager application. As a result, all communication to the other controller in the EF280 array is carried out 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 between them, both controllers must present a self-signed certificate to the other controller. This process happens automatically when the admin or security user logs in to each controller and opens the Certificates tile. Figure 6 shows the pop-up menu that is displayed the first time the tile is opened.

Figure 6) Initial step that is required to set up web server certificates.



You must select the link to accept the self-signed certificate to proceed with setting up additional certificates. The process takes you to another webpage, where the self-signed 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. At this time, both controllers are displayed with valid local host certificates, as shown in Figure 7.

Figure 7) SANtricity System Manager Certificates tile expanded.



To enable the E-Series onboard web servers to validate new CA certificates, the controllers are preloaded with industry-standard CA root certificates. The standard root certificates can be viewed by selecting the Trusted tab in the Certificates tile window shown in Figure 7 and then selecting show preinstalled certificates from the drop-down menu. To complete the setup, use the Complete CSR (certificate signing request) wizard to create a certificate request file. Send the file to a certificate authority when requesting a new official certificate for each controller.

When external key management has been enabled from the Settings tile, use the Key Management tab to generate a CSR file for the key server communications. Import the client certificate using the Key Management tab to enable secure communications between the E-Series controllers and the external key management server. See the E-Series online help center and TR:4474: NetApp SANtricity Drive Security - Feature Details Using SANtricity OS 11.40 for additional information about support for an external key manager.

2.3 ALUA and TPGS Support with Implicit Path Failover

When considering the elements of E-Series multipath functionality, two concepts are important to understand. The first is controller-to-volume ownership and how path failover between controllers is managed using asymmetrical logical unit access (ALUA). This scenario is when the primary paths to an E-Series volume (I/O paths through the owning controller) are lost. The second element of managing multiple paths is how the multipath driver on the host interacts with the multiple ports on each E-Series controller (target port group support [TPGS]) to spread I/O across the interfaces and maximize performance. The following sections provide a brief explanation of each. See TR-4604: Clustered File Systems with E-Series Products: Best Practices for Media and Entertainment Customers for a deep explanation of E-Series multipath behaviors.

ALUA with TPGS

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

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

These attributes allow host multipath drivers to spread I/O across a set of ports on each controller that are associated to the volumes owned by that controller (TPGS) using path policies such as least queue depth and round robin. Depending on the host operating system, the default path policy varies between 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 the affected controller is routed to ports on the nonowning E-Series controller, where it is shipped across the shelf midplane to the controller that owns the volumes. In parallel, an ALUA timer is set, and changes in controller-to-volume ownership are delayed until the timer expires. This delay time is long enough for one or more links to reset and return to service (default is 5 minutes). When the ALUA timer expires, the array decides whether to initiate a change of volume ownership to the peer controller based on whether the nonowning controller is still receiving >75% of the I/O destined for the other controller.

Recent improvements to some of the SANtricity host types with respect to multipath functionality now enable implicit path failover with path failback based on enhanced decision making on the array controllers for SANtricity host types indicated in Table 2.

Table 2) SANtricity host types and associated failover behavior in SANtricity OS 11.40.

Host Type	ALUA/AVT Status	Implicit Failover	Implicit Failback	Automatic Load Balance
Linux device mapper multipathing (kernel 3.10 or later)	Enabled	Supported	Supported	Supported
VMware	Enabled	Supported	Supported	Supported

Host Type	ALUA/AVT Status	Implicit Failover	Implicit Failback	Automatic Load Balance
Windows	Enabled	Supported	Supported	Supported
Windows cluster	Enabled	Supported	Supported	Supported
ATTO cluster (all OSs)	Enabled	Supported	Not supported	Not supported

The multipath enhancements are particularly helpful in clustered host environments where one host in the cluster could experience a path fault and cause the back-end storage to change LUN ownership (explicit failover method), while other hosts in the cluster try to change ownership back to the original state. The result can be rapid thrashing of volume ownership between the two E-Series controllers. The updated, storage-led path management logic helps stop one host in a cluster with path issues from affecting all the hosts in the cluster. As a result, NetApp recommends using host types listed in Table 2 that support implicit path failover.

2.4 SANtricity OS 11.40.1 Feature Additions and Changes

Three significant changes were introduced with SANtricity OS 11.40.1:

- Expanded list of common workload tags
- Improved SSD wear-life tracking and reporting
- Expanded Dynamic Disk Pool (DDP) allowable maximum capacity per array

The following sections provide a brief explanation of each item.

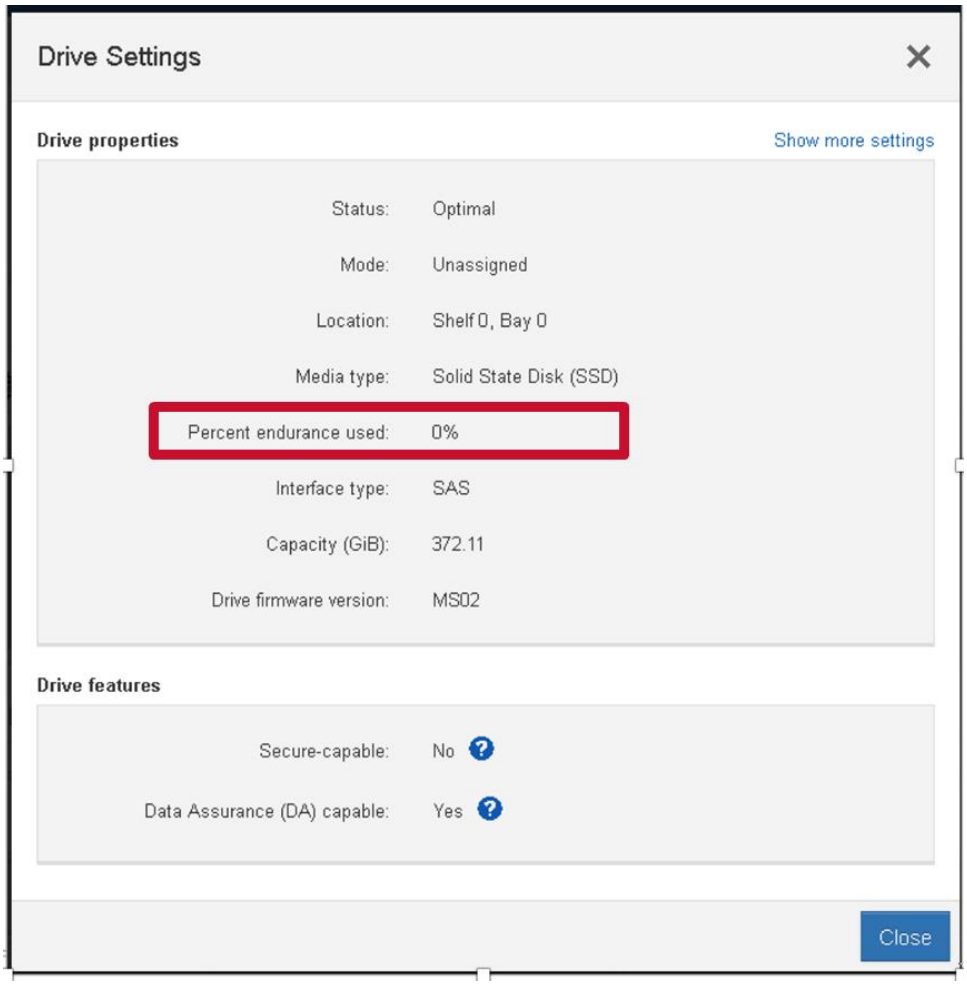
New Volume Workload Tags

SANtricity OS 11.40.1 improved the user experience with more default volume workload tagging options that further simplify capacity management. These workloads are presented to storage administrators as an expanded list of common data center workloads from which administrators can choose when provisioning volumes on E2800 storage by using the SANtricity System Manager GUI. If your workload is not in the default workload list, you can still create a custom workload to match any specialty requirements.

SSD Wear-Life Tracking and Reporting

In addition, a new SSD wear-life tracking metric has been added to the Drive Settings dialog box. The new metric clearly 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 OS. Figure 8 shows the Drive Settings dialog box with the new, easy-to-understand wear-life indicator percent endurance used.

Figure 8) A simplified SSD wear-level indicator is new in SANtricity OS 11.40.1.



In addition to clearly indicating the SSD life span in the Drive Settings dialog box, a new informational event log is raised when an SSD reaches 90% of its life span. The SANtricity Recovery Guru also provides an alert at 95% drive-life utilization, indicating that an SSD is nearing the end of its life.

DDP Capacity Limits

DDP capacity limits cover two categories. One is the maximum volume size in a single pool, and the other is the maximum total capacity associated to all pools in a storage array. These limits have grown over time, and SANtricity OS 11.40.1 further extends the DDP maximum total capacity limit from 2PiB to 6PiB. This capacity includes RAID overhead, drive space reserve capacity, a DDP-specific overhead, and a small additional overhead based on multiple pool factors. The maximum standard, thick volume capacity remained unchanged at 2PiB.

Note: The current maximum volume capacity for a thin-provisioned volume is 256TiB. See Table 11 for additional software specification details.

2.5 SANtricity OS 11.40.2 Feature Additions and Changes

Several new security enhancements and additional usability features have been added in SANtricity OS 11.40.2 for E2800 and other latest generation E-Series arrays:

- **Authentication with Security Assertion Markup Language (SAML) 2.0 to support multifactor authentication (MFA).** Authentication can be managed through an identity provider (IdP) 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. See Multifactor Authentication, later, for further information.
- **Digitally signed firmware.** The controller firmware verifies the authenticity of any downloadable SANtricity firmware. Digitally signed firmware is required in version 8.42 and later. If you attempt to download unsigned firmware, an error is displayed, and the download is aborted.
- **Certificate revocation checking using Online Certificate Status Protocol (OCSP).** Certificate management includes certificate revocation checking using an OCSP server. The OCSP server determines if the certificate authority (CA) has revoked any certificates before their scheduled expiration date and 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 (EKMS), Lightweight Directory Access Protocol over SSL (LDAPS) server, or syslog server. Configuration tasks are available from Settings > Certificates and require security admin permissions.
- **Syslog server configuration for audit log archival.** 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.

Other enhancements include:

- **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 case with Support if there is an issue. The options for enabling and disabling the AutoSupport Maintenance window are available from Support > Access Management > AutoSupport tab.
- **Host connectivity enhancements.** For all host types that support automatic load balancing (ALB), host connectivity reporting can now be enabled or disabled independent of the ALB feature. This feature can be useful in specific, highly tuned environments where ALB movement is not desired, but connectivity reporting is useful. When enabled (the default), host connectivity reporting monitors the connection between the controllers and the configured hosts and then alerts you if the connection is disrupted. When disabled, this feature suppresses Recovery Guru messages regarding host connectivity. Host connectivity reporting is available from Settings > System > Additional Settings.

2.6 Multifactor Authentication

Multifactor authentication is provided through an industry-standard protocol known as Security Assertion Markup Language (SAML). The implementation of SAML does not directly provide the MFA functionality. Instead, it provides the mechanism to allow the web service to send a request to an external system that provides the functionality of requesting credentials from the user and verifying the entered credentials are acceptable to authenticate the user. Information about the authenticated user is then returned to the web service to allow the user to be assigned roles to provide the appropriate authorization for the user. With the previous E-Series authentication methods, the web service was responsible for requesting the user credentials and authenticating the user. With SAML, all authentication activity is provided by an external system. The external system can be configured to require any number and types of evidence from the user to allow the user to be authenticated.

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 the entered credentials are valid for the user. Maintenance and configuration of the IdP are the customer's responsibility.

- **Service provider.** The service provider (SP) is the system that requires users to be authenticated to provide access to functionality and data. The service provider sends a request to the IdP to have a user authenticated. For E-Series storage arrays, the controllers are the service providers, with each controller being a separate SP.

Using SAML to provide multifactor authentication also allows for single sign-on (SSO) capabilities. SSO allows for multiple applications to use the same user credentials without requiring the user to enter the credentials more than once if the applications are configured to use the same IdP. The SSO feature is available only if the user is accessing the multiple applications with the same browser.

Configuring SAML on E-Series

Before an identity provider and a service provider are allowed to exchange information, a trust relationship must be established between the providers. The trust relationship is created by exchanging metadata between the systems. Both the IdP and SP provide a mechanism to export an XML file that defines the functionality and security information (such as public keys) of the provider. The metadata from each provider is then imported into the other provider to be able to identify any incoming messages from the provider as being from a trusted source. For example, the SP metadata is exported from the SP application, and the exported XML data is then imported into the IdP application. Likewise, the IdP metadata is exported from the IdP application, and the exported XML data is then imported into the SP application. The exchange of metadata to both providers must be completed before authentication requests can be processed. Because E-Series considers each controller to be a separate SP, the export of SP metadata and import of the exported XML file into the IdP must be done twice, once for each controller. The import of the IdP metadata into the controllers can be done only once because the IdP metadata is shared across the controllers.

After SAML is configured and enabled, all non-web-based management access to the storage array is disabled. The following are disabled while SAML is enabled:

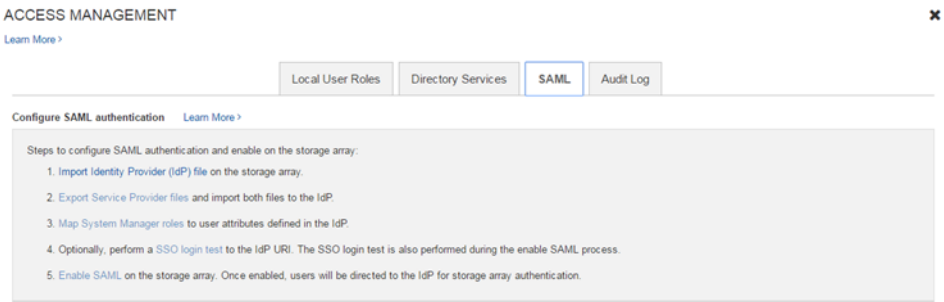
- Native SYMbol access, which disables legacy CLI
- SYMbol HTTP tunnel, which prevents EMW from accessing the array
- Secure CLI
- All in-band management

SSH is not disabled automatically but is disabled by default and must be enabled by the user.

Note: When SAML is enabled, there is not a way to disable SAML through the System Manager application. This limitation is an intentional security requirement to prevent an attacker from disabling the authentication mechanism to allow easier access to the array. SAML can be disabled only through the Admin menu, which is available only when connected to the serial port of a controller.

To configure SAML on E-Series, navigate to the new tab SAML, under Settings > Access Management, as shown in Figure 9.

Figure 9) System Manager SAML tab.



Steps to be performed are described in Table 3.

Table 3) Configuring SAML on E-Series.

Step	Description
external	The user exports or is provided metadata from the identity provider.
1	The user imports the IdP metadata into the System Manager application using Import Identity Provider (IdP) file.
2	The user exports the SP metadata from each of the controllers through the System Manager application using Export Service Provider files.
external	The user imports the SP metadata from each controller into the IdP application to build a trust relationship between the controllers and IdP.
3	The user maps roles with the System Manager application using Map System Manager roles. This capability allows the user to map attributes returned by the IdP to roles to provide authorization to the System Manager application. The IdP might need to have configuration changes to provide the appropriate user attributes to be able to do the role mapping.
4	The user tests the configuration with the System Manager application using SSO login test. The user may test as many times as necessary to verify the configuration for the IdP and the controllers is correct.
5	After the configuration has been successfully verified for both controllers, SAML can be enabled with the System Manager application using Enable SAML. The System Manager application runs one more test to verify the configuration before enabling SAML.

Note: After SAML is enabled, the E-Series array disables the legacy management interface to close any open security holes, and access to the System Manager application must be authenticated through the IdP.

Table 4 describes how E-Series authenticates using SAML.

Table 4) How E-Series authenticates using SAML.

Step	Description
1	The System Manager application determines the user does not have an authenticated session and a request is sent to log in the user.
2	The System Manager application retrieves the metadata for the identity provider and sends a request to the IdP to authenticate the user; the user and the request are sent to the identity provider using a browser redirection.
3	The identity provider receives the request and verifies the request originated from a service provider that has been identified as a trusted provider. The identity provider displays an HTML webpage to the user, the user enters their credentials, and the IdP verifies the credentials are correct for the user. If the credentials are correct, a response is returned to the SP to provide user information for the authenticated user. The response is sent back using redirection through the browser; the response is not sent directly to the SP system.
4	The System Manager application receives the response for an authenticated user and verifies the response originated from a trusted provider. The user information provided in the response is then used to determine the roles that should be assigned to the user for authorization.
5	If the user has the correct roles, they are authorized to use System Manager.

See the E-Series online help center and the E-Series Documentation Center for additional information about multifactor authentication.

2.7 Features Introduced with SANtricity System Manager 11.30

SANtricity OS 11.30 added the embedded System Manager for the E2800 as well as improvements to an already impressive list of RAS features and capabilities offered with the entire E-Series portfolio. A complete list is provided in Table 5.

Table 5) New features of SANtricity System Manager 11.30.

New Feature	Description
Automatic load balancing	The new automatic load-balancing feature provides automated I/O workload balancing and makes sure that incoming I/O traffic from the hosts is dynamically managed and balanced across both controllers. The workload of each controller is continually monitored and, with cooperation from the multipath drivers installed on the hosts, can be automatically brought into balance whenever necessary. For more information, search for “what is automatic load balancing?” in the System Manager online help.
AutoSupport automatic checking	When the EMW launches, it checks whether the Event Monitor is running. If the Event Monitor is running, it sends a test message to the technical support AutoSupport server to see whether communication is successful. This test message helps you know if AutoSupport is set up correctly. For more information, refer to “Setting the transport protocol for sending AutoSupport messages” in the EMW online help and to “Manage AutoSupport” in the System Manager online help.
Battery learn cycles	In storage arrays with two controllers, the learn cycles for the controllers start simultaneously, but they are not linked together. If the learn cycle for one controller stops for some reason, the learn cycle for the other controller keeps going. In previous versions of the software, if one controller failed its battery during a learn cycle, the alternate controller would stop its learn cycle. For more information, search for “what are battery learn cycles?” in the System Manager online help.
CLI changes for the E2800 controller (now extended on the E5700, EF570, and EF280 controllers)	Some CLI commands do not apply to the new E2800 controller, because its Event Monitor is embedded instead of being a separate process as it was for previous controllers. See the E-Series SANtricity Management Software for CLI documentation. **Note:** The CLI cannot be used from System Manager and requires the installation of SANtricity Storage Manager.
Embedded SNMP agent for the E2800 controller (now extended on the E5700, EF570, and EF280 controllers)	For the E2800 controller, SNMP is supported natively. Installing and running Event Monitor for generating traps are no longer required. The embedded SNMP agent is compliant with the SNMP V2C standard and RFC 1213 (MIB-II). For more information, search for “manage SNMP alerts” in the System Manager online help.

2.8 SANtricity OS Standard Features

E-Series EF280 systems ship with significant storage management features that can be simply activated from SANtricity System Manager. Table 6 provides a consolidated list of EF280 standard features when running SANtricity OS 11.40.

Table 6) EF280 standard features with SANtricity OS 11.40.

EF280 Standard Features with SANtricity OS 11.40
Storage partitions. Individual host without shared LUNs to host groups with shared LUNs or a combination of both. This concept has been abstracted in the new System Manager, but it is possible to see the partitions using the CLI.
Data assurance (T10 PI). Confirms data integrity from HIC to the drive (end to end in the storage array), which is especially important with large-capacity drives.
Media scan with redundancy check. Background scan of media that is run on a set schedule and detects data integrity issues.
Automatic load balancing. Built-in logic that uses internal port and system metrics to monitor I/O load, and, for some host types, the feature can automatically change controller LUN ownership over a period of hours to achieve a better balance of I/O across the controllers. The feature can be turned off in the `Settings` tab of the SANtricity System Manager or SANtricity Storage Manager GUIs.
Nondisruptive SANtricity OS upgrade. Using an ALUA host type with multiple paths to hosts combined with a wizard-driven upgrade process that activates one controller at a time, confirms that upgrades do not affect host-to-LUN access. **Note:** Not all host OSs support the ALUA host type.
Online drive firmware upgrade. Upgrades one drive at a time and tracks writes to the affected drives during the upgrade window; should be used only during very low write I/O periods. **Note:** Parallel drive firmware upgrades are supported offline to upgrade multiple drives more quickly during a maintenance window.
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 picks up where the evacuator was disrupted, thus reducing the rebuild time.
Drive encryption (full-disk encryption [FDE]). Encryption for data at rest; no external key management required and a minimal performance impact.
Standard AutoSupport. E-Series has supported basic AutoSupport for several releases.
Changing host protocol. Supported using new feature pack keys. Go to https://mysupport.netapp.com/eseries (Upgrading > Hardware Upgrade) to obtain the free activation codes and detailed instructions for each starting and ending protocol.
Thin provisioning. Generally not used with all-flash arrays due to performance overhead. Overcommit storage and add capacity when you need it. **Note:** To make sure that the performance characteristics of thin volumes are understood, the SANtricity System Manager GUI option for creating a thin volume has been removed. Thin volumes can be created with the SANtricity CLI or the SANtricity web services REST API. Thin volumes continue to be reported on and monitored in the System Manager GUI.
SSD read cache. Is not used with all-flash arrays.

EF280 Standard Features with SANtricity OS 11.40
Secure SSD read cache. The SSD read cache can be secured with a nonsecure base volume or a secure base volume (FIPS drive). However, when there is a FIPS secure base volume, the storage management software alerts you if the SSD read cache does not have the same security capabilities as the base volume. **Note:** If drive security is enabled and the SSD is secure capable, the SSD read cache can be secured only on creating the SSD read cache.

