Technical Report

Introduction to NetApp E-Series E2800

Feature Overview with SANtricity OS 11.40.2

Mitch Blackburn, NetApp

May 2018 | TR-4631

Abstract

The NetApp® E-Series E2800 storage system is an excellent choice for wide-ranging data center storage requirements. This report provides detailed information about the multiple system configuration options NetApp SANtricity® OS 11.40.xx provides, including an overview of the embedded management software, SANtricity System Manager. It is also a great starting point to introduce E2800 system details to sales engineers, partners, service providers, and customers.

NetApp®

TABLE OF CONTENTS

© 2018 NetApp, Inc. All rights reserved.

LIST OF TABLES

© 2018 NetApp, Inc. All rights reserved.

LIST OF FIGURES

© 2018 NetApp, Inc. All rights reserved.

© 2018 NetApp, Inc. All rights reserved.

© 2018 NetApp, Inc. All rights reserved.

1 E2800 Storage Systems

NetApp E-Series E2800 storage systems address wide-ranging data storage requirements with balanced performance that is equally adept at handling large sequential I/O for video, analytical, and backup applications, as well as small random I/O requirements for small and medium-sized enterprise mixed workloads. The E2800 brings together the following advantages:

- Support for hybrid drive configurations
- Modular host interface flexibility (SAS, FC, and iSCSI)
- High reliability (99.999% reliability)
- Intuitive management: simple administration for IT generalists, detailed drill-down for storage specialists

The entry-level E2800 is a 12Gb SAS 3 system now shipping with SANtricity OS 11.40.2 software. The E2800 was introduced in 2016 with the new embedded browser-based SANtricity System Manager, which featured the following new capabilities:

- Embedded web services
- Embedded SANtricity System Manager, with an easy-to-use GUI
- The ability to store and present up to 30 days of performance data, including I/O latency, IOPS, CPU utilization, and throughput
- The ability to do application/workload tagging
- Easier alert management, including an embedded SNMP agent and MIB
- Embedded AutoSupport® functionality

SANtricity OS 11.40 adds important new security features to the new generation E-Series product line, with:

- Support for authentication using Lightweight Directory Access Protocol (LDAP)
- Support for role-based access control (RBAC) with five distinct user levels provided
- Support for web browser CA certificates
- A new secure CLI interface
- Support for an external drive encryption key manager (KMIP compliant)

SANtricity OS 11.40.1 added feature changes not included in the initial SANtricity OS 11.40 release:

- New SSD wear-life tracking metric and proactive wear-life notification
- Extended the maximum DDP capacity limits for E2800, E5600, E5700, and EF570 arrays

SANtricity OS 11.40.2 continued improving security features by adding:

- Authentication with Security Assertion Markup Language (SAML) 2.0 to support multifactor authentication (MFA).
- Digitally signed firmware
- Certificate revocation checking using Online Certificate Status Protocol (OCSP)
- Syslog server configuration for audit log archival

Together, these features create an entry-level storage system with the flexibility and performance capabilities to support enterprise environments and workloads without sacrificing simplicity and efficiency. In addition, the E2800 storage system's fully redundant I/O paths, advanced protection features, and extensive diagnostic capabilities deliver a high level of availability, data integrity, and security. One example is the ongoing commitment to providing the latest I/O path protection and load balancing capabilities on a per–host type basis, including a relatively new host type for mixed-host clustered environments found in the media and entertainment industry.

© 2018 NetApp, Inc. All rights reserved.

1.1 E2800 Primary Use Cases

The flexible host interface options and wide range of drive choices make E-Series E2800 storage systems an ideal storage platform for enterprises that want powerful storage systems with easy growth strategies at the lowest possible initial investment. E2800 storage systems scale up for dedicated workloads such as:

- Business-critical backup environments for any size enterprise
- Video applications and video surveillance environments
- Mixed host environments found in media and entertainment use cases
- Common IT applications such as Microsoft Exchange and SQL Server for small and medium enterprises
- Efficient block storage behind virtualization platforms such as NetApp FlexArray®

1.2 E2800 System Options

As shown in Table 1, the E2800 is available in three shelf options, which support both hard-disk drives (HDDs) and solid-state drives (SSDs), to meet a wide range of performance and application requirements.

Table 1) E2800 controller shelf and drive shelf models.

Controller Shelf Model	Drive Shelf Model	Number of Drives per Shelf	Type of Drives
E2812	DE212C	12	3.5" NL-SAS drives 2.5" SAS SSDs
E2824	DE224C	24	2.5" SAS drives (HDDs and SSDs)
E2860	DE460C	60	3.5" NL-SAS drives 2.5" SAS drives (HDDs and SSDs)

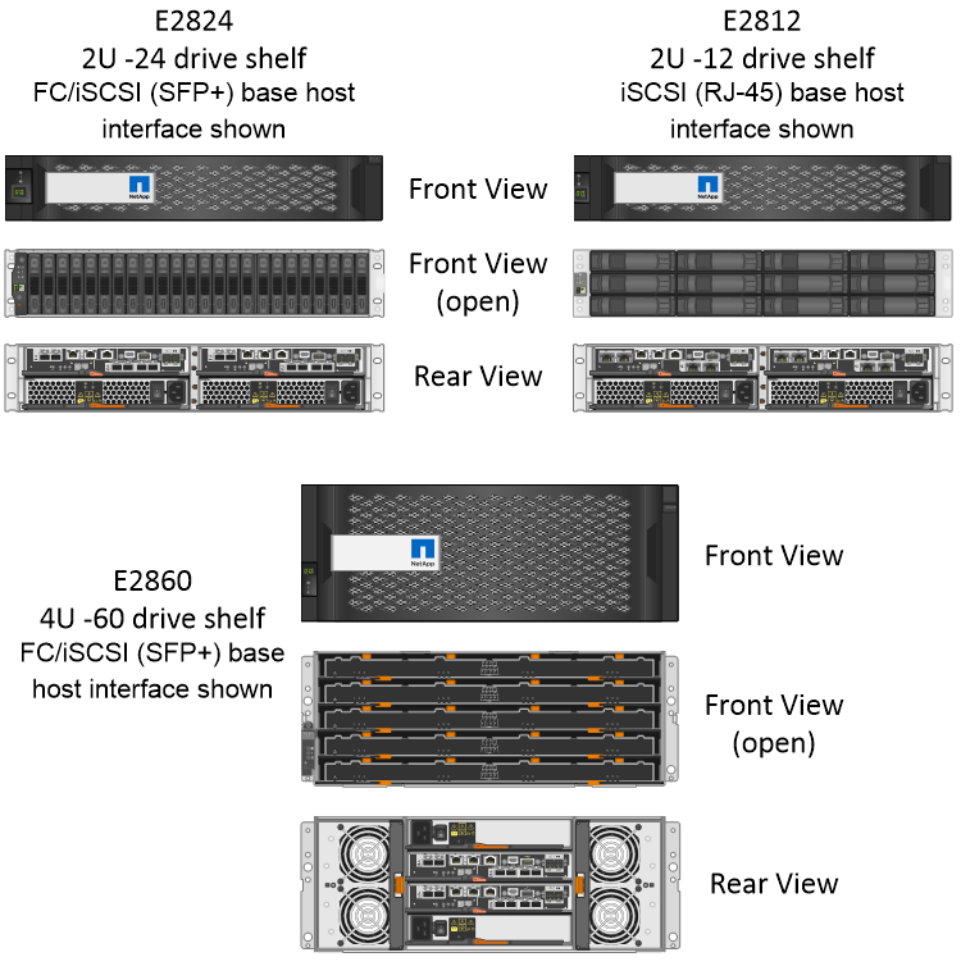
Note: The E2812 supports a maximum of four total 12-drive shelves, one controller drive shelf, and up to three expansion drive shelves. The same shelf count applies to the E2824, so 96 total drive slots (4 x 24-drive shelves). The E2860 supports up to two expansion drive shelves for a total of 180 drive slots. All shelf models can be mixed in the same storage array, but 180 total drive slots are the maximum drive slot count supported with the E2800 array family.

The E2812 and E2824 shelf options support one (simplex configuration) or two controller canisters, while the E2860 supports only two controller canisters. All shelves support dual power supplies and dual fan units for redundancy, but the 12- and 24-drive shelves have dual integrated power and fan canisters, whereas the 60-drive shelf (DE460C) has separate dual power supplies and fan units. The shelves are sized to hold 12 drives, 24 drives, or 60 drives, as shown in Figure 1.

Note: In a duplex configuration, both controllers must be identically configured.

© 2018 NetApp, Inc. All rights reserved.

Figure 1) E2800 shelf options (duplex configurations shown).



Note: The DE460C 4–rack unit (RU) 60-drive shelf requires dual ~220VAC power sources to power each shelf.

Each E2800 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 E2800 controllers also include two built-in host ports, either two optical 16Gb FC/10Gb iSCSI or two 10Gb iSCSI Base-T ports, but one of the following host interface cards (HICs) can also 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 port protocol of the optical baseboard ports and the optical HIC ports from FC to iSCSI or from iSCSI to FC. Mixed protocol configurations are supported when the baseboard host ports are set for one protocol and the expansion HIC ports are set for a different protocol.

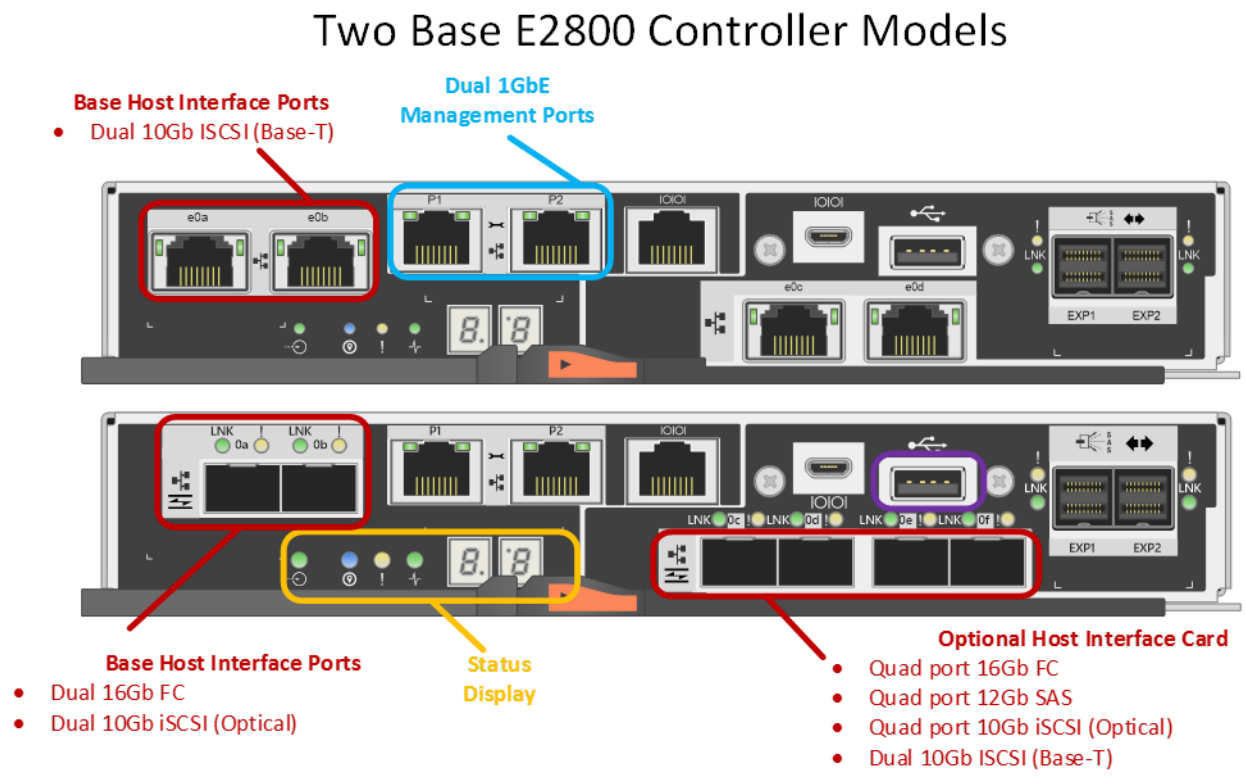
- 2-port 10Gb iSCSI (Cat6e/Cat7 RJ-45)

© 2018 NetApp, Inc. All rights reserved.

Note: If the base ports on the controller are configured with 10Gb iSCSI Base-T, then the only expansion HIC option supported is the 2-port 10Gb iSCSI (Cat6e/Cat7 Base-T) or the 4-port SAS HIC.

For optical connections, the appropriate SFPs must be ordered for the specific implementation, and all E2800 optical connections use OM4 fiber cable. Consult the Hardware Universe for a full listing of available host interface equipment. Figure 2 provides a close-up view of the E2800 onboard host interface options.

Figure 2) E2800 controller with onboard iSCSI Base-T ports vs. E2800 controller with optical base ports.



Note: For 16Gb/8Gb/4Gb FC or 10Gb iSCSI, use the unified SFP (X-48895-00-R6-C), but for 1Gb iSCSI, you must use the 1Gb iSCSI SFP (X-48896-00-C).

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

2 SANtricity OS Features

E-Series systems have a rock-solid reputation for reliability, availability, simplicity, and security. The SANtricity OS 11.40 release builds on that legacy by adding new security options and enhanced multipath state management capabilities.

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

© 2018 NetApp, Inc. All rights reserved.

- Implementation of 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 that extend to the onboard web services API where user account passwords are now required

Note: If you want to run in the previous security mode with a single administrative password and still use symbols to communicate 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 that in turn are used by many devices in a network infrastructure to identify and authenticate users seeking access to devices in the network.

RBAC is software on the E-Series array that defines standard user levels, each with a well-defined set of access permissions. The combination of authenticating a user as an individual or member of a group and then having specific permissions set on the array side to define the type of access that user or group is allowed enables SANtricity OS 11.40 to provide the granularity of access that our customers requested.

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 a couple of 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` is the fully qualified domain name made up of one or more commonNames separated by commas followed by one or more domainComponents 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 only requires a few pieces of information, as shown in Table 2.

Table 2) 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 users accessing the storage array are members.
Server URL	Could be a fully qualified domain name or IP and port number with format `ldap://<IP:port_number>` (port 389 or port 636 for LDAPs).
Bind account	Format is `CN=binduser,CN=Users,DC=<some_name>,DC=com`.

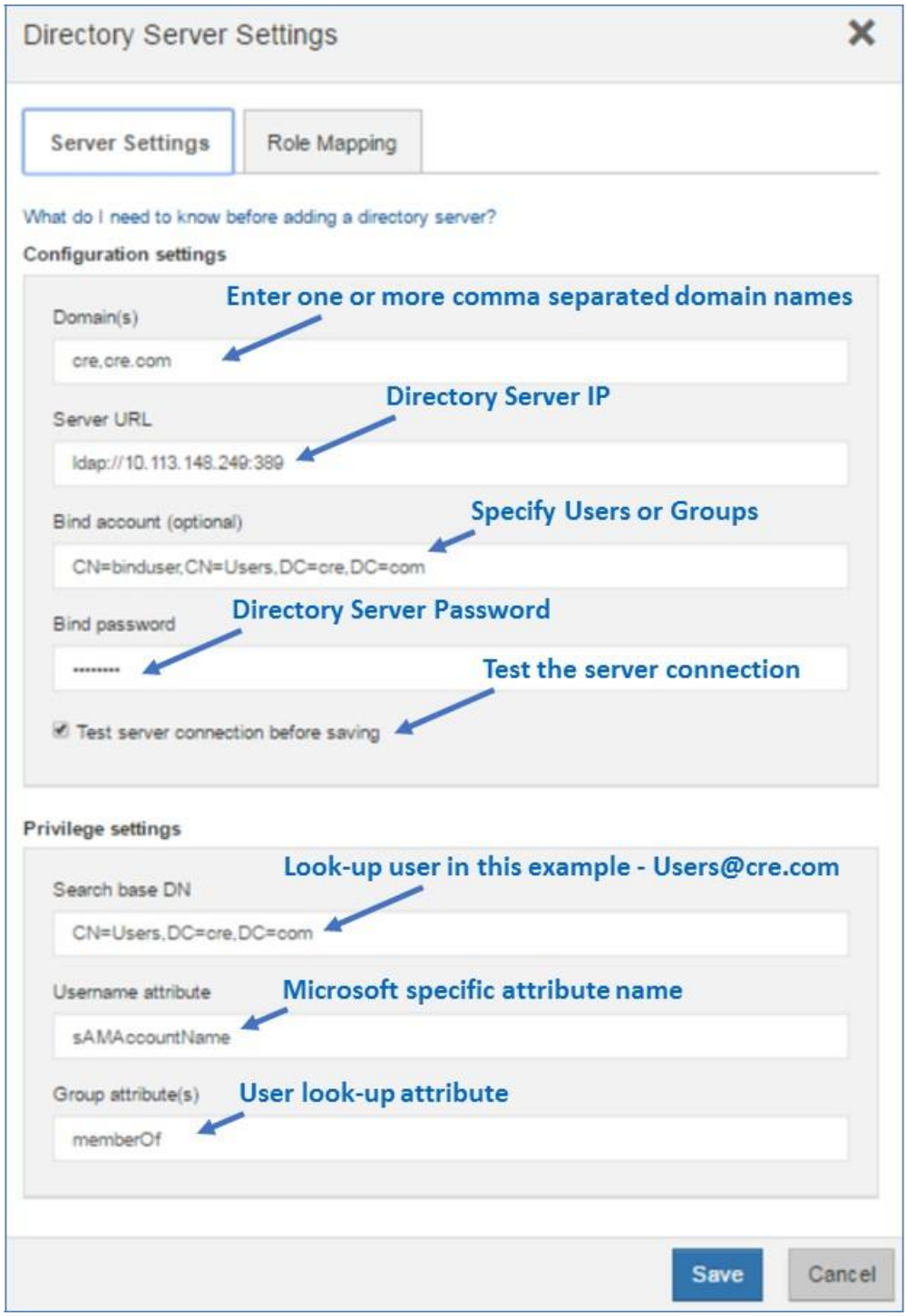
© 2018 NetApp, Inc. All rights reserved.

Field Name	Definitions
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. 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. 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 are not likely to change for most implementations.

© 2018 NetApp, Inc. All rights reserved.

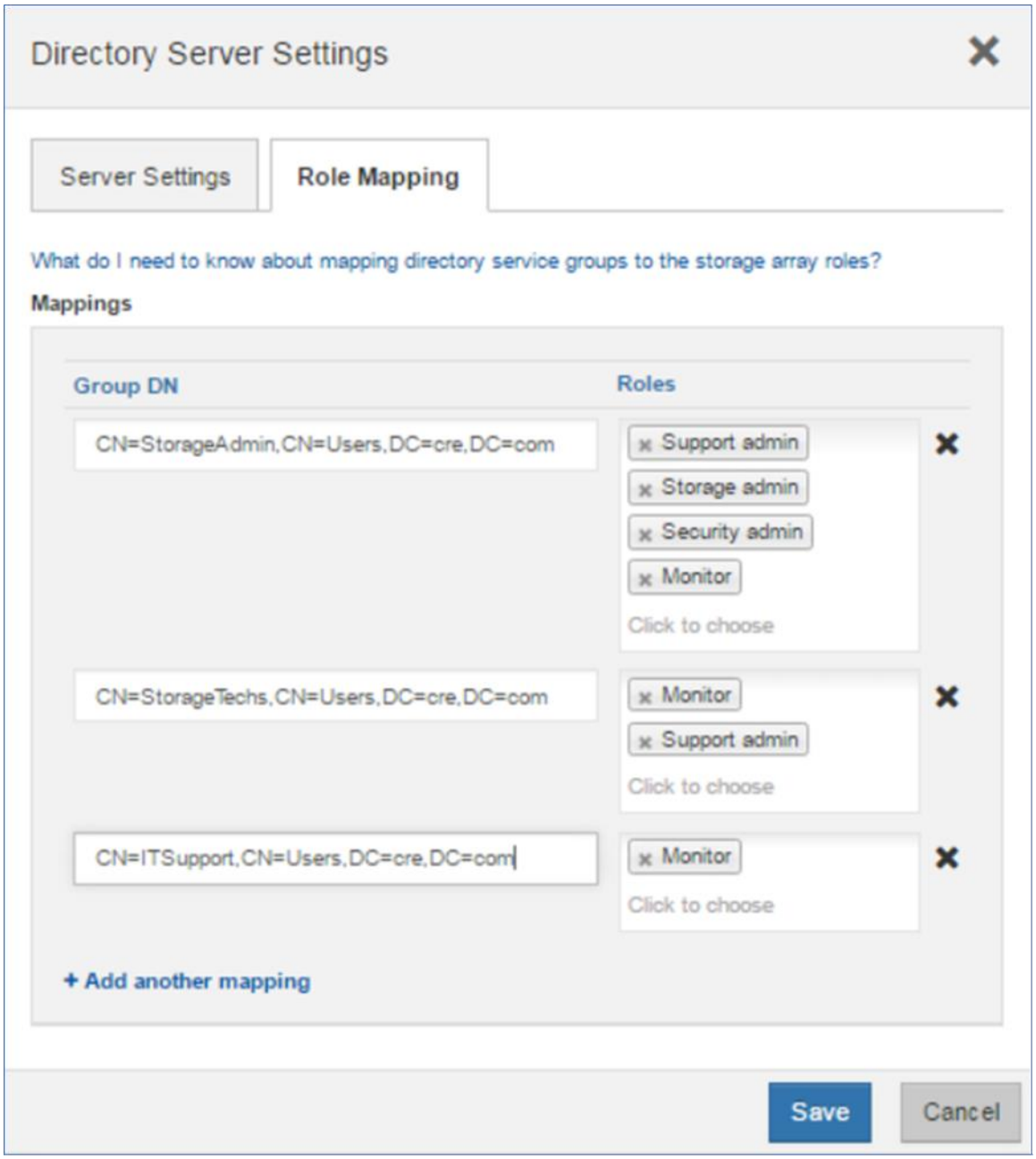
Figure 3) SANtricity System Manager directory server setup wizard.



The array roles for the specified user groups are set in the Role Mapping tab. 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.

© 2018 NetApp, Inc. All rights reserved.

Figure 4) Role Mapping tab in the directory server settings wizard.

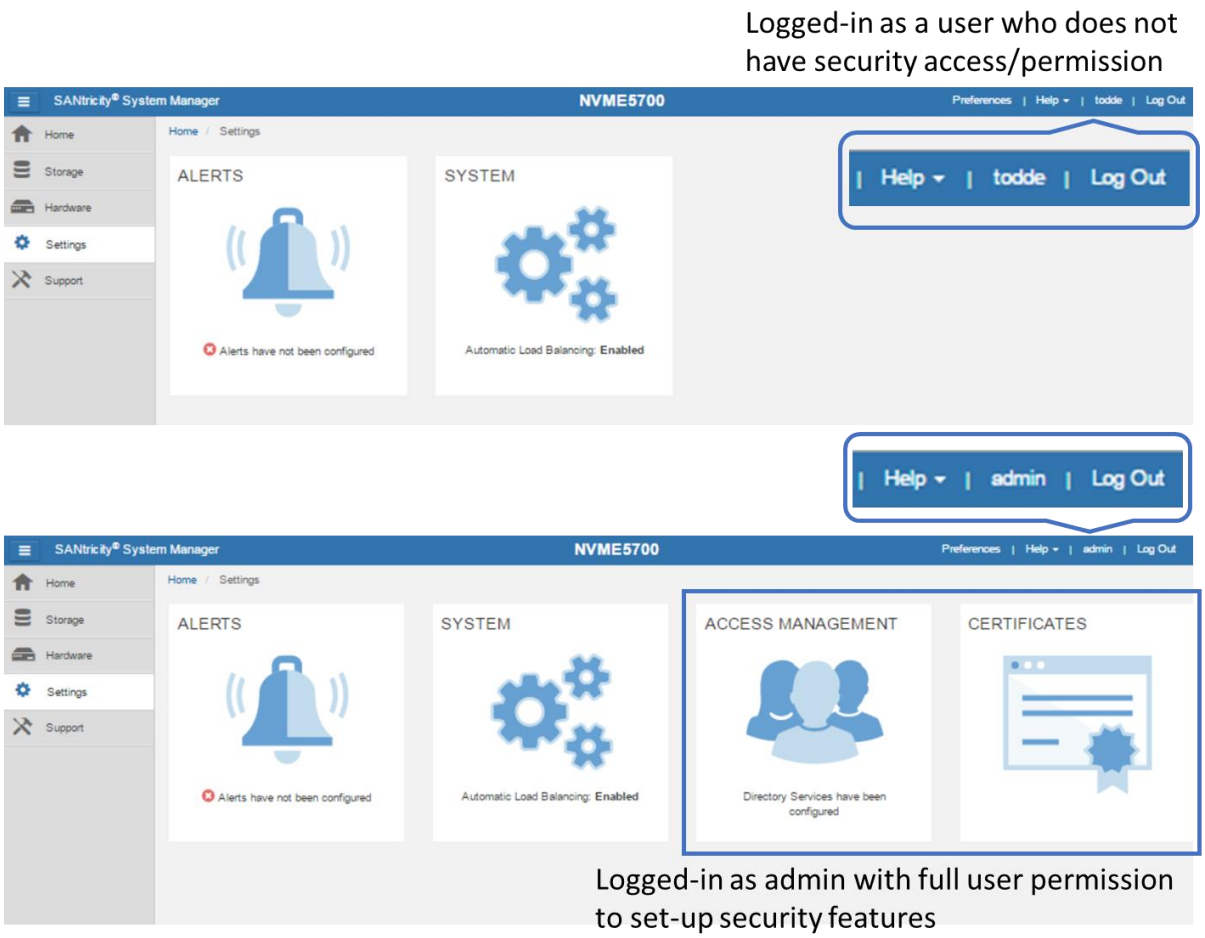


Note: The monitor role is automatically added to all group DNs. Without monitor permission, users in the associated mapped group are not able to log in to the array.

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.

© 2018 NetApp, Inc. All rights reserved.

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

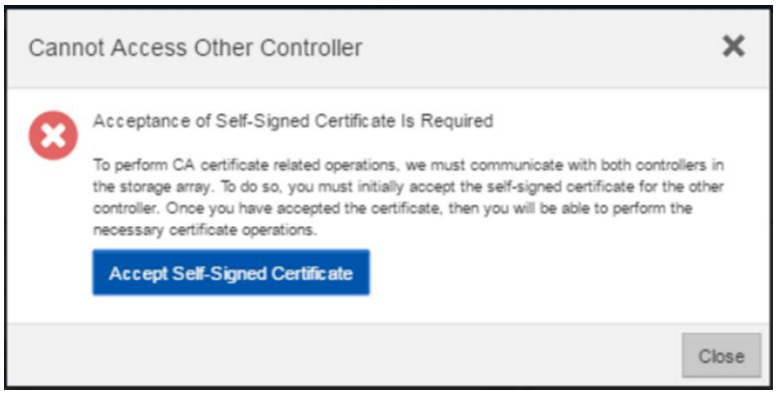


SANtricity Web Server Security Certificates

In addition to authentication and access control, SANtricity OS 11.40 supports standard CA certificates. This support enables secure communications (SSL/TLS) between browser clients and the E-Series built-in web servers on the controllers. On new E52800 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 communications to the other controller in the E2800 array are done through the midplane in the shelf. Because you can log in to either of the controllers through the web browser, both controllers must run a web server instance. To make sure of proper communications 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.

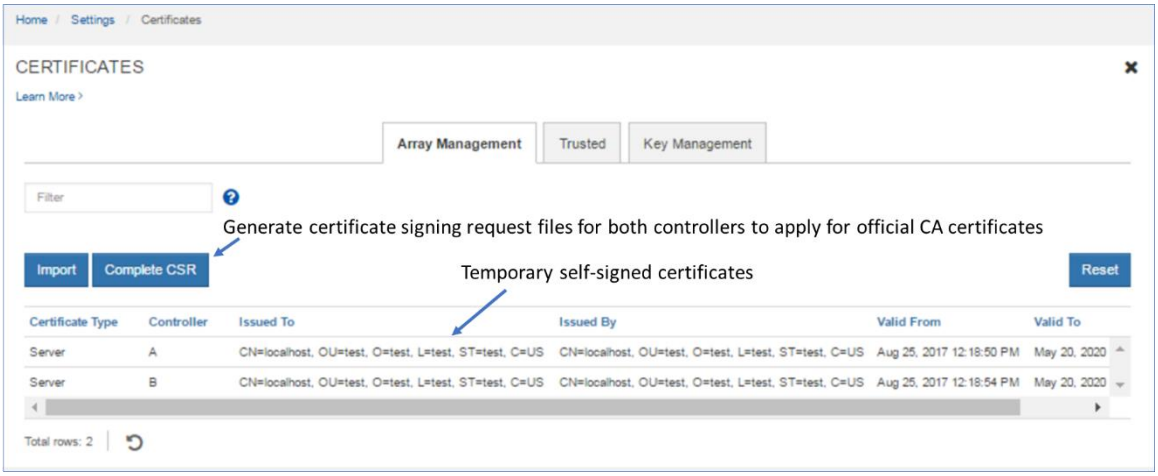
© 2018 NetApp, Inc. All rights reserved.

Figure 6) Initial step 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 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**Error! Reference source not found.** and then selecting show preinstalled certificates from the drop-down menu.

When external key management has been enabled from the Settings tile, use the Key Management tab to generate a CSR file. Use the CSR file on the key management server to generate a client certificate. Import the client certificate from the Key Management tab to enable secure 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 State Management

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

© 2018 NetApp, Inc. All rights reserved.

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: BPG for Media 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 new 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:

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

These attributes allow host multipath drivers to spread I/O across 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 I/O 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). After the ALUA timer expires, the array decides whether or not 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.

Recent improvements to some of the SANtricity management software host types with respect to multipath functionality now enable implicit path failover with failback based on enhanced decision making on the array, as indicated in Table 3.

Table 3) 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 DM-MP (kernel 3.10 or later)	Enabled	Supported	Supported	Supported
VMware	Enabled	Supported	Supported	Supported
Windows	Enabled	Supported	Supported	Supported
Windows cluster	Enabled	Supported	Supported	Supported
ATTO cluster (all 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 new

© 2018 NetApp, Inc. All rights reserved.

storage-led path management logic is intended to 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 **Error! Reference source not found.** that support implicit path failover and failback where applicable.

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

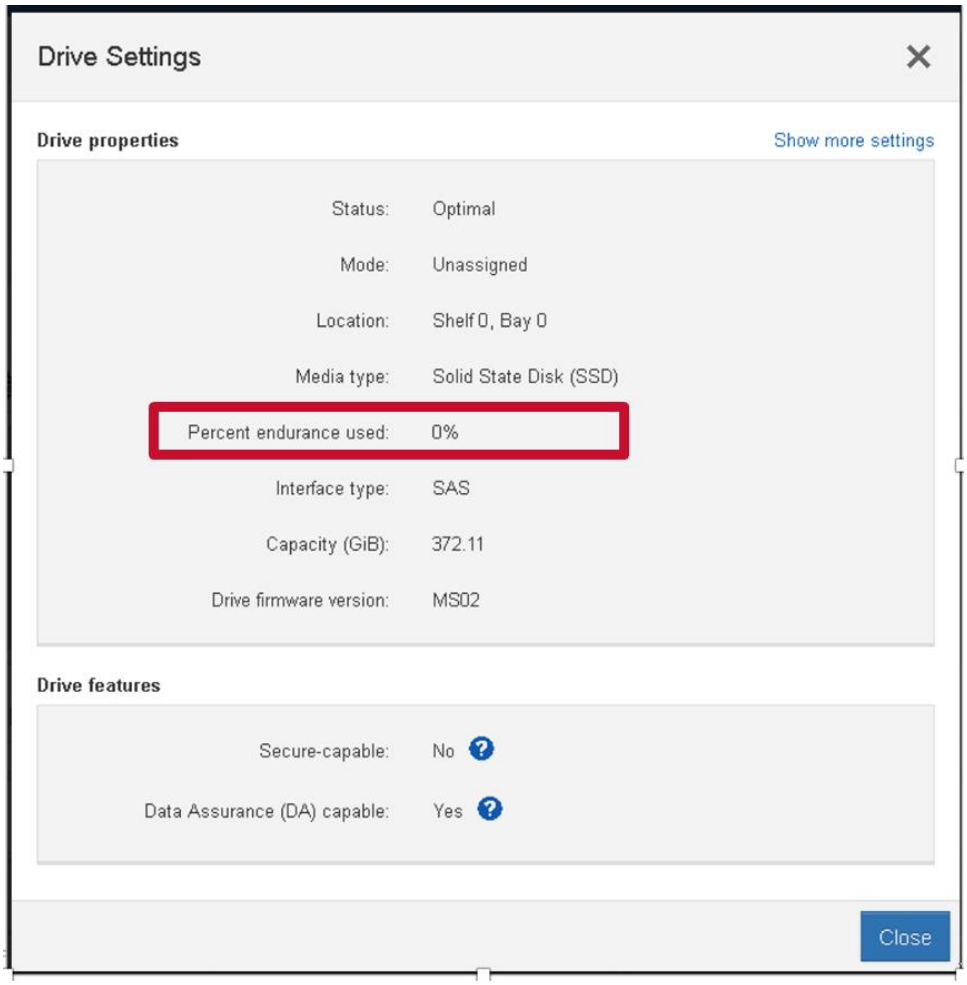
SANtricity OS 11.40.1 improved the user experience with more default volume workload tagging options that further simplify capacity management. These workloads are presented to storage administrators as an expanded list of common data center workloads from which administrators can choose when provisioning 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 the SANtricity OS. Figure 8 shows the Drive Settings dialog box with the new, easy-to-understand wear-life indicator percent endurance used.

© 2018 NetApp, Inc. All rights reserved.

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 12 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:

© 2018 NetApp, Inc. All rights reserved.

- **Authentication with Security Assertion Markup Language (SAML) 2.0 to support 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 OS firmware. Digitally signed firmware is required in controller firmware version 8.42 (SANtricity OS 11.40.2) and later. If you attempt to download unsigned firmware during the controller upgrade process, an error is displayed, and the download is aborted.
- **Certificate revocation checking using Online Certificate Status Protocol (OCSP).** Certificate management includes certificate revocation checking using an OCSP server. The OCSP server determines if the certificate authority (CA) has revoked any certificates before the 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:

- **Ability to enable or disable AutoSupport maintenance window.** AutoSupport includes an option for enabling or suppressing automatic ticket creation on error events. Under normal operation mode, the storage array uses AutoSupport to open a 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.

The following sections elaborate on each of the items listed.

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:

© 2018 NetApp, Inc. All rights reserved.

- **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

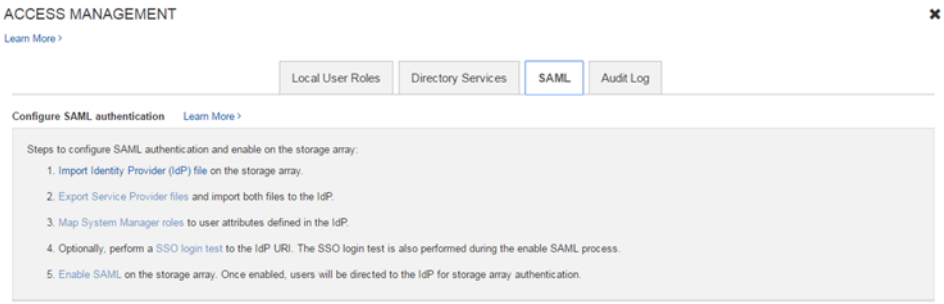
SSH is not disabled automatically but is disabled by default and must be enabled by the user.

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.

© 2018 NetApp, Inc. All rights reserved.

Figure 9) System Manager SAML tab.



Steps to be performed are described in Table 4Table 4.

Table 4) 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 the 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 the 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 that provide authorization to the System Manager application. The IdP might need to have configuration changes to provide the appropriate user attributes to execute 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, including all API access, to close any open security holes, and access to the System Manager application must be authenticated through the IdP.

Table 5 describes how E-Series authenticates using SAML.

Table 5) 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.

© 2018 NetApp, Inc. All rights reserved.

Step	Description
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 SANtricity Features Introduced with SANtricity 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 6.

Table 6) New features with SANtricity System Manager 11.30.

New Feature	Description
SANtricity System Manager: browser-based application	There are now two different versions of the storage management software: System Manager is used to manage individual E2800 storage arrays, while SANtricity Storage Manager, with its enterprise management window (EMW), provides an aggregated view of all E-Series arrays. The array management window (AMW) of SANtricity Storage Manager is used to manage the E2700, E5600, EF560, and all earlier storage arrays. When you select to manage a storage array from the EMW, the EMW opens the appropriate software (AMW or System Manager), depending on what controller the storage array contains. The key features of System Manager include the following: • Runs on box: You do not have to install any storage management software unless you need an aggregated view or use a mirroring feature. • Displays in a browser and is mobile ready. • Has modern look and feel with a tile-based GUI and easy-to-use online help system. • Uses simplified workflows and simplified terminologies. • Includes new functionality, including application/workload tagging, enhanced performance data, embedded monitor, and a graphical view of thin volume usage. • Includes embedded RESTful API that can be used for management.
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.

© 2018 NetApp, Inc. All rights reserved.

New Feature	Description
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	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	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.
Maximum volume size for disk pool volumes	The maximum volume size for a standard volume in a disk pool has increased from 64TB to 1PB for E2700 and E2800 storage arrays and to 2PB for E5600 storage arrays. The maximum volume size for a thin volume in a disk pool has increased from 64TB to 256TB. For more information, search for “learn about volumes” in the System Manager online help.
SSD cache performance improvements	SSD cache now employs a set of workload analytics-based algorithms to provide adaptive tuning of the cache based on the specific workload. This tuning results in significant improvements in both IOPS and latency for read-intensive workloads. The new adaptive algorithms also mean that administrators no longer need to specify an application type when configuring the cache. The system figures out the application type automatically. All read-intensive workloads benefit, including relational databases (Oracle and SQL Server), NoSQL databases, and analytics applications. For more information, search for “create SSD cache” in the System Manager online help.

2.8 SANtricity OS Standard Features

E-Series systems ship with significant storage management features that can be simply activated from SANtricity Storage Manager. Table 7 provides a consolidated list of E2800 standard features when running SANtricity OS 11.40.

© 2018 NetApp, Inc. All rights reserved.

Table 7) E2800 standard features using SANtricity OS 11.40.

E2800 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 a CLI.
Thin provisioning. Overcommit storage and add capacity when you need it.
SSD read cache. Accelerate 85% or higher random read workloads using a few SSDs. Recommended to accelerate 85% or higher random read workloads.
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.
Data assurance (T10 PI). Makes sure of data integrity from HIC to the drive (end to end in the storage array), which is especially important with large-capacity drives.
Nondisruptive controller firmware upgrade. Using ALUA host type with multiple paths to hosts combined with a wizard-driven upgrade process that activates one controller at a time, makes sure 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 more quickly upgrade multiple drives 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 in an effort to move the data before the drive actually 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.

Table 8 provides a comprehensive list of standard copy services features with E2800 storage arrays.

Table 8) SANtricity OS 11.40 copy services features.

SANtricity OS Copy Services Features
SANtricity Snapshot copies. Point-in-time Snapshot™ copies.
Synchronous mirroring. Real-time mirroring to a remote site (usually within 10km).

© 2018 NetApp, Inc. All rights reserved.

SANtricity OS Copy Services Features
Asynchronous mirroring. Mirroring to a remote site where RPO = 0 is not 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 array management 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 is the SANtricity VMware VASA provider (VMware APIs for storage awareness) because it still fits the future strategy for E-Series array management integration.

Table 9 shows the SANtricity management 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 9) SANtricity APIs and toolkits.

APIs and Toolkits	Description
SANtricity web services proxy **Note:** You can use either the proxy or the embedded REST API for E2800.	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 platforms.

Table 10 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 E5700 storage systems.

Table 10) 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.

© 2018 NetApp, Inc. All rights reserved.

3 SANtricity System Manager

As previously discussed, E2800 storage systems are managed by the browser-based application SANtricity System Manager. The E2800 controller and SANtricity OS 11.40/11.40.2 use the new browser-based management capabilities.

The major components of the legacy SANtricity storage management software such as the EMW can still be used with the E2800-based storage arrays, so the installation flow is similar to that of older E-Series arrays. The only GUI component never used with E2800 storage systems is the AMW that is still used with E5600, EF560, and other older E-Series systems. The AMW has been replaced on the E2800 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 E2800 controller. Previous controllers such as the E2700, E5600, and EF560 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 E2800 storage array and older E-Series storage arrays, there are a variety of management options. Table 11 provides an overview of management use cases.

Table 11) Management use cases.

Task	E2700 and E5600	E2800 and E5700
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 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		

© 2018 NetApp, Inc. All rights reserved.

Task	E2700 and E5600	E2800 and E5700
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 remote volume mirroring groups and pairs	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

© 2018 NetApp, Inc. All rights reserved.

Task	E2700 and E5600	E2800 and E5700
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 E5700 and E2800 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 configuration for E5700	N/A	System Manager REST
Save up to 30 days of historical statistical I/O data for E2800	N/A	System Manager REST
Perform application tagging of volumes, Snapshot copies for E5700	N/A	System Manager REST

E2800 storage systems are shipped preloaded with SANtricity OS 11.40.2 and include SANtricity System Manager bundled with the controller firmware. The SANtricity Storage Manager software version 11.40 must be downloaded from the NetApp Support site and loaded on a local management server if you want to discover E2800 storage systems and other E-Series arrays running SANtricity controller firmware version 8.40. Versions of SANtricity Storage Manager (EMW) prior to version 11.40 cannot connect to E2800 arrays running SANtricity OS 11.40, but the SANtricity Storage Manager version 11.40 can discover the new E2800 arrays and all the previous E-Series array software versions from at least the last six years.

If you do not want to use the EMW to discover all 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 SMUtil software, 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 on a local management host with IP access to the storage arrays or to I/O-generating hosts that are connected to E-Series arrays. The various SANtricity host packages based on your OS type should 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.

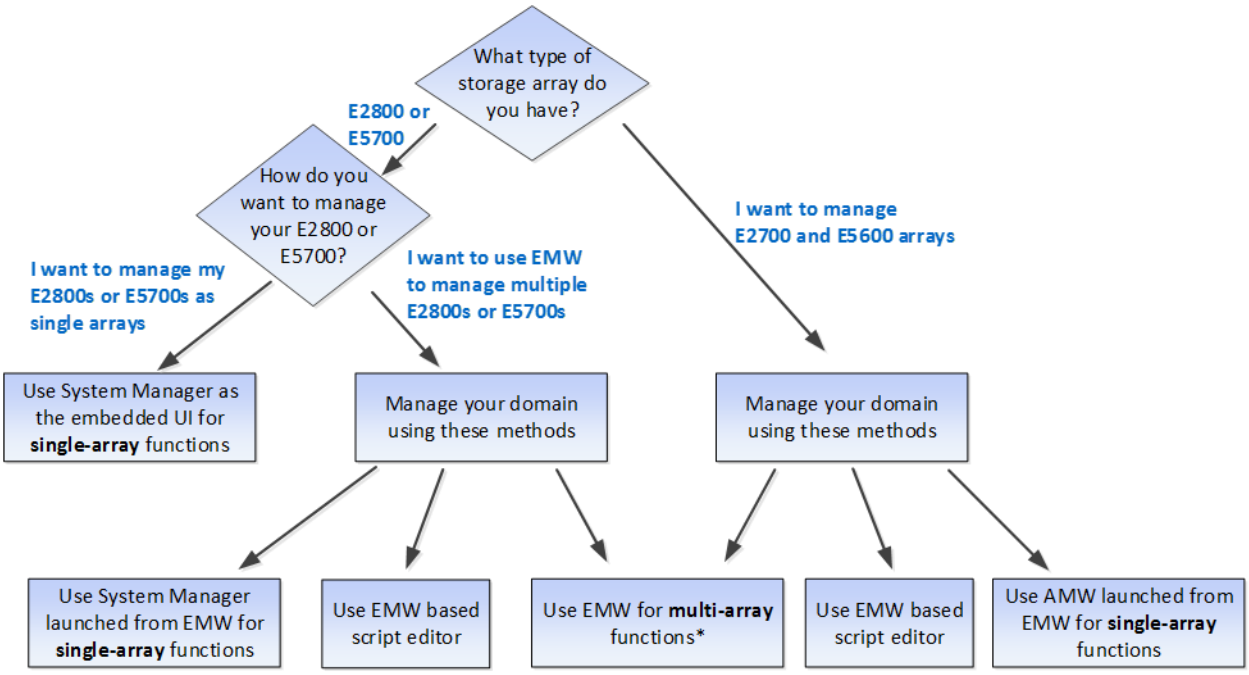
© 2018 NetApp, Inc. All rights reserved.

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 what components to install if you have purchased an E2800-based storage array depend on how you answer the questions shown in Figure 10.

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



If you are not using synchronous or asynchronous mirroring features, only have new generation E5700 or E2800 storage arrays, and do not want to use the SANtricity script editor, an alternative to installing the EMW to manage multiple arrays is to simply bookmark each array in a web browser.

Single E2800 Storage Array

If you have only a single new array, 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, as shown in Figure 11.

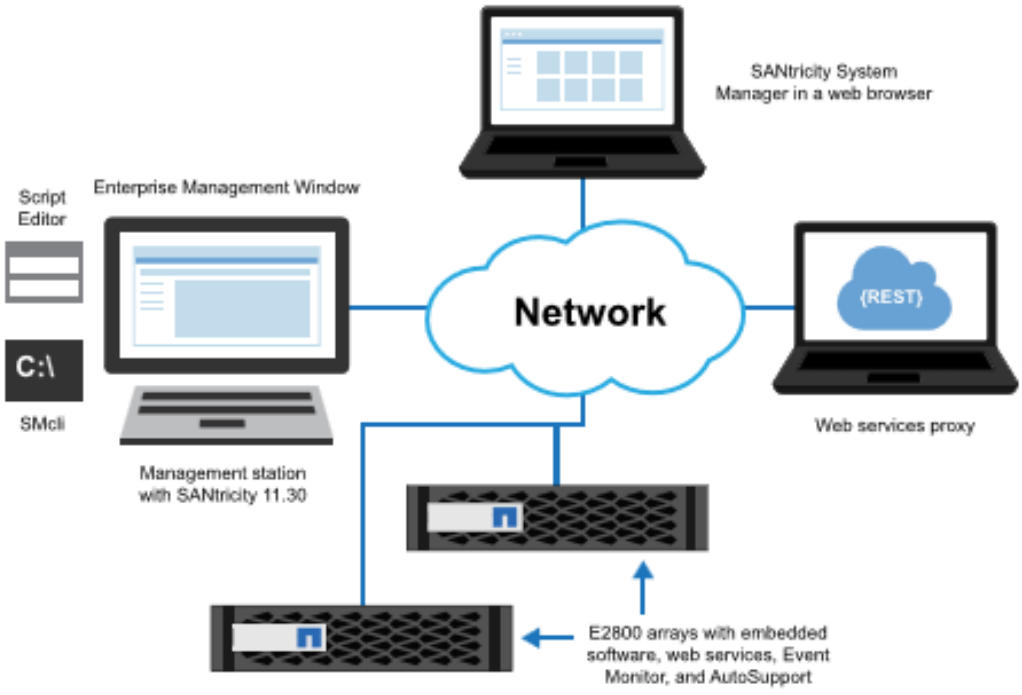
Figure 11) Managing a single E2800 with SANtricity System Manager.

© 2018 NetApp, Inc. All rights reserved.

Multiple E2800 Storage Arrays

If you have one or more E2800 storage arrays, you can install the EMW to manage your overall environment, while 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 E2800s with SANtricity Storage Manager and System Manager.

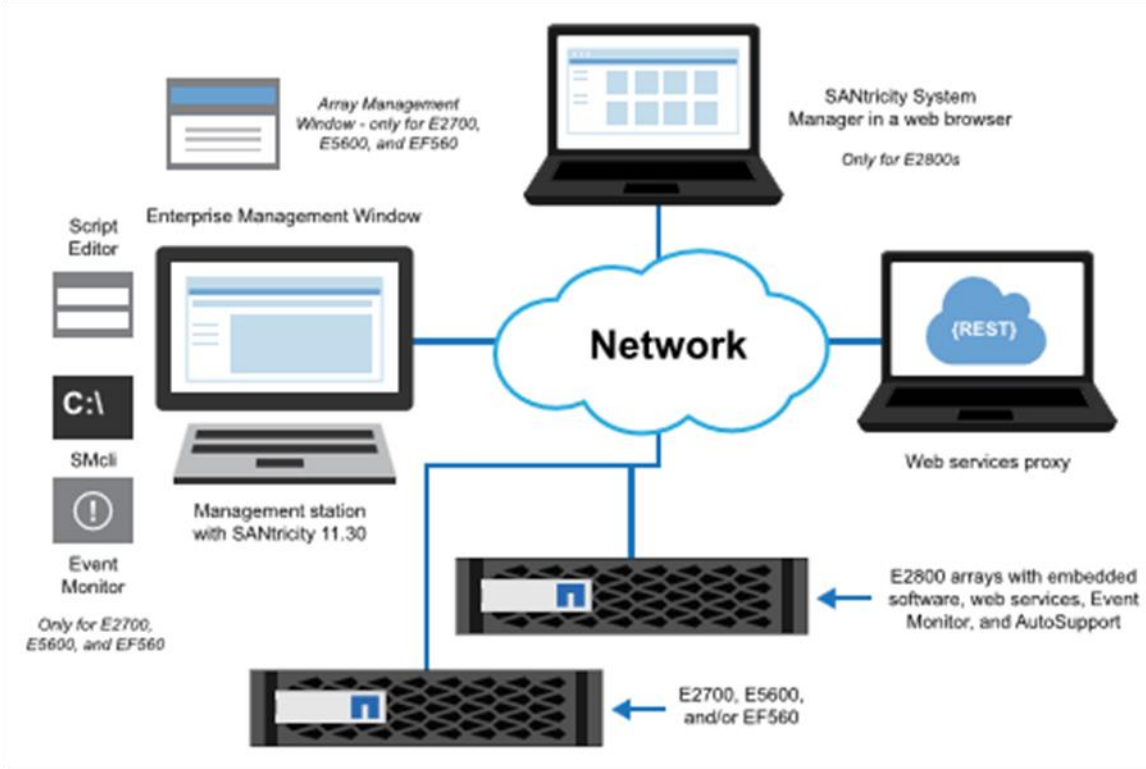


Mixed-Array Environment

If you have one or more E2800 storage arrays and any other E-Series storage arrays and want to have the E2800 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 E2800 storage arrays and the AMW for array-based tasks on other E-Series storage arrays, as shown in Figure 13.