Table 7 provides a comprehensive list of standard copy services features with EF280 storage arrays.

Table 7) SANtricity 11.40 copy services features.

Standard SANtricity Copy Services Features
SANtricity Snapshot copies. Point-in-time NetApp Snapshot™ copies.
Asynchronous mirroring. Mirroring to a remote site where recovery point objective (RPO) = 0 is not a requirement.
Synchronous mirroring. Mirroring to a remote site where recovery point objective (RPO) = 0 is a requirement.
Volume copy. Used to spin off volumes for test/dev or analytics purposes.

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

2.9 SANtricity Management Integration

Starting with SANtricity OS 11.40, the E-Series SANtricity integration model is changing focus. We have stopped future development on most of our legacy plug-ins and instead have increased our focus on API integration to support specialty workloads and partner appliances. The exception to this change in plug-in support is the SANtricity VMware VASA provider (VMware APIs for storage awareness) because it still fits the future strategy for SANtricity integration.

Table 8 shows the SANtricity APIs and toolkits that can be used for scripting and custom integration into other management tools and appliance architectures. Go to http://mysupport.netapp.com/NOW/cgi-bin/software/ and select E-Series/EF-Series SANtricity Management Plug-Ins for the web services software and documentation. Go to http://mysupport.netapp.com/NOW/download/tools/santricity_powershell_toolkit for the PowerShell toolkit.

Table 8) SANtricity APIs and toolkits.

APIs and Toolkits	Description
SANtricity web services proxy **Note:** You can use either the external proxy installation or the embedded REST API for EF280. If you want to collect data from multiple systems, you must use the external web services software on a local server with IP access to the arrays.	Web APIs that provide a collection of REST interfaces to configure, manage, and monitor E-Series systems.
NetApp PowerShell toolkit	The unified toolkit provides end-to-end automation and storage management across NetApp storage systems.

Table 9 provides a list of third platform plug-ins that leverage E-Series storage systems as storage building blocks in cloud storage environments. The SANtricity web services proxy is available on the NetApp Support site at http://mysupport.netapp.com/NOW/download/software/eseries_webservices/1.3/. In most cases, the plug-ins listed are available on the various provider websites. Contact your NetApp sales representative for more information about third platform integration with EF280 storage systems.

Table 9) Third platform plug-ins that leverage the SANtricity web services proxy.

Software Package	Use
SANtricity plug-in for CHEF	CHEF agent uses the SANtricity web services proxy for configuration of E-Series storage.
SANtricity performance application for Splunk	Display and monitor tool to report about configuration and performance aspects of multiple E-Series systems in one interface.
SANtricity plug-in for Nagios	Custom plug-in for monitoring E-Series storage arrays in Nagios framework.

3 SANtricity System Manager

As previously discussed, the NetApp EF280 controller and SANtricity OS 11.40/11.40.2 use the new browser-based management interface that was introduced in 2016 with the entry-level E-Series E2800 storage system. However, the major components of the legacy SANtricity storage management software, such as the EMW, can still be used with EF280 storage arrays, so the installation flow is similar to legacy E-Series arrays. The only GUI component that is never used with EF280 storage systems is the AMW, which is still used with EF560 and other legacy E-Series systems. The AMW has been replaced on the EF280 by the embedded, browser-based SANtricity System Manager.

3.1 Overview

SANtricity System Manager provides embedded management software, web services, event monitoring, and AutoSupport for the EF280 controller. Previous controllers such as the EF560, E5600, and E2700 do not have this embedded functionality or the new security features introduced in SANtricity System Manager 11.40. Because you might have a mixed environment, with both the new EF280 all-flash array and older E-Series storage arrays, there are a variety of management options. Table 10 provides an overview of management use cases.

Table 10) Management use cases.

Task	EF560	EF280
Manage and Discover		
Discover an array in your management domain	EMW	EMW
Add an array to or remove an array from your management domain	EMW SANtricity storage management CLI (SMcli)	EMW SMcli (requires EMW)
Launch SANtricity System Manager	N/A	EMW Browser
Launch AMW	EMW	N/A

AutoSupport and Legacy Support Bundle Collection		
Enable/disable AutoSupport, AutoSupport OnDemand, and AutoSupport remote diagnostics features	EMW SMcli	System Manager REST
Show AutoSupport logs for all arrays or a select storage array	EMW SMcli	System Manager REST
Enable or disable legacy support bundle collection for a select storage array	EMW SMcli	N/A
Specify support bundle collection schedule	EMW SMcli	N/A
Configuration and Status		
Display information (other than alert settings) about configured arrays	AMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager SMcli Secure—CLI EMW script editor CLI REST
Show IP address of each array	AMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager SMcli Secure—CLI EMW script editor CLI
Show WWN of each array	AMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager AMW SMcli Secure—CLI EMW script editor CLI
Show status of each array	AMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager AMW SMcli Secure—CLI EMW script editor CLI
Set up synchronous or asynchronous mirroring	EMW/AMW SMcli EMW script editor CLI REST (requires web services proxy)	EMW/AMW SMcli Secure—CLI EMW script editor CLI
Show array-level configuration, provisioning, and tuning	AMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager REST
Alert and SNMP Configuration		

Show global alert settings	EMW SMcli EMW script editor CLI REST (requires web services proxy)	N/A REST
Specify email server and other configuration for global alert settings	EMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager REST
Remove an email from configuration for a specific array	EMW SMcli EMW script editor CLI REST (requires web services proxy)	System Manager REST
Add or remove SNMP trap information for a specific array	EMW SMcli REST (requires web services proxy)	System Manager REST
Send a test email based on global alert settings	EMW SMcli REST (requires web services proxy)	N/A REST
New Features for E2800, EF280, E5700, and EF570 Arrays Only (see SANtricity System Manager online help for descriptions)		
Certificate handling: view SSL information, get a certificate signing request (CSR), import a new certificate	N/A	System Manager REST
More convenient syslog	N/A	System Manager REST
Save up to 30 days of historical statistical I/O data	N/A	System Manager REST
Perform application tagging of volumes, NetApp Snapshot copies	N/A	System Manager REST

EF280 storage systems are shipped from the factory preloaded with SANtricity OS 11.40.2, which includes the associated SANtricity System Manager bundled with the controller firmware. You can discover and manage from a central view EF280 storage systems that are running either SANtricity OS 11.40 or SANtricity OS 11.40.2. Earlier versions of SANtricity Storage Manager (EMW) cannot discover the EF280 arrays that run SANtricity OS 11.40 or 11.40.2. However, SANtricity Storage Manager 11.42 can discover the new EF280 arrays and all the earlier E-Series array software versions from the past six years.

If you do not want to use the EMW to discover your E-Series arrays, you do not use or want to use SANtricity mirroring features, and you are not running bare-metal Windows or Linux hosts requiring

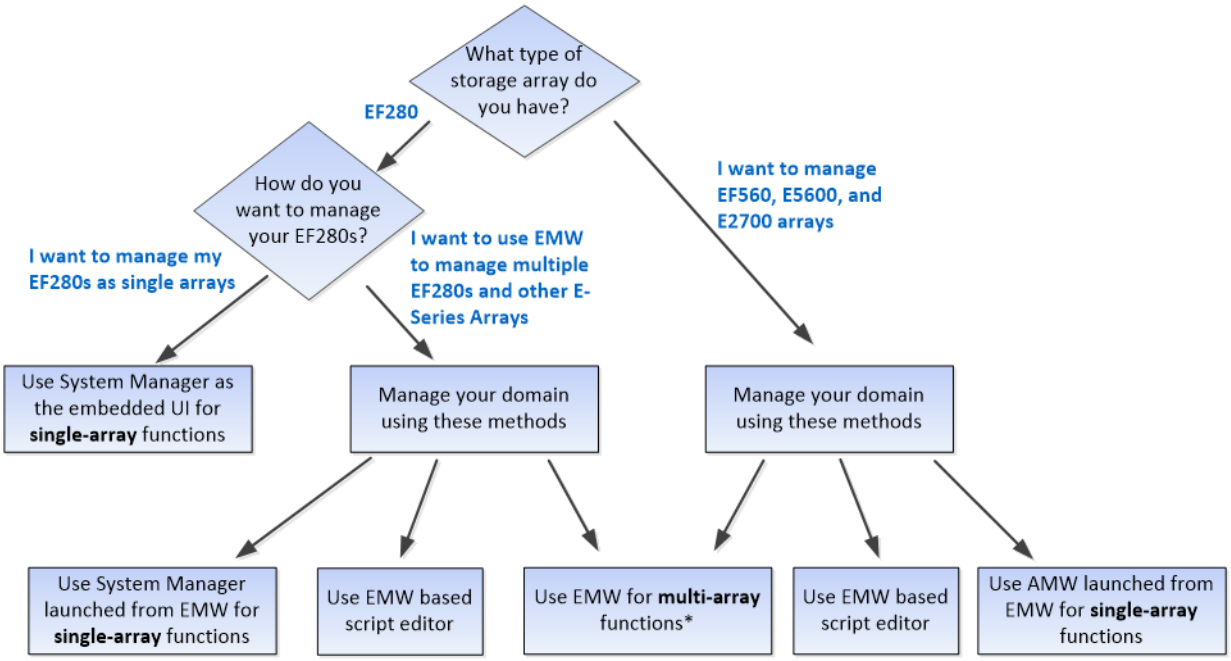
multipath or other SANtricity storage management utilities (SMutils) support, you do not need to download and install the legacy SANtricity Storage Manager software. If you do want to use any of this functionality, you must download and install the desktop thick client software or host package on a local management host or to bare-metal I/O-generating hosts that require multipath drivers. The various SANtricity host packages based on your OS type should also be installed when recommended by the NetApp Interoperability Matrix Tool (IMT). See the appropriate OS documentation to find specific host setup instructions and requirements. The guides are available from the NetApp Support site at https://mysupport.netapp.com/eseries.

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

3.2 Deployment

The decisions about which components to install if you have purchased an EF280 all-flash array depend on how you answer the questions that are shown in Figure 10.

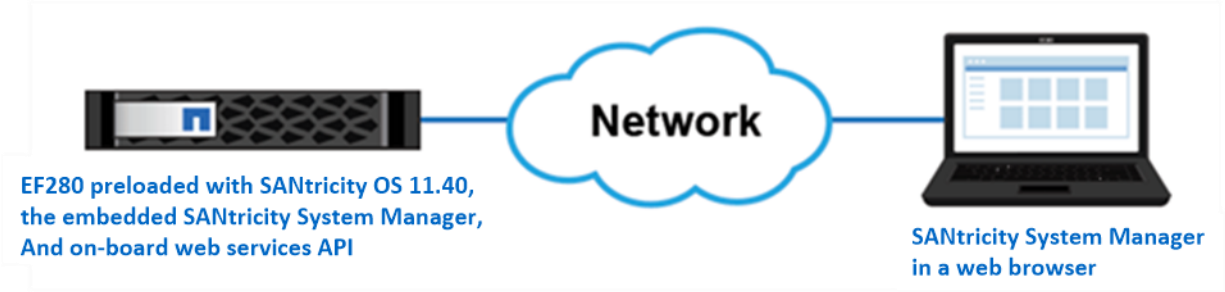
Figure 10) Decision tree for SANtricity management components to install.



Single EF280 Storage Array

If you have only a single new array and are not using either the synchronous mirroring or asynchronous mirroring feature and do not require the CLI, then all configuration can be handled from SANtricity System Manager. See Figure 11.

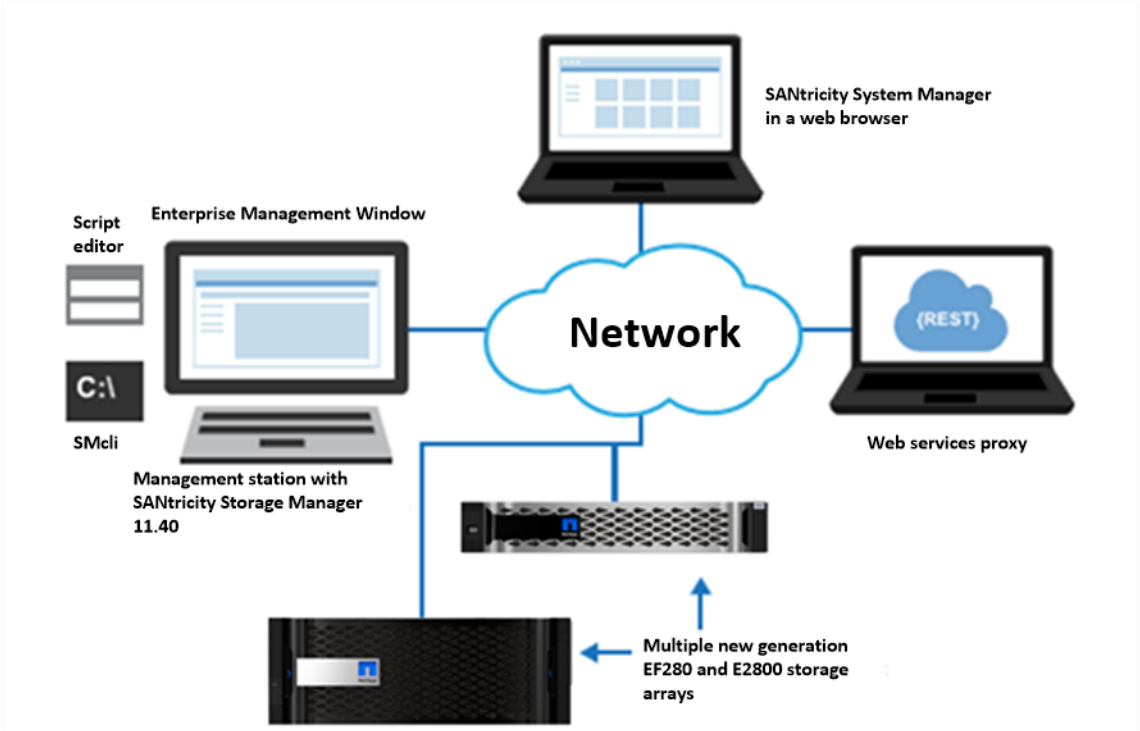
Figure 11) Managing a single EF280 with SANtricity System Manager.



Multiple EF280 Storage Arrays

If you have one or more EF280 storage arrays, you can install the EMW to manage your overall environment while still handling all storage array–based configuration through SANtricity System Manager. The EMW comes with SANtricity Storage Manager for managing multiple arrays, as shown in Figure 12.

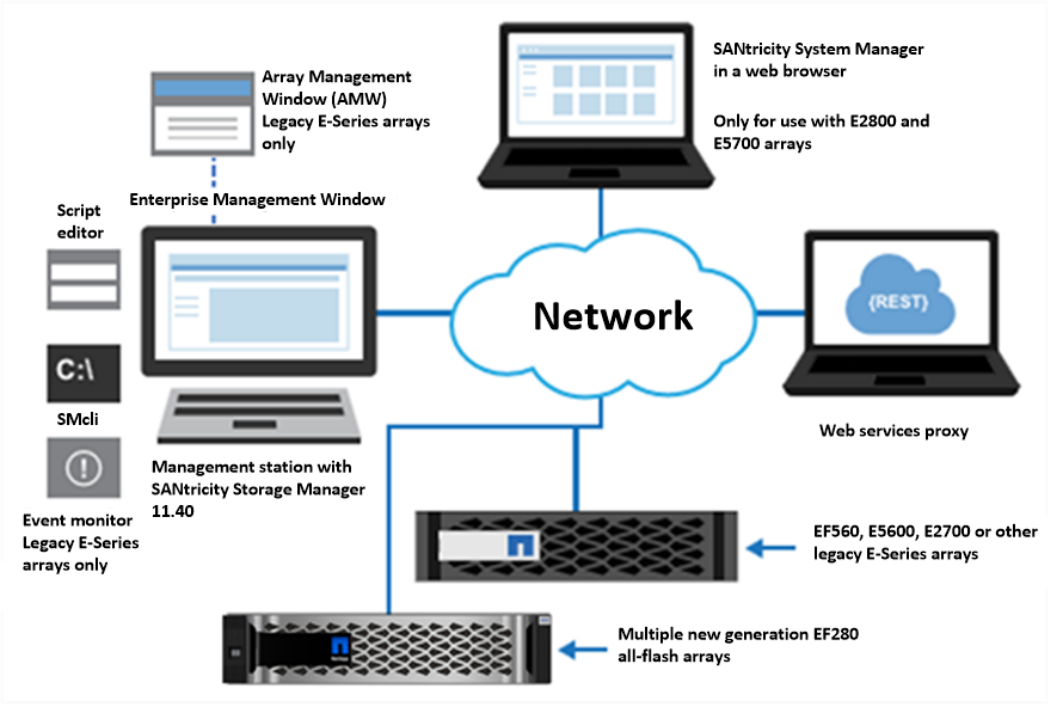
Figure 12) Managing multiple EF280 systems and E2800 systems with SANtricity Storage Manager and System Manager.



Mixed-Array Environment

If you have one or more EF280 all-flash arrays and any other E-Series storage arrays and want to have the EF280 included in your aggregate view or use synchronous or asynchronous mirroring, you must install the EMW. Use the SANtricity System Manager for array-based tasks on the EF280 all-flash arrays and use the AMW for array-based tasks on other E-Series storage arrays, as shown in Figure 13.

Figure 13) Managing a mixed-array environment with SANtricity Storage Manager and System Manager.



For a detailed description of installing and configuring the components you choose, refer to the E-Series Documentation Center at https://mysupport.netapp.com/eseries.

3.3 System Manager Navigation

After you log in to SANtricity System Manager, the home page is displayed, as shown in Figure 14:

- The icons on the left of the home page are used to navigate through the System Manager pages and are available on all pages. The text can be toggled on and off.
- The items on the top right of the page (Preferences, Help, Log Out) are also available at any location in the System Manager.
- Highlighted on the bottom-right corner is the drop-down menu used extensively in System Manager.

Figure 14) System Manager home page.

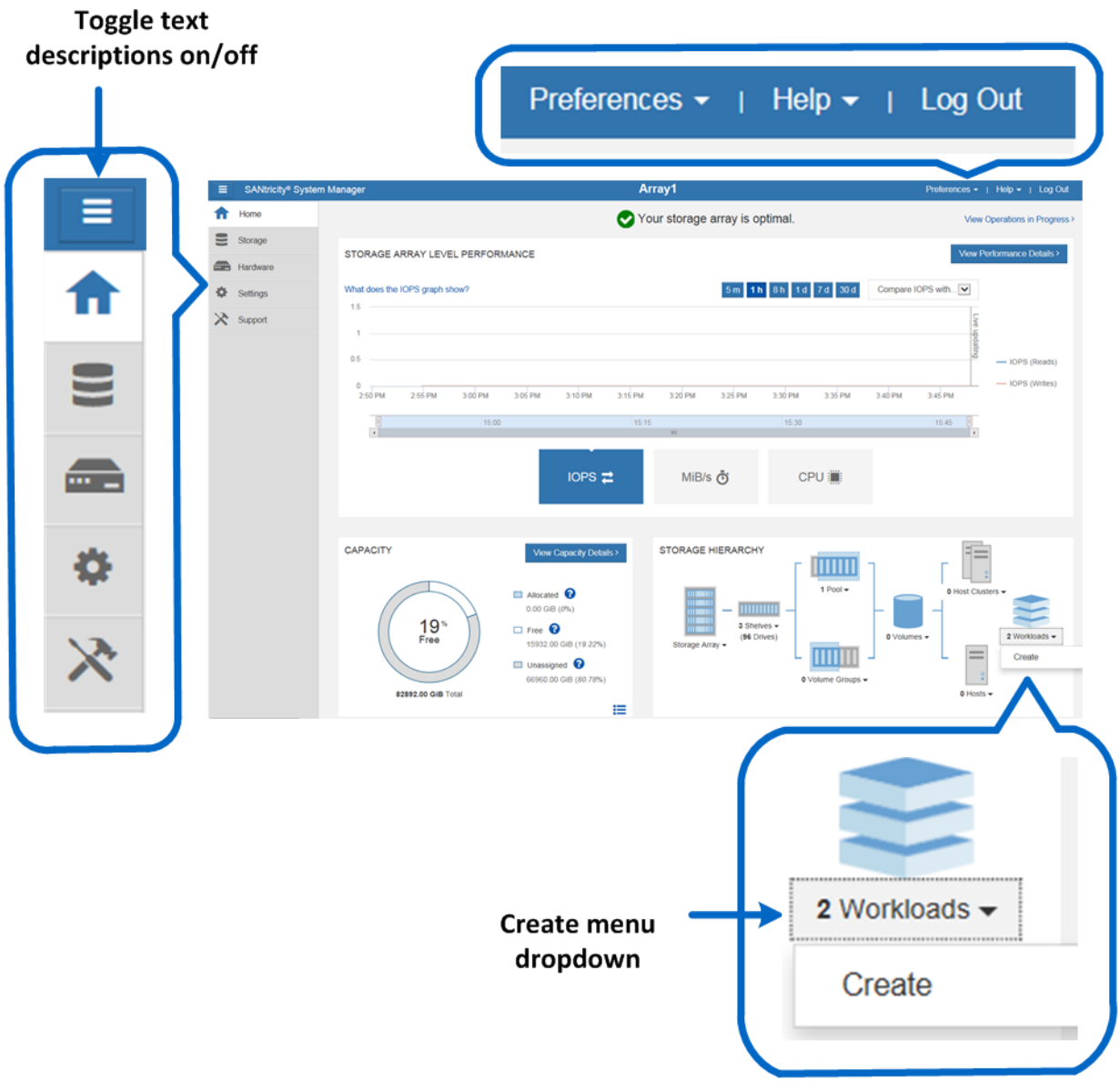


Figure 15, Figure 16, Figure 17, and Figure 18 show the other four main pages that are used in SANtricity System Manager and that are accessible from anywhere in the application.