© 2018 NetApp, Inc. All rights reserved.

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 style menu used extensively in System Manager.

© 2018 NetApp, Inc. All rights reserved.

Figure 14) System Manager home page.

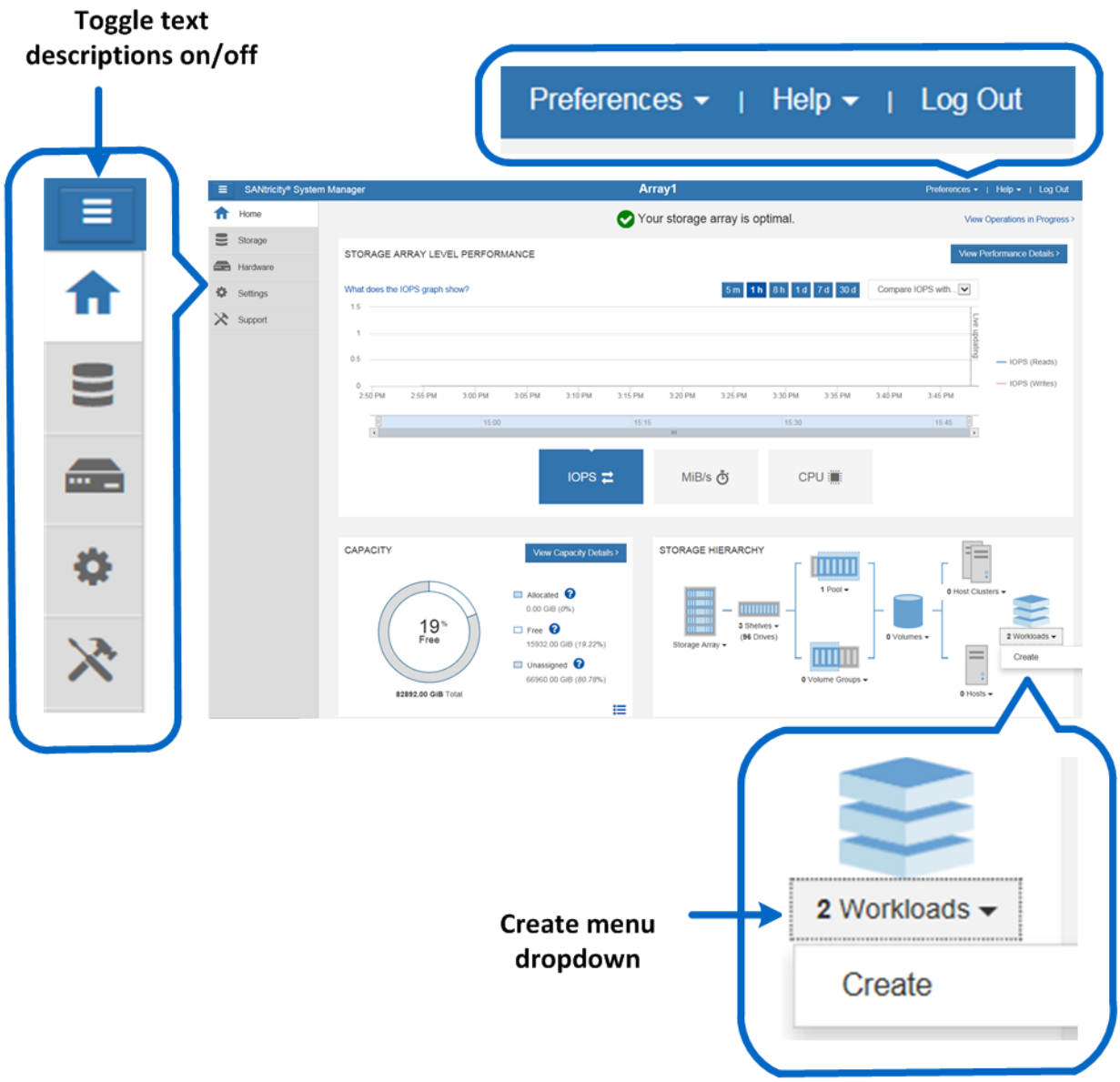
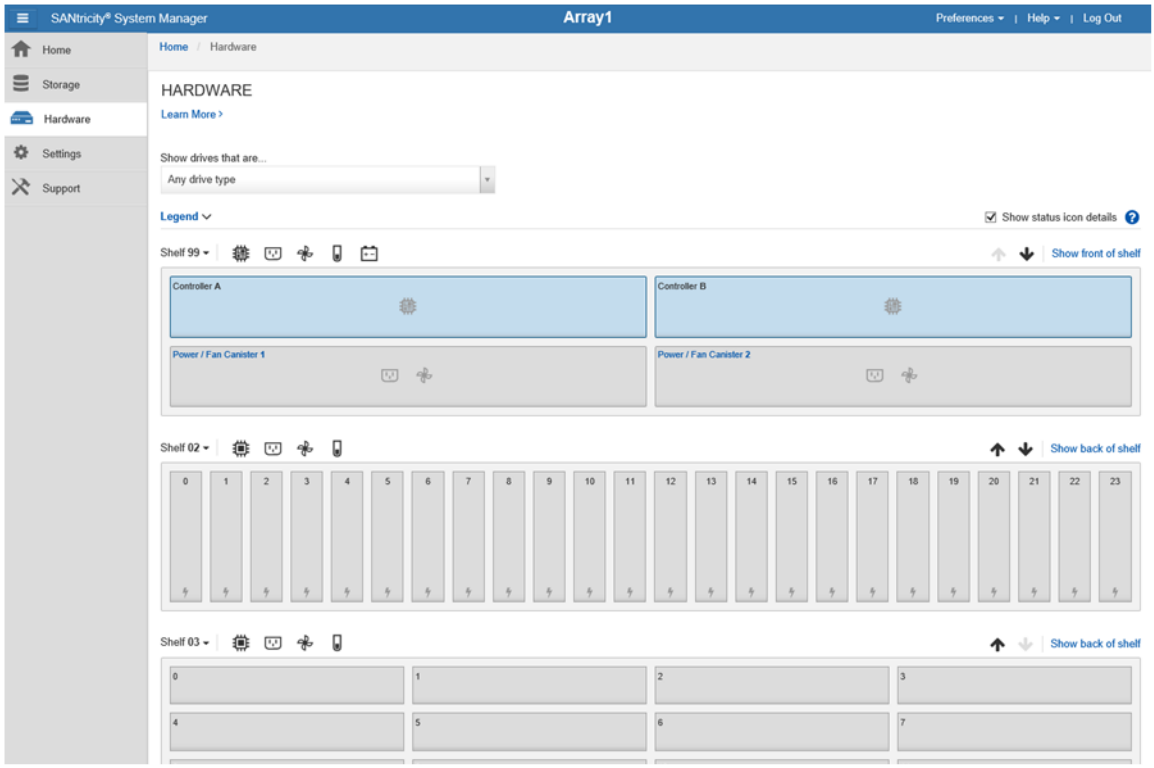


Figure 15, Figure 16, Figure 17, and Figure 18 show the other four main pages used in System Manager and accessible from anywhere in the application.

© 2018 NetApp, Inc. All rights reserved.

Figure 15) System Manager storage page.

Figure 16) System Manager hardware page.



© 2018 NetApp, Inc. All rights reserved.

Figure 17) System Manager settings page.

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.

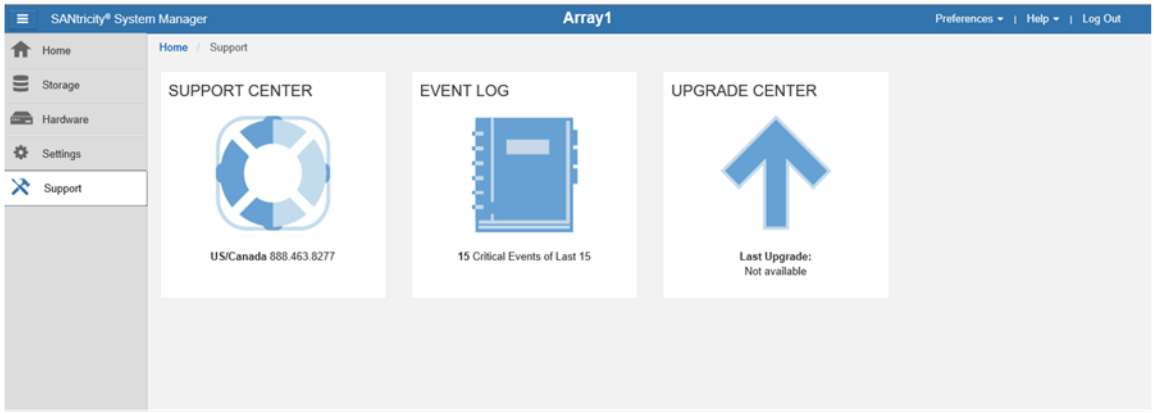
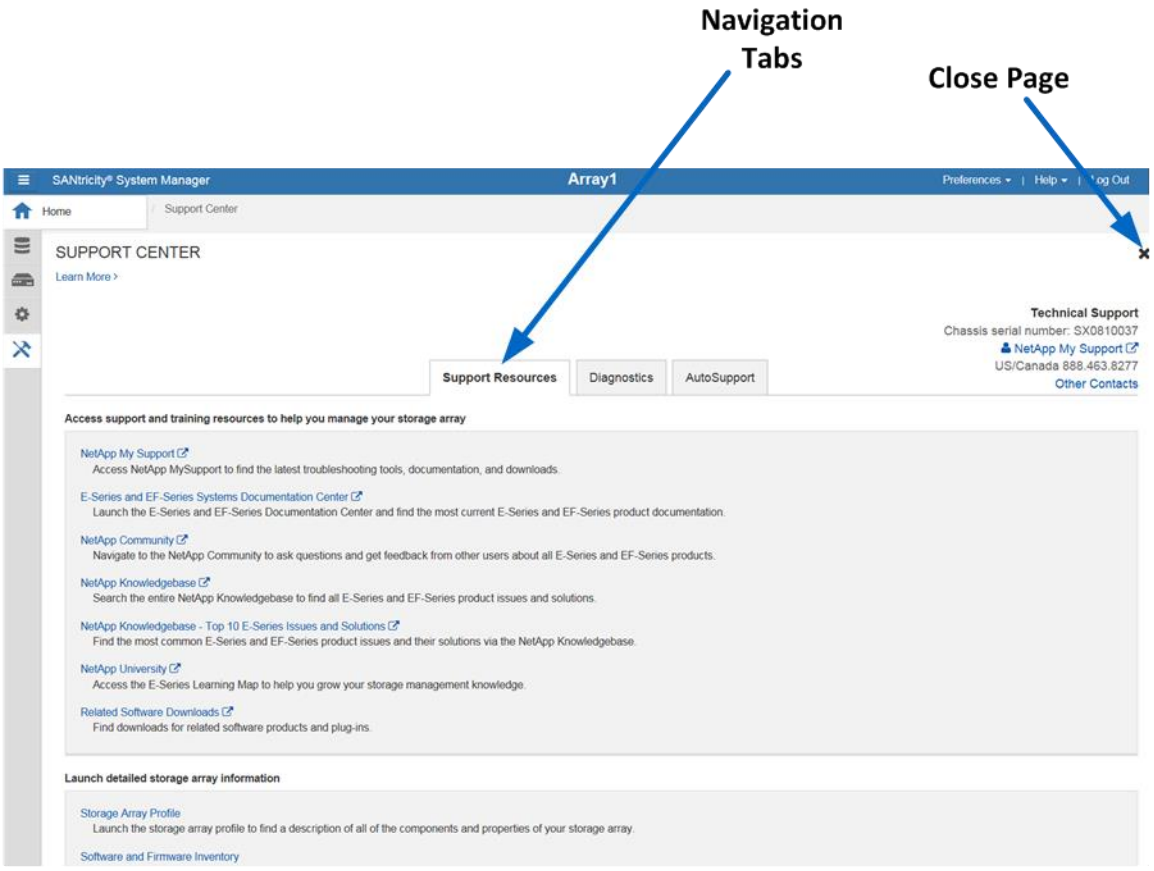


Figure 19 displays the Support Center, reached by selecting the Support Center tile on the support page. From the Support Center, navigation tabs are used to reach support topics.

© 2018 NetApp, Inc. All rights reserved.

Figure 19) System Manager Support Center.

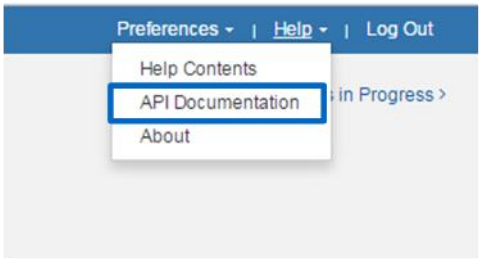


See the System Manager Tables in the appendix for a list of AMW functions and their corresponding locations in System Manager. The SANtricity System Manager online help also provides an excellent reference guide.

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 dialogs. 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.

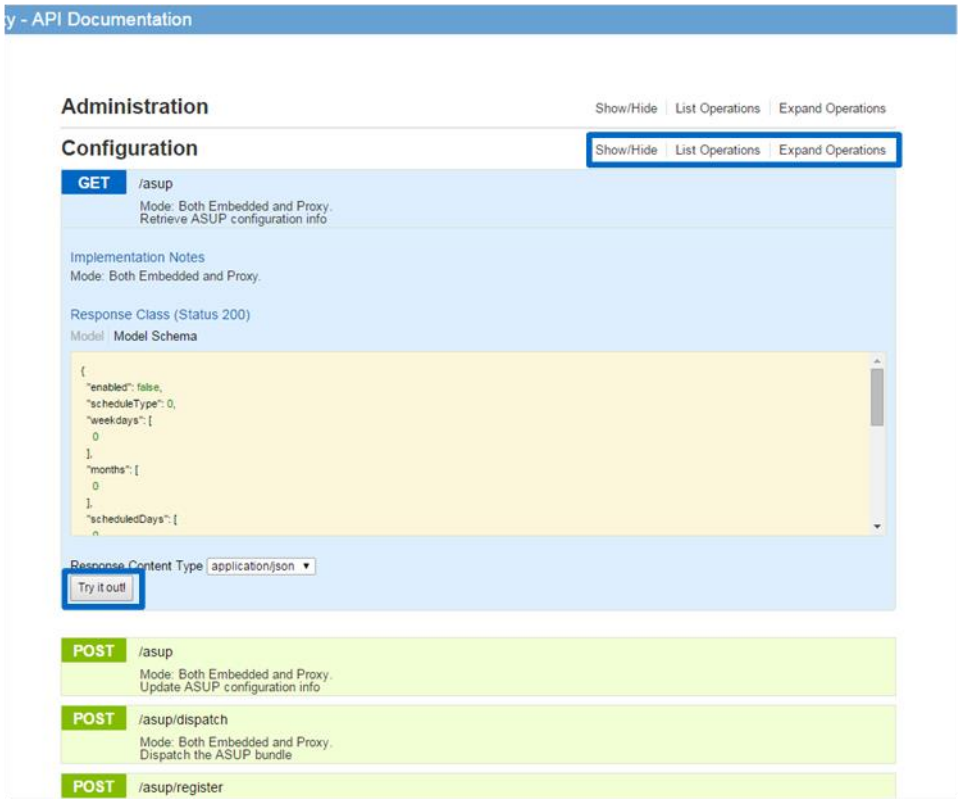
Figure 20) Opening the API documentation.



© 2018 NetApp, Inc. All rights reserved.

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.

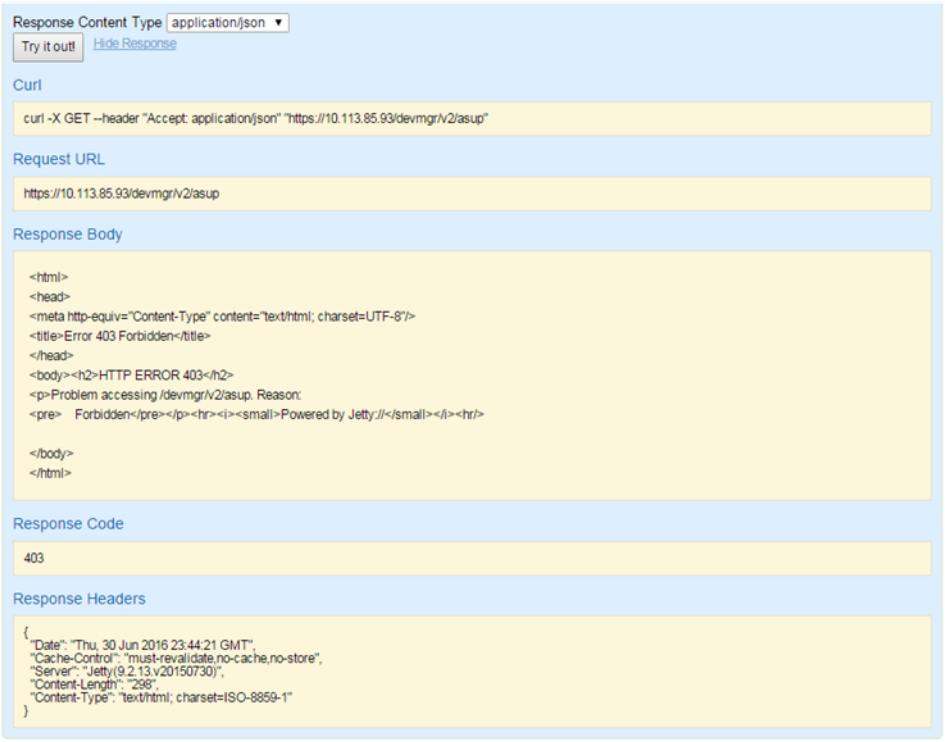
Figure 21) REST API documentation sample.



Also, the HTTP verbs can be tested using the `Try it out!` button. The corresponding output for the `GET` verb shown in Figure 21 is displayed in Figure 22.

© 2018 NetApp, Inc. All rights reserved.

Figure 22) Sample output from Try it out! button.



Data in the REST API is encoded through JavaScript object notation (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.

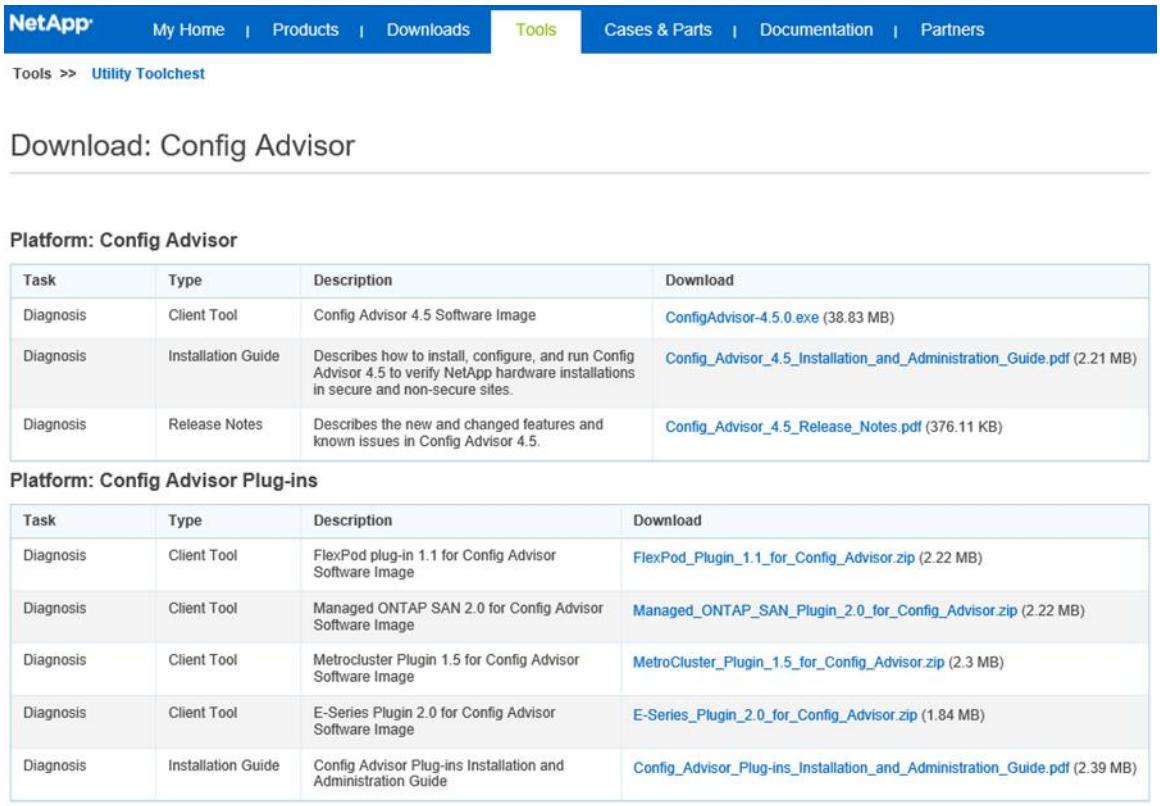
The Config Advisor 4.5 release enables support for SAS 3 cabling and visualization (cable diagrams). It also continues support for E-Series host-side checks and E-Series configuration checks in addition to the standard checks.

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.

© 2018 NetApp, Inc. All rights reserved.

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. It also performs specific checks for clustered Data ONTAP®, Data ONTAP operating in 7-Mode, MetroCluster™, FlexPod®, and E-Series systems.
- **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 MS Word reports for these contents.

4.2 E-Series Sizer

The E-Series Performance Sizing tool allows sales engineers and partners to make sure that specific customer architectures are properly sized to meet customer performance requirements.

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

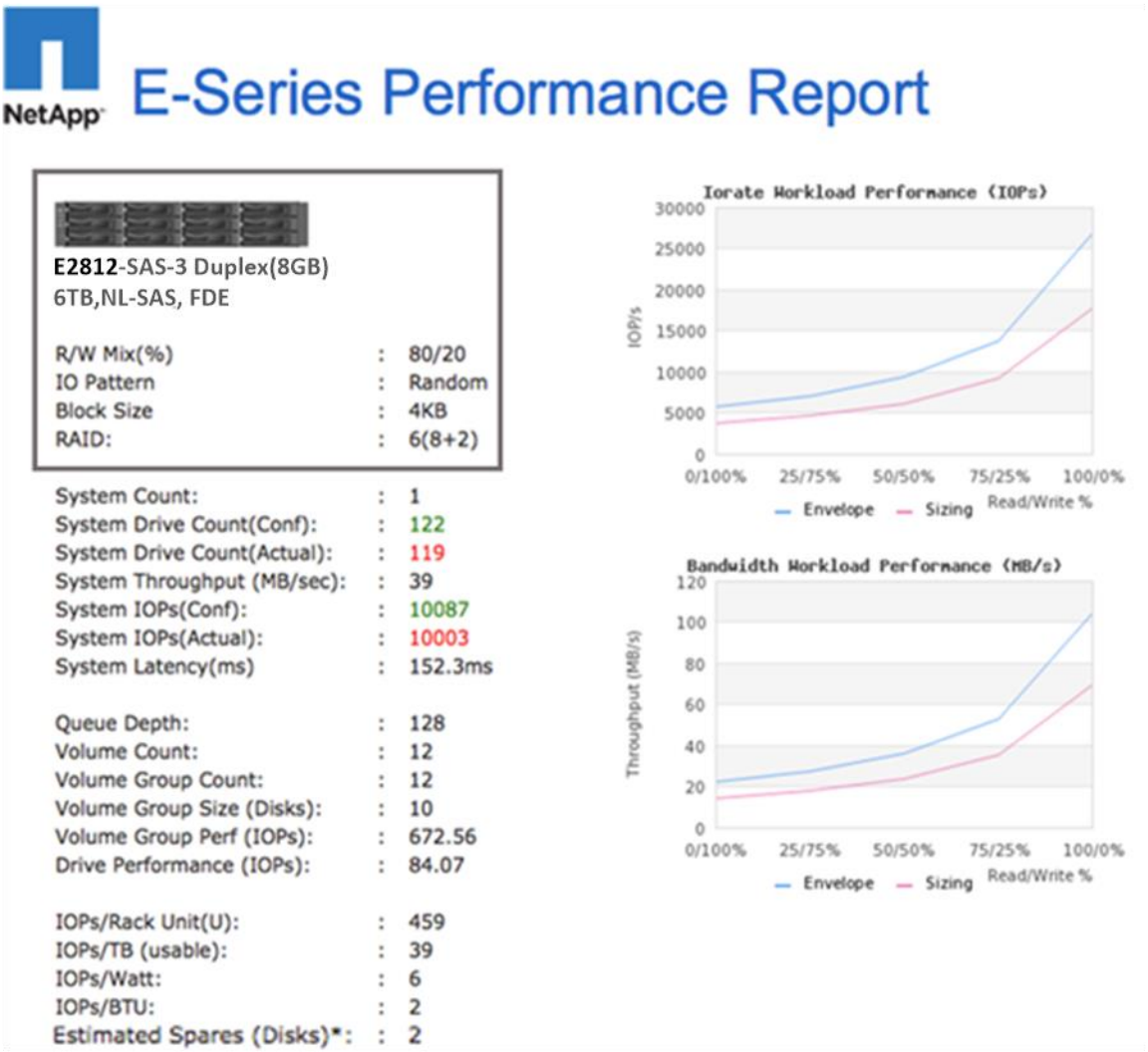
Note: If you are unable to access this tool, contact your NetApp or partner sales representative.