Figure 15) System Manager storage page.

Figure 16) System Manager hardware page, back-of-shelf view.

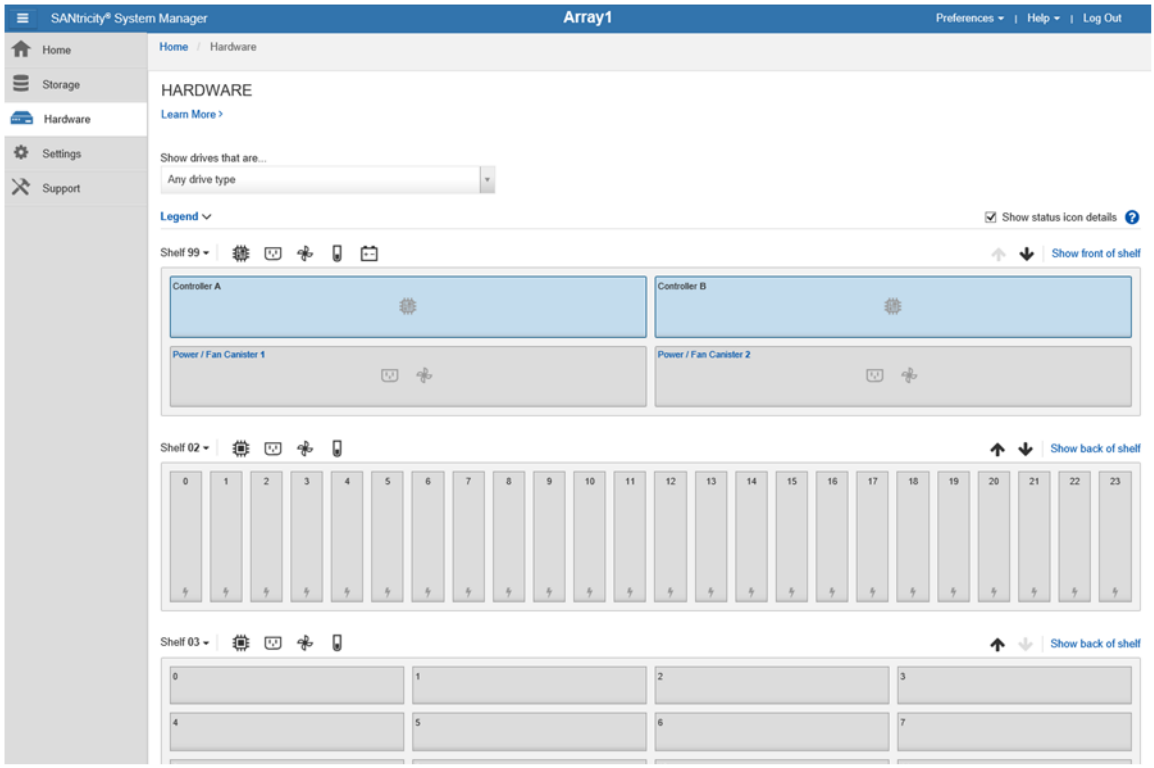
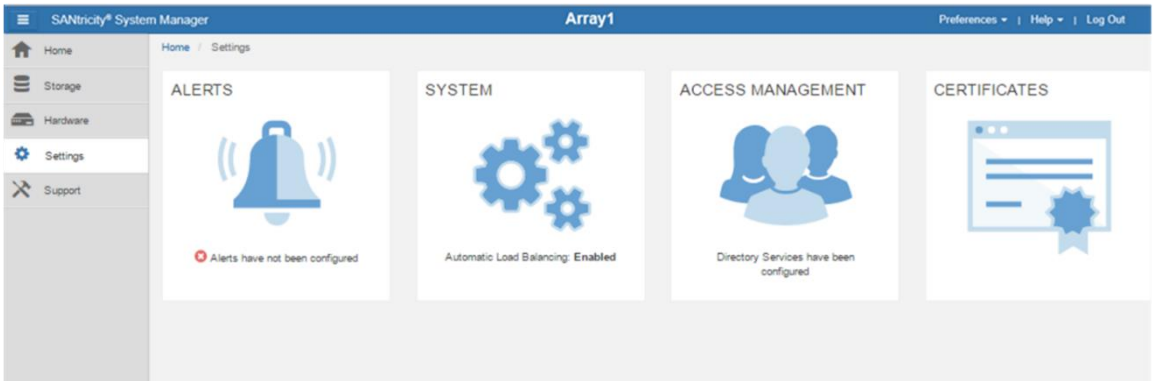


Figure 17) System Manager settings page with new security tiles.



Note: Figure 17 shows the view that the master admin or security admin would see. Others with a lower access permission level would see only the Alerts and System tiles.

Figure 18) System Manager support page.

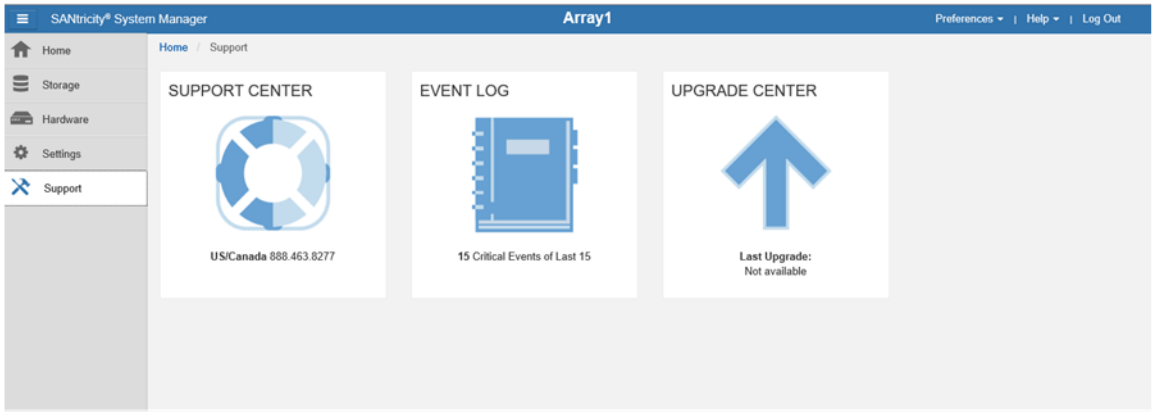
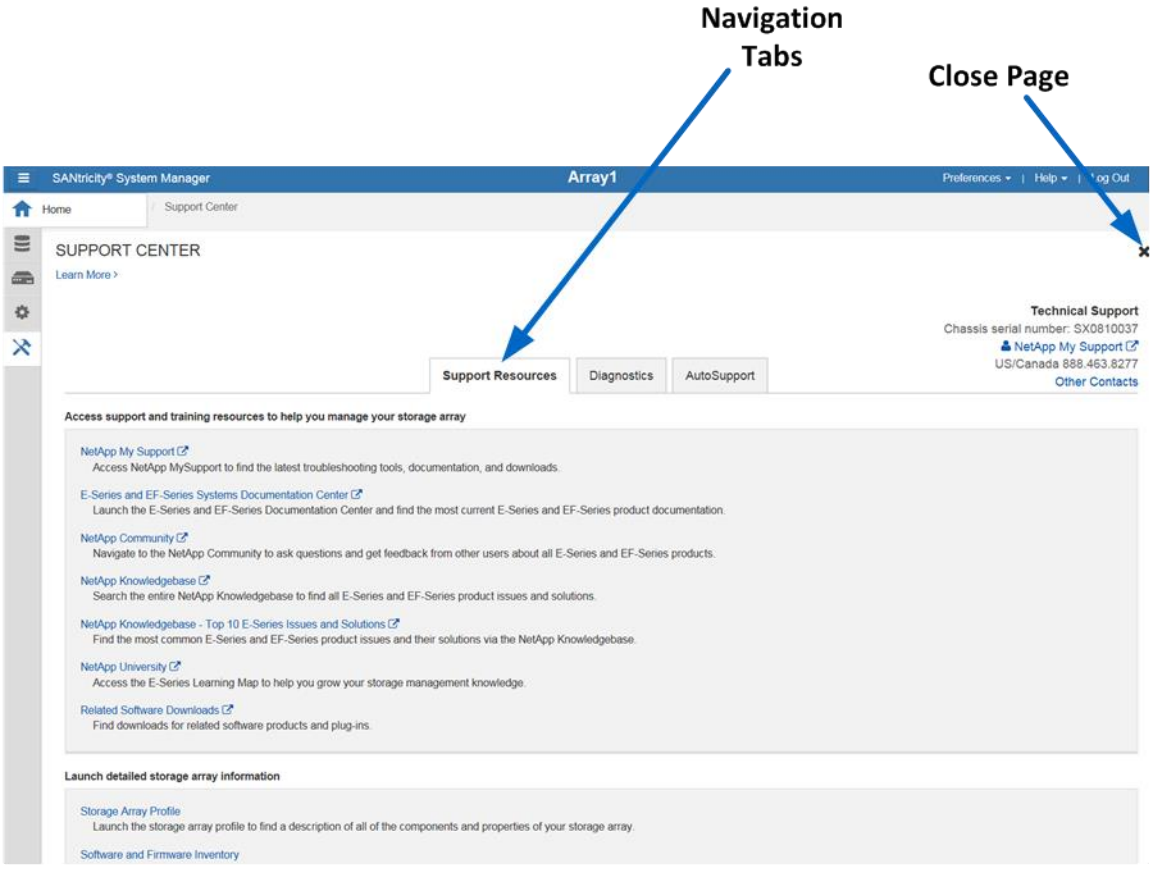


Figure 19 displays the Support Center, reached by selecting the Support Center tile on the support page. From the Support Center, navigation tabs are used to reach support topics.

Figure 19) System Manager Support Center.

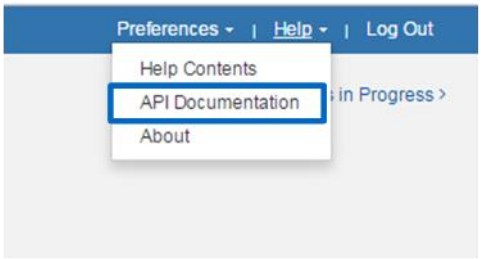


See the System Manager Tables in the appendix for a list of legacy SANtricity Storage Manager AMW functions and their corresponding locations in SANtricity System Manager. The SANtricity System Manager online help also provides an excellent reference guide.

3.4 Native REST API

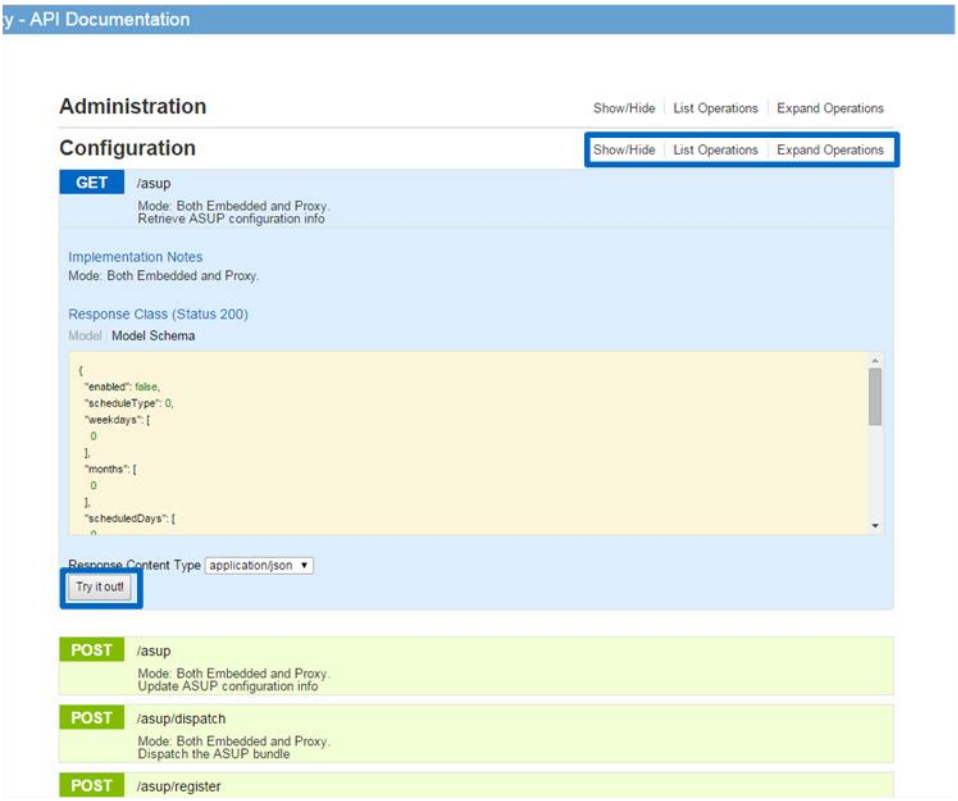
The SANtricity REST API is an application programming interface designed for experienced developers. Actions performed through the REST API are applied on execution and without user prompts or confirmation dialog boxes. The REST API is URL based, and the accompanying API documentation is completely interactive. Each URL contains a description of the corresponding operation and the ability to perform the action directly through the API documentation. The API documentation is accessible by selecting API Documentation under the Help drop-down menu from any page in System Manager, as shown in Figure 20.

Figure 20) Opening the API documentation.



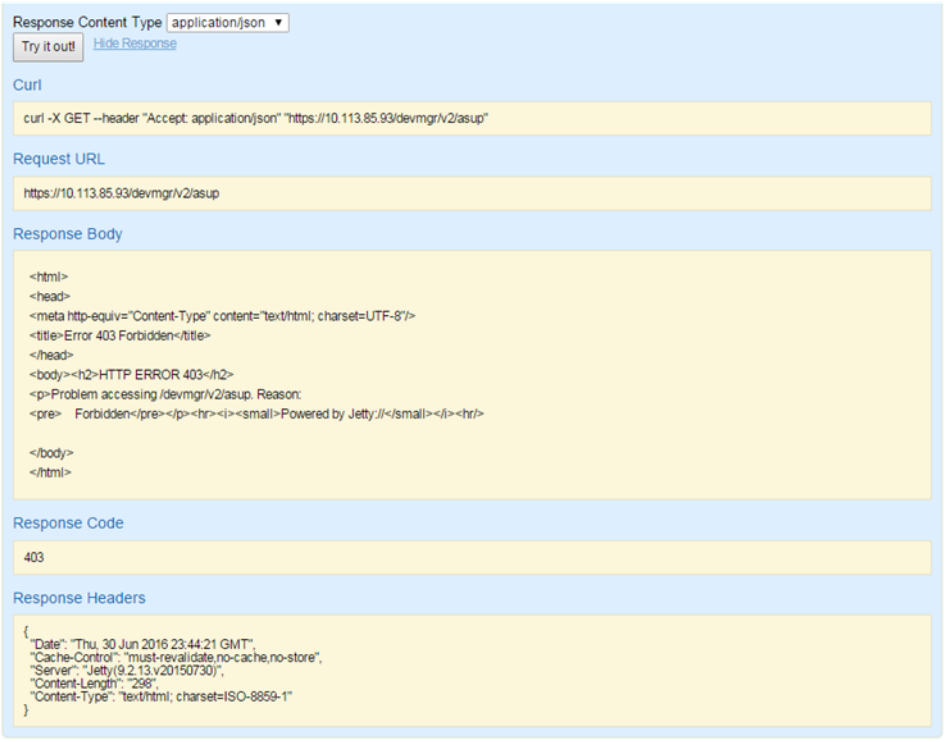
Each URL endpoint presented in the API documentation has a corresponding POST, DELETE, or GET option. These URL endpoint options, more properly known as HTTP verbs, are the actions available to the developer through the API documentation. A sample from the REST API documentation is shown in Figure 21. As shown, expanding or hiding operations can be done by selections to the right of the topic.

Figure 21) REST API documentation sample.



Also, the HTTP verbs can be tested by using the Try It Out! button. The corresponding output for the GET verb that is shown in Figure 21 is displayed in Figure 22.

Figure 22) Sample output from the Try It Out! button.



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 key-value pair-based encoding with support for list and subject objects. Objects start and end with curly braces (that is, { }), while 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.

Also, see the E-Series Documentation Center.

4 Support Tool Enhancements

Improving the customer experience is the central goal of NetApp enablement tools. To continue the legacy of prioritizing enablement tools, several key enhancements have been implemented.

4.1 Config Advisor

Config Advisor is a configuration validation and health check tool for NetApp systems. Config Advisor can be used to check a NetApp system for the correctness of hardware installation and conformance to NetApp recommended settings. It collects data and runs a series of commands on the hardware, then checks for cabling, configuration, availability, and best practice issues.

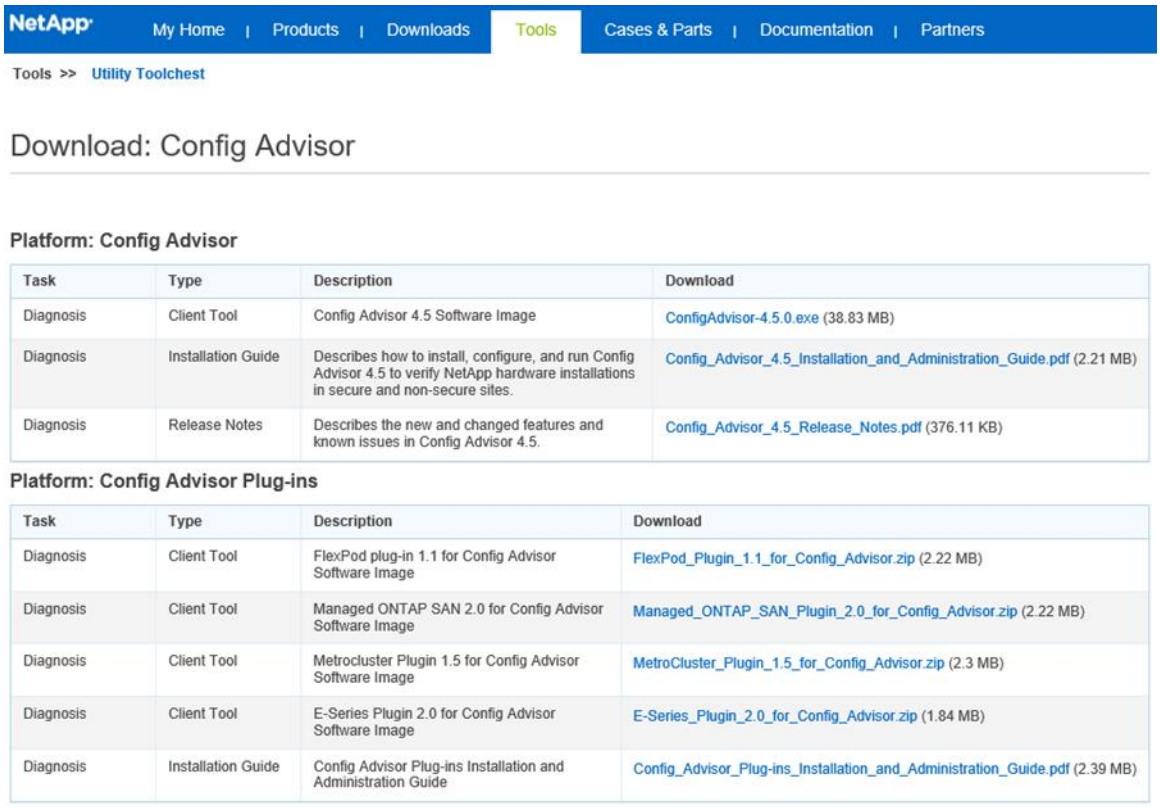
Tool Description

The Config Advisor 4.5 release enables support for SAS 3 cabling and visualization (cable diagrams). There is continuing support for E-Series host-side checks and E-Series configuration checks in addition to the standard checks.

Config Advisor creates PDF, Word, and Excel reports about the system configuration summary and health check results. It also sends Config Advisor AutoSupport data back to NetApp over HTTP; this data can be viewed through SmartSolve.

To download the Config Advisor tool, the additional plug-in for E-Series, and associated installation documentation for both software packages (see Figure 23), use the Config Advisor link, acknowledge the EULA, and select Continue. For general installation instructions, use the Config Advisor 4.5 Installation and Administration Guide. For details about how to install the E-Series plug-in, use the Config Advisor Plug-Ins Installation and Administration Guide.

Figure 23) Config Advisor download site landing page.



Config Advisor Workflow and Key Features

Config Advisor has three major components:

- **Data collector.** The data collector supports multiple data input methods, including support for secure site data collection.
- **Analysis engine.** The analysis engine takes the collected data and performs a series of configuration validation and best practices checks. The analysis engine checks for at-risk systems, checks for systems that require firmware updates, and performs network switch checks.
- **Presentation layer.** The presentation medium is very flexible. Users can view the output using Config Advisor's intuitive UI, or they can generate PDF, Excel, or Microsoft Word reports for these contents.

4.2 E-Series Sizer

The E-Series Performance Sizing tool helps sales engineers and partners properly size specific customer architectures to meet customer performance requirements.

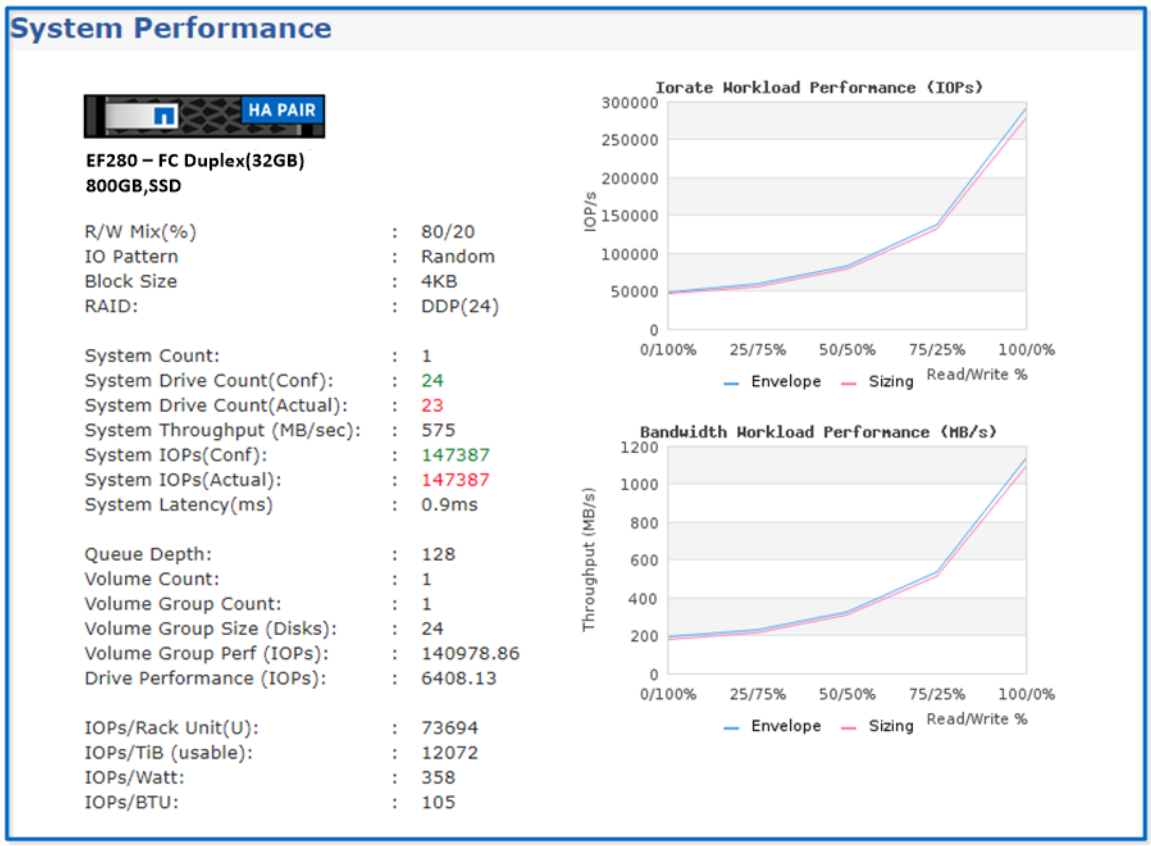
The E-Series Sizer tool is available for NetApp employees and is also open for partner access.

Note: If you are unable to access this tool, contact your NetApp or partner sales representative.

Figure 24 shows a performance sizing report, which includes four major sections:

- **Hardware and workload.** The boxed area in Figure 24 represents the hardware and workload section where users enter the expected hardware and workload.
- **Sizing.** The next section shows the sizing output:
  - The numbers in red show the actual system drive count and the actual system IOPS. These values are used to determine the drive count needed to meet the performance and IOPS targets.
  - The numbers in green show the configured system drive count and the configured system IOPS. These values are used to determine the drive count needed based on RAID group size and IOPS performance.
- **Metrics.** This section shows various metrics such as volume group performance, drive performance, and IOPS/rack unit.
- **Charts.** The charts on the right side of the report present performance as two sets of data points. Envelope is the performance curve representing a fully configured system, and sizing is the performance curve representing the sized solution.

Figure 24) Performance sizing report.



4.3 Synergy

NetApp Synergy is a NetApp tool used for accurately designing NetApp configurations. An emphasis is placed on showing realistic capacity yield and environmental details. Advantages of using Synergy over traditional spreadsheets or alternative tools include automatic product updates, best practices enforcement, alignment to the sales workflow, and data sharing with users and tools.

Note: If you are unable to access this tool, contact your NetApp or partner sales representative.

Synergy 6, the latest release, is a full web-accessible experience that is compatible with mainstream browsers such as Microsoft Internet Explorer, Google Chrome, and Mozilla Firefox.

Note: The Synergy user guide is at https://forums.netapp.com/docs/DOC-14888.

4.4 Hardware Universe

Hardware Universe is a web-based tool that provides a visual presentation of the complete NetApp line of hardware products.

Hardware Universe provides the information needed to make side-by-side comparisons of the various NetApp systems in terms of capacity, memory size, maximum spindle count, and other features.

Note: If you are unable to access this tool, contact your NetApp or partner sales representative.

Hardware Universe has three components:

- **HWU poster** is a one-stop location to find specifications for all NetApp products.
- **HWU application** provides the complete NetApp hardware portfolio in a web application.
- **HWU mobile application** represents the complete NetApp hardware portfolio in a mobile application for iPhone or Android.

The Hardware Universe user guide is at http://hwu.netapp.com/Resources/hwu_ug.pdf.

4.5 Host Utilities

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. The settings are based on the latest Interoperability Matrix Tool (IMT) guidance. The kits are on the NetApp Support site at Downloads > Software > Host Utilities—SAN. Currently, the Linux and Windows kits support E-Series and FAS implementations. Other available kits support FAS implementations only.

5 Software Specifications for EF280 Hardware

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

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

Components	Maximum
Storage Hardware Components	
Shelves (controller drive and expansion drive)	4 total (1x controller + 3x expansion)
Drives	96 SSDs
SSD cache capacity	N/A
Logical Components	
Partitions	128
Volumes per partition	256
Volumes	512
Thin volumes per system	512
Disk pools per system	20

Components	Maximum
Total DDP capacity in an array (maximum capacity includes RAID overhead, DDP reserve capacity, and a small DDP-specific overhead based on the number of drives in the pool and other factors)	SANtricity OS 11.40: • 2PB maximum DDP capacity per EF280 array SANtricity OS 11.40.1 and later: • 6PB maximum DDP capacity per EF280 array
Maximum standard RAID capacity limits	Limits for standard RAID based on maximum supported drives per RAID type: • 30 drives any supported capacity for RAID 5 and RAID 6 • All drives any supported capacity for RAID 10
Maximum single-volume capacity (SANtricity OS 11.40/11.40.1 and later)	2PB
Consistency Groups	
Volumes per consistency group	32
Consistency groups per system	16
Snapshot Copies	
Per Snapshot group	32
Per volume	128
Per storage system	512
Snapshot Volumes	
Per Snapshot copy	4
Per system	256
Snapshot Groups	
Per volume	4
Per system	256
Mirrors	
Mirrors per system	32
Mirrors per volume	1
Mirrors per asynchronous mirror consistency group	32
Asynchronous mirror consistency groups per system	4

Note: See Hardware Universe for additional software limits and specifications.

6 Hardware Configurations

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

6.1 Controller Shelf Configurations

The following sections provide detailed information about the EF280 shelf configuration.

EF280 Controller Shelf

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

Figure 25, Figure 26, and Figure 27 show the front and rear views of the EF280 controller shelf. In the example, the EF280 controllers have two optical base ports and no HIC.

Figure 25) EF280 front view with bezel.

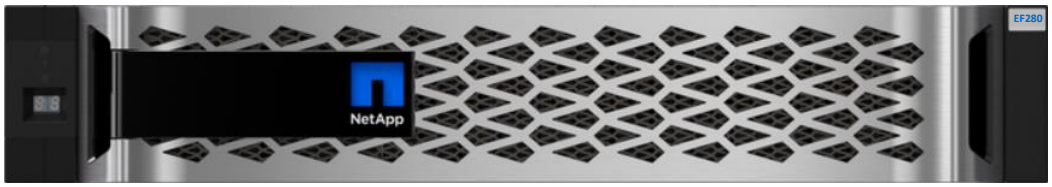


Figure 26) EF280 front view (open).

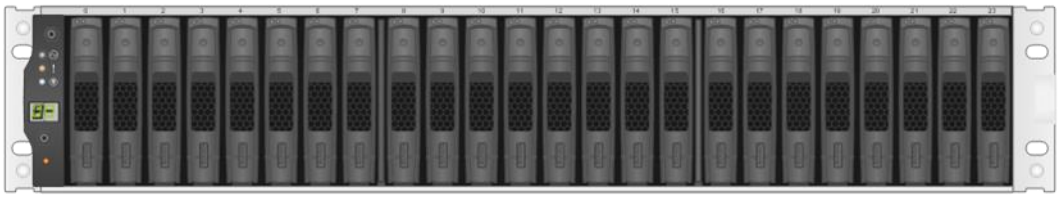


Figure 27) EF280 rear view.

EF280 Hardware Specifications

The EF280 controller has the following base hardware features:

- Dual Ethernet ports for management-related activities
- Dual optical 16Gbps FC or 10Gbps iSCSI baseboard ports for host connection
- SAS drive expansion ports to attach expansion drive shelves

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

Table 12) EF280 technical specifications.

Specification	EF280
Current maximum raw system capacity (assumes 120 SSDs)	1468TB (96 x 15.3TB SSDs)
Maximum number of drives per system (assumes not mixing shelf models)	96 SSDs maximum
Shelf form factor	2RU, 24 drives
SSD types (FIPS drives are also supported with some capacities; see Hardware Universe for details)	15.3TB, 7.6TB, 3.8TB, 1.6TB, or 800GB 2.5" SSDs
Memory	8GB or 32GB per controller
	16GB or 64GB per duplex system
Onboard host interface	2-port 10Gb iSCSI (Base-T) per controller or 2-port 10Gb iSCSI (optical)/16Gb FC per controller **Note:** Only one interface can be configured per system on the onboard host ports.
Optional host I/O (HIC) • Controllers must match • The Base-T iSCSI onboard controller can use only the 2-port Base-T HIC • A software feature pack can be applied to convert the FC HIC ports to iSCSI or to convert iSCSI HIC ports to FC	2-port 10Gb iSCSI (Base-T) per controller
	4-port 12Gb SAS (wide-port) per controller
	4-port 10Gb iSCSI (optical)/16Gb FC per controller
Drive shelves supported for expansion drive offerings	DE224C (2RU, 24 drives): 3 x SAS 3 12Gbps expansion shelves maximum
	DE5600 (2RU, 24 drives): 3 x expansion shelves maximum Note: Supports only SAS 2 (6Gbps) transfer speeds.
High-availability (HA) features	Dual active controllers with automated I/O path failover
	Support for RAID 0, 1 (10 for 4 drives or more), 5, 6, and Dynamic Disk Pools technology **Note:** It is only possible to create RAID 3 volumes through the CLI. For more information, search for “using the create volume group wizard” in SANtricity System Manager online help.
	Redundant, hot-swappable storage controllers, disks, and power fan canisters

Specification	EF280
	Support for ALUA and TPGS with implicit path management for the most popular host types, including clustered host environments
	Proactive drive health monitoring with the drive evacuator feature to identify problem drives and begin removing data before hard failures occur
	Automatic drive fault detection, failover, and rebuild by using global hot spare drives for standard RAID and spare pool capacity in the case of DDP
	Mirrored data cache with battery-backed destage to flash
	Online controller firmware and NVSRAM upgrade
	Online IOM12 firmware and drive firmware upgrade (consult CSD for guidance before performing ESM upgrades)
	Online drive firmware upgrades (consult CSD for guidance before performing drive firmware upgrades)
	SANtricity Event Monitor and AutoSupport, for making periodic copies of the storage system configuration
	Automatic load balancing and path connectivity monitoring

*See the Controller Host Interface Features section for details about the available feature pack SMIDs for EF280 controllers.

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

6.2 Controller Host Interface Features

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

- 2-port 10Gb iSCSI (Cat6e/Cat7 RJ-45)
- 2-port 12Gb SAS (SAS 3 connector)
- 4-port 12Gb SAS (SAS 3 connector)
- 2-port optical HIC, which can be configured as either 16Gb FC or 10Gb iSCSI
- 4-port optical HIC, which can be configured as either 16Gb FC or 10Gb iSCSI

Note: A software feature pack can be applied in the field to change the host protocol of the optical baseboard ports or the 4-port optical HICs:

  - From FC to iSCSI
  - From iSCSI to FC

For step-by-step instructions for obtaining and applying software feature packs to change baseboard and HIC protocol, go to the E-Series and EF-Series Systems Documentation Center, locate the Upgrading > Hardware Upgrade section of the page, select Changing the Host Protocol, and download the “Converting EF280 Host Protocol” document.

The optical HIC supports several SFP options, including several 16Gb FC or 10Gb SFP+ options and a unified adapter that supports both 16Gb FC and 10Gb iSCSI.

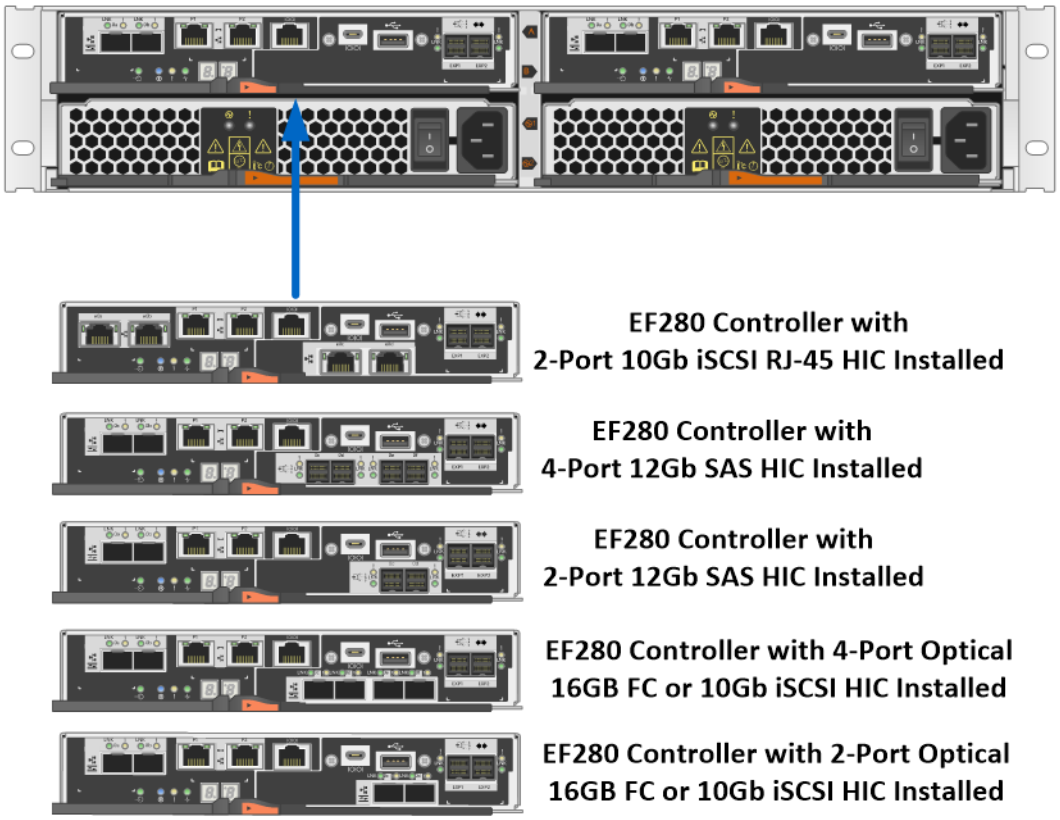
Note: The unified SFP does not support 1Gb iSCSI. It does support 4/8/16Gb FC and 10Gb iSCSI.

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.

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

The five HIC options are shown in Figure 28.

Figure 28) EF280 with optional HICs.



6.3 Hardware LED Definitions

EF280 Controller Shelf LEDs

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

Figure 29 shows the ODP of the EF280 controller shelf.

Figure 29) ODP on front panel of EF280 controller shelf.

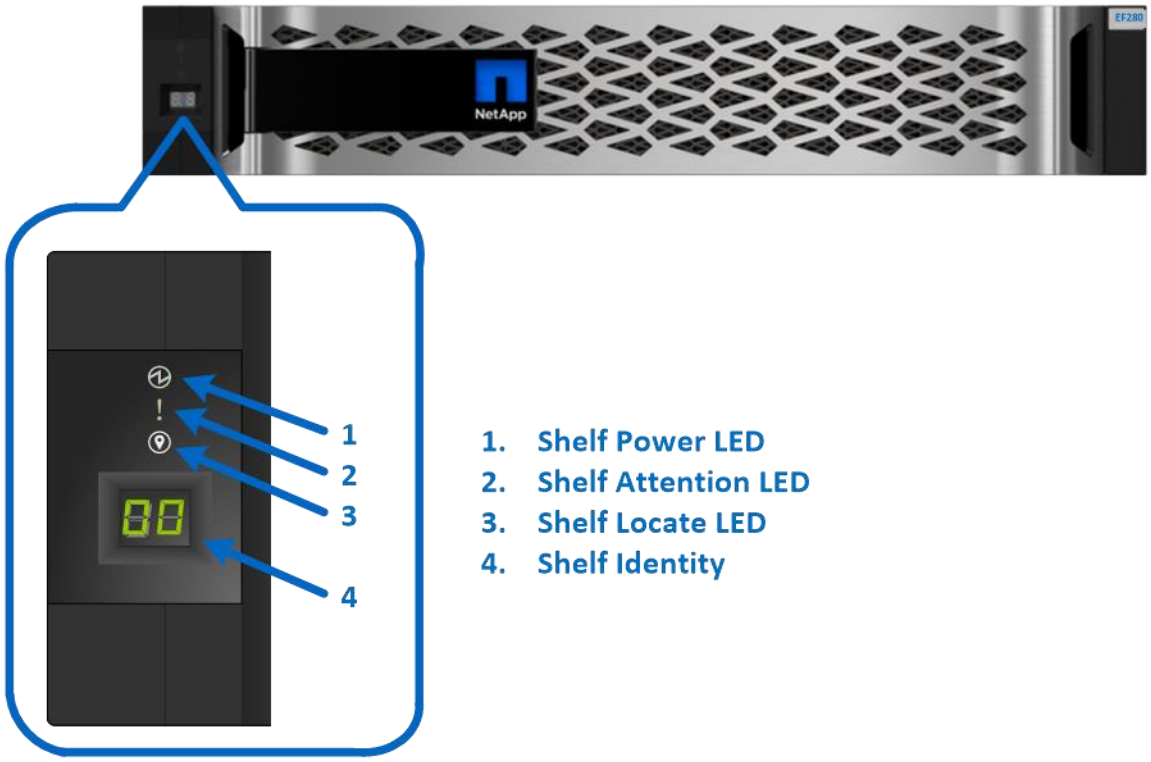


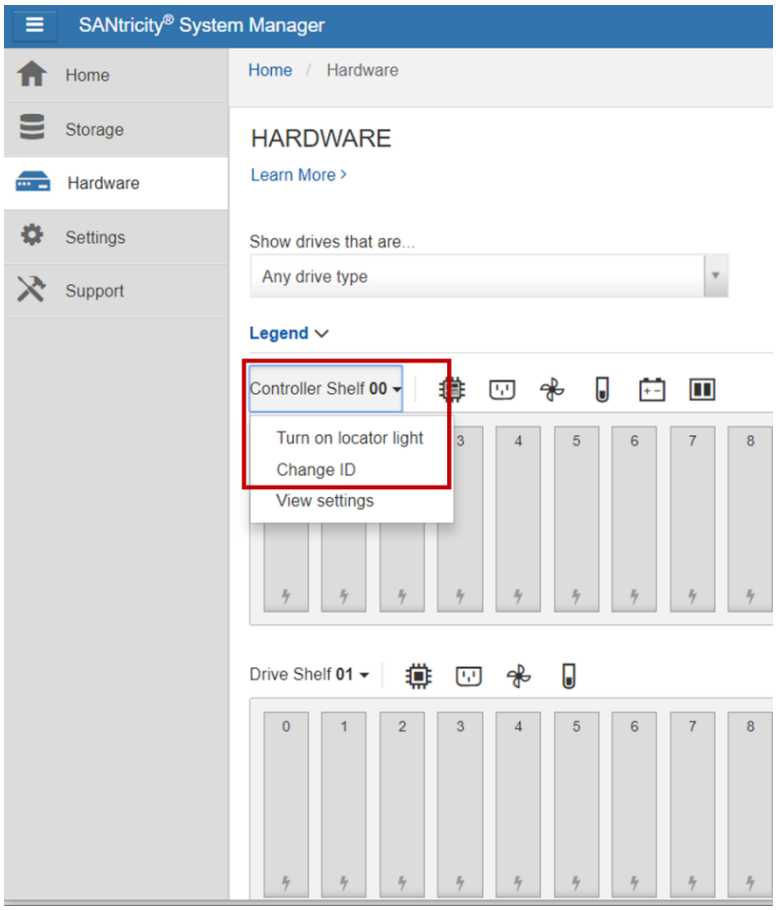
Table 13 defines the ODP LEDs on the EF280 controller shelf.

Table 13) EF280 controller shelf LED definitions (front panel).