© 2018 NetApp, Inc. All rights reserved.

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.



© 2018 NetApp, Inc. All rights reserved.

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 located at https://forums.netapp.com/docs/DOC-14888.

4.4 Hardware Universe

Hardware Universe (HWU) 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 platforms 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.

HWU 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.

Note: The Hardware Universe user guide is located 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 kits to properly configure each host, according to 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 E2800 Hardware

Table 12 lists the software specifications for E2800-based storage systems.

Table 12) SANtricity software boundaries for E2800-based storage systems.

Components	Maximum
Storage Hardware Components	
Shelves (controller drive and expansion drive)	(1x controller + 3x expansion)
Drives	180 (120 SSDs)
SSD cache capacity	5TB
Logical Components	
Partitions	128

© 2018 NetApp, Inc. All rights reserved.

Components	Maximum
Volumes per partition	256
Volumes	512
Thin volumes per system	512
Disk pools per system	20
Total DDP capacity in an array (maximum capacity includes RAID overhead, DDP reserve capacity, and a small DDP-specific overhead based on the number of drives in the pool and other factors)	SANtricity OS 11.40: • 2PiB maximum DDP capacity per E2800 array SANtricity OS 11.40.1 and later: • 6PiB maximum DDP capacity per E2800 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)	2PiB
Maximum single-DDP thin volume capacity (SANtricity OS 11.30 and later)	256TB
Consistency Groups	
Volumes per consistency group	32
Consistency groups per system	16
Snapshot Copies	
Per Snapshot group	32
Per volume	128
Per storage system	512
Snapshot Volumes	
Per Snapshot copy	4
Per system	256
Snapshot Groups	
Per volume	4
Per system	256
Mirrors	
Mirrors per system	32
Mirrors per volume	1
Mirrors per asynchronous mirror group	32

© 2018 NetApp, Inc. All rights reserved.

Components	Maximum
Asynchronous mirror groups per system	4

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

6 Hardware Configurations

E2800 storage systems use a modular approach to hardware configuration. This approach can meet most customer SAN storage requirements for flexible host interfaces and versatile drive choices without sacrificing supportability, ease of implementation, and long-term stability. E-Series has a proven track record of reliability and scalability to satisfy requirements in remote dedicated environments or primary data centers.

6.1 Controller Shelf Configurations

E2800 controllers can be paired with DE212C, DE224C, or DE460C E-Series shelves. The following sections provide detailed information about each shelf configuration.

E2812 Controller Shelf

The E2812 is a 2RU shelf that holds up to 12 3.5" drives or 2.5" drives with adapter. It features one or two RAID controllers and one or two Energy Star Platinum-rated high-efficiency power supplies (913W) with integrated fans. An E2812-based storage system supports a maximum of 180 HDDs (120 SSDs) and a mix of drive shelf models.

Figure 25, Figure 26, and Figure 27 show the front and rear views of the E2812 controller shelf. In the example, the E2800 controllers have two optical base ports and no HIC.

Figure 25) E2812 front view with bezel.

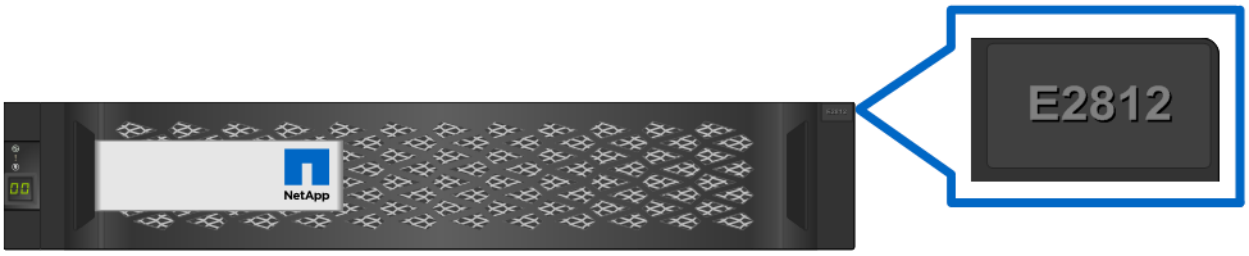
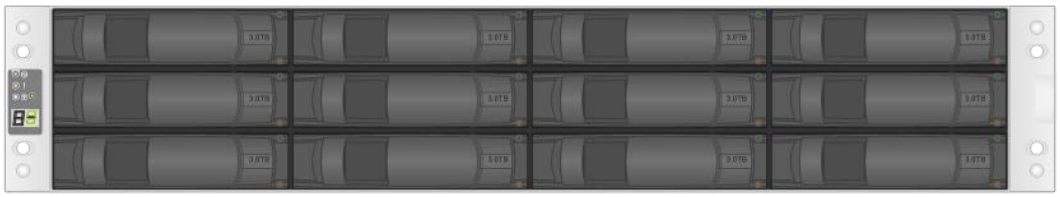
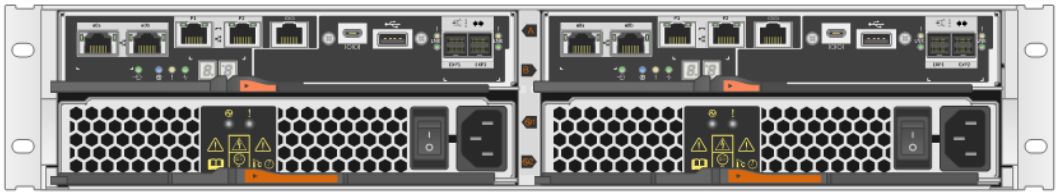


Figure 26) E2812 front view (open).



© 2018 NetApp, Inc. All rights reserved.

Figure 27) E2812 rear view.



E2824 Controller Shelf

The E2824 is a 2RU shelf that holds up to 24 2.5" drives. It features one or two RAID controllers and one or two Energy Star Platinum-rated high-efficiency power supplies (913W) with integrated fans. An E2824-based storage system supports a maximum of 180 HDDs (120 SSDs) and a mix of drive shelf models in a single system.

Figure 28, Figure 29, and Figure 30 show the front and rear views of the E2824 controller shelf. In the example, the E2800 controllers have two optical base ports and no HIC.

Figure 28) E2824 front view with bezel.

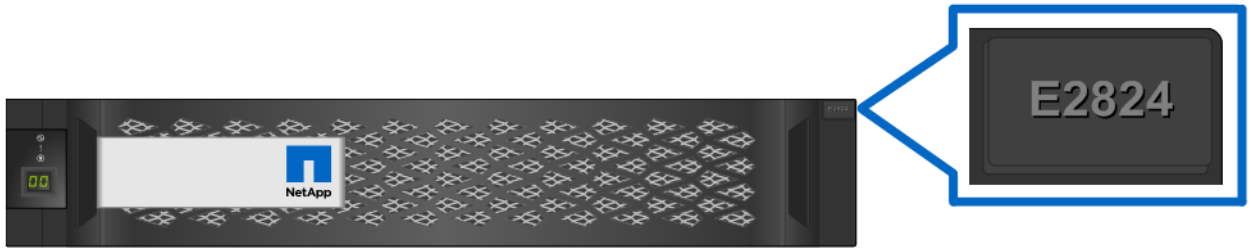


Figure 29) E2824 front view (open).

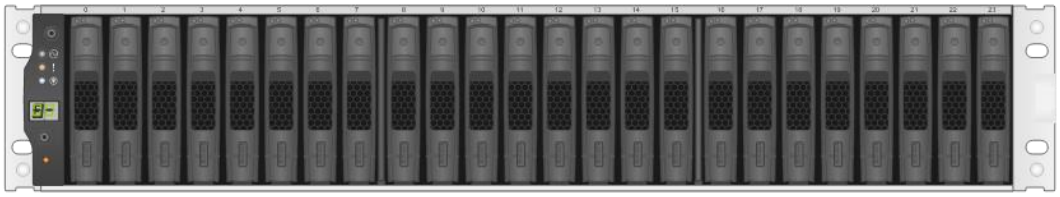
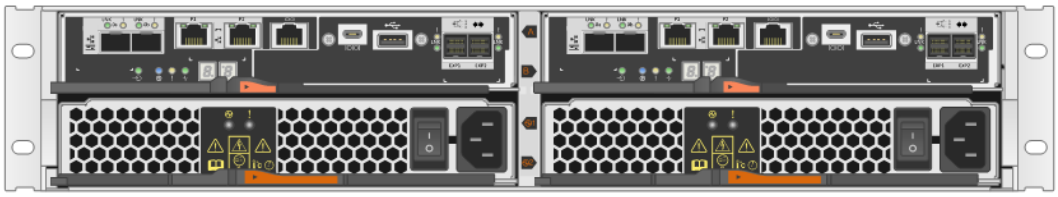


Figure 30) E2824 rear view.



E2860 Controller Shelf

The E2860 is a 4RU shelf that holds up to 60 3.5" drives or 2.5" drives with adapter. It features two RAID controllers and two Energy Star Platinum-rated high-efficiency power supplies (2325W) with separate dual fan modules. An E2860-based storage system supports a maximum of 180 HDDs (120 SSDs). When mixing shelf models, maximum drive counts vary and are governed by a maximum shelf count of 4 total shelves (a controller drive shelf and up to 3 expansion drive shelves), and the system must not exceed 180 total drive slots.

© 2018 NetApp, Inc. All rights reserved.

Figure 31, Figure 32, Figure 33 and show the front and rear views of the E2860 controller shelf. In the example, the E2800 controllers have two optical base ports and no HIC.

Figure 31) E2860 front view with bezel.

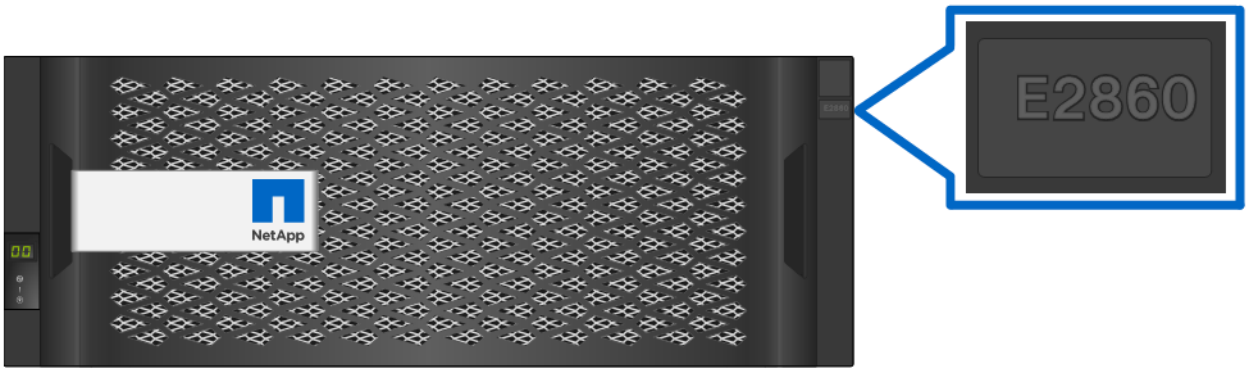


Figure 32) E2860 front view (open).

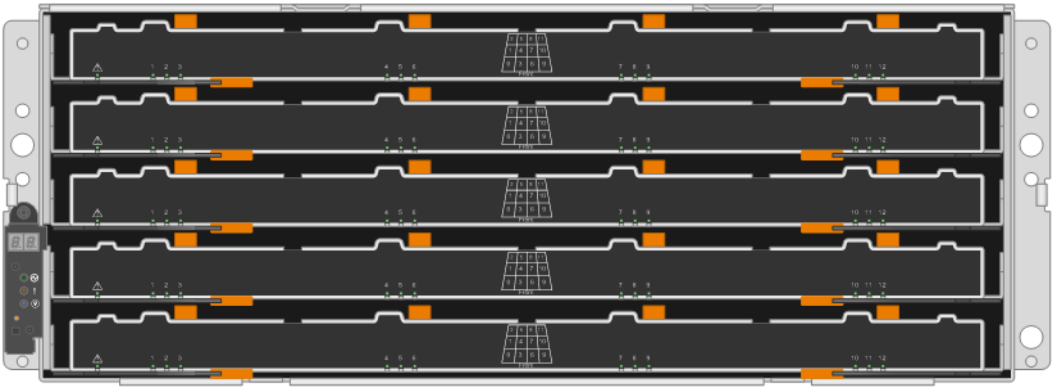


Figure 33) E2860 rear view.

E2800 Hardware Specifications

The E2800 controller has the following base hardware features:

- Dual Ethernet ports for management-related activities
- Either two optical FC/iSCSI or two RJ-45 iSCSI baseboard ports for host connection
- Dual 12Gb SAS drive expansion ports to attach expansion drive shelves

© 2018 NetApp, Inc. All rights reserved.

Note: Adding an optional HIC is needed only if you want to use the SAS protocol, need more than two host ports per controller, or want to use both FC and iSCSI protocols.

Table 13 lists the technical specifications for the E2800-based storage systems.

Table 13) E2800 technical specifications.

Specification	E2812	E2824	E2860
Maximum raw system capacity	480TB	1.4PB (15.3TB SSDs)	1800TB
Maximum number of drives per system	84 HDDs (84 SSDs)	96 HDDs (96 SSDs)	180 HDDs (120 SSDs)
Shelf form factor	2RU, 12 drives	2RU, 24 drives	4RU, 60 drives
SSD types (FIPS drives are also supported)	3.2TB, 1.6TB, or 800GB 2.5" SSDs	15.3TB, 3.2TB, 1.6TB, or 800GB 2.5" SSDs	3.2TB, 1.6TB, or 800GB 2.5" SSDs
HDD types supported (FIPS drives are supported)	Not supported	2.5" 10K RPM SAS: 1.8TB, 1.2TB, or 900GB	2.5" 10K RPM SAS: 1.8TB, 1.2TB, or 900GB
	3.5" 7.2K RPM NL-SAS: 10TB, 8TB, or 4TB	Not supported	3.5" 7.2K RPM NL-SAS: 10TB, 8TB, 6TB, or 4TB

Memory	4GB or 16GB per controller: simplex system
	8 GB or 32GB per duplex system
Onboard host I/O	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
	2-port 12Gb SAS (wide-port) per controller
	4-port 12Gb SAS (wide-port) per controller
	2-port 10GB iSCSI (optical)/16Gb FC per controller
	4-port 10Gb iSCSI (optical)/16Gb FC per controller
Drive shelves supported for expansion drive offerings	DE212C (2RU, 12 drives): 3 expansion shelves maximum; supports the same drive types as E2812 controller shelf
	DE224C (2RU, 24 drives): 3 expansion shelves maximum; supports the same drive types as E2824 controller shelf
	DE460C (4RU, 60 drives): 2 expansion shelves maximum; supports the same drive types as E2860 controller shelf

© 2018 NetApp, Inc. All rights reserved.

Specification	E2812	E2824	E2860
	DE6600 (4RU, 60 drives): 2 expansion shelves maximum; supports the same drive types as E2824 and/or E2812 controller drive shelves **Note:** Supports only SAS 2 (6Gbps) transfer speeds.		
	DE5600 (2RU, 24 drives): 3 expansion shelves maximum; supports the same drive types as E2824 controller shelf **Note:** Supports only SAS 2 (6Gbps) transfer speeds.		
	DE1600 (2RU, 12 drives): 3 expansion shelves maximum; supports only NL-SAS drive types **Note:** Supports only SAS 2 (6Gbps) transfer speeds.		
High-availability (HA) features	Dual active controllers with automated I/O path failover		
	Support for RAID 0, 1 (10 for 4 drives or more), 5, and 6 and Dynamic Disk Pools **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 the System Manager online help.		
	Redundant, hot-swappable storage controllers, disk drives, and power fan canisters		
	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 ESM 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		

Table 14 provides a reference matrix of supported drive types. Refer to the Hardware Universe for encryption capability by drive capacity (FDE, FIPS) and current drive availability information.

Table 14) Supported drive types in SAS 3 enclosures.

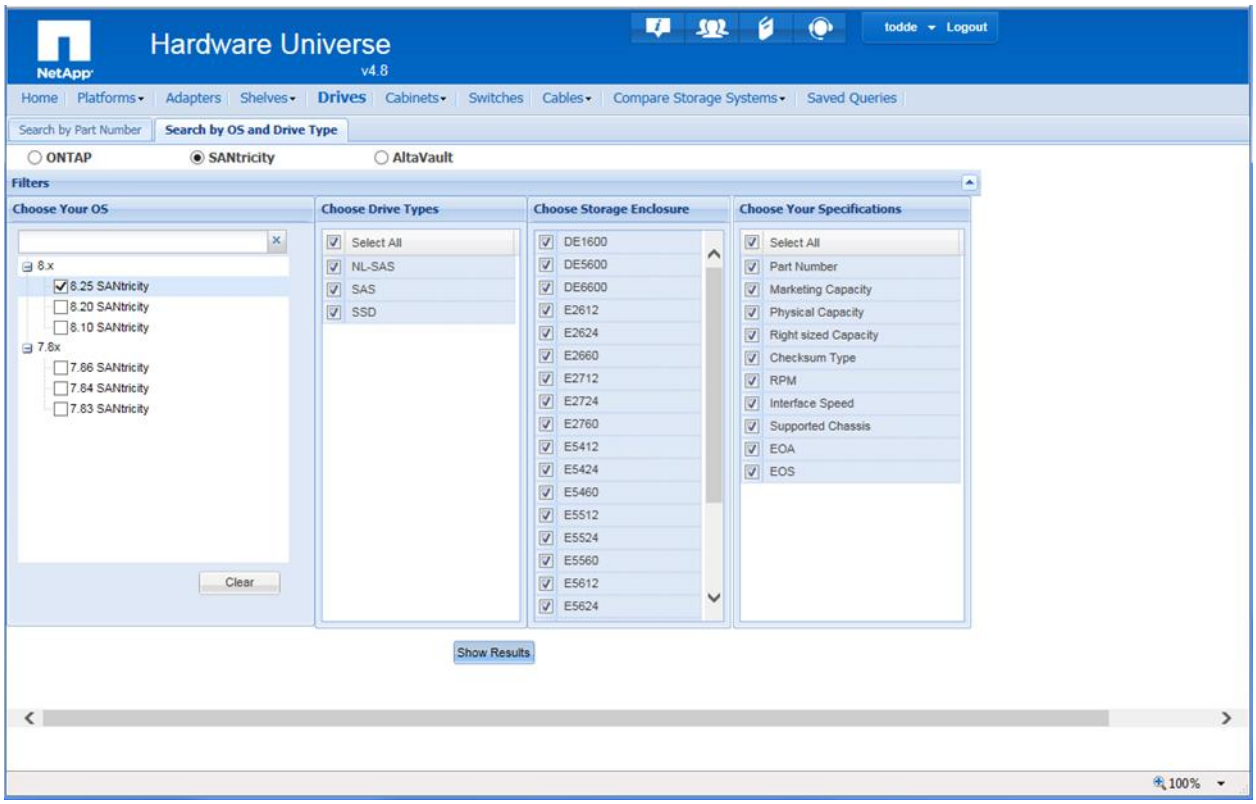
Drive Types	NL-SAS	SAS	SSD
DE212C	4TB		800GB
	8TB		1.6TB
	10TB		3.2TB

© 2018 NetApp, Inc. All rights reserved.

Drive Types	NL-SAS	SAS	SSD
DE224C		900GB	800GB
		1.2TB	1.6TB
		1.8TB	3.2TB
DE460C	4TB, 6TB	900GB	800GB
	8TB	1.2TB	1.6TB
	10TB	1.8TB	3.2TB

Figure 34 shows the navigation to select drives by OS and platform compatibility.

Figure 34) Hardware Universe drives by OS and platform.



For additional information, refer to the NetApp E2800 datasheet at E-Series and EF-Series Datasheets.

6.2 Controller Host Interface Features

By default, the E2800 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 E2800 controller also supports five 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

© 2018 NetApp, Inc. All rights reserved.

- 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 2-port and 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 E2800 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, part # X-48895-00-R6-C, does not support 1Gb iSCSI. It does support 4/8/16Gb FC and 10Gb iSCSI. Use SFP part # X-48896-00-C for 1Gb iSCSI connections.

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 35.

© 2018 NetApp, Inc. All rights reserved.

Figure 35) E2800 with optical base ports HIC options.

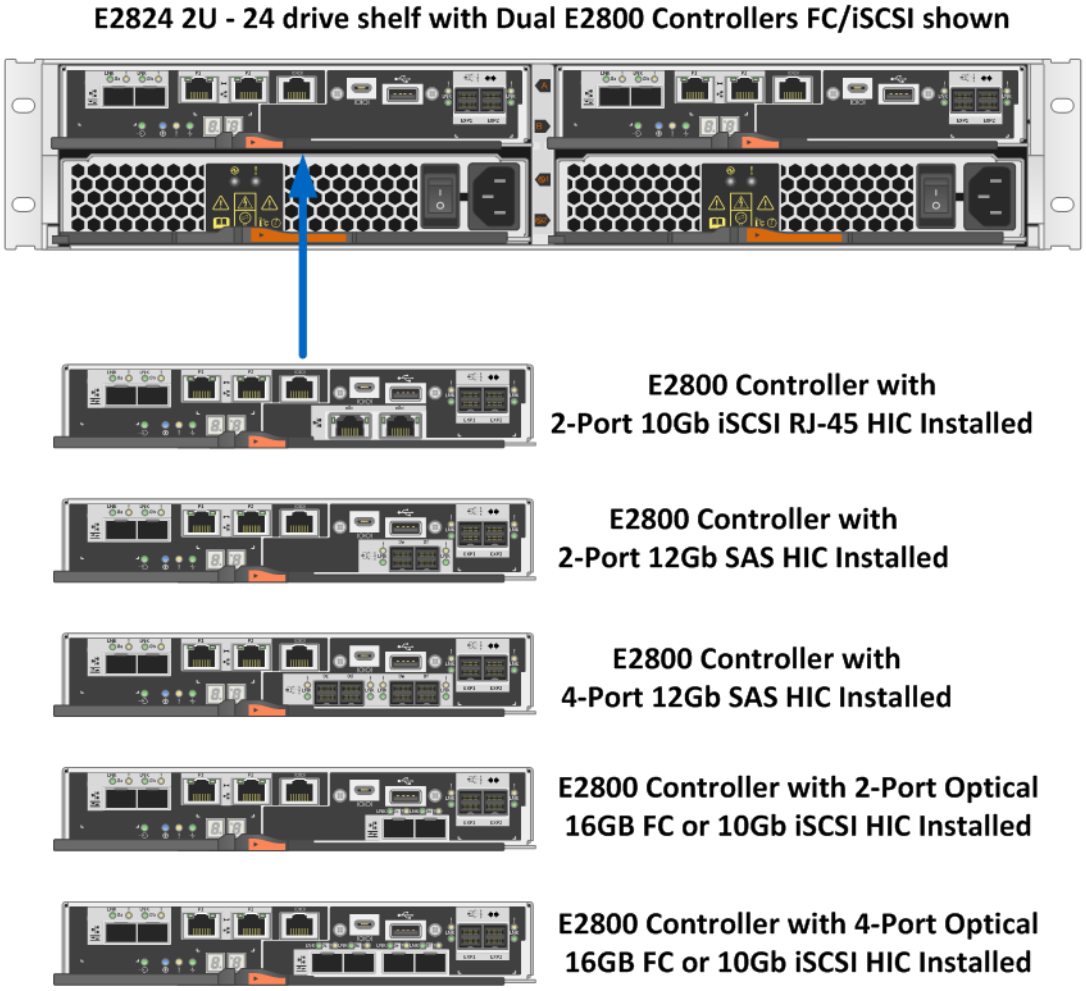
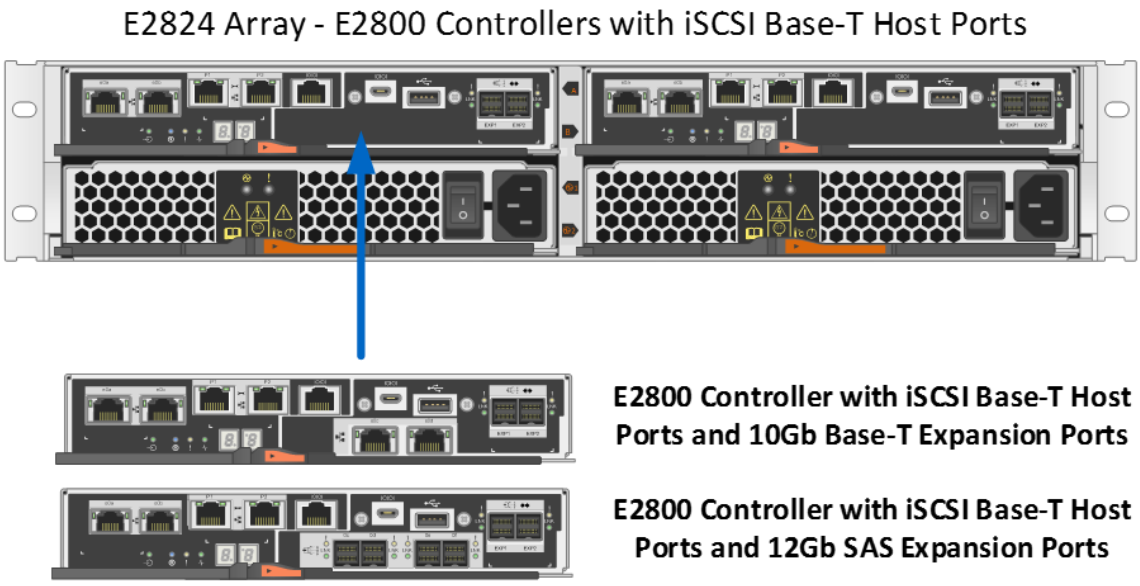


Figure 36 shows the single-HIC option available when the baseboard host ports are 10Gb iSCSI Base-T.

© 2018 NetApp, Inc. All rights reserved.

Figure 36) E2800 with Base-T iSCSI onboard host ports: HIC options.



Note: All HIC options support link speed autonegotiation.

6.3 Hardware LED Definitions

E2800 Controller Shelf LEDs

The E2800 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 E2800 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 indicate the status of the individual units.

Figure 37 shows the ODP of the E2812 and E2824 controller shelves. Figure 38 shows the ODP of the E2860 controller shelf.

© 2018 NetApp, Inc. All rights reserved.

Figure 37) ODP on front panel of E2824 and E2812 controller shelves.

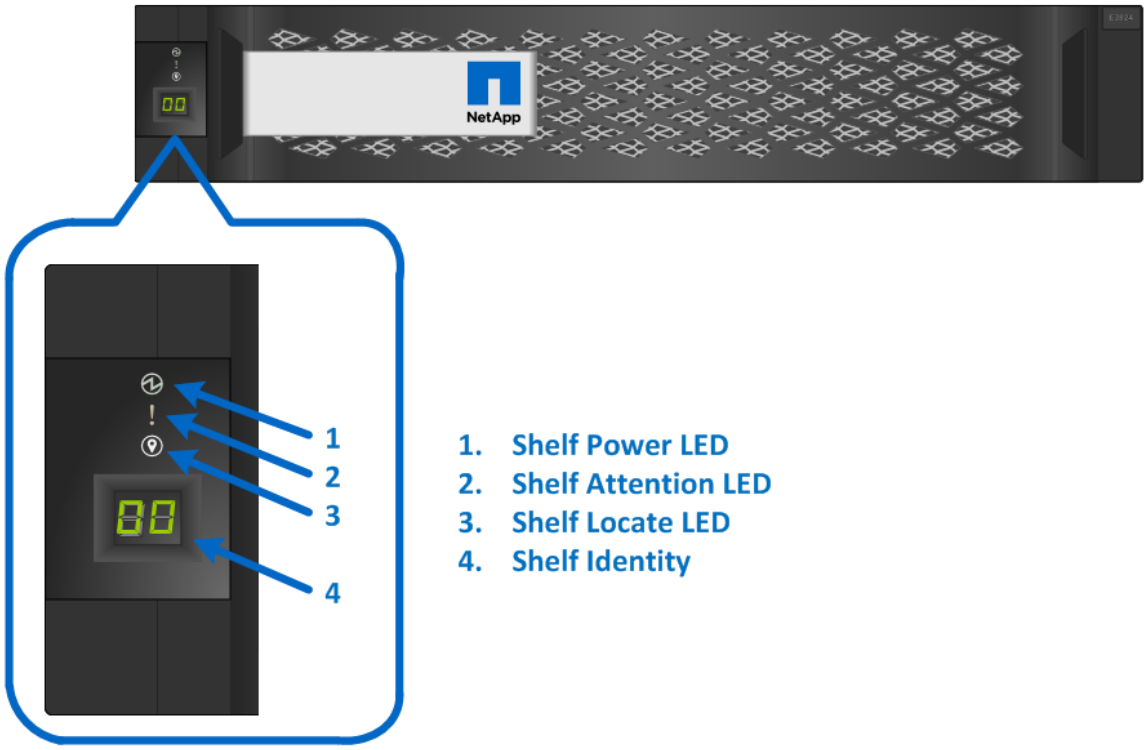
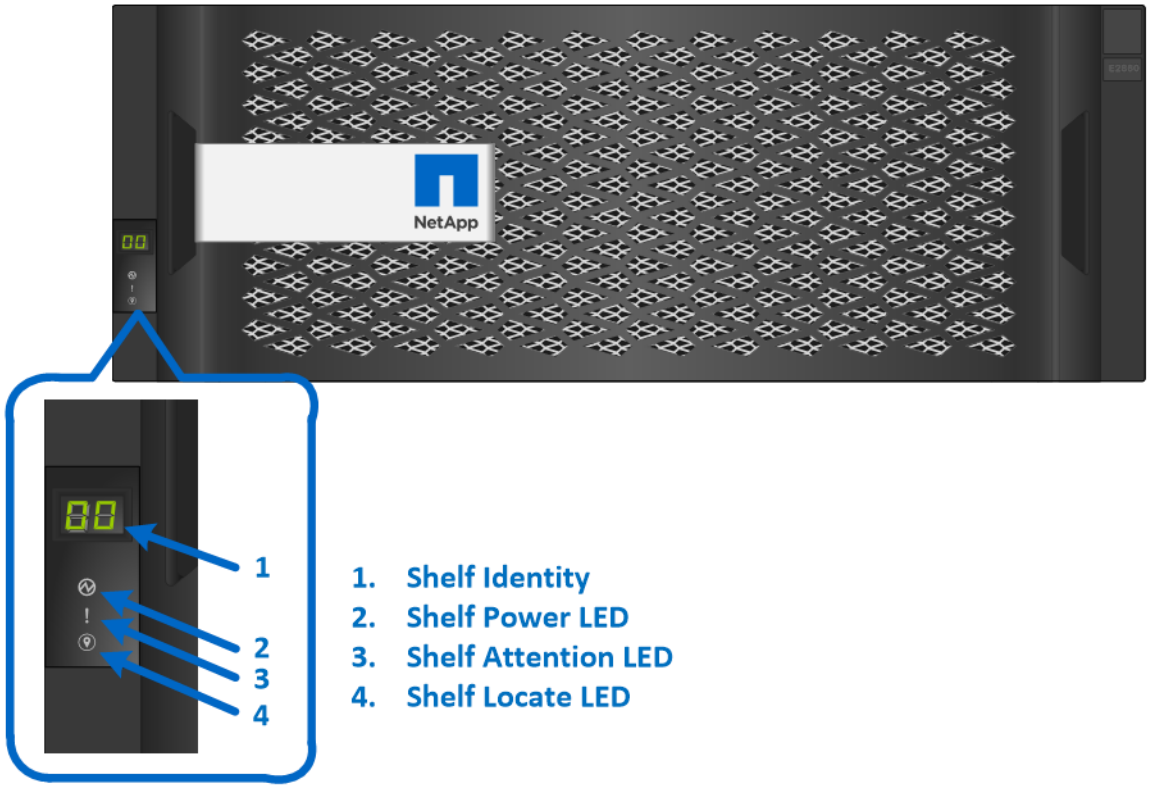


Figure 38) ODP on front panel of E2860 controller shelves.



© 2018 NetApp, Inc. All rights reserved.

Table 15 defines the ODP LEDs on the E2800 controller shelf.

Table 15) E2800 controller shelf LED definitions (front panel).

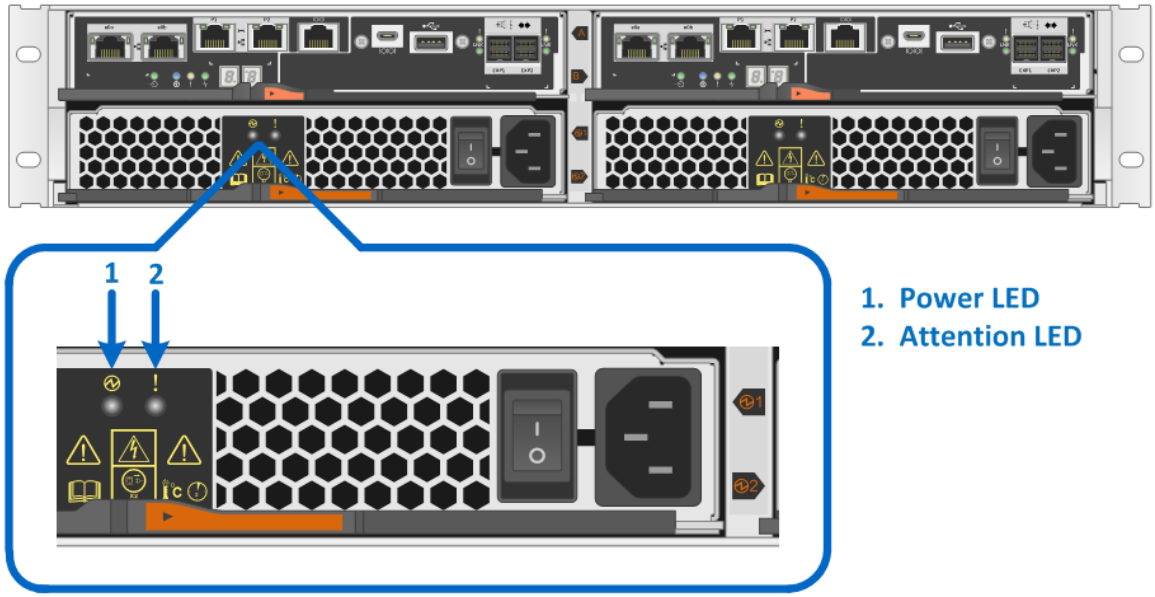
LED Name	Color	LED On	LED Off
Power	Green	Power is present.	Power is not present.
Attention	Amber	A component in the controller shelf requires attention.	Normal status.
Locate	Blue	There is an active request to physically locate the shelf.	Normal status.

Note: The shelf-identity feature displays a numerical value to identify the shelf. The dual seven-segment display indicates values from 00 to 99.

Power Fan Canister Status LEDs

The power fan canisters for the E2824 and E2812 controller shelves are identical. The LEDs on the rear panel are shown in Figure 39 and are defined in Table 16.

Figure 39) LEDs on E2824 and E2812 power fan canister (rear view).



The power and fan canisters are separate for the E2860 controller shelf. The LEDs on the rear panel of each are shown in Figure 40 and defined in Table 16.

© 2018 NetApp, Inc. All rights reserved.

Figure 40) LEDs on E2860 power canister (rear view).

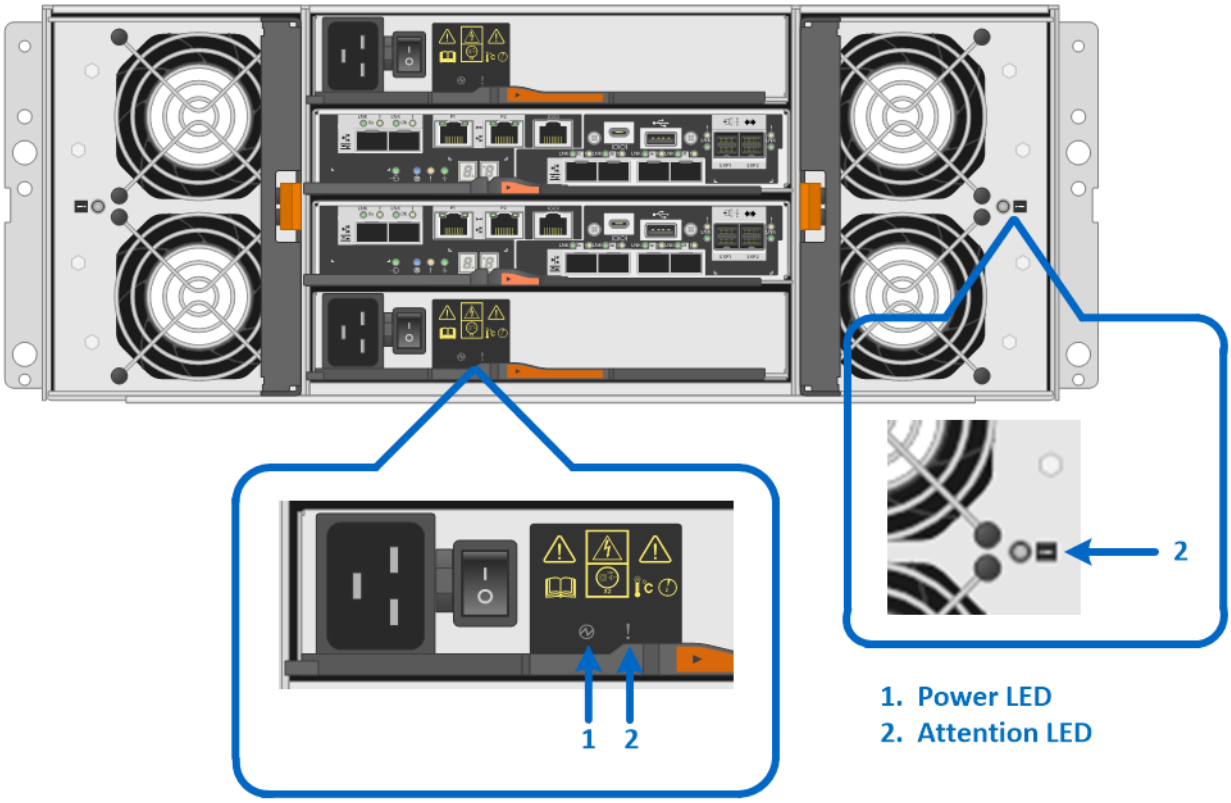


Table 16) E2812, E2824, and E2860 controller shelf power and fan canister LED definitions.

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.

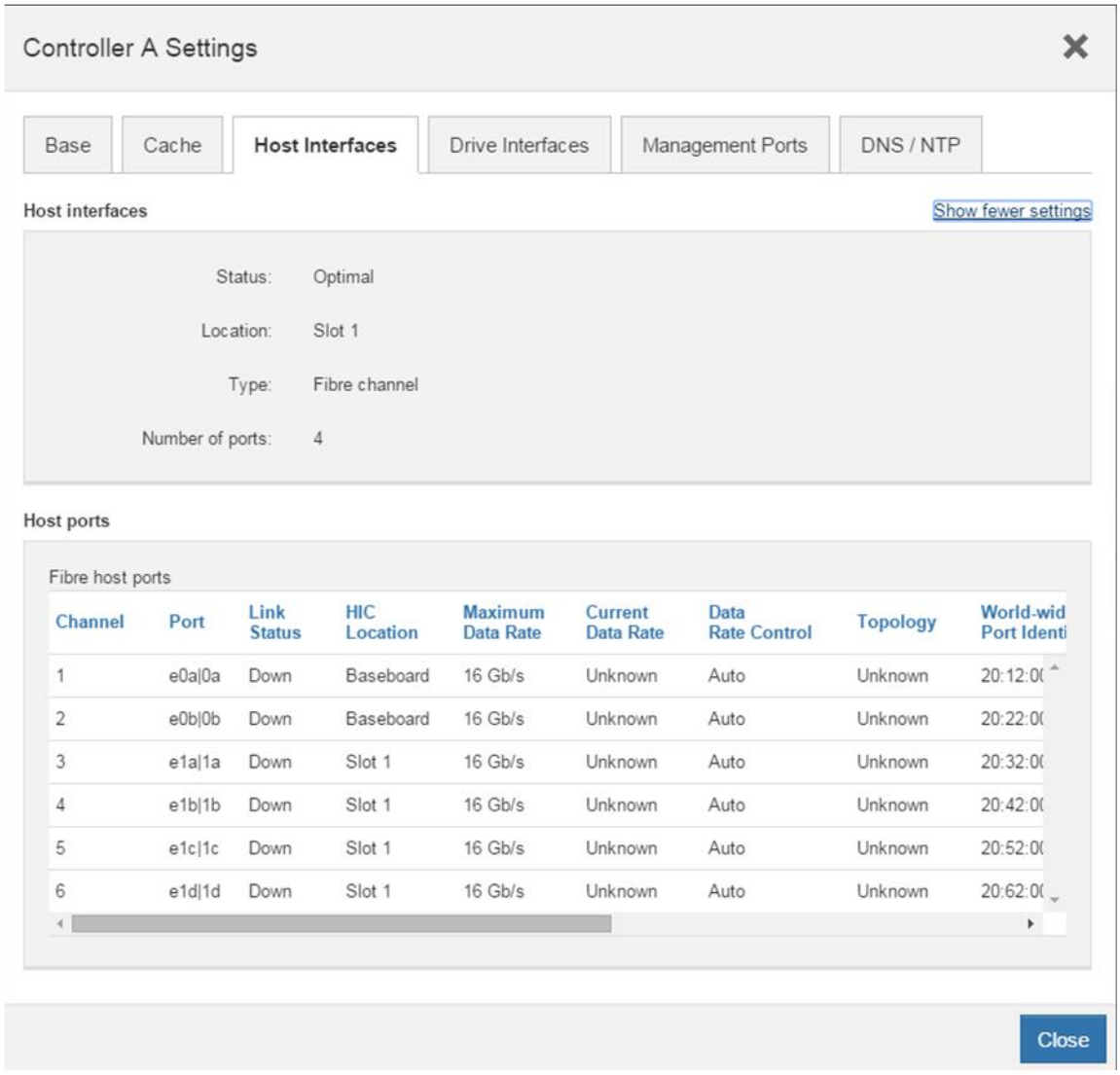
E2800 Controller Canister LEDs

The E2800 controller canister has several LED status indicators. The LEDs on the left side of the module refer to the overall controller status and to the onboard host ports. The LEDs on the right side of the module refer to the drive expansion ports and to the optional HIC ports.

Host port status can be verified by directly checking the port LEDs or by using the SANtricity System Manager GUI. The Host Interfaces tab of the Controller Settings dialog box, shown in Figure 41, details the status of each host I/O interface that is connected to the storage system.

© 2018 NetApp, Inc. All rights reserved.

Figure 41) Controller settings dialog box.

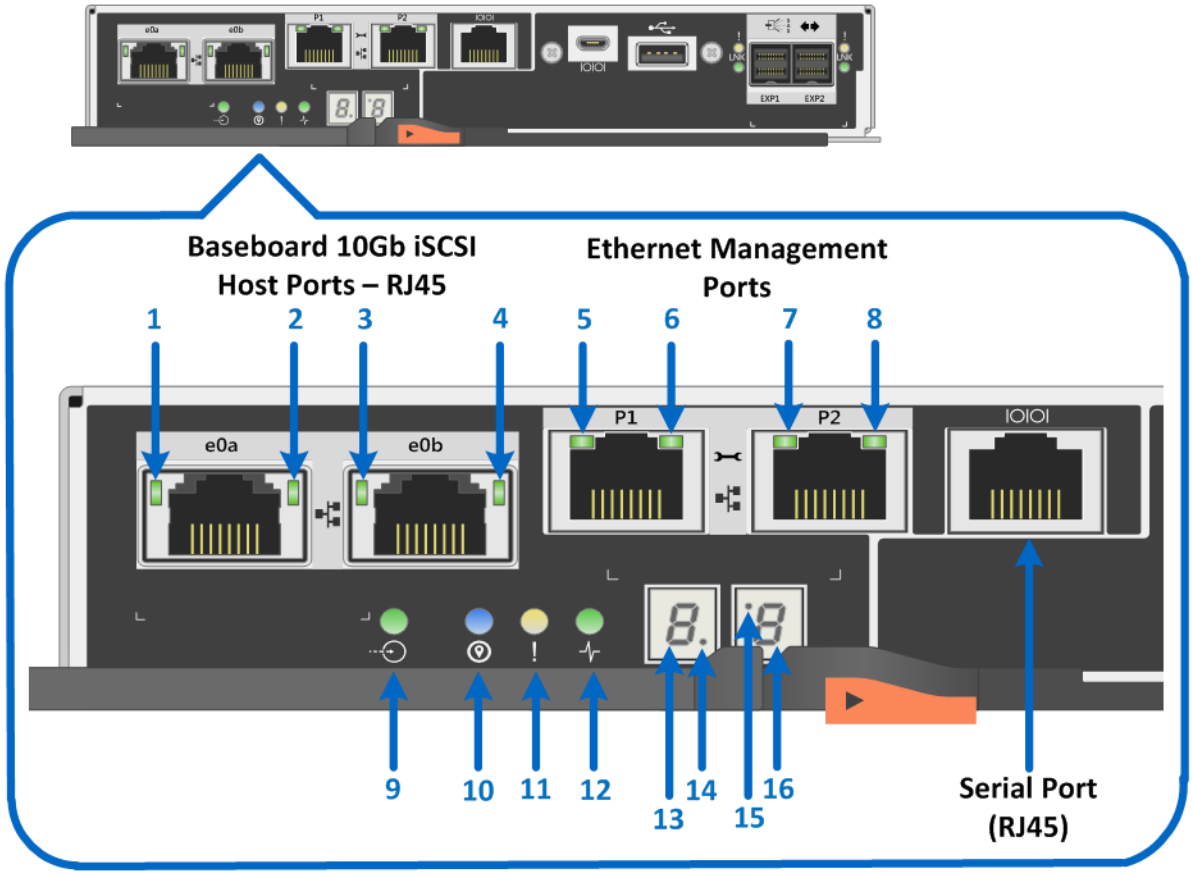


Controller Base Port Status LEDs

Figure 42 shows the onboard LED status indicators on the left side of the E2800 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.

© 2018 NetApp, Inc. All rights reserved.

Figure 42) LEDs on left side of E2800 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 17 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 42). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

© 2018 NetApp, Inc. All rights reserved.

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

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

Table 18 defines the Ethernet management port LEDs on the controller (LEDs 5 through 8 in Figure 42).

Table 18) Ethernet management port LED definitions.

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

Table 19 defines the controller status LEDs (LEDs 9 through 15 in Figure 42).