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

The shelf-identity feature displays a numerical value to identify the shelf. The dual seven-segment display indicates values from 00 to 99 that can be set from the SANtricity System Manager hardware tab shown in Figure 30.

Figure 30) Setting shelf ID by using SANtricity System Manager.



Power Fan Canister Status LEDs

The LEDs on the rear panel of the EF280 integrated power and fan canisters are shown in Figure 31 and are defined in Table 14.

Figure 31) LEDs on EF280 power fan canister (rear view).

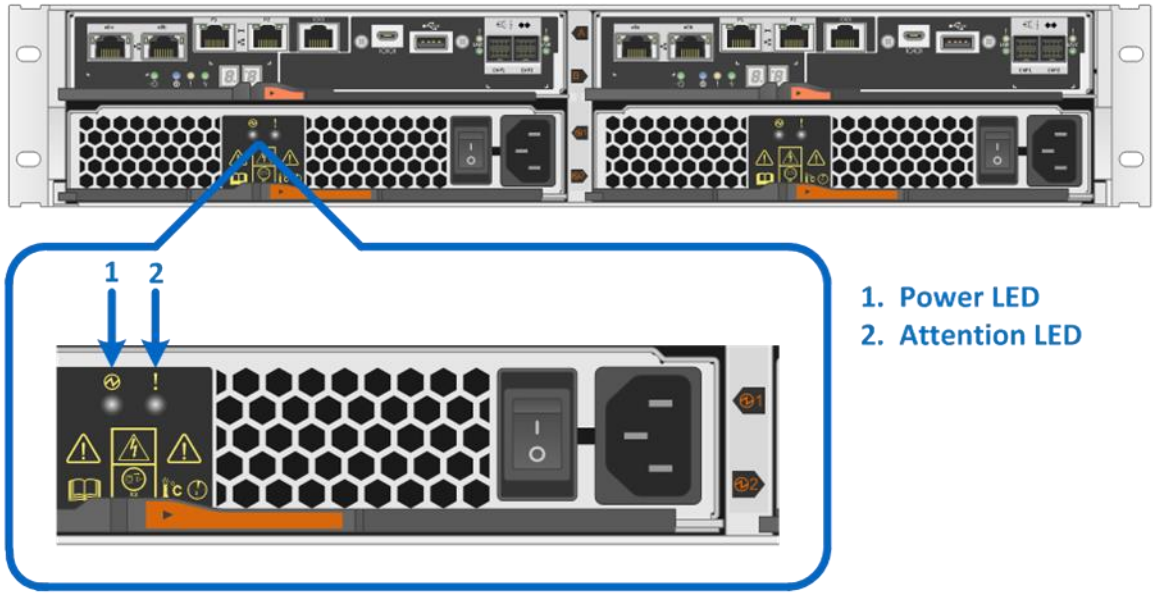


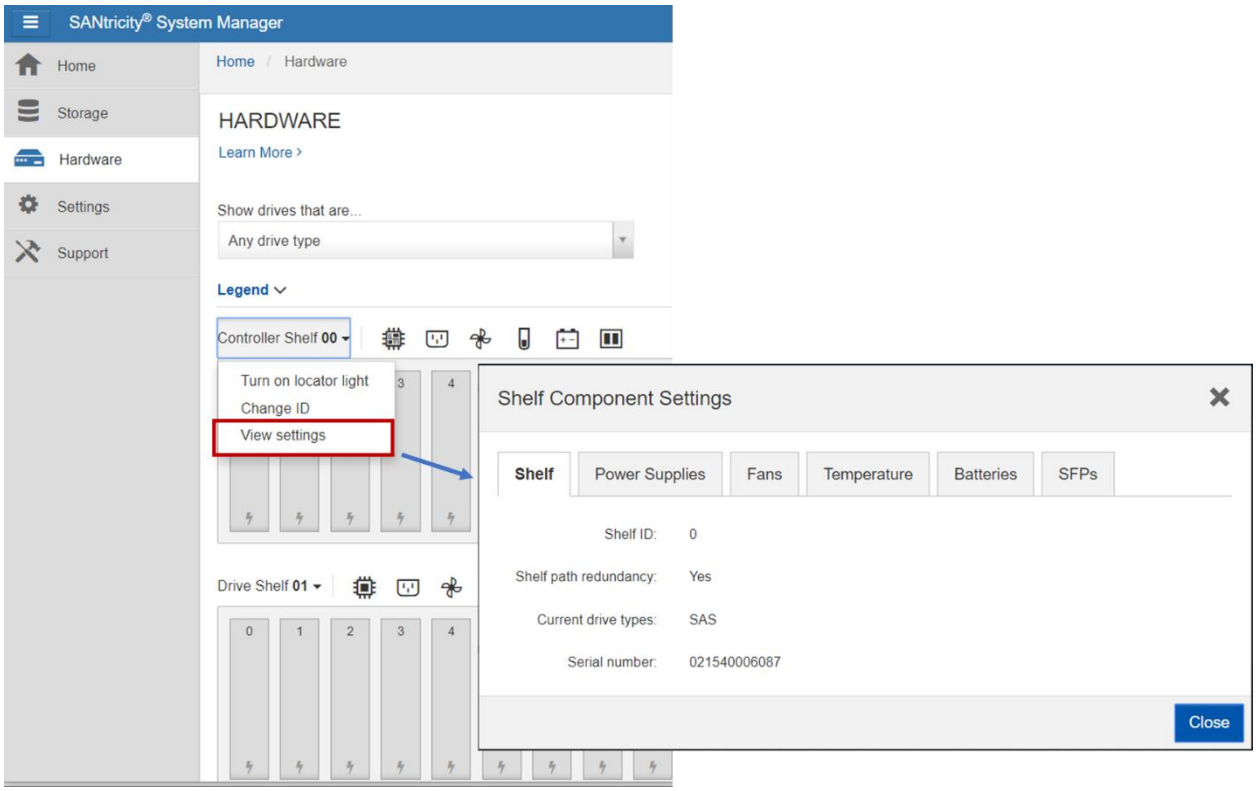
Table 14) EF280 controller shelf power and fan canister LED definitions.

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

EF280 Controller Canister LEDs

The EF280 controller canister has several LED status indicators. Host port status and other system-level status information can be verified by directly checking the port LEDs or by using the SANtricity System Manager GUI. For example, systemwide status information is displayed in the view settings window shown in Figure 32.

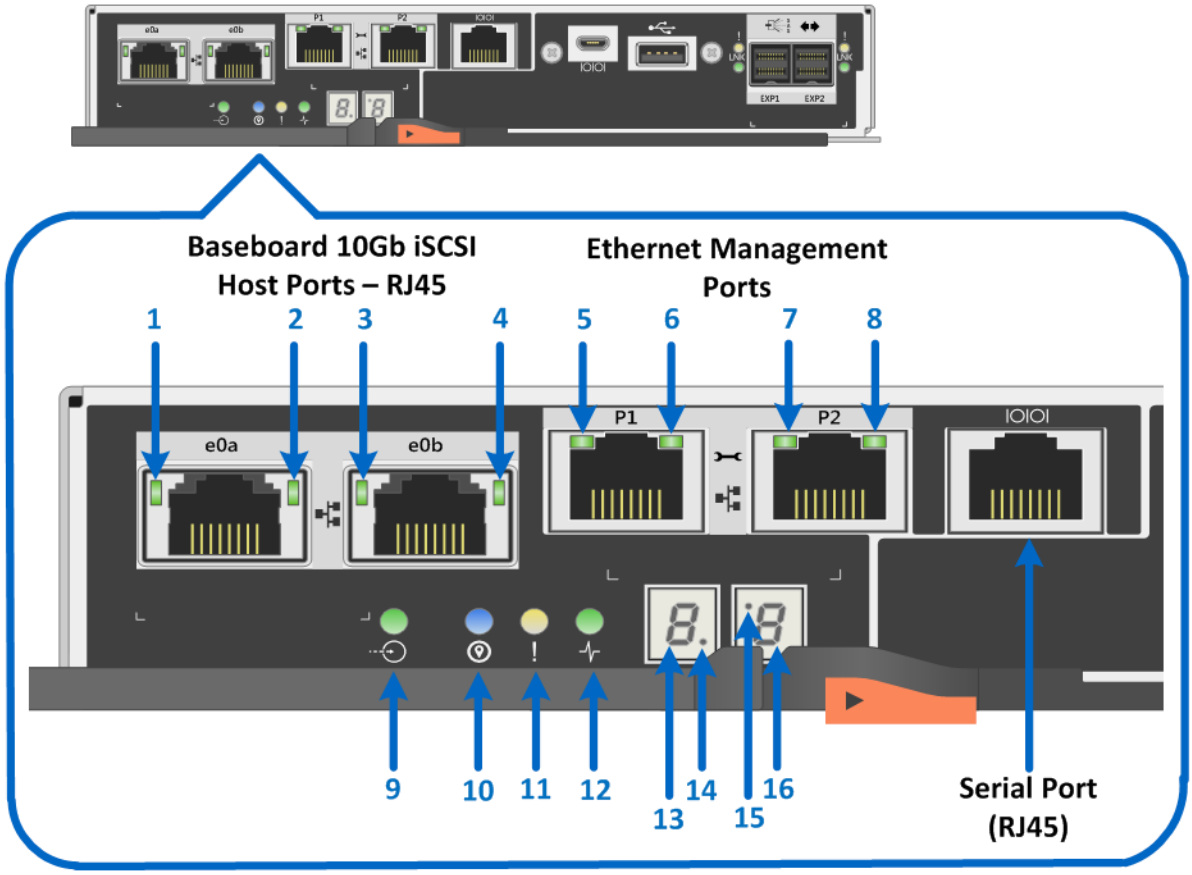
Figure 32) Viewing system status information by using SANtricity System Manager.



Controller Base Port Status LEDs

Figure 33 shows the onboard LED status indicators on the left side of the EF280 controller canister with the RJ-45 iSCSI baseboard host ports. Most of the LEDs are lit when a fault condition exists. However, the cache active LED is lit when the cache is active. The seven-segment LEDs provide status codes for both normal operation and fault conditions. The dot in the first seven-segment LED is the controller heartbeat indicator, which comes on when an intercontroller communication link has been established. The dot in the second seven-segment LED is on to indicate a diagnostic code. Otherwise, the display indicates the shelf ID.

Figure 33) LEDs on left side of EF280 controller canister with RJ-45 iSCSI host ports.



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

Table 15 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 33). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

Table 15) iSCSI RJ-45 baseboard host port LED definitions.

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

Table 16 defines the Ethernet management port LEDs on the controller (LEDs 5 through 8 in Figure 33).

Table 16) Ethernet management port LED definitions.

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

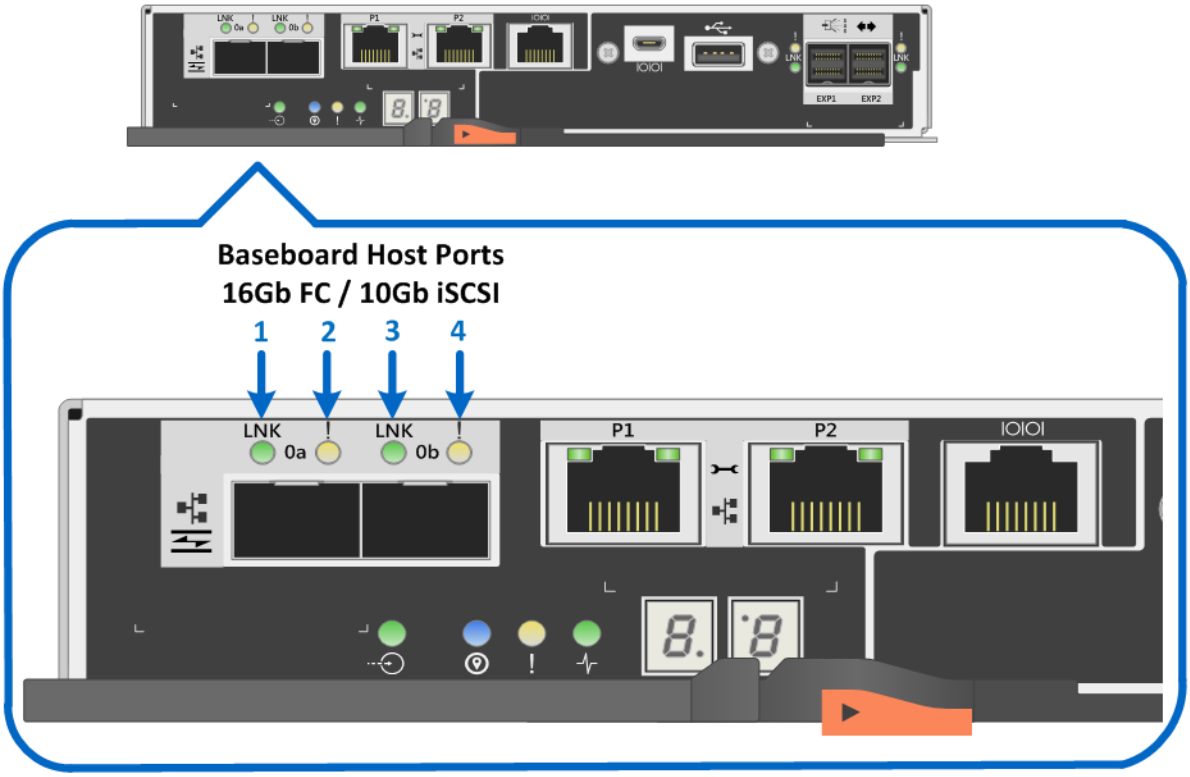
Table 17 defines the controller status LEDs (LEDs 9 through 15 in Figure 33).

Table 17) Controller base features LED definitions.

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

Figure 34 shows the onboard LED status indicators on the left side of the EF280 controller canister with the 16Gb FC/10Gb iSCSI baseboard host port LEDs indicated.

Figure 34) LEDs on left side of EF280 controller canister with 16Gb FC/10Gb iSCSI host ports.



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

Table 18 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 34). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

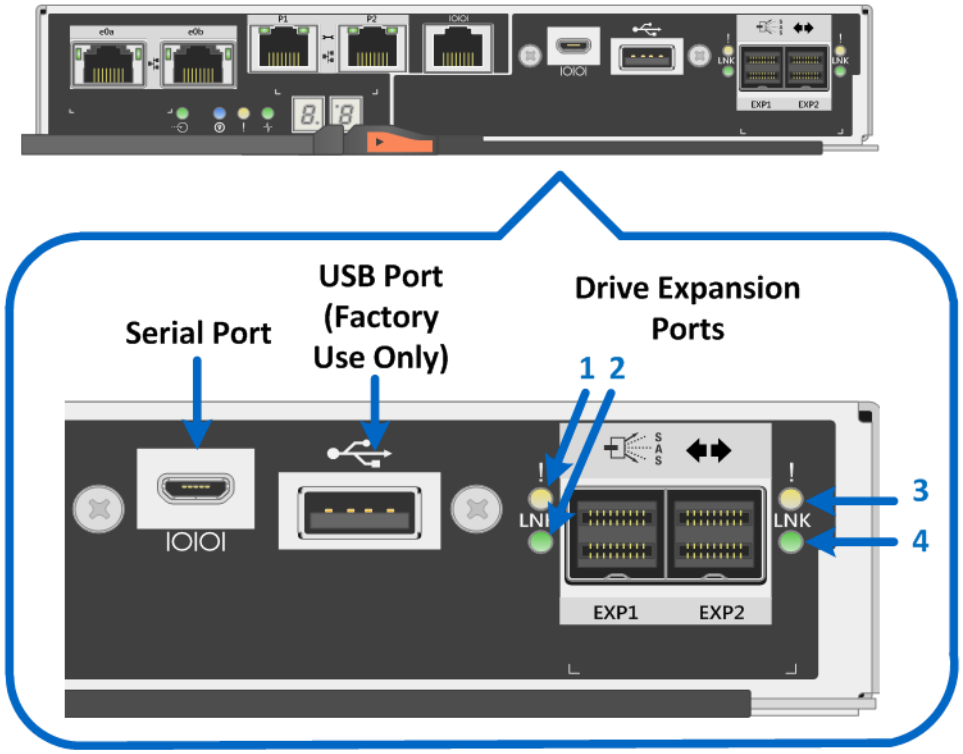
Table 18) 16Gb FC/10Gb iSCSI baseboard host port LED definitions.

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

Drive-Side SAS Expansion Port LEDs

The EF280 controller canister is equipped with two SAS expansion ports that are used to connect expansion drive shelves to the EF280 controller shelf. Figure 35 shows the SAS expansion port LEDs.

Figure 35) LEDs for drive expansion ports (no HIC installed).



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

Table 19 defines each drive-side LED (LEDs 1 through 4 in Figure 35).

Table 19) Drive expansion port LED definitions.

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

EF280 Optional Host Interface Cards

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

2-Port 100Gb IB HIC LEDs

The 2-port 100Gb IB HIC is shown in Figure 36.

Figure 36) LEDs on 2-port 100Gb IB HIC.

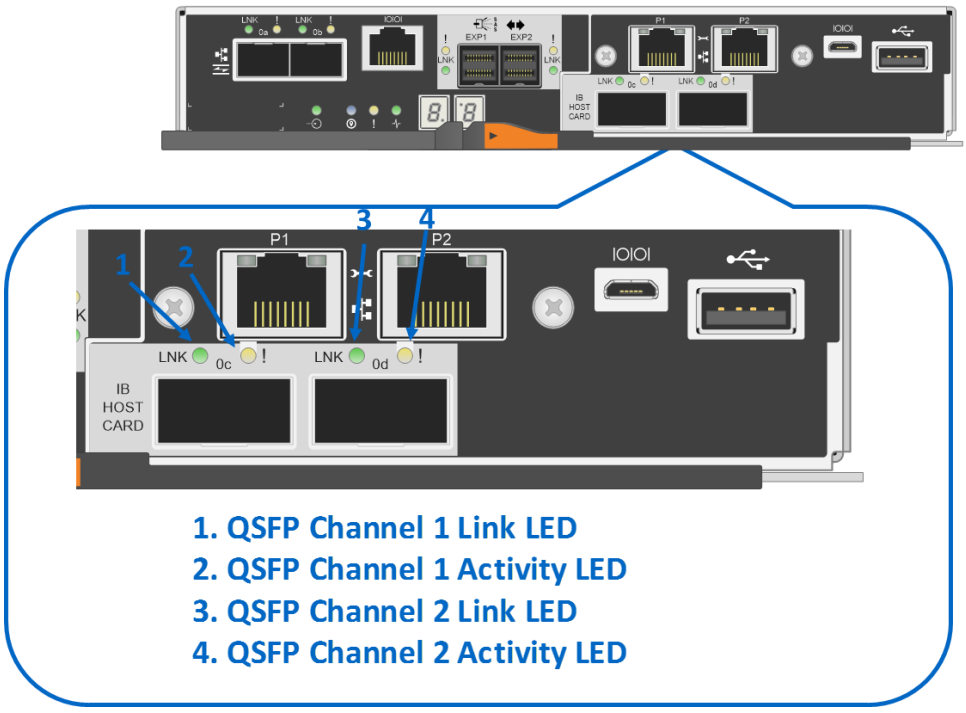


Table 20 defines the LEDs on the 2-port 100Gb IB HIC.

Table 20) 2-port 100Gb IB HIC LED definitions.

LED Name	Color	LED On	LED Off
QSFP link	Amber	The physical link is active.	The physical link is not active.
QSFP activity	Green	• Solid: Link is up without activity. • Blinking: Link is up with activity.	The controller has not yet loaded the driver for the ConnectX host channel adapter.

4-Port 12Gb SAS HIC LEDs

Figure 37 shows the LEDs for the 4-port 12Gb SAS HIC. As shown, the ports use mini-SAS 3 cables.

Figure 37) LEDs for 4-port 12Gb SAS HIC.

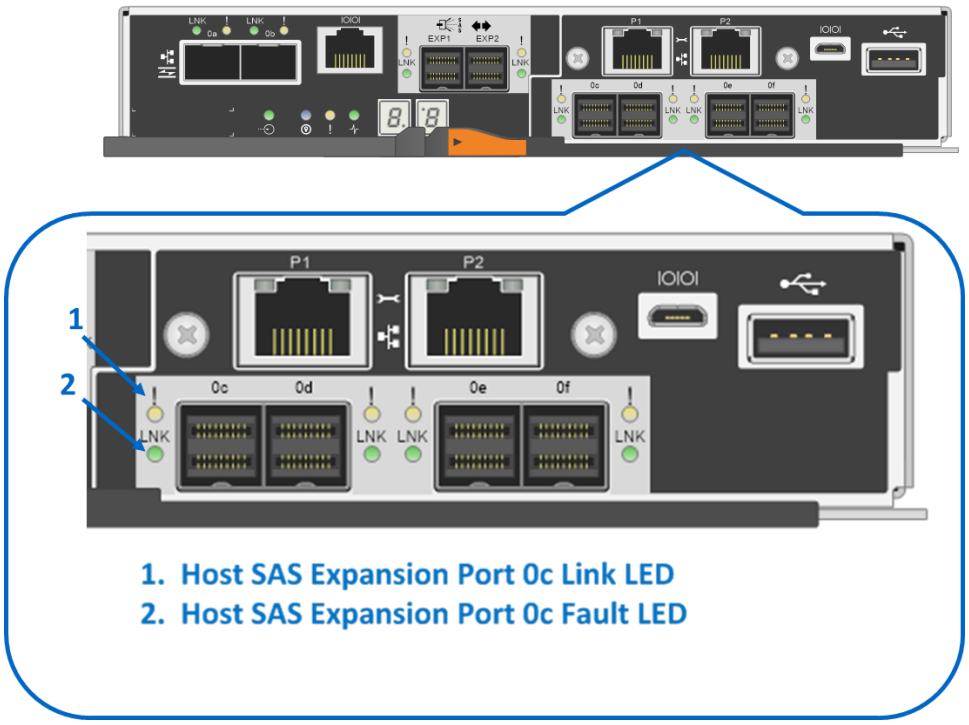


Table 21 defines the LEDs for the 12Gb SAS HICs.