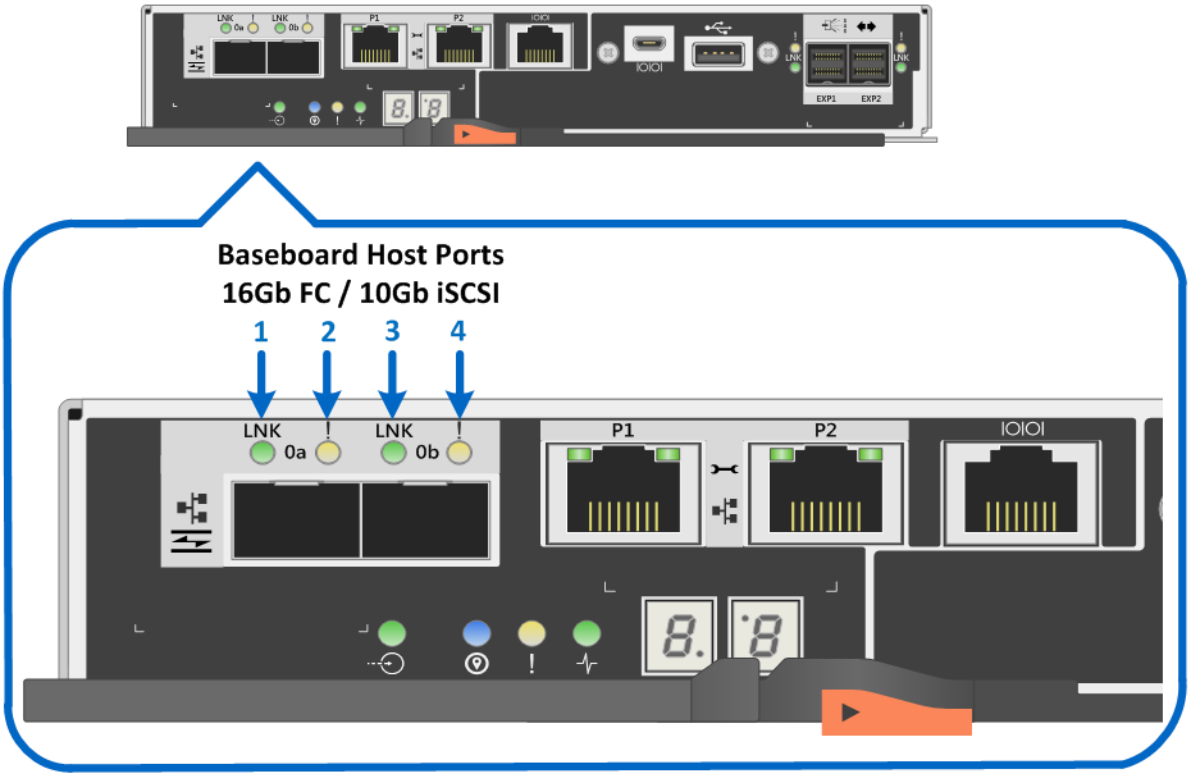
Table 19) Controller base features LED definitions.

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

Figure 43 shows the onboard LED status indicators on the left side of the E2800 controller canister with the 16Gb FC/10Gb iSCSI baseboard host port LEDs indicated.

© 2018 NetApp, Inc. All rights reserved.

Figure 43) LEDs on left side of E2800 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 20 defines the baseboard host interface port LEDs (LEDs 1 through 4 in Figure 43). These LEDs indicate the connection status for each link between the storage system and host-side hardware.

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

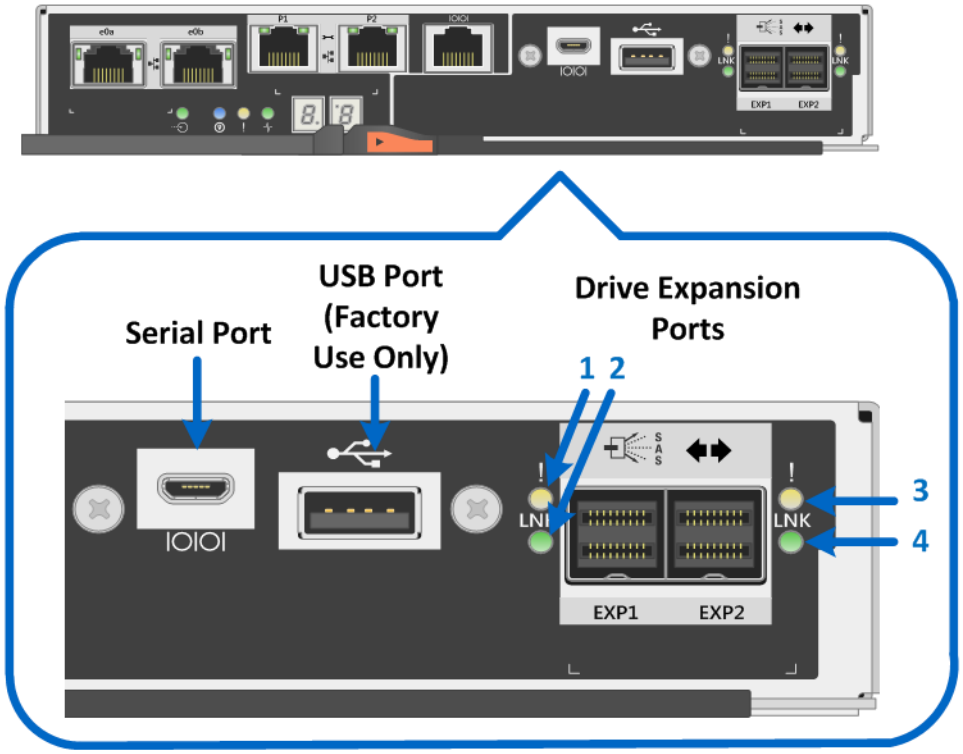
LED Name	Color	LED On	LED Off
Host port link/activity	Green	• Solid: link up with no activity. • Blinking: link up with activity.	Link is down.
Host port attention	Amber	Port requires operator attention.	Normal status.

Drive-Side SAS Expansion Port LEDs

The E2800 controller canister is equipped with two SAS expansion ports that are used to connect expansion drive shelves to the E2800 controller shelf. Figure 44 shows the SAS expansion port LEDs.

© 2018 NetApp, Inc. All rights reserved.

Figure 44) LEDs for drive expansion ports (no HIC installed).



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

Table 21 defines each drive-side LED (LEDs 1 through 4 in Figure 44).

Table 21) Drive expansion port LED definitions.

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

E2800 Optional Host Interface Cards

The E2800 supports several host interface expansion options, including SAS, FC, and iSCSI:

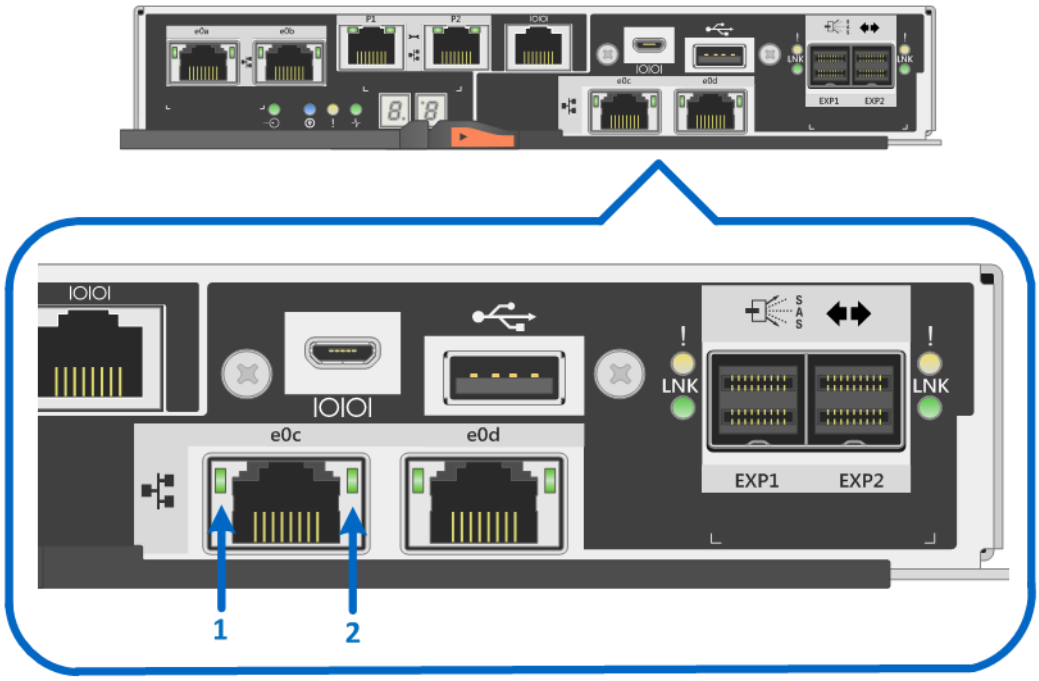
- When the baseboard host ports are optical, as shown in Figure 35, all five HIC options are available.
- When the baseboard host ports are 10Gb iSCSI Base-T, as shown in Figure 36, the only expansion HICs supported are the 2-port 10Gb iSCSI Base-T HIC or the 2-port and 4-port 12Gb SAS HICs.

© 2018 NetApp, Inc. All rights reserved.

2-Port 10Gb iSCSI RJ-45 HIC LEDs

The 2-port 10Gb iSCSI copper HIC has two standard RJ-45 connectors, as shown in Figure 45, and uses standard RJ-45 twinax cables to connect to switches or directly to hosts.

Figure 45) LEDs on 2-port 10Gb iSCSI RJ-45 HIC.



1. Host iSCSI Expansion (RJ45) Port e0c Link State LED
2. Host iSCSI Expansion (RJ45) Port e0c Link Activity LED

Table 22 defines the LEDs on the 2-port 10Gb iSCSI HIC.

Note: The drive expansion port LEDs are defined in Table 21.

Table 22) 2-port 10Gb iSCSI HIC 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.

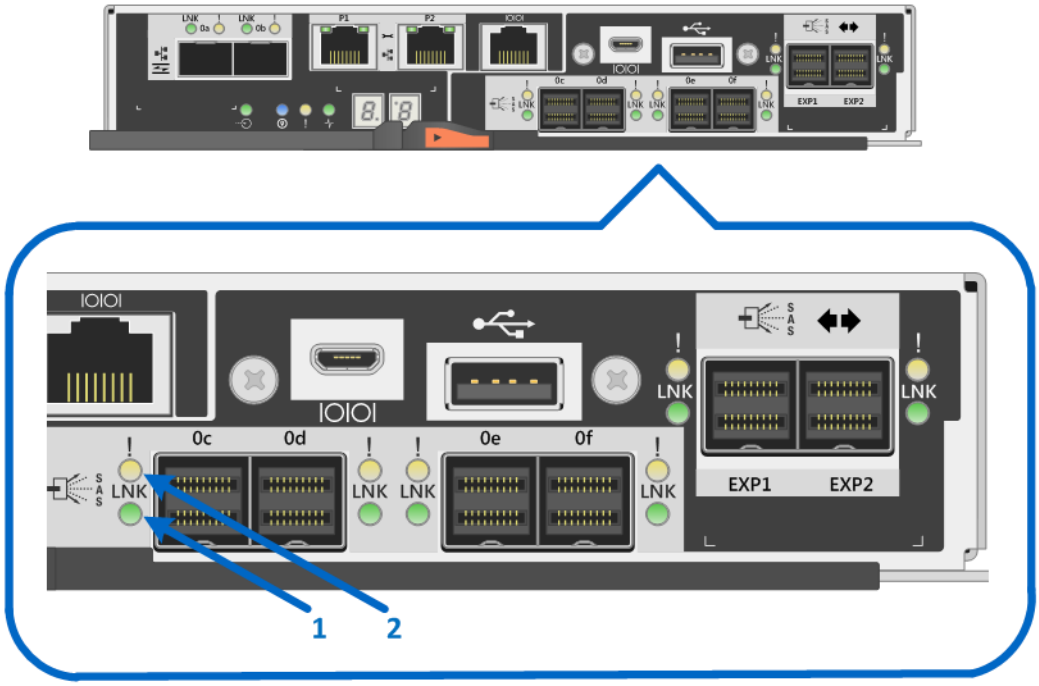
2-Port and 4-Port 12Gb SAS HIC LEDs

Figure 46 and Figure 47 show the LEDs for the 4-port and 2-port 12Gb SAS HICs. LEDs are called out for only the 4-port SAS HIC; the 2-port HIC LEDs are the same.

Note: The SAS expansion HICs are the same for both E2800 controller models. The E2800 controller with the 2-port optical onboard ports is pictured in Figure 46 with the 4-port optional SAS HIC installed.

© 2018 NetApp, Inc. All rights reserved.

Figure 46) LEDs for 4-port 12Gb SAS HIC.



1. Host SAS Expansion Port 0c Link LED
2. Host SAS Expansion Port 0c Fault LED

Figure 47) LEDs for 2-port 12Gb SAS HIC.

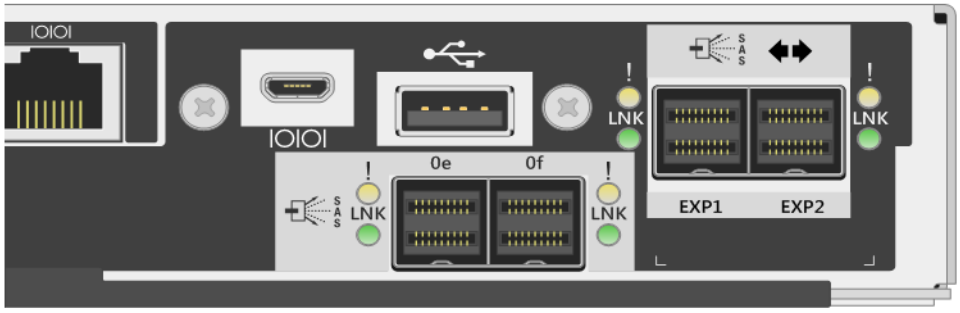


Table 23 defines the LEDs for the 12Gb SAS HICs.

Note: The drive expansion port LEDs are defined in Table 21.

Table 23) 2-port and 4-port 12Gb SAS HIC LED definitions.

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

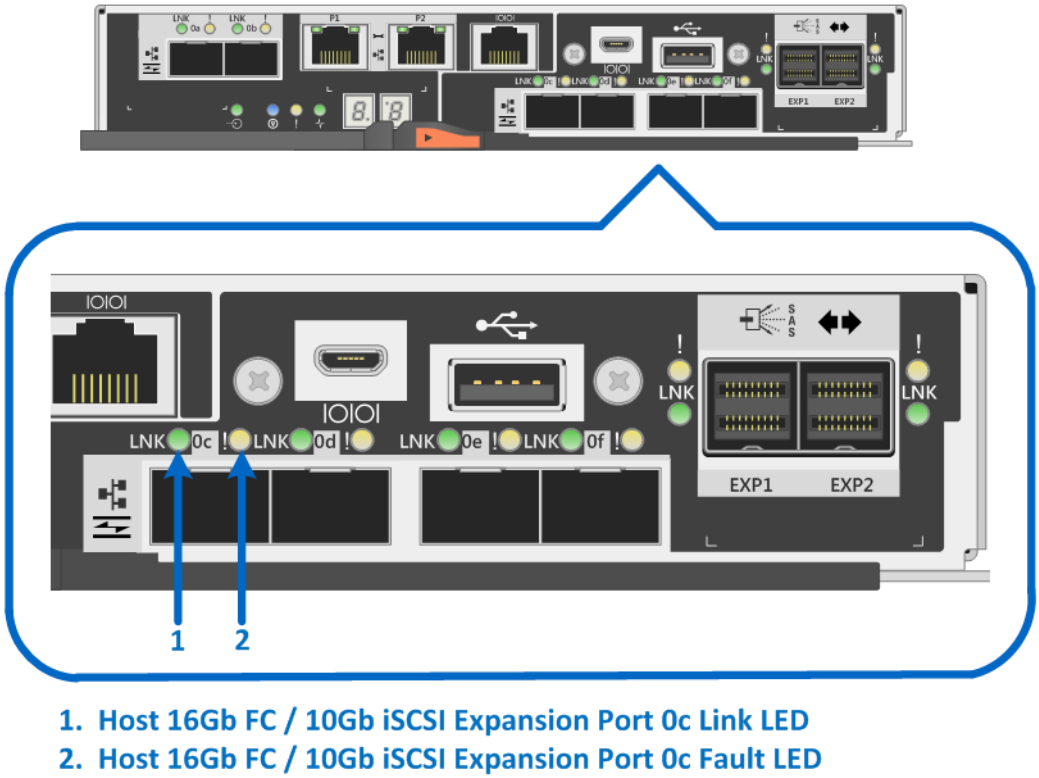
© 2018 NetApp, Inc. All rights reserved.

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

The E2800 controller supports a 2-port or 4-port optical HIC that offers 16Gb FC protocol or 10Gb iSCSI protocol. The 2-port HIC is functionally equivalent to the 4-port HIC. When using the 4-port HIC and dual controllers, the E2800 storage system provides a maximum of 12 16Gb FC or 12 10Gb iSCSI ports or a mixture of 16Gb FC and 10Gb iSCSI ports.

Figure 48 and Figure 49 show the LEDs for the 4-port and 2-port optical HIC. LEDs are called out for only the 4-port optical HIC; the 2-port HIC LEDs are the same.

Figure 48) LEDs for 4-port optical HIC (16Gb FC or 10Gb iSCSI).



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

Figure 49) LEDs for 2-port optical HIC (16Gb FC or 10Gb iSCSI).

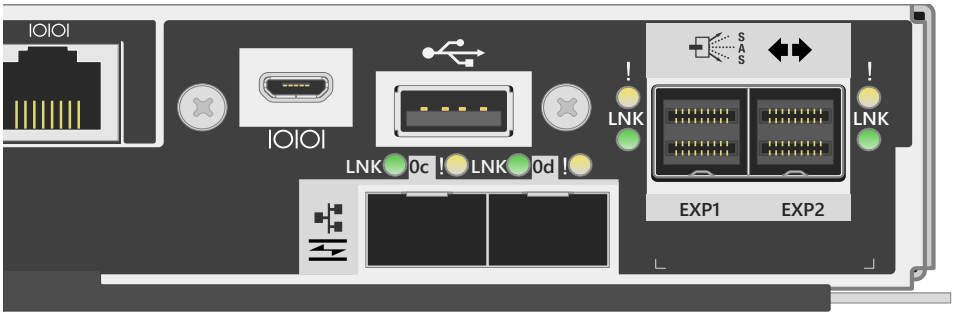


Table 24 defines the LEDs on the 2-port and 4-port optical HICs (16Gb FC or 10Gb iSCSI).

Note: The drive expansion port LEDs are defined in Table 21.

© 2018 NetApp, Inc. All rights reserved.

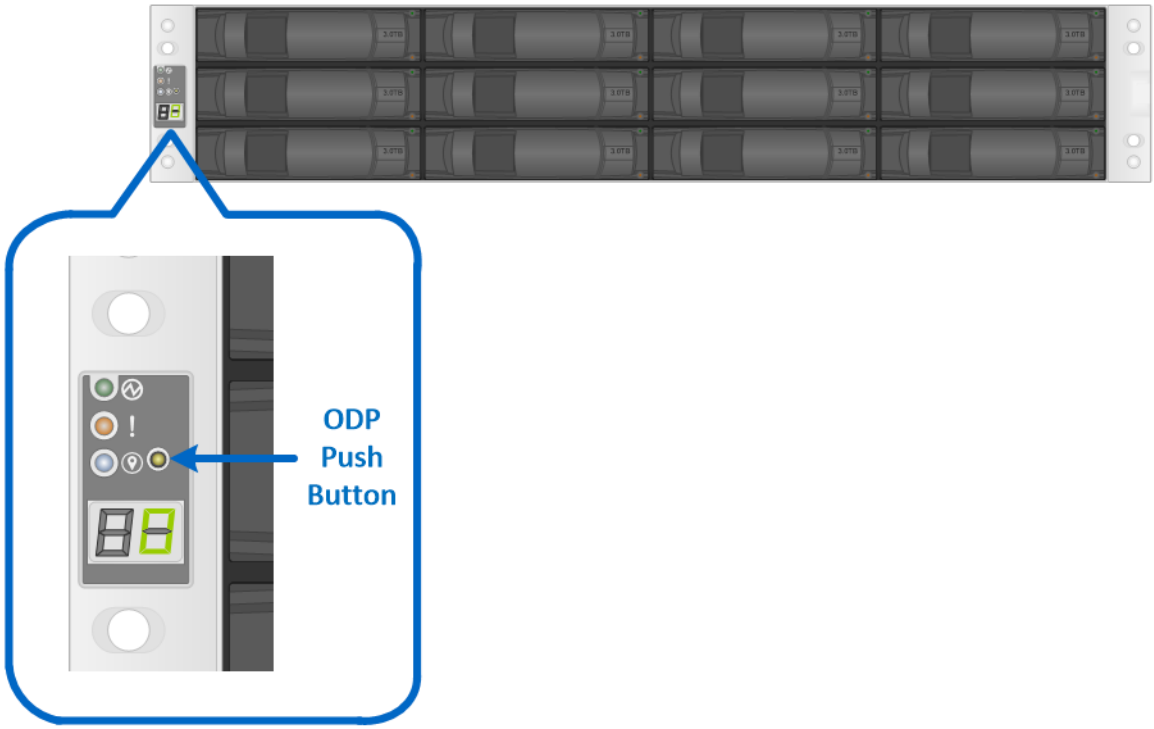
Table 24) 2-port and 4-port optical HIC (16Gb FC or 10Gb iSCSI) LED definitions.

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

6.4 Setting Shelf ID with ODP Pushbutton

The shelf ID for the controller shelves and drive shelves can be changed externally using the ODP pushbutton, shown in Figure 50, Figure 51, and Figure 52 for the E2812 (DE212C), E2824 (DE224C), and E2860 (DE460C).

Figure 50) ODP on the E2812 or DE212C (front bezel or end caps removed).



© 2018 NetApp, Inc. All rights reserved.

Figure 51) ODP on the E2824 or DE224C (front bezel or end caps removed).

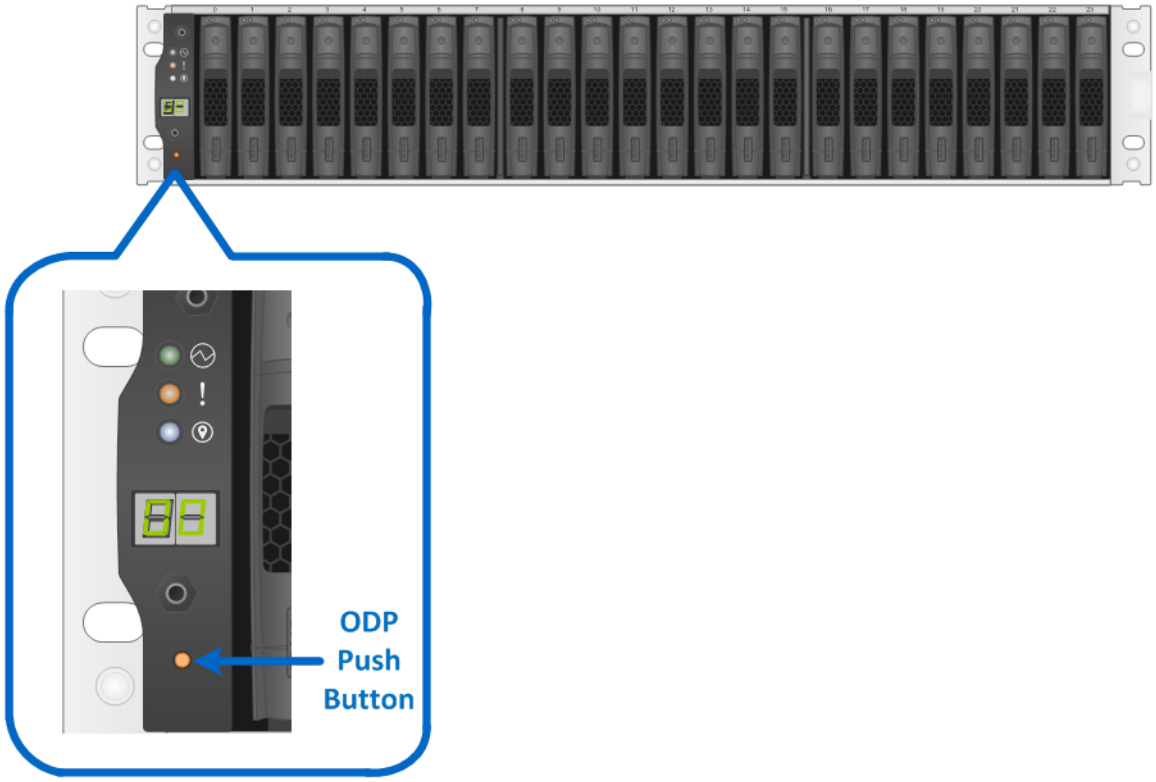


Figure 52) ODP on the E2860 or DE460C (front bezel removed).

Follow these steps to modify the shelf ID:

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

© 2018 NetApp, Inc. All rights reserved.

6. Change the second number of the shelf ID by pressing and holding the button until the second number on the digital display blinks, which can take two to three seconds. The first number on the digital display stops blinking.
7. Press the button to advance the number until you reach the desired number from 0 to 9. The second number continues to blink.
8. Lock in the desired number and exit the programming mode by pressing and holding the button until the second number stops blinking, which can take two to three seconds.
9. Repeat steps 1 through 8 for each additional shelf.

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

For additional information about the E2800 storage systems and related hardware, refer to the E2800 series documentation at http://mysupport.netapp.com/eseries.

7 Drive Shelves

The E2800 controller shelf supports 12, 24, or 60 drives based on the shelf model (DE212C, DE224C, or DE460C, respectively), but the system capacity can be further expanded by adding additional expansion drive shelves to the controller shelf. The E2800 supports up to 4 total shelves, the controller shelf plus three expansion drive shelves, for a maximum of 180 HDDs (120 SSDs). Drive shelf options are shown in Table 25.

Table 25) Drive shelf options for E2800.