Table 21) 4-port 12Gb SAS HIC LED definitions.

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

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

4-Port 32Gb FC HIC LEDs

The EF280 controller supports a 4-port 32Gbps FC HIC that offers the ability to autonegotiate down to 16Gbps using the 32Gbps SFP. The new 32Gbps FC HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 38 shows the LEDs for the 4-port 32Gbps FC HIC.

Figure 38) LEDs for 4-port 32Gb FC HIC.

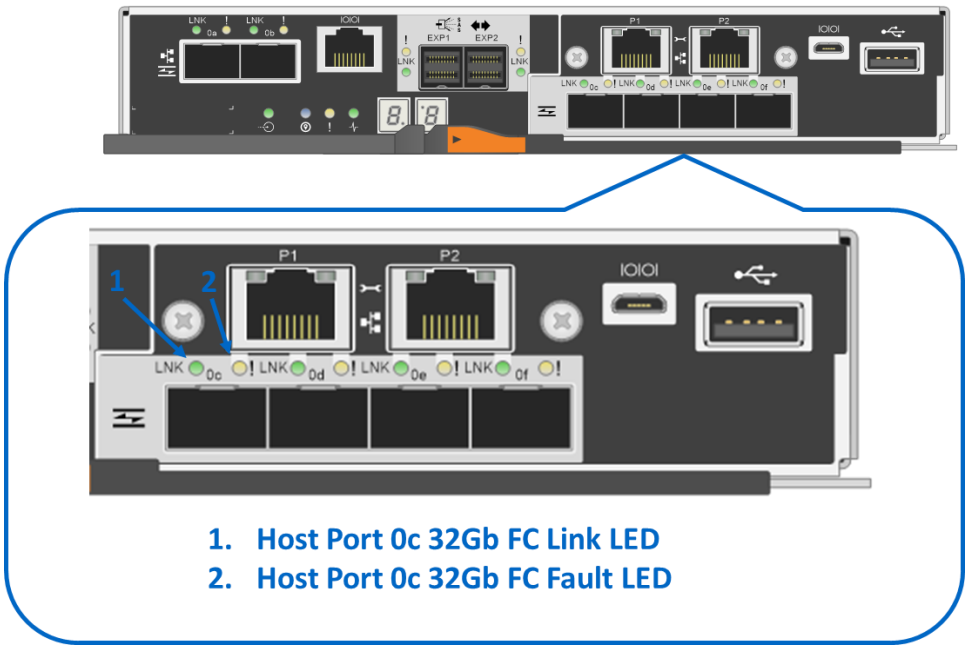


Table 22 defines the LEDs on the 4-port 32Gbps optical HIC.

Table 22) 4-port 32Gb FC HIC LED definitions.

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

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

4-Port 25Gb iSCSI HIC LEDs

The EF280 controller supports a 4-port 25Gbps iSCSI HIC that offers the ability to also run at 10Gbps by changing the port speed on each controller in SANtricity System Manager without changing the 25Gbps SFP (25Gbps SFP supports 10Gbps speed). The new 25Gbps iSCSI HIC does require OM4 fiber cable to connect to switches or directly to hosts. Figure 39 shows the LEDs for the 4-port 25Gbps iSCSI HIC.

Figure 39) LEDs for 4-port 25Gb iSCSI HIC.

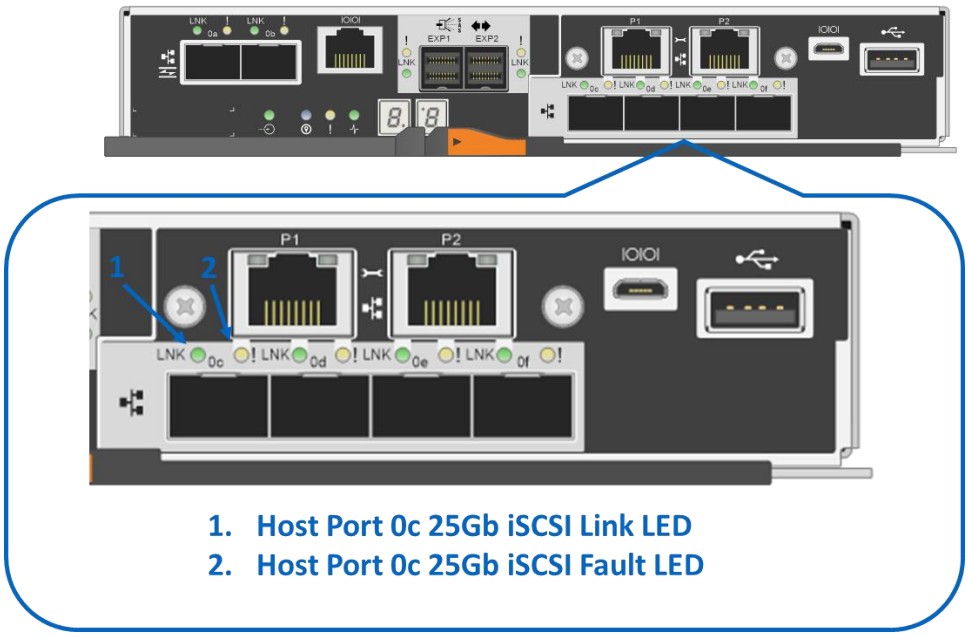


Table 23 provides the LED definitions for the 25Gbps iSCSI HIC.

Table 23) 4-port optical 25Gb iSCSI HIC LED definitions.

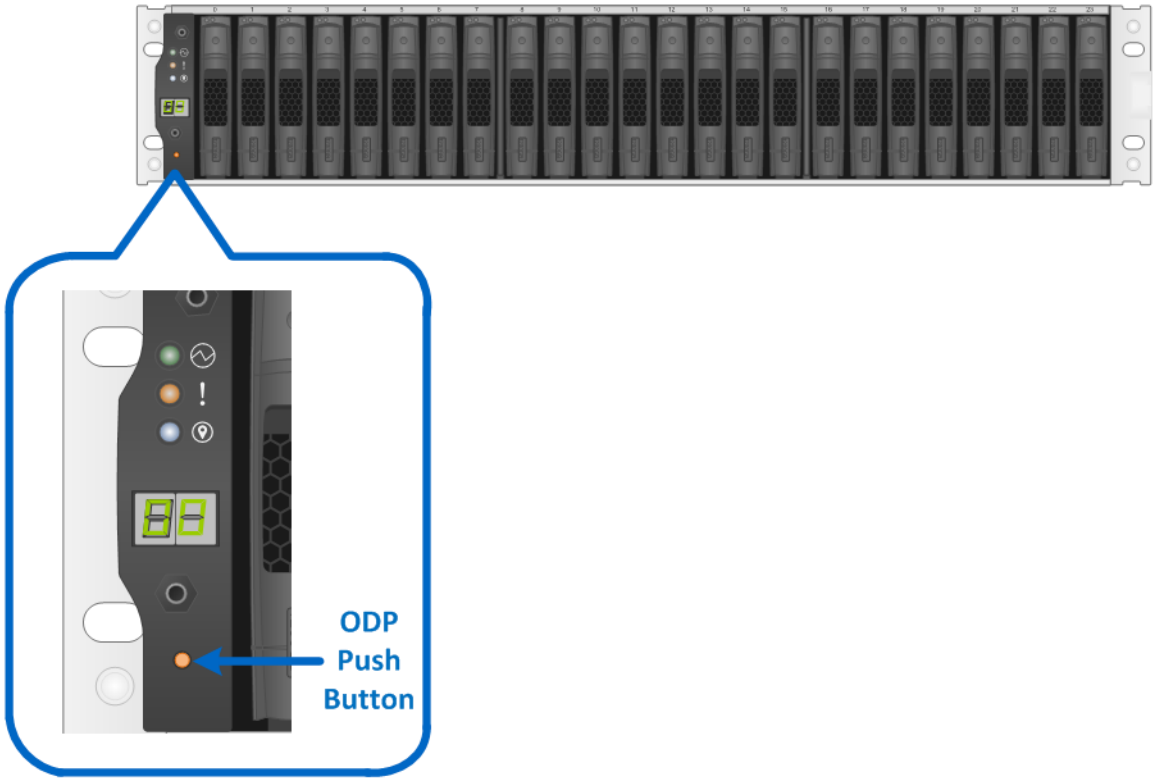
LED Speed (Left Side)	LED Activity (Right Side)	Link Rate	Color
On	On	Link operating at 25Gbps; no activity.	Green
	Blinking	Link operating at 25Gbps with active I/O in progress.	Green
Off	On	Link operating at 10Gbps; no activity.	Green
	Blinking	Link operating at 10Gbps with active I/O in progress.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

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

6.4 Setting Shelf ID with ODP Pushbutton

The shelf ID for the controller shelves and drive shelves can be changed externally by using the ODP pushbutton, shown in Figure 40 for the EF280 (DE224C).

Figure 40) ODP on the DE224C (front bezel or end caps removed).



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

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

For additional information about the EF280 storage systems and related hardware, refer to the EF280 documentation at http://mysupport.netapp.com/eseries.

7 Drive Shelves

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

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

Figure 41, Figure 42, and Figure 43 show the front and rear views of the DE224C drive shelf.

Figure 41) DE224C front view with end caps.

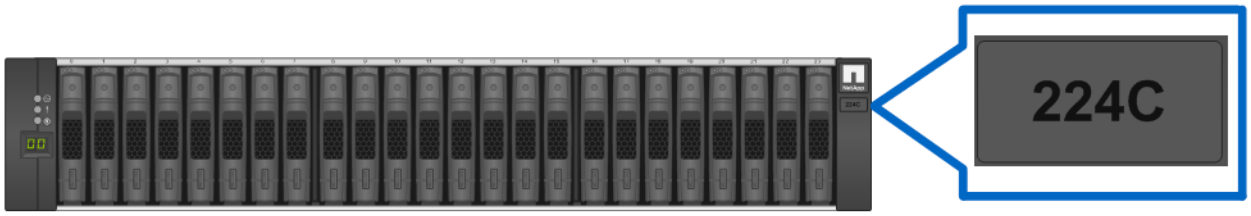


Figure 42) DE224C front view without end caps.

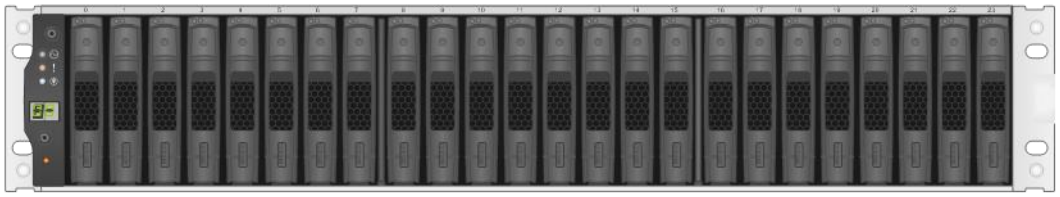
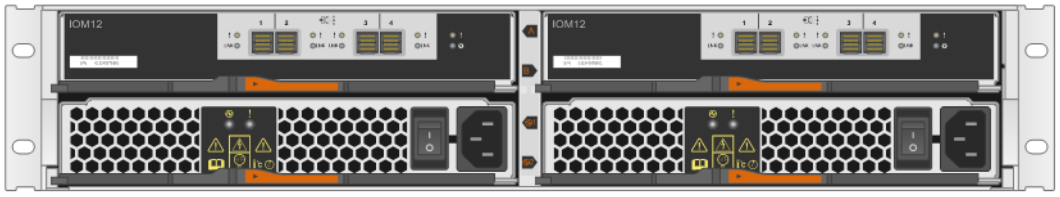


Figure 43) DE224C rear view.

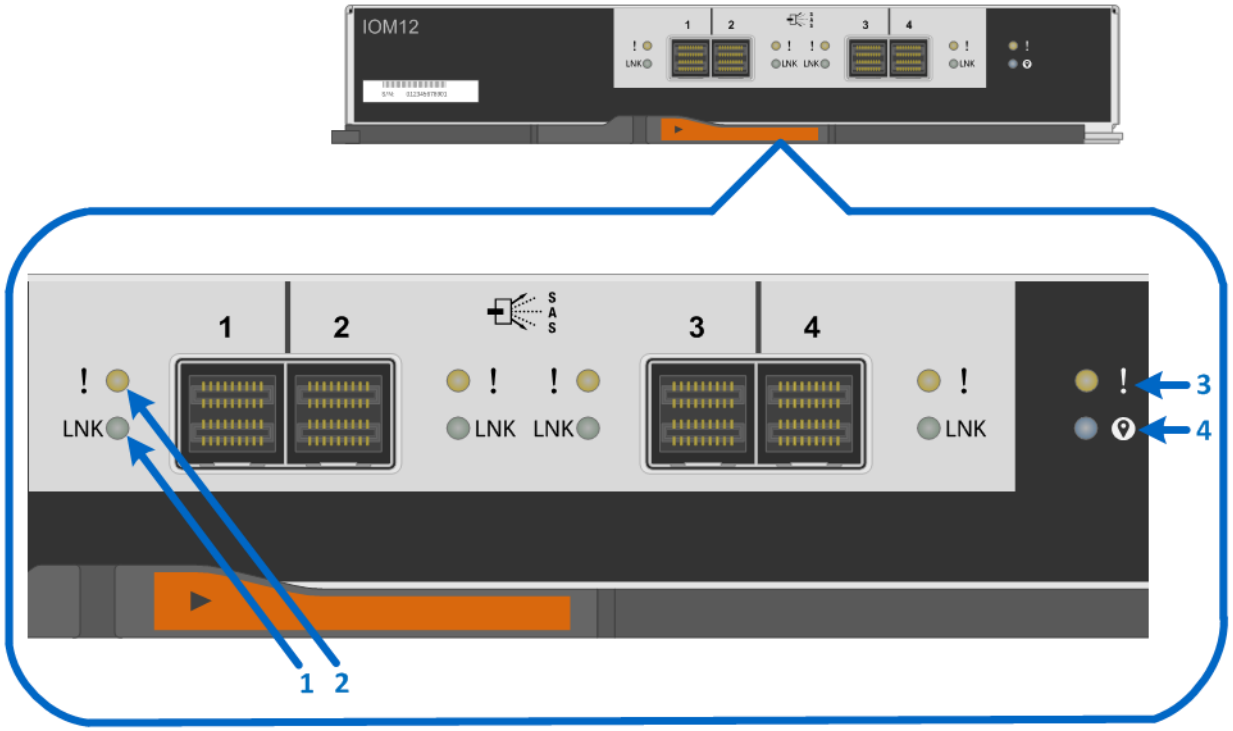


The modular design of the DE224C make the hardware easy to deploy and maintain over the life of the storage system.

IOM LED Definitions

Figure 44 shows the LEDs for the 4-port 12Gb SAS 3 IOM. LEDs are highlighted only for SAS expansion port 1 and for the IOM. SAS expansion ports 2 through 4 have the same LEDs.

Figure 44) LEDs for IOM.



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

Table 24 defines the LEDs for the IOM.

Table 24) IOM LED definitions.

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

Drive LED Definitions

Figure 45 shows the LEDs on the drive carriers for the EF280 SSDs. The DE224C shelf in the EF280 architecture supports only 2.5-inch form-factor SSDs.

Figure 45) EF280 drive carrier LEDs.

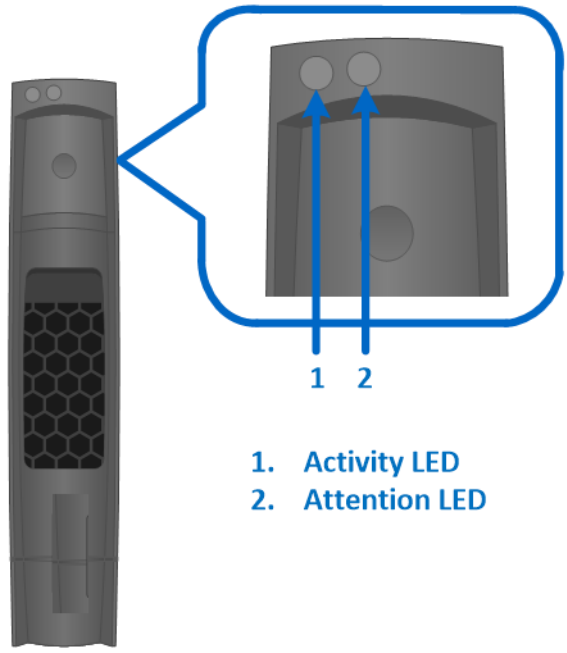


Table 25 defines the LEDs for the drives.

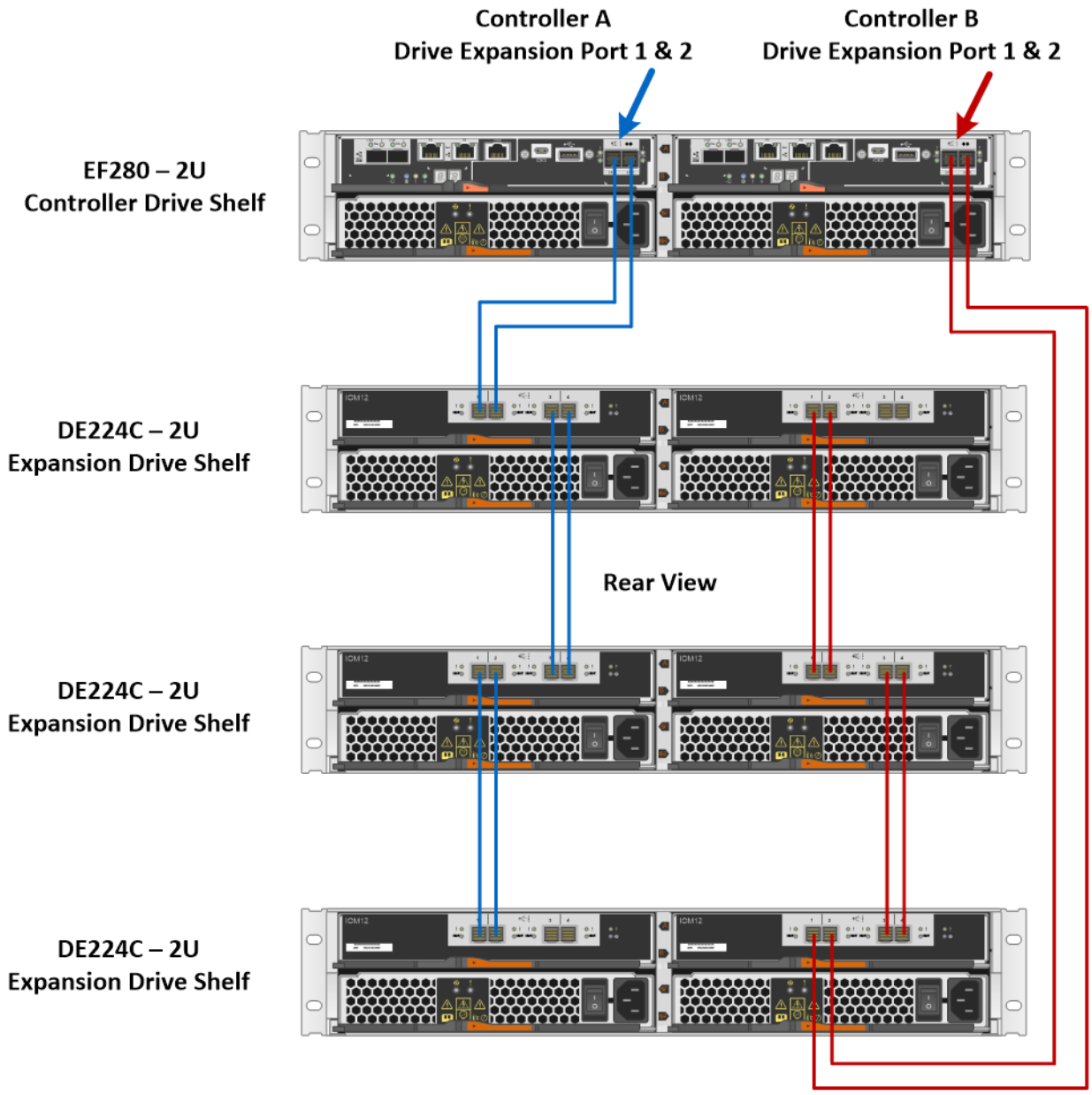
Table 25) EF280 drive LED definitions.

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

7.1 Greenfield Installation

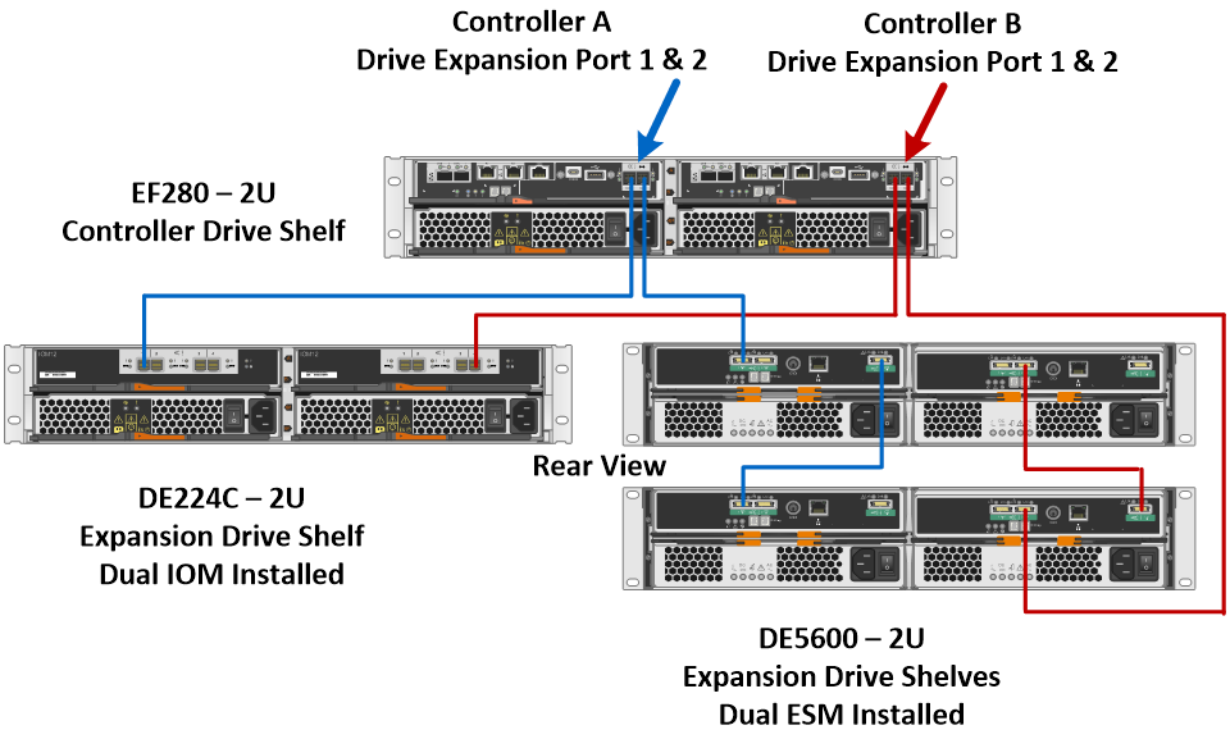
EF280 storage systems use a single-stack method where both controllers have a 12Gbps SAS path to both the expansion port 1 and expansion port 2 paths, as shown in Figure 46.

Figure 46) EF280 expansion drive shelf cabling example for maximum DE224C shelf configuration.



For optimal performance, SAS 2 and SAS 3 drive shelves should be isolated into different storage systems. If you decide to combine SAS 2 and SAS 3 shelves on the same EF280, use the double-stack cabling method shown in Figure 47.

Figure 47) EF280 with mixed 6Gbps and 12Gbps expansion shelves.



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

Best Practice

When initially powering on an E-Series storage system that includes expansion drive shelves, power on the expansion drive shelves first and wait one to two minutes per drive shelf before powering on the controller shelf.

Best Practice

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

7.2 Drive Shelf Hot Add

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

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

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

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

Figure 48 and Figure 49 show the hot-add connectivity when a drive shelf is added as the last shelf in the system.

Figure 48) Drive shelf hot-add controller expansion A-side cabling.

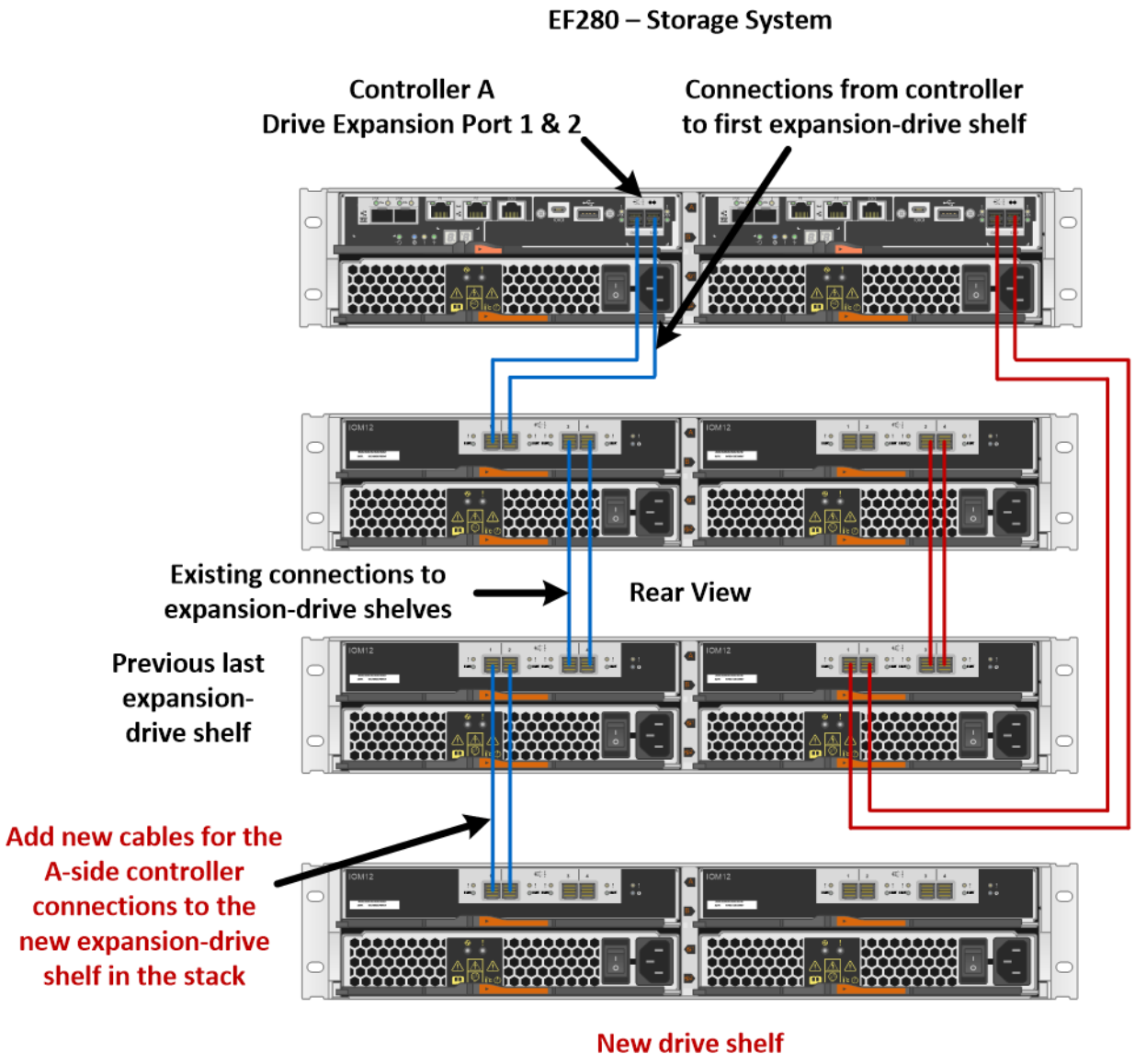
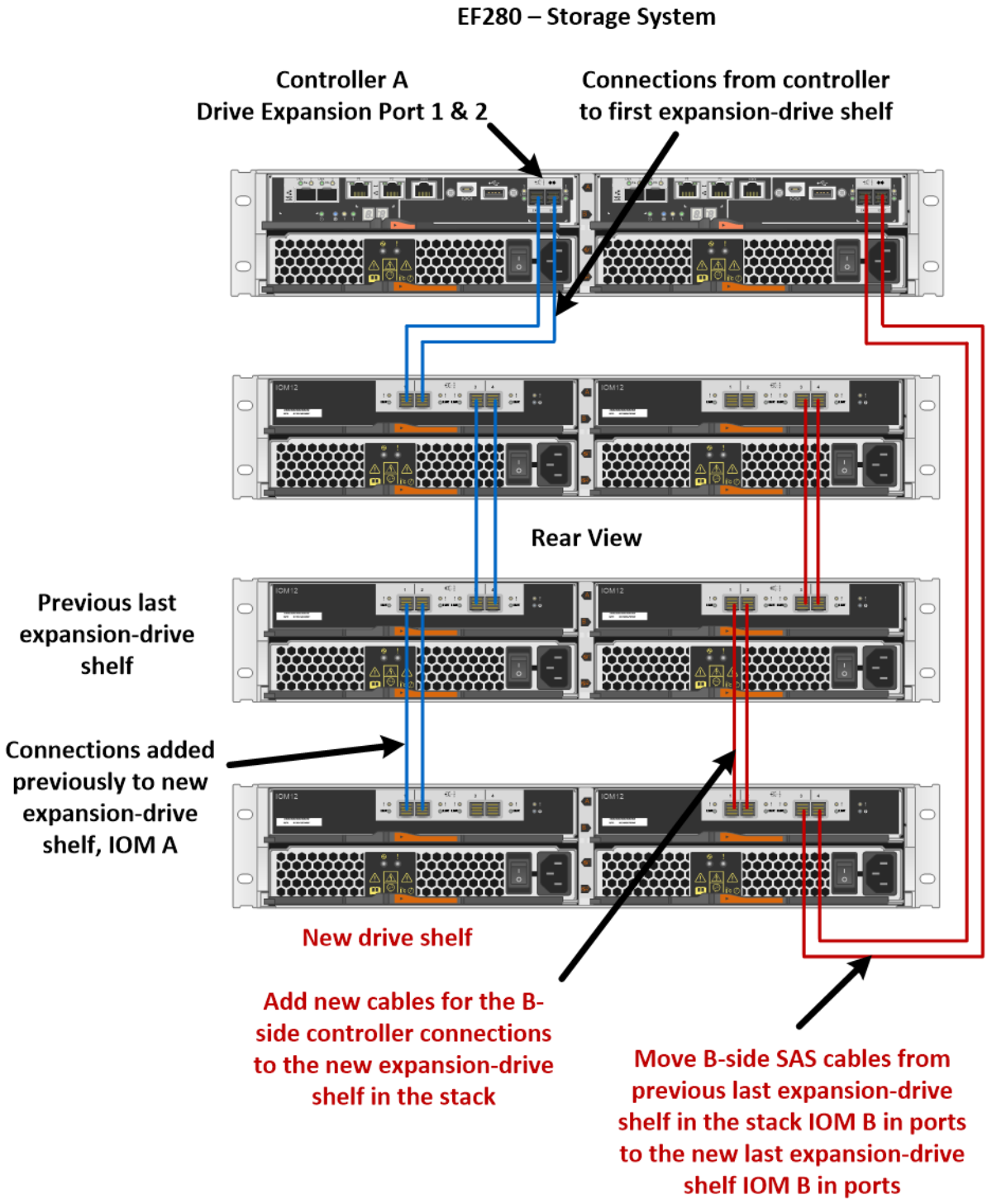


Figure 49) Drive shelf hot-add controller expansion B-side cabling.



Best Practice

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

- The existing power infrastructure can support the additional hardware.
- The cabling plan for the new shelf does not simultaneously interrupt both SAS expansion paths for controller A and controller B to the expansion drive shelves.
- The new expansion port 1 path is confirmed to be good, and the new shelf is visible in the SANtricity management software before expansion path 2 is disconnected and moved to the new shelf.

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

8 E-Series Product Support

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

8.1 Controller Shelf Serial Number

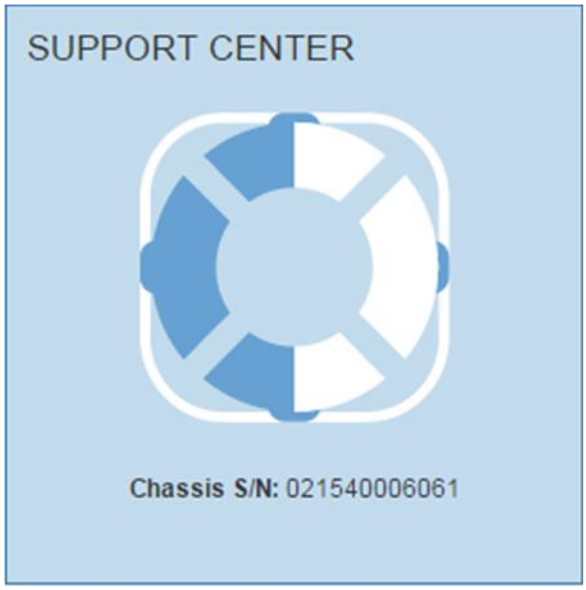
The EF280 storage systems are shipped preconfigured from the factory (controllers have HICs and batteries installed, and controllers are installed in the controller shelf). The chassis serial number is printed on a white label that is affixed to the controller shelf behind the right end cap on the front of the chassis. The SN is identified by the text “SN,” which is shown in Figure 50.

Figure 50) Controller shelf SN.

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

On a running storage system, the chassis serial number is also available through SANtricity System Manager by hovering your cursor over the Support Center tile, as shown in Figure 51.

Figure 51) SANtricity System Manager Support Center tile showing chassis serial number.



8.2 License Keys

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

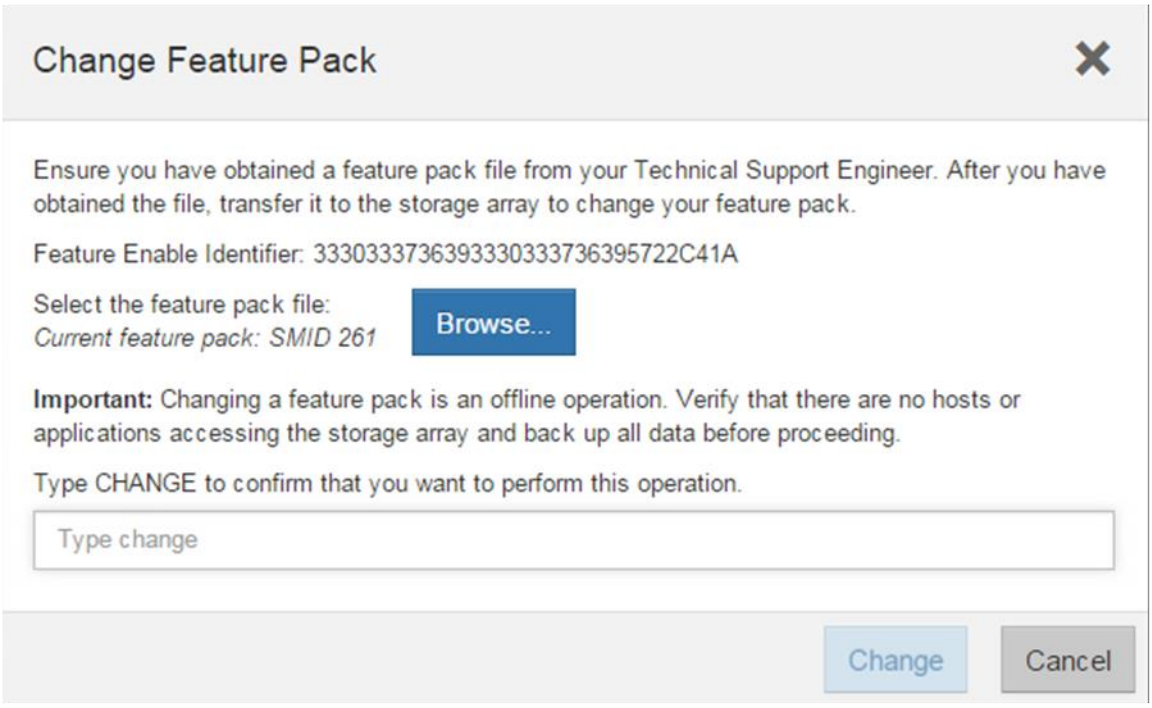
For the EF280 system, there is currently one premium feature, synchronous mirroring. All other features are enabled out of the box.

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

The EF280 controllers are equipped with onboard FC or iSCSI base ports from the factory, but feature pack keys are used to change the host interface protocol from FC to iSCSI or from iSCSI to FC. The feature pack keys are also used to change the protocol on IB HIC cards between iSER, SRP, and NVMe-oF (IB). 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 at https://mysupport.netapp.com/eseries.

After the feature pack file has been downloaded to the host server, use SANtricity System Manager to change the feature pack, as shown in Figure 52.

Figure 52) Change Feature Pack option.



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

Summary

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

EF280 storage systems provide extreme performance and versatility, including multiple host interface choices, multiple RAID choices, and the ability to scale up to 1.4PB of raw capacity. The EF280 is a modern, ready-to-work, all-flash storage system. For high–random IOPS environments, the EF280 supports 300k 4KB read IOPS, and for high-bandwidth workloads, the EF280 supports up to 10GBps of sequential reads.

Appendix

System Manager Tables

SANtricity System Manager includes many of the same array-based tasks for the EF280 storage arrays that are also included in the SANtricity AMW for other types of arrays. If you previously used the AMW, but are now using System Manager, you can refer to the following tables for a list of AMW functions and their corresponding locations in System Manager. The SANtricity System Manager online help is also an excellent reference guide.

Storage Array Options

Table 26 details how functions performed on the storage array are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 26) Storage array options: AMW compared with System Manager.

Function	AMW	System Manager		
	Storage Array > Option	Page	Tile	Option
Enable Premium features and feature pack	Premium Features	Settings	System	• Enable Premium Feature • Change Feature Pack
Set array password	Security > Set Password	Top, right area	N/A	• Preferences > Change Password • When you first log in and a password has not been set, you are required to enter a password.
Use drive security feature	Security > Create Key & Change Key	Settings	System	Change/Create Key
	Security > Save Key			Back Up Key
	Security > Validate Key			Validate Key
	Security > Import Key			Unlock Secure Drives
Change cache settings	Change > Cache Settings	Settings	System	Change Cache Settings
Set failover alert delay	Change > Failover Alert Delay	CLI/script editor only: Default is 5 minutes.		
Change iSCSI settings	iSCSI > Manage Settings	Settings	System	Configure Authentication View/Edit Target Discovery Settings

Function	AMW	System Manager		
	iSCSI > View/End Sessions			View/End iSCSI Sessions; also available under Support > Support Center > Diagnostics tab
Set automatic configuration	Configuration > Automatic > Disk Pools	Storage	Pools & Volume Groups	More > Launch pool autoconfiguration
	Configuration > Automatic > Volume Groups	CLI/script editor only		
Set automatic load balancing	Configuration > Automatic Load Balancing > Enable/Disable	Settings	System	Enable/Disable Automatic Load Balancing
Configure hot spares	Configuration > Hot Spare Coverage	Hardware	N/A	Highlight a drive and select Assign hot spare
Clear configuration	Configuration > Clear > Storage Array	Settings	System	Clear Storage Array Configuration
	Configuration > Clear > Volume			Clear Storage Array Configuration
Rename array	Rename			Select Name field edit icon
Set preferences	Preferences	Top, right area	N/A	Preferences > Set preferences
Quit the program	Exit			Logout

Disk Pool Options

Table 27 details how functions performed on disk pools are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 27) Disk pool options: AMW compared with System Manager.

Function	AMW	System Manager		
	Storage > Disk Pool > Option	Page	Tile/Tab	Option
Create pools	Create	Settings	Pools & Volume Groups > All Capacity tab	Create > Pool Also available on Home under the Storage Hierarchy, Pool Object
Locate pools	Locate			More > Turn on locator lights
View associated physical components	View Associated Physical Components	Hardware	N/A	Use filter control in top area

Function	AMW	System Manager		
Enable security for pools	Secure Drives	Storage	Pools & Volume Groups > All Capacity tab	More > Enable security
Add drive capacity	Add Drives (Capacity)			Add Capacity
Remove drive capacity	Remove Drives (Capacity)			More > Remove capacity
Replace drives (logical replacement)	Replace Drives	Hardware	N/A	Highlight a drive and select Logically replace
Change capacity settings	Change > Settings	Storage	Pools & Volume Groups > All Capacity tab	View/Edit Settings
Change ownership	Change > Ownership/Preferred Path	Storage	Volumes	More > Change ownership
Rename disk pool	Rename	Storage	Pools & Volume Groups > All Capacity tab	• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Delete disk pool	Delete			Uncommon Tasks > Delete
Check volume redundancy	Advanced > Check Redundancy			Uncommon Tasks > Check volume redundancy

Volume Group Options

Table 28 details how functions performed on volume groups are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 28) Volume group options: AMW compared with System Manager.

Function	AMW	System Manager		
	Storage > Volume Group > Option	Page	Tile/Tab	Option
Create volume group	Create	Settings	Pools & Volume Groups > All Capacity tab	• Create > Volume group • Also available on Home under the Storage Hierarchy, Volume Group Object
Locate volume group	Locate			More > Turn on locator lights

Function	AMW	System Manager		
View associated physical components	View Associated Physical Components	Hardware	N/A	Use filter control in top area
Enable security	Secure Drives	Storage	Pools & Volume Groups > All Capacity tab	More > Enable security
Add capacity	Add Drives (Capacity)			Add Capacity
Replace drives (logical replacement)	Replace Drives	Hardware	N/A	Highlight a drive and select Logically replace
Change ownership	Change > Ownership/Preferred Path	Storage	Volumes	More > Change ownership
Change RAID level	Change > RAID level	Storage	Pools & Volume Groups > All Capacity tab	View/Edit Settings
Rename volume group	Rename	Storage	Pools & Volume Groups > All Capacity tab	• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Delete volume group	Delete			Uncommon Tasks > Delete
Export and import volume group	Advanced > Export & Import	CLI/script editor only		
Initialize volumes	Advanced > Initialize	Storage	Volumes	More > Initialize volumes
Defragment volume groups	Advanced > Defragment	Storage	Pools & Volume Groups > All Capacity tab	• Uncommon Tasks > Consolidate volume group free capacity • Also available on the Home page in the notification area if there is a volume group with more than one free capacity area
Check redundancy	Advanced > Check Redundancy			Uncommon Tasks > Check volume redundancy

Volume Options

Table 29 details how functions performed on volumes are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 29) Volume options: AMW compared with System Manager.