Property	DE212C	DE224C	DE460C	DE1600	DE5600	DE6600
Form factor	2RU	2RU	4RU	2RU	2RU	4RU
Drive size	3.5" 2.5" (with bracket)	2.5"	3.5" 2.5" (with bracket)	3.5"	2.5"	3.5" 2.5" (with bracket)
Drive types	NL-SAS SSD	SAS SSD	SAS NL-SAS SSD	NL-SAS	SAS SSD	SAS NL-SAS SSD
Total drives	12	24	60	12	24	60
Drive interface	12Gb SAS	12Gb SAS	12Gb SAS	6Gb SAS	6Gb SAS	6Gb SAS

Note: DE1600, DE5600, and DE6600 are supported only as part of in-place data migration from E2700/E5400/E5500/E5600 to E2800.

7.1 Drive Shelf Configurations

E2800 controllers can be paired with all five E-Series shelves, and the shelves can be mixed in the same storage system. The older 6Gb SAS 2 drive shelves (DE1600, DE5600, and DE6600) are not covered in detail in this document. Refer to the E-Series Disk Shelves documentation for further information. The following sections provide detailed information about the 12Gb SAS 3 drive shelves (DE212C and DE224C).

DE212C Drive Shelf

The DE212C is a 2RU shelf that holds up to 12 3.5" drives or 2.5" SSDs with adapter. It features dual high-speed 12Gb SAS 3 I/O modules (IOMs) and dual Energy Star Platinum-rated high-efficiency power

© 2018 NetApp, Inc. All rights reserved.

supplies (913W) with integrated fans, in a duplex system. It is fully redundant with hot-swappable components.

Figure 53, Figure 54, and Figure 55 show the front and rear views of the DE212C drive shelf.

Figure 53) DE212C front view with end caps.

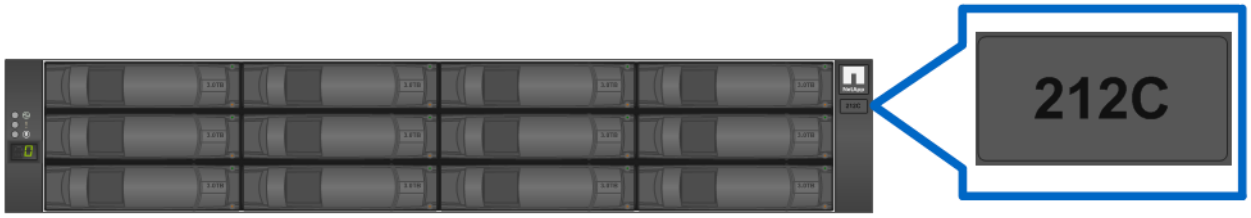


Figure 54) DE212C front view without end caps.

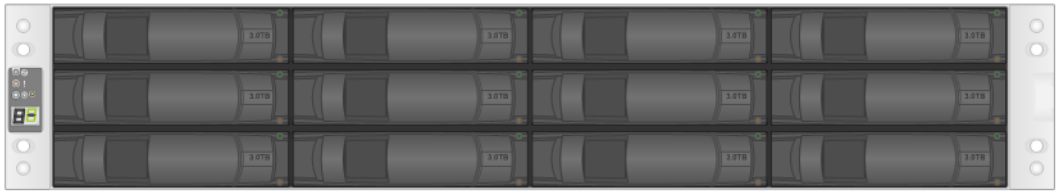
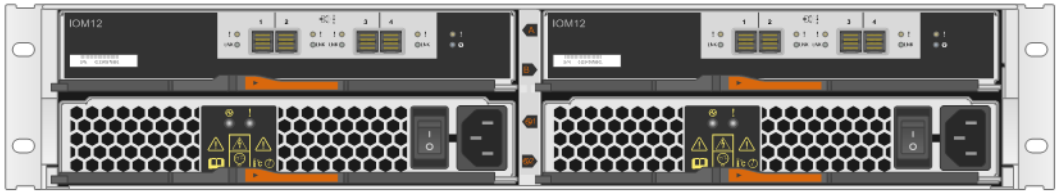


Figure 55) DE212C rear view.

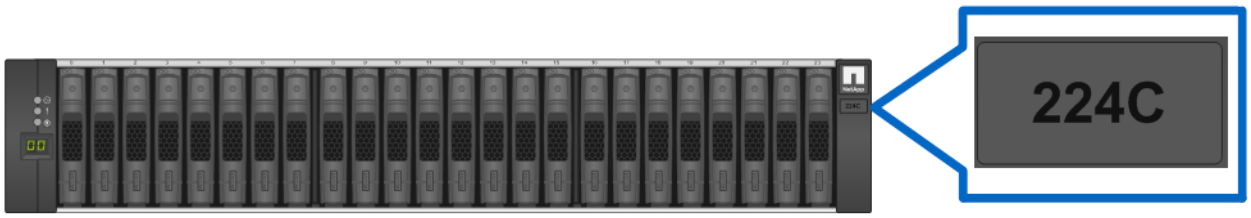


DE224C Drive Shelf

The DE224C is a 2RU shelf that holds up to 24 2.5" drives. It features dual high-speed 12Gb SAS 3 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 56, Figure 57, and Figure 58 show the front and rear views of the DE224C drive shelf.

Figure 56) DE224C front view with end caps.



© 2018 NetApp, Inc. All rights reserved.

Figure 57) DE224C front view without end caps.

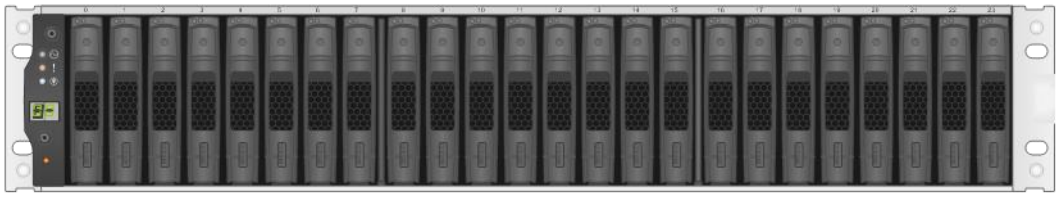
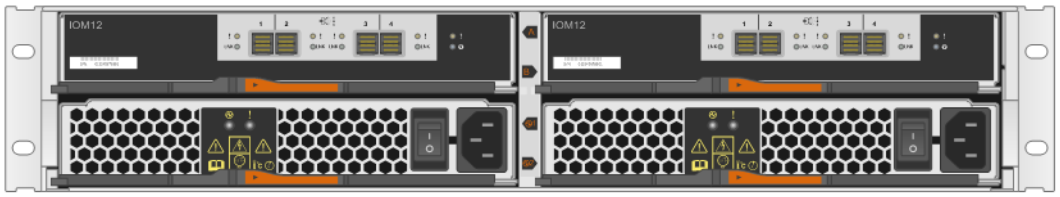


Figure 58) DE224C rear view.



DE460C Drive Shelf

The DE224C is a 2RU shelf that holds up to 24 2.5" drives. It features dual high-speed 12Gb SAS 3 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 59, Figure 60, and Figure 61 show the front and rear views of the DE460C drive shelf.

Figure 59) DE460C front view with bezel.

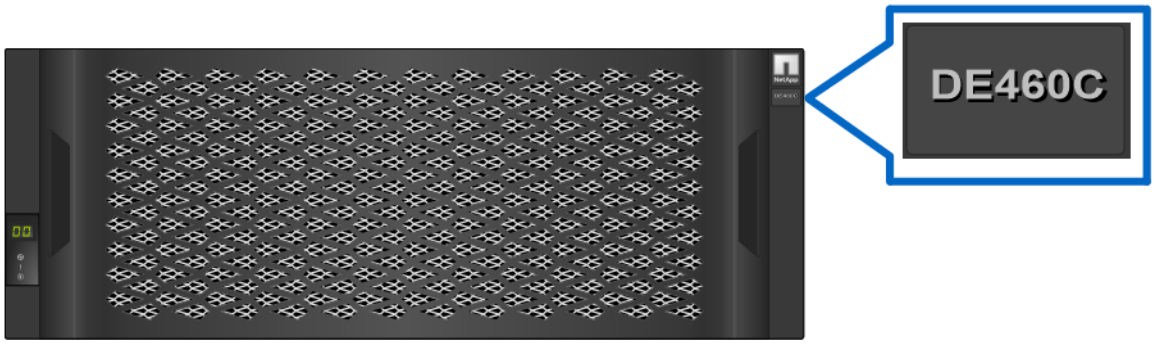
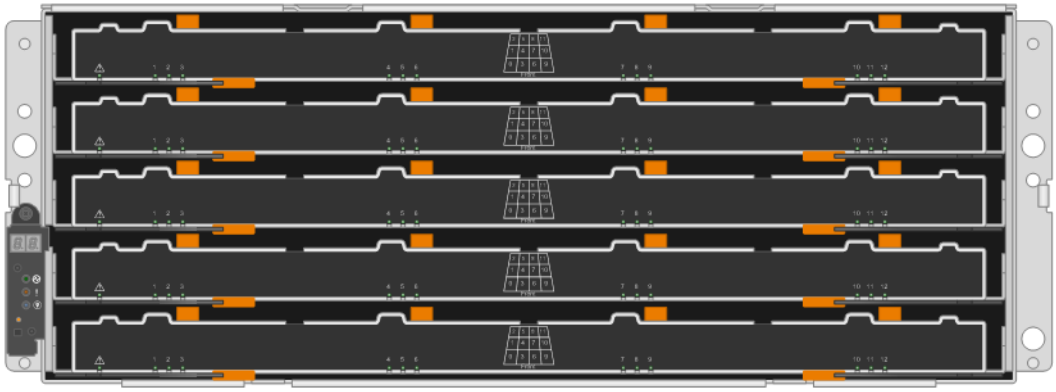


Figure 60) DE460C front view without bezel.



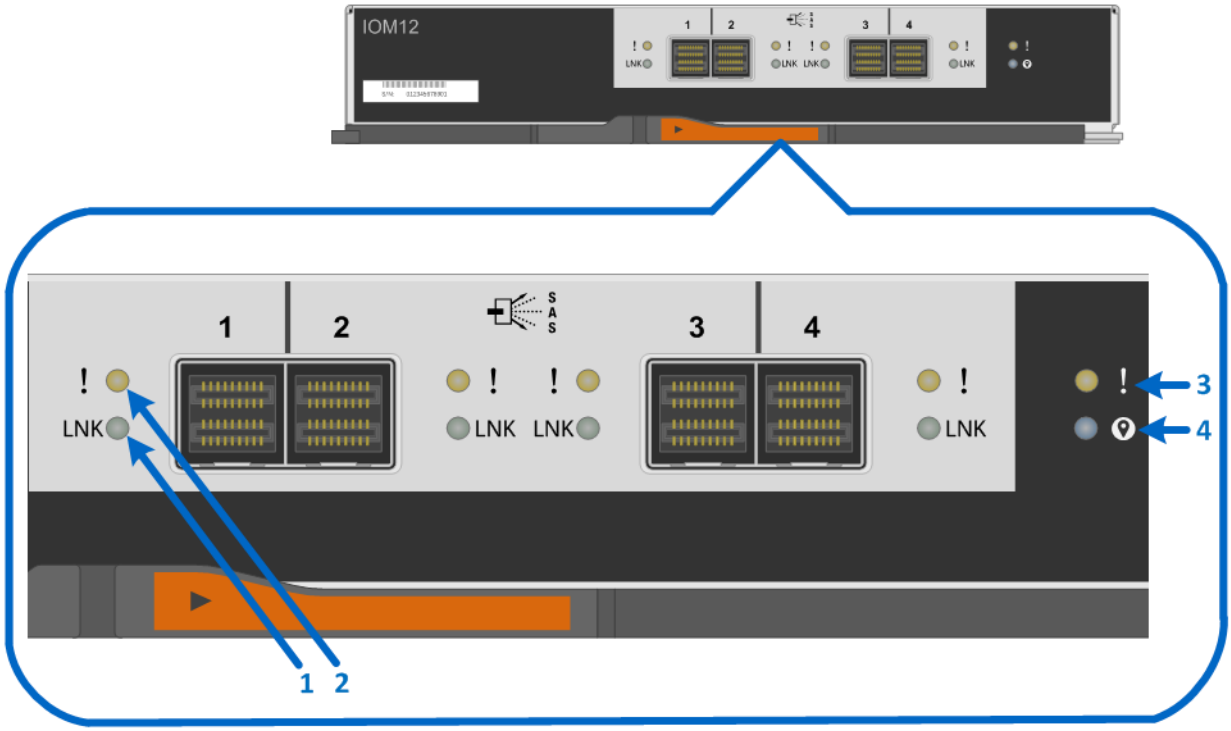
© 2018 NetApp, Inc. All rights reserved.

Figure 61) DE460C rear view.

IOM LED Definitions

Figure 62 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 similar LEDs.

Figure 62) LEDs for IOM.



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

Table 26 defines the LEDs for the IOM.

© 2018 NetApp, Inc. All rights reserved.

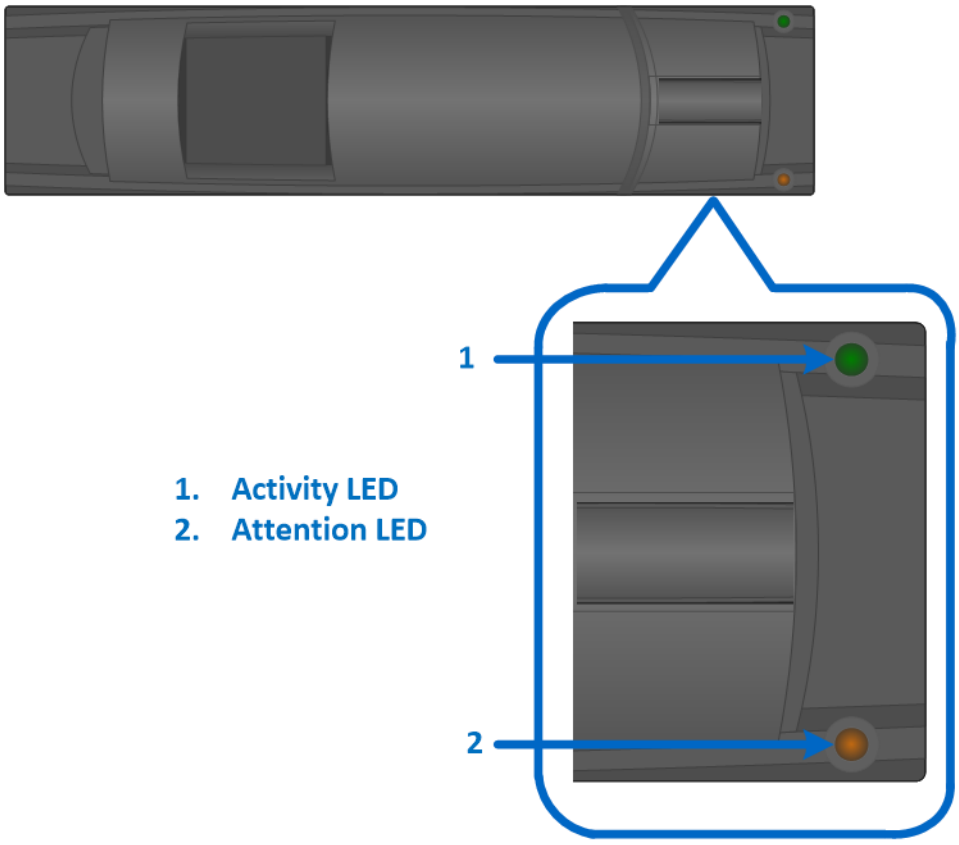
Table 26) IOM LED definitions.

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

Drive LED Definitions

Figure 63 and Figure 64 show the LEDs on the drive carriers for the E2812 and E2824, respectively.

Figure 63) E2812 drive carrier LEDs.



© 2018 NetApp, Inc. All rights reserved.

Figure 64) E2824 drive carrier LEDs.

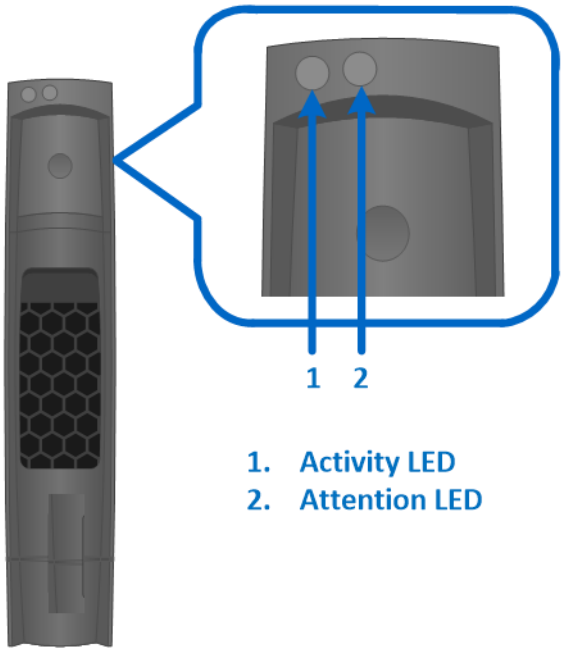


Table 27 defines the LEDs for the drives.

Table 27) E2812 and E2824 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.
Attention	Blinking amber	Drive locate turned on.	Normal status.

For the DE460C shelf, the drive activity and attention LEDs are displayed by the drawer, as shown in Figure 65. It has an attention LED, as shown in Figure 66, that is displayed when the drawer is open. The drawer and shelf also have attention LEDs to indicate the location of the drive, as shown in Figure 65. Note that the drive activity LED is not illuminated for a failed drive.

© 2018 NetApp, Inc. All rights reserved.

Figure 65) E2860 shelf and drawer attention LEDs.

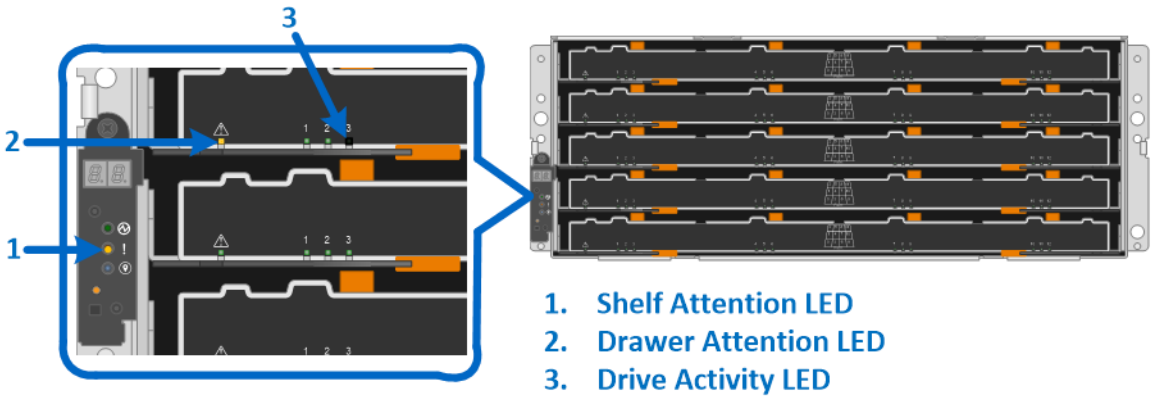


Figure 66) E2860 drive attention LED.

Table 28 defines the LEDs for the drives, drawers, and shelf of the E2860.

Table 28) E2860 drive LED definitions.

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

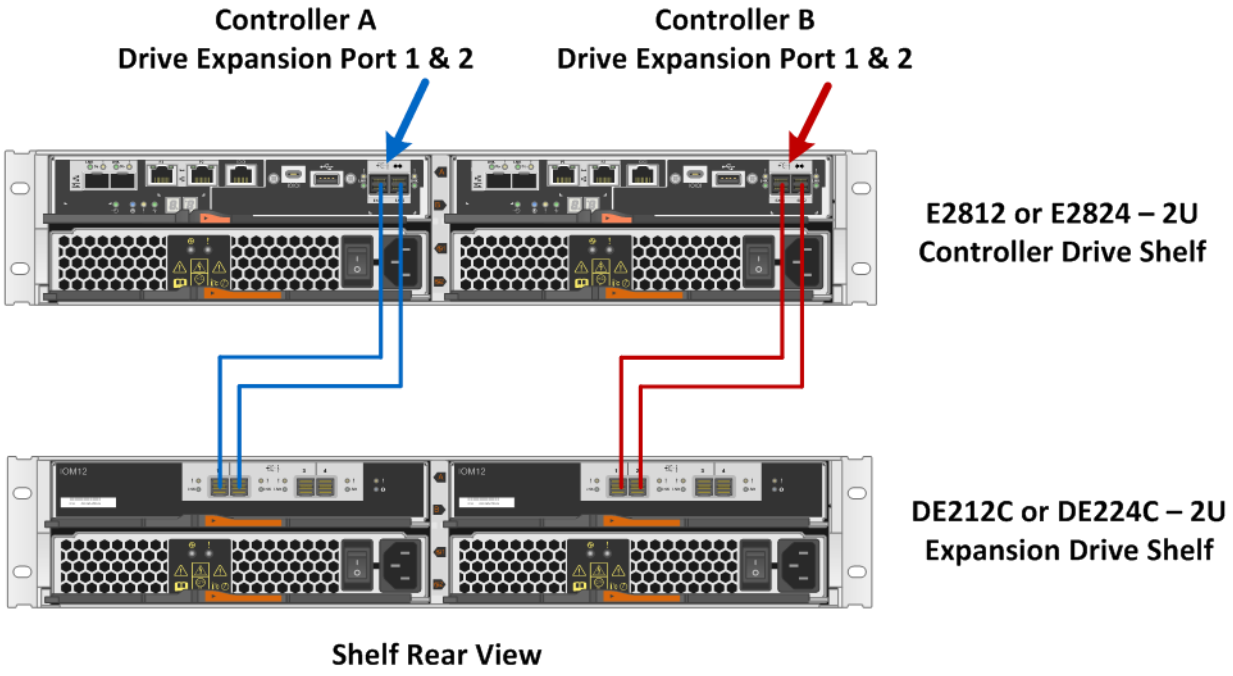
© 2018 NetApp, Inc. All rights reserved.

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

7.2 Greenfield Installation

E2800 storage systems use two cabling methods: single stack and dual stack. The single-stack method is used only when the storage system has a controller shelf and a single drive shelf, as shown in Figure 67.

Figure 67) E2800 single-stack system configuration.

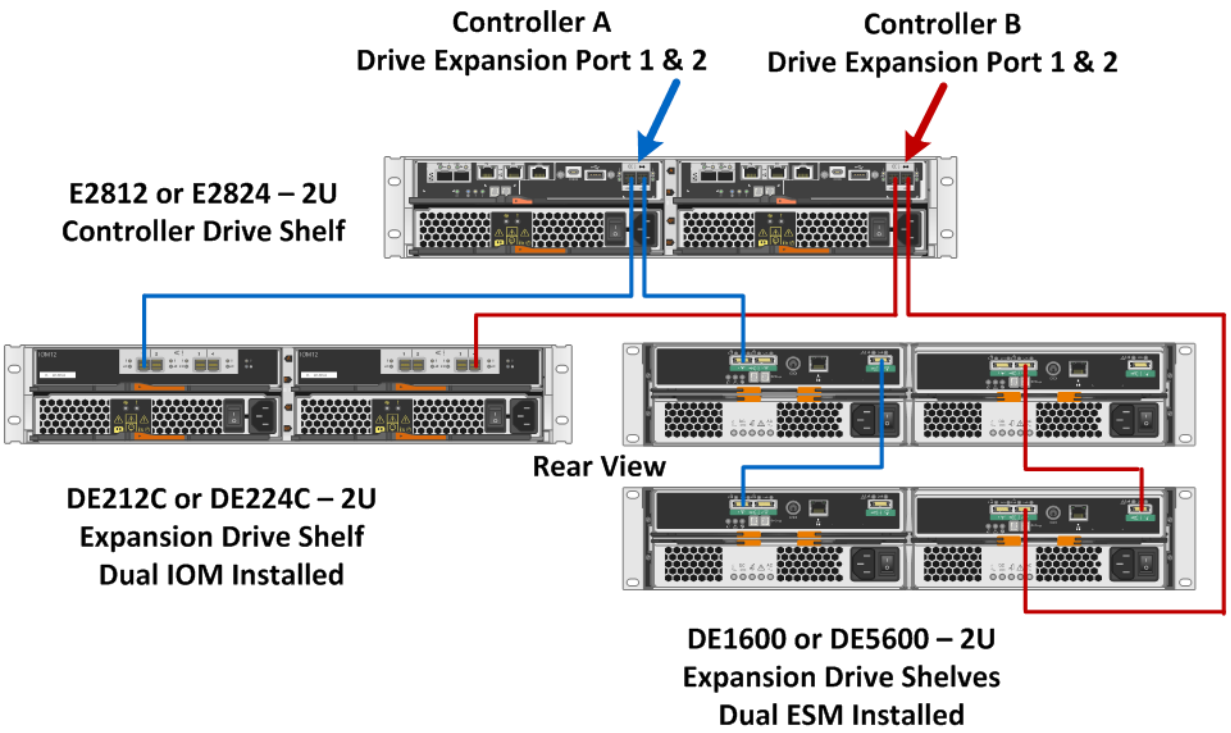


For E2800 storage systems with two or more drive shelves or a mix of SAS 3 and SAS 2 drive shelves, use the dual-stack cabling method, as shown in Figure 68.