Function	AMW	System Manager		
	Storage > Volume > Option	Page	Tile/Tab	Option
Create volume	Create	Storage	Volumes > All Volumes tab or Applications & Workloads tab	• Create > Volume • Also available on Home under the Storage Hierarchy, Volume Object • Also available under the Pools & Volume Groups tile and the Host tile
Increase volume capacity	Increase Capacity			Increase Capacity
Increase or decrease repository capacity	Increase/Decrease Repository Capacity	Storage	Pools & Volume Groups > Reserved Capacity tab	• Increase Capacity • Decrease Capacity
Enable or disable SSD cache	SSD Cache > Enable/Disable	Storage	Volumes > All Volumes tab or Applications & Workloads tab	View/Edit Settings
Change modification priority	Change > Modification Priority			View/Edit Settings
Change cache settings	Change > Cache Settings			More > Change cache settings
Change media scan settings	Change > Media Scan Settings			More > Change media scan settings
Change preread redundancy check	Change > Pre-Read Redundancy Check			View/Edit Settings
Change ownership/ preferred path	Change > Ownership/Preferred Path	Storage	Volumes > All Volumes tab or Applications & Workloads tab	More > Change ownership
Change segment size	Change > Segment Size			View/Edit Settings (only on volumes in volume groups)
Change repository settings	Change > Repository Settings	Storage	Pools & Volume Groups > Reserved Capacity tab	View/Edit Settings

Function	AMW	System Manager		
Add volume to consistency group	Add to Consistency Group	Storage	Snapshots > Snapshot Consistency Group tab	Add Members
Remove volume from consistency group	Remove from Consistency Group			Remove: must expand consistency group and highlight individual volume member
View associated physical components	View Associated Physical Components	Hardware	N/A	Use filter control in top area. Can perform the filter on only a volume group or disk pool, not an individual volume.
Rename volume	Rename	Storage	Volumes > All Volumes tab or Applications & Workloads tab	View/Edit Settings Edit directly in the table view by selecting the pencil icon in the Edit column
Delete volume	Delete			Delete
Disable data assurance (DA)	Advanced > Disable Data Assurance (DA)	Storage	Volumes > All Volumes tab or Applications & Workloads tab	View/Edit Settings
Initialize volumes	Advanced > Initialize			More > Initialize volumes
Place volumes online	Advanced > Place Volumes Online	CLI/script editor only		
Redistribute volumes	Advanced > Redistribute Volumes	Storage	Volumes > All Volumes tab or Applications & Workloads tab	More > Initialize volumes
View repository expansion history	Advanced > View Repository Expansion History	Storage	Volumes > Thin Volume Monitoring tab	Select and expand a thin volume to see expansion history

Copy Services Options

Snapshot Group

Table 30 details how functions performed on Snapshot groups are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 30) Snapshot group options: AMW compared with System Manager.

Function	AMW	System Manager		
	Copy Services > Snapshot Group > Option	Page	Tile/Tab	Option
Create, Create Snapshot Image, Revive, Overall Repository > Change Modification Priority, Change Media Scan Settings, Change Pre-Read Redundancy Check		The Snapshot group object has been abstracted as much as possible from the end user and is created because of other Snapshot operations. The only aspects that are still exposed are the items shown.		
Create or edit Snapshot image schedule	Create/Edit Snapshot Image Schedule	Storage	Snapshots > Schedule tab	All options (Create, Edit, Activate/Suspend, and Delete)
Change Snapshot group settings, including rename and properties	Change Settings	Storage	Pools & Volume Groups > Reserved Capacity tab	View/Edit Settings
Increase or decrease capacity of overall repository	Overall Repository > Increase/Decrease Capacity			Increase Capacity and Decrease Capacity
Delete Snapshot group	Delete			Uncommon Tasks > Delete Snapshot group
Cancel pending Snapshot image	Cancel Pending Snapshot Image			Uncommon Tasks > Cancel pending Snapshot image

Snapshot Image

Table 31 details how functions performed on Snapshot images are completed in the SANtricity Storage Manager AMW and how the same function is completed employing the SANtricity System Manager.

Table 31) Snapshot image options: AMW compared with System Manager.

Function	AMW	System Manager		
	Copy Services > Snapshot Image > (Option)	Page	Tile/Tab	Option
Create Snapshot image	Create	Storage	• Volumes > All Volumes tab or Applications & Workloads tab • Snapshots > Snapshot Images tab	• Copy Services > Create instant Snapshot image • Create > Instant Snapshot images
Create Snapshot volume	Create Snapshot Volume	Storage	Snapshots > Snapshot Images tab	Create > Snapshot volume
Start or resume rollback	Rollback > Start/Resume			Rollback> Start or Resume
Change priority of rollback	Rollback > Change Priority			Available as part of the Rollback > Start option
Cancel rollback	Rollback > Advanced > Cancel			Rollback > Cancel
Delete Snapshot image	Delete			Delete
View properties	Properties			View Settings

Snapshot Volume

Table 32 details how functions performed on Snapshot volumes are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 32) Snapshot volume options: AMW compared with System Manager.

Function	AMW	System Manager		
	Copy Services > Snapshot Volume > Option	Page	Tile/Tab	Option
Create Snapshot volume	Create	Storage	• Snapshots > Snapshot Images tab • Snapshots > Snapshot Volumes tab	• Create > Instant Snapshot image • Create
Create volume copy	Create Snapshot Volume	Storage	Snapshots > Snapshot Volumes tab	Copy Volume
Re-create and disable Snapshot volume	Rollback > Start/Resume			Uncommon Tasks > Re-create and Disable
Convert to read/write volume	Rollback > Change Priority			Convert to Read/Write
Enable or disable SSD cache for a Snapshot volume	Rollback > Advanced > Cancel			• As part of Create wizard • View/Edit Settings
Change settings	Change Settings			View/Edit Settings
Rename Snapshot volume	Rename			• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Delete Snapshot volume	Delete			Uncommon Tasks > Delete
View properties of a Snapshot volume	Properties			View/Edit Settings

Function	AMW	System Manager		
Increase or decrease overall repository capacity	Overall Repository > Increase and Decrease Capacity	Storage	Pools & Volume Groups > Reserved Capacity tab	Increase Capacity and Decrease Capacity
Revive Snapshot volume	Advanced > Revive	CLI/script editor only		
Modify overall repository	Overall Repository > Change > Modification Priority > Media Scan Settings > Pre-Read Redundancy Check	CLI/script editor only: the end user does normally not change these. The defaults should suffice.		

Volume Copy

Table 33 details how functions performed for volume copy are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 33) Volume copy options: AMW compared with System Manager.

Function	AMW	System Manager		
	Copy Services > Volume Copy > Option	Page	Tile/Tab	Option
Copy volume	Create	Storage	Volumes > All Volumes tab or Applications & Workloads tab	Copy services > Copy volume
Manage copies	Manage Copies	CLI/script editor only: You can also stop a volume copy and change priority in the Operations in Progress from Home.		

Asynchronous Mirroring

Table 34 details how functions performed for asynchronous mirroring are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 34) Asynchronous mirroring options: AMW compared with System Manager.

Function	AMW	System Manager		
	Copy Services > Asynchronous Mirroring > Option	Page	Tile/Tab	Option
Activate mirroring	Activate	The activation takes place automatically when the first mirror consistency group is created.		

Function	AMW	System Manager		
Deactivate mirroring	Deactivate	Storage	Asynchronous Mirroring > Mirror Consistency Groups tab	Uncommon Tasks > Deactivate
View mirroring port connections	View Mirroring Port Connections	CLI/script editor only: Although some of the same information is included in the Test Communication option.		
Create mirror group	Mirror Group > Create	Storage	Asynchronous Mirroring > Mirror Consistency Groups tab	• Create Mirrored Pair: If needed the mirror group is created as part of this sequence. **Note:** You can also mirror a volume from the Volumes tile by highlighting a volume and selecting Copy Services > Mirror a volume asynchronously.
Create mirrored pair	Mirror Group > Create Mirrored Pair	Storage	Asynchronous Mirroring > Mirror Consistency Groups tab Asynchronous Mirroring > Mirrored Pairs tab	Create Mirrored Pair
Complete mirrored pair	Mirror Group > Complete Mirrored Pair	Storage	Asynchronous Mirroring > Mirrored Pairs tab	Complete link in table
Suspend or resume mirroring	Mirror Group > Suspend/Resume	Storage	Asynchronous Mirroring > Mirror Consistency Groups tab	More > Suspend/Resume
Manually resynchronize mirror group	Mirror Group > Manual Resynchronization			More > Manually resynchronize
Change sync settings	Mirror Group > Change > Synchronization Settings			More > Edit settings
Change role from primary to secondary	Mirror Group > Change > Role to Primary or Secondary			More > Change role
Change communication settings	Mirror Group > Test Communication Link			Test Communication

Function	AMW	System Manager		
Update remote IP address	Mirror Group > Update Remote IP Address			More > Update remote IP address
Rename mirror group	Mirror Group > Rename			Edit directly in the table view by selecting the pencil icon in the Edit column
Delete mirror group	Mirror Group > Delete			Uncommon Tasks > Delete
Cancel pending role change	Mirror Group > Advanced > Cancel Pending Role Change	CLI/script editor only		
Create mirrored pair	Mirrored Pair > Create	Storage	Asynchronous Mirroring > Mirror Consistency Groups tab Asynchronous Mirroring > Mirrored Pairs tab	Create Mirrored Pair
Remove mirrored pair	Mirrored Pair > Remove	Storage	Asynchronous Mirroring > Mirror Consistency Groups tab	Uncommon Tasks > Remove
Increase capacity and settings for overall repository	Mirrored Pair > Overall Repository > Increase Capacity and Settings	Storage	Pools & Volumes Groups > Reserved Capacity tab	Increase Capacity and View/Edit Settings
Modify overall repository	Mirrored Pair > Overall Repository > Change > Modification Priority > Media Scan Settings > Pre-Read Redundancy Check	CLI/script editor only: the end user does normally not change these. The defaults should suffice.		

Synchronous Mirroring

Table 35 details how functions performed for synchronous mirroring are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 35) Synchronous mirroring options: AMW compared with System Manager.

Function	AMW	System Manager		
	Copy Services > Snapshot Group > Option	Page	Tile/Tab	Option
Activate mirroring	Activate	The activation takes place automatically when the first mirrored pair is created.		
Deactivate mirroring	Deactivate	Storage	Synchronous Mirroring	Uncommon Tasks > Deactivate
View mirroring port connections	View Mirroring Port Connections	CLI/script editor only: Although some of the same information is included in the Test Communication option.		
Create mirrored pair	Create Mirrored Pair	Storage	Synchronous Mirroring	• Mirror volume or create mirrored pair **Note:** You can also mirror a volume from the Volumes tile by highlighting a volume and selecting Copy Services > Mirror a volume synchronously.
Suspend or resume mirroring	Suspend/Resume			More > Suspend or Remove
Change role from primary to secondary	Change > Role to Primary/Secondary			More > Change role
Change sync settings	Change > Synchronization Settings			More > View/Edit settings
Change write mode	Change > Write Mode	Obsolete; no longer applicable		
Remove mirror relationship	Remove Mirror Relationship	Storage	Synchronous Mirroring	Uncommon Tasks > Remove
Test communication link	Test Communication Link			Test Communication

Host Mapping Options

Table 36 details how functions performed for host mapping are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 36) Host mapping options: AMW compared with System Manager.

Function	AMW	System Manager		
	Host Mapping > Option	Page	Tile/Tab	Option
Define host group	Define Host Group	Storage	Hosts	Create > Host cluster
Define host	Define Host			Create > Host
Define storage partition	Define Storage Partition	N/A: Storage partition concept is abstracted from the end user.		
Add LUN mapping	LUN Mapping > Add	Storage	Hosts	Assign Volumes
Remove LUN mapping	LUN Mapping > Remove			Unassign Volumes
Change LUN mapping	LUN Mapping > Change	Storage	Volumes > All Volumes tab or Applications & Workloads tab	View/Edit Settings: can change host cluster/host assignment or LUN assignment
Manage host port identifiers	Manage Host Port Identifiers	Storage	Hosts	View/Edit Settings > Host Ports
View unassociated host port identifiers	View Unassociated Host Port Identifiers	Storage or CLI/Script Editor	Hosts	Create > Host and select the Host Ports drop-down menu to see any host ports that are currently not associated with a host
Change default host operating system	Default Group > Change Default Host Operating System **Note:** The default host cluster is shown in the GUI only if the user assigned at least one volume to it in the CLI.	Storage	Hosts	• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Rename host group	Host Group > Rename			• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Remove host group	Host Group > Remove			Delete

Function	AMW	System Manager		
Move host group	Host > Move			• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Change host operating system	Host > Change Host Operating System			• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Rename host	Host > Rename			• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Remove host	Host > Remove			Delete
View or edit host properties	Host > Properties			View/Edit Settings **Note:** Can also view/edit settings for a host cluster.

Hardware Options

Table 37 details how functions performed on hardware are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 37) Hardware options: AMW compared with System Manager.

Function	AMW	System Manager		
	Hardware > Option	Page	Tile/Tab	Option
Locate storage array	Locate Storage Array	Settings	System	Turn On Storage Array Locator Lights
Locate drive shelf	Locate (controller/drive tray, drive shelf)	Hardware	N/A	Select Shelf Number drop-down menu on left side of each shelf and then select Turn on locator light
Locate drive	Locate Drive			Select drive and then select Turn on locator light
View shelf components	Tray > View/Edit (Controller/Drive Components, Drive Components)			• Select Shelf Number drop-down menu on left side of each shelf and then select View settings • Select one of the icons at the top of each shelf

Function	AMW	System Manager		
View or edit drive channels	Tray > View/Edit Drive Channels			Select one of the controllers and then select View settings > Drive Interfaces tab
Change shelf ID	Tray > Change > ID			Select Shelf Number drop-down menu on left side of each shelf and then select Change ID
Change shelf view order	Tray > Change > Hardware View Order			Select either the up or down arrow on the right side of the shelf to move it up or down in the view
Change shelf battery settings	Tray > Change > Battery Settings			• Select Shelf Number drop-down menu on left side of each shelf and then select View settings • Select the battery icon at the top of each shelf
Change shelf alarm settings	Tray > Change > Alarm Settings	Not applicable for hardware platforms managed by System Manager		
Synchronize controller clocks	Controller > Synchronize Clocks	Settings	System	Synchronize Storage Array Clocks
Configure controller ports	Controller > Configure (Management ports, iSCSI ports, DNS Server, Network Time Protocol [NTP] Server)	Hardware	N/A	• Select one of the controllers and then select the appropriate option • Configure iSCSI ports is also available under Settings > System
Change preferred loop ID	Controller > Change > Preferred Loop ID	Not applicable for hardware platforms managed by System Manager		
Change remote login	Controller > Change > Remote Login	Hardware	N/A	Select one of the controllers and then select Change remote login
Place controller online or offline	Controller > Advanced > Place > Online/Offline			Select one of the controllers and then select Place online or Place offline
Place controller in service mode	Controller > Advanced > Place > In Service Mode			Select one of the controllers and then select Place in service mode
Run controller diagnostics	Controller > Advanced > Run Diagnostics (all options)	CLI/script editor only: Many of these diagnostics are not applicable for hardware platforms managed by System Manager.		

Function	AMW	System Manager		
Reset controller	Controller > Advanced > Reset	Hardware	N/A	Select one of the controllers and then select Reset
Enable data transfer	Controller > Advanced > Enable Data Transfer	CLI/script editor only		
Replace drive logically	Drive > Replace	Hardware	N/A	Select drive and then select Logically replace
Erase a secure drive	Drive > Erase Security	Hardware	N/A	• Select a secure, unassigned drive and then select Secure Erase • The option also comes up when you are creating a new pool or volume group
Import security key	Drive > Import Security Key	Settings	System	Unlock Secure Drives
Initialize drive	Drive > Initialize	Hardware	N/A	Select drive and then select Initialize
Manually reconstruct drive	Drive > Manually Reconstruct	CLI/script editor only		
Manually fail a drive	Drive > Fail	Hardware	N/A	Select drive and then select Fail
Revive drive	Drive > Revive	CLI/script editor only		
Assign a hot spare	Hot Spare Coverage	Hardware	N/A	Highlight a drive and select Assign hot spare
Prepare for removal	Prepare for Removal	CLI/script editor only		

Monitor Options

Health

Table 38 details how functions performed for health monitoring are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 38) Health monitoring options: AMW compared with System Manager.

Function	AMW	System Manager		
	Monitor > Health > Option	Page	Tile/Tab	Option
View health (Recovery Guru)	View Health (Recovery Guru)	Home	N/A	Click Recover from <n> problems link at top of home page
View real-time performance	Monitor Performance > Real-time performance monitor (graphical/textual)	• Home • Storage	• N/A • Performance	• Performance shown at the storage array level • Various options
View background performance	Monitor Performance > Background performance monitor (all options)			
Collect support data manually	Collect Support Data Manually	Support	Support Center > Diagnostics tab	Collect Support Data
Set AutoSupport options	AutoSupport (all options from both EMW and AMW)	Support	Support Center > AutoSupport tab	Various options
Retrieve trace buffers	Retrieve Trace Buffers	Storage	Support Center > Diagnostics tab	Retrieve Trace Buffers
Read link status	Storage Array Diagnostics > Read Link Status	Not applicable for hardware platforms managed by System Manager		
Collect I/O path statistics	Storage Array Diagnostics > Collect I/O Path Statistics	Support	Support Center > Diagnostics tab	Collect I/O Path Statistics
Validate configuration database	Storage Array Diagnostics > Validate Configuration Database	CLI/script editor only		
Retrieve controller health image	Storage Array Diagnostics > Retrieve Controller Health Image	Support	Support Center > Diagnostics tab	Retrieve Health Image
Collect drive data	Collect Drive Data (all options)	Support	Support Center > Diagnostics tab	Collect Drive Data
Capture state information	Capture State Information	CLI/script editor only		

Function	AMW	System Manager		
View iSCSI statistics	iSCSI Statistics	• Support • Settings	• Support Center > Diagnostics tab • System	• View iSCSI Statistics Packages • iSCSI settings grouping > View iSCSI Statistics Packages
Clear recovery mode	Clear Recovery Mode	Support	Support Center > Diagnostics tab	Clear Recovery Mode
Reenable drive ports	Re-enable Drive Ports			Re-enable Drive Ports

Reports

Table 39 details how functions performed for reporting are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 39) Report-monitoring options: AMW compared with System Manager.

Function	AMW	System Manager		
	Monitor > Reports > Option	Page	Tile/Tab	Option
View operations in progress	Operations in Progress	Home	N/A	View Operations in Progress
View storage array profile	Storage Array Profile	Support	Support Center > Support Resources tab	Storage Array Profile
View cable connections	Cable Connections	CLI/script editor only		
View event log	Event Log (all options)	Support	Event Log	Various options
View unreadable sectors log	Unreadable Sectors Log	Support	Support Center > Diagnostics tab	View/Clear Unreadable Sectors
View persistent reservations	Persistent Reservations	CLI/script editor only		

Upgrade Options

Table 40 details how functions performed for upgrading are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager. For further information, see the E-Series Documentation Center.

Table 40) Upgrade options: AMW compared with System Manager.

Function	AMW	System Manager		
	Upgrade > Option	Page	Tile/Tab	Option
View firmware inventory	View Firmware Inventory	Support	• Upgrade Center • Support Center > Support Resources tab	• Software and Firmware Inventory • Software and Firmware Inventory
Upgrade controller firmware	Upgrade controller firmware (all options)	Support	Upgrade Center	All options. The SANtricity OS Software bundle includes management software, controller firmware, supervisor (DOM 0) software, and IOM (ESM) firmware.
Upgrade controller NVSRAM	Upgrade controller NVSRAM (all options)			Can upgrade NVSRAM only as part of the SANtricity OS Software bundle (see preceding entry). Can also use the CLI/script editor to upgrade NVSRAM individually.
Upgrade drive firmware	Upgrade drive firmware (all options)			All options
Upgrade ESM firmware	Upgrade ESM firmware			Can upgrade IOM (ESM) firmware only as part of the SANtricity OS Software bundle (see preceding entry). Can also use the CLI/script editor to upgrade IOM (ESM) firmware individually.
Upgrade shelf configuration settings	Upgrade Tray Configuration Settings	CLI/script editor only		

Alert Options (EMW)

Table 41 details how functions performed for alerting are completed in the SANtricity Storage Manager EMW and how the same functions are completed employing the SANtricity System Manager.

Table 41) Alert options: EMW compared with System Manager.

Function	EMW	System Manager		
	Edit > Configure Alerts	Page	Tile/Tab	Option
Configure alerts	All options (email, SNMP)	Settings	Alerts > Email, SNMP, and Syslog tabs	Various options for email, SNMP, and syslog

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- E-Series EF280 datasheet: E-Series and EF-Series Datasheets
- E-Series Documentation Center
- E-Series SANtricity 11.40 statement of work (not publicly available)

Version History

Version	Date	Document Version History
Version 1.0	May 2018	Initial release.

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

TR-4685-0518