Note: For optimal performance, SAS 2 and SAS 3 drive shelves should be isolated into different stacks.

© 2018 NetApp, Inc. All rights reserved.

Figure 68) E2800 storage system dual-stack configuration with SAS 3 and SAS 2 shelves.



For simplex controller systems, use the same cabling methods shown in Figure 67 and Figure 68 (blue paths) for the A-side controller as appropriate based on whether the system has just 12Gb drive shelves versus 12Gb shelves and 6Gb shelves connected to the same E2800 controller shelf.

Note: Only use dual-stack cabling if you have a mix of 12Gb and 6Gb expansion drive shelves. Otherwise, use the single-stack cabling method when all expansion drive shelves are new generation 12Gb 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.

7.3 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

© 2018 NetApp, Inc. All rights reserved.

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.

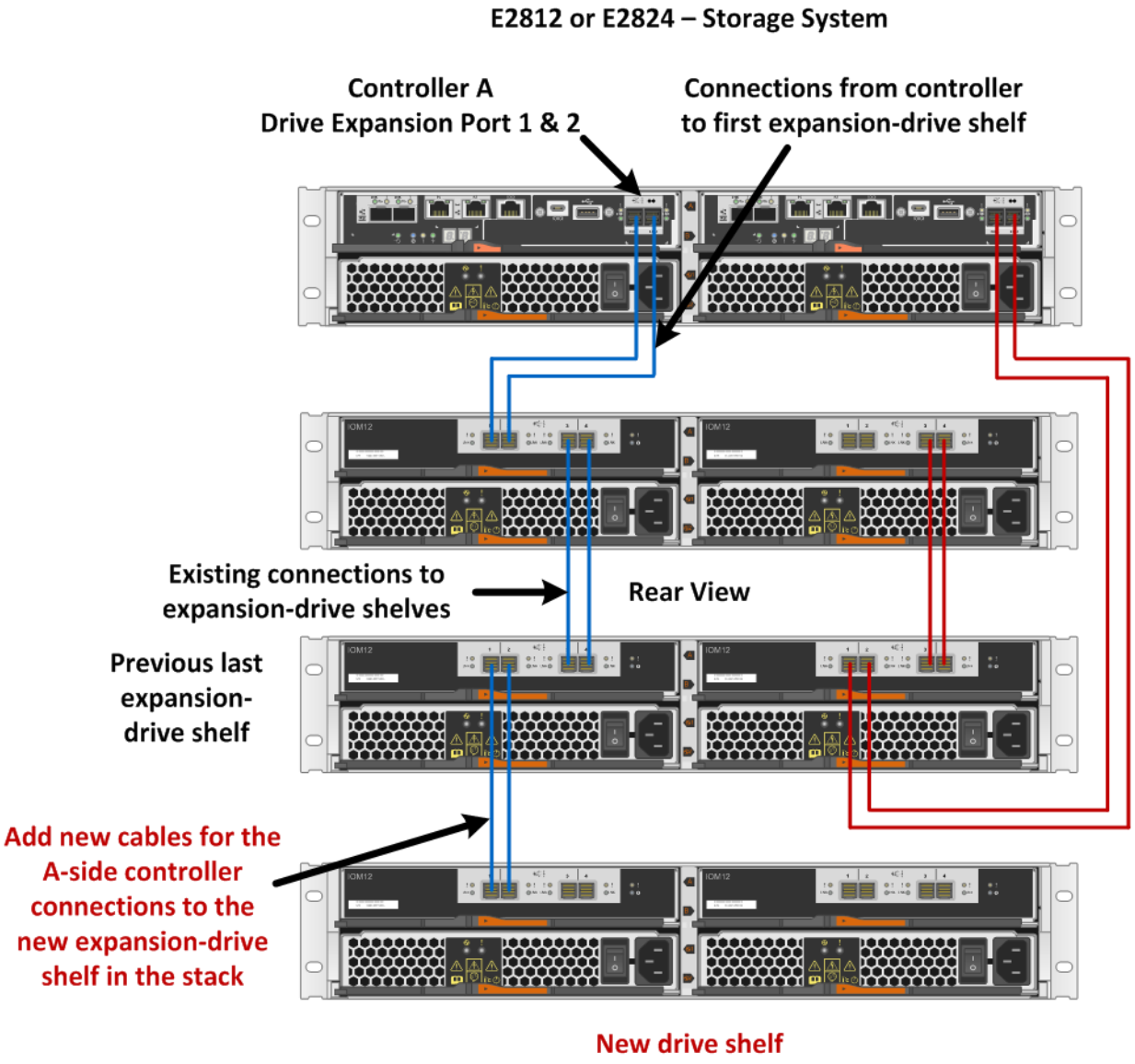
After additional drive shelves have been successfully added to a storage system, SANtricity can be used to add capacity to existing volume groups and disk pools or to create new volume groups and disk pools.

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.

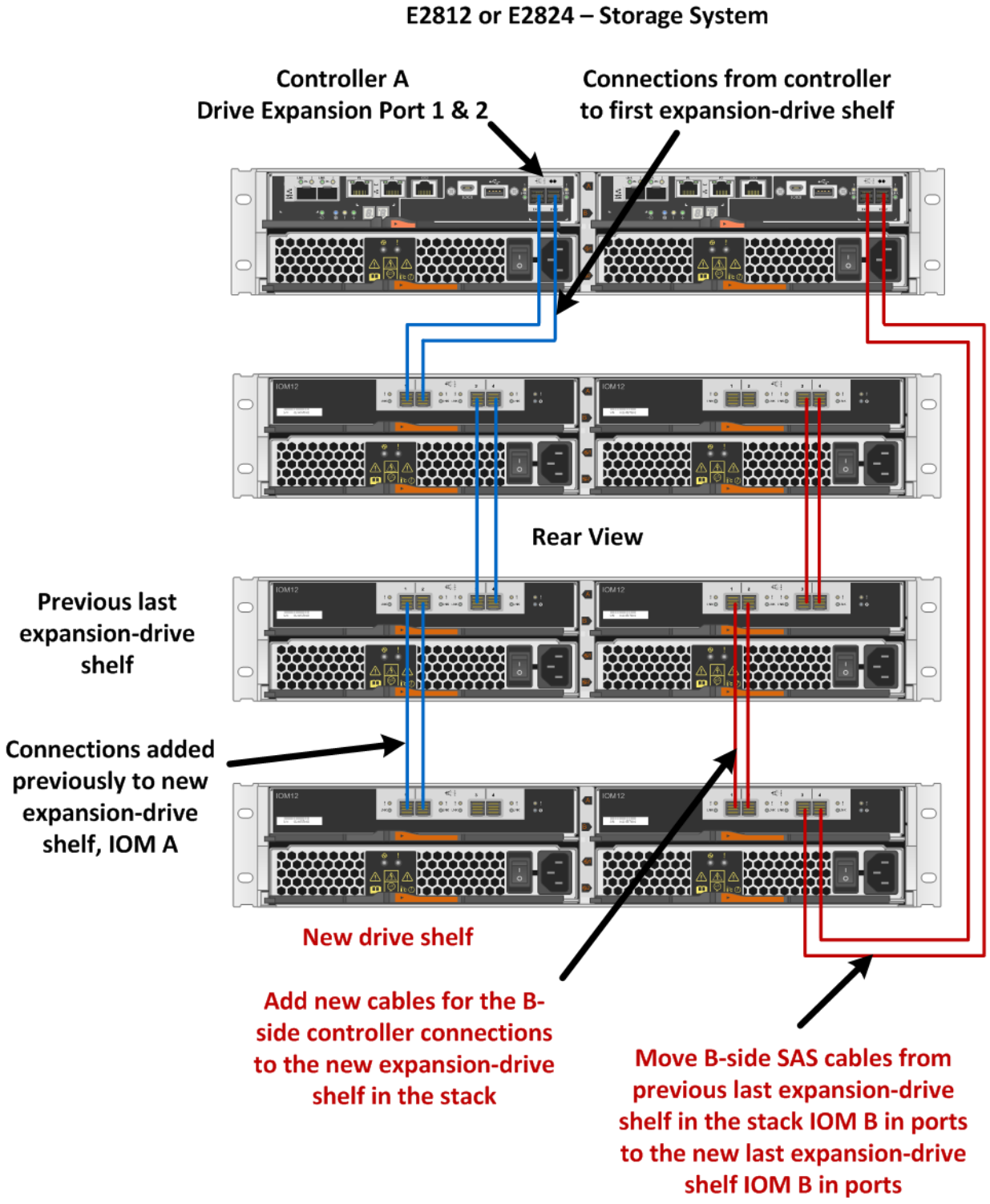
Figure 69 and Figure 70 show the hot-add connectivity when a drive shelf is added as the last shelf in the system. The E2812 and E2824 are shown; the E2860 cabling is similar.

Figure 69) Drive shelf hot-add A-side cabling.



© 2018 NetApp, Inc. All rights reserved.

Figure 70) Drive shelf hot-add B-side cabling.



© 2018 NetApp, Inc. All rights reserved.

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 the SAS expansion paths for controller A and controller B.

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 E2812 and E2824 storage systems are shipped preconfigured from the factory (controllers have HICs and batteries installed, and controllers are installed in the controller shelf). The chassis serial number is printed on a white label affixed to the controller shelf behind the right end cap on the front of the chassis. The SN is identified by the text “SN,” which is shown in Figure 71.

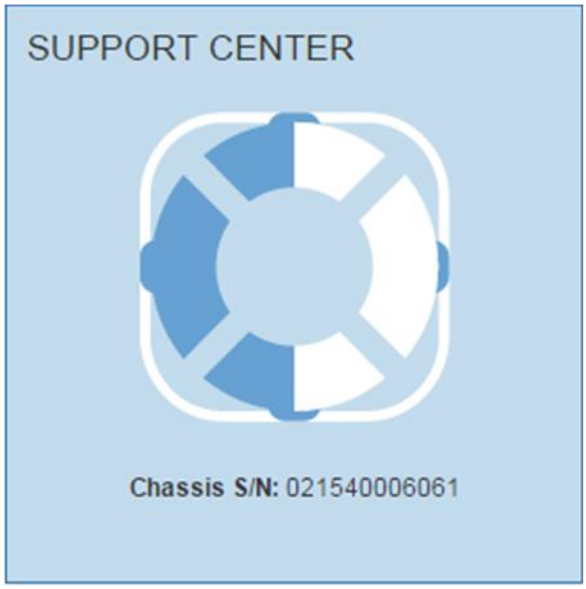
Figure 71) Controller shelf SN.

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 .

© 2018 NetApp, Inc. All rights reserved.

Figure 72) 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).

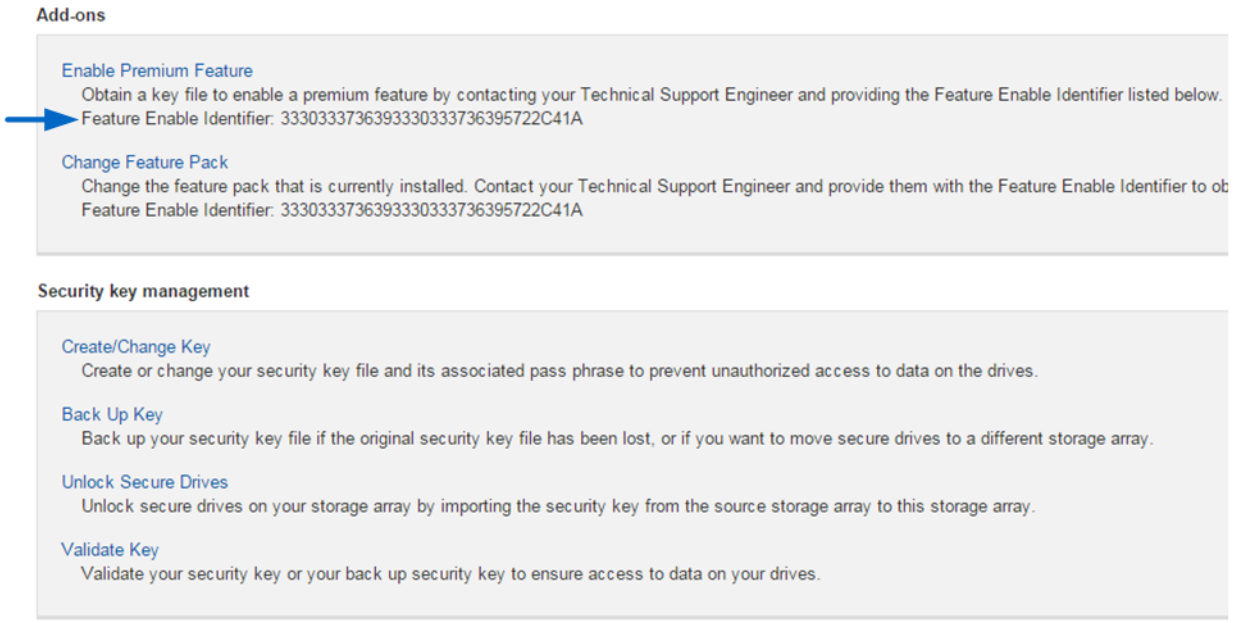
For the E2800, all features are enabled out of the box. The only exception is for drive security. For restricted countries, this feature is not enabled.

Premium Feature Keys

To illustrate activating a premium feature, we demonstrate activating drive security. Assume a license key file is required to activate the functionality. License keys for premium features are system specific and can be purchased by sending a request to a sales representative. The request must include the feature enable identifier that is found under the Settings tab, System tile, Add-ons section of the System Manager, shown in Figure . The request must also include the chassis serial number: the serial number of the E-Series controller shelf, as shown in Figure .

© 2018 NetApp, Inc. All rights reserved.

Figure 73) SANtricity OS 11.30 Enable Premium Features feature enable identifier.



When the license key for the drive security feature has been purchased and the order has been processed in the NetApp order system, the key file can be generated by using the NetApp Storage Array Premium Feature Activation tool. The tool requires two types of information to generate license key files: the key activation code and the feature enable identifier.

The 11-digit key activation code is system generated for purchased licenses and is attained by logging in to NetApp Support and viewing the system details under My Support > Software Licenses. The storage system controller shelf chassis serial number should be used to access the specific system details and key codes.

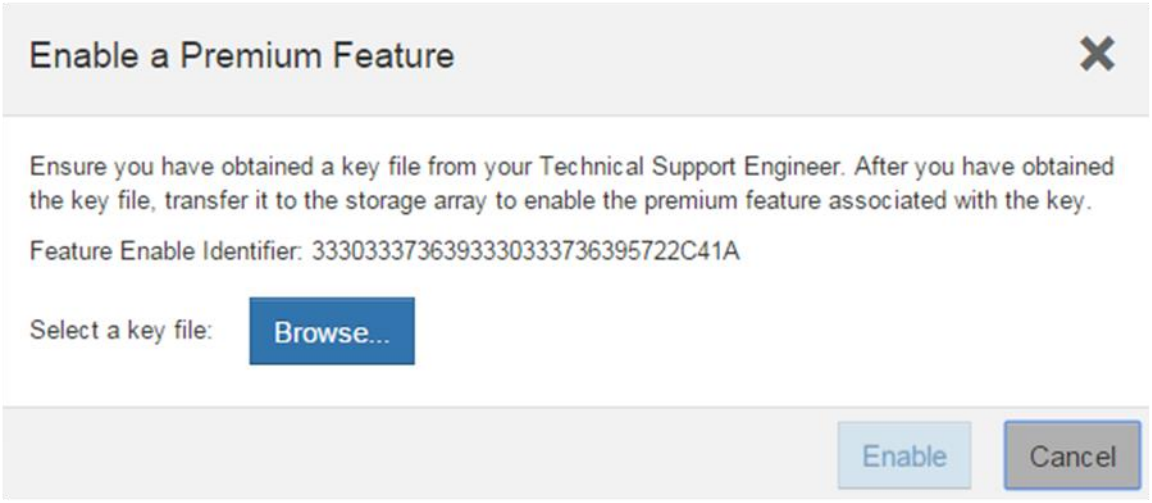
Customers must have a valid Support site account login and password to access, generate, and download the license key file.

Note: First-time users who apply for a new Support site account have access to their system details and to the license key site delayed for up to five business days while the registration information is validated and the user account is created. For this reason, NetApp recommends that customers create their Support site accounts as soon as their purchase order has been received by NetApp.

After the key file has been downloaded to the host server, click Enable Premium Feature, as shown in Figure 73, and then follow the prompts, beginning with browsing to the key file, as shown in Figure 74Figure .

© 2018 NetApp, Inc. All rights reserved.

Figure 74) Enable a premium feature.

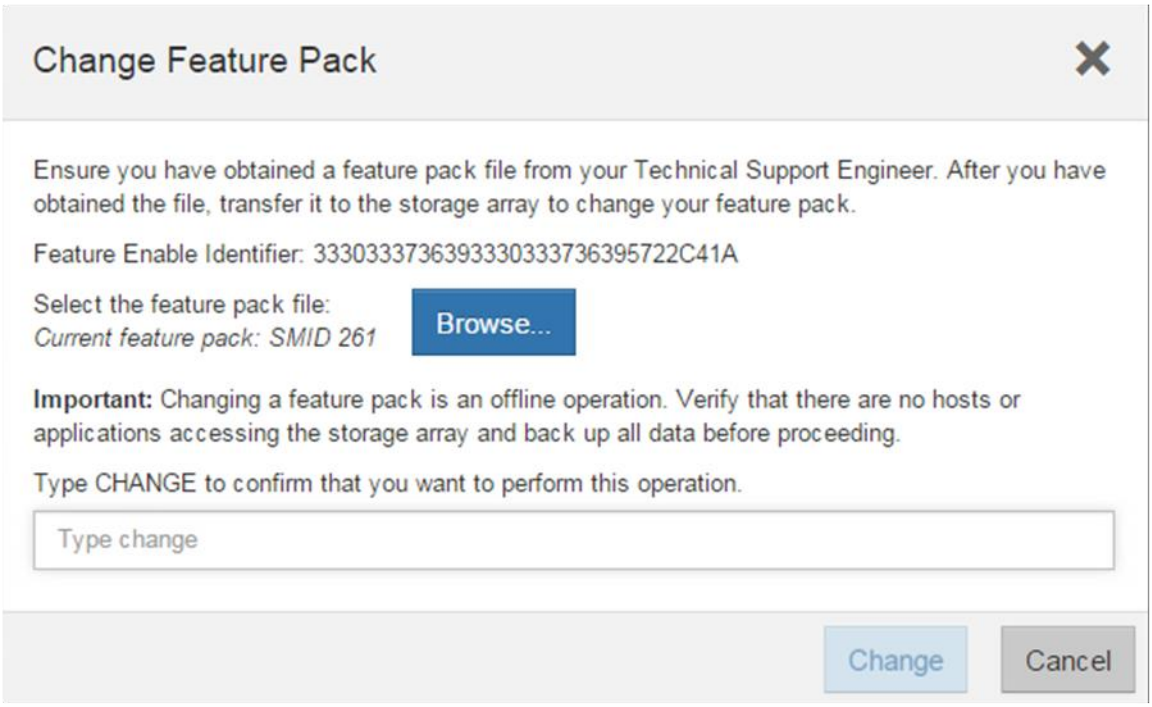


Feature Pack Keys

When E2800 controllers are equipped with either the two-port optical baseboard or the two-/four-port optical HIC, feature pack keys are used to change the host interface protocol from FC to iSCSI or from iSCSI to FC. The process to generate a new feature pack key for your storage array is the same as the process to generate a premium feature key, except 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, click Change Feature Pack, as shown in Figure , and then follow the prompts, beginning with browsing to the feature pack file, as shown in Figure .

Figure 75) Change feature pack.



© 2018 NetApp, Inc. All rights reserved.

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 E-Series E2800 storage system allows customers to cut operational costs with ultradense drive shelves for capacity-hungry applications while improving storage utilization with the intuitive, easy-to-learn SANtricity System Manager web-based GUI.

E2800 storage systems offer balanced throughput performance for backup, video, and analytical environments and other sequential workloads, but they also support demanding IOPS workloads in small and medium enterprise data centers. The wide choice of drive speeds, capacities, and storage features combined with multiple host connectivity interface options makes the E2800-based storage system the perfect choice for environments where simplicity, seamless integration with wide-ranging workloads, and a streamlined price/performance product focus are the key elements to customer success.

Add on the new SANtricity OS 11.40 security features (LDAP, RBAC, MFA, Secure CLI, and external encryption key management), support for high-capacity 15.3TB SSDs, and the flexibility to run more than one host protocol at a time, and the E2800 becomes a clear fit for dedicated workloads in any size enterprise.

Appendix

System Manager Tables

System Manager includes many of the same array-based tasks for the E2800 series 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 29 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 29) Storage array options: AMW compared to 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.

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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
	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

© 2018 NetApp, Inc. All rights reserved.

Disk Pool Options

Table 30 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 30) Disk pool options: AMW compared to 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
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

© 2018 NetApp, Inc. All rights reserved.

Volume Group Options

Table 31 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 31) Volume group options: AMW compared to 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
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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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 32 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 32) Volume options: AMW compared to 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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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
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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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

SSD Cache Options

Table 33 details how functions performed on the SSD cache are completed in the SANtricity Storage Manager AMW and how the same functions are completed employing the SANtricity System Manager.

Table 33) SSD read cache options: AMW compared to System Manager.

Function	AMW	System Manager		
	Storage > SSD Cache > Option	Page	Tile/Tab	Option
Create SSD cache	Create	Storage	Pools & Volume Groups > All Capacity tab	Create > SSD Cache
Add capacity	Add Drives (Capacity)			Add Capacity
Remove drives	Remove Drives (Capacity)			More > Remove capacity
Suspend or resume	Suspend/Resume			More > Suspend/Resume SSD Cache
View statistics	View Statistics link (in right side properties)			More > View SSD Cache Statistics
Rename	Rename			• View/Edit Settings • Edit directly in the table view by selecting the pencil icon in the Edit column
Delete	Delete			Uncommon Tasks > Delete
Locating SSD cache	Locate			More > Turn on locator lights
View associated physical components	View Associated Physical Components	Hardware	N/A	Use filter control in top area
Run performance modeling	Run Performance Modeling	CLI/script editor only		

© 2018 NetApp, Inc. All rights reserved.

Copy Services Options

Snapshot Group

Table 34 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 34) Snapshot group options: AMW compared to 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 as a result 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 35 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.

© 2018 NetApp, Inc. All rights reserved.

Table 35) Snapshot image options: AMW compared to 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 36 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.

© 2018 NetApp, Inc. All rights reserved.

Table 36) Snapshot volume options: AMW compared to 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
Recreate 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
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		

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager
Modify overall repository	Overall Repository > Change > Modification Priority > Media Scan Settings > Pre-Read Redundancy Check	CLI/script editor only: These are normally not changed by the end user. The defaults should suffice.

Volume Copy

Table 37 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 37) Volume copy options: AMW compared to 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 38 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 38) Asynchronous mirroring options: AMW compared to 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.		
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.		

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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
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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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: These are normally not changed by the end user. The defaults should suffice.		

Synchronous Mirroring

Table 39 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 39) Synchronous mirroring options: AMW compared to 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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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 40 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 40) Host mapping options: AMW compared to 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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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
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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
View or edit host properties	Host > Properties			View/Edit Settings **Note:** Can also view/edit settings for a host cluster.

Hardware Options

Table 41 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 41) Hardware options: AMW compared to 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 tray (shelf)	Locate (controller/drive tray, drive tray)	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 tray (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
View or edit drive channels	Tray > View/Edit Drive Channels			Select one of the controllers and then select View settings > Drive Interfaces tab
Change tray (shelf) ID	Tray > Change > ID			Select Shelf Number drop-down menu on left side of each shelf and then select Change ID
Change tray (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 tray (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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
Change tray (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, 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.		
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

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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 42 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 42) Health monitoring options: AMW compared to 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		

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	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		
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 43 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 43) Report-monitoring options: AMW compared to 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		

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager		
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 44 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 44) Upgrade options: AMW compared to 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 earlier). Can also use the CLI/script editor to upgrade IOM (ESM) firmware individually.

© 2018 NetApp, Inc. All rights reserved.

Function	AMW	System Manager
Upgrade tray (shelf) configuration settings	Upgrade Tray Configuration Settings	CLI/script editor only

Alert Options (EMW)

Table 45 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 45) Alert options: EMW compared to System Manager.

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

© 2018 NetApp, Inc. All rights reserved.

References

The following references were used in this TR:

- E-Series E2800 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	September 2017	Initial release concurrent with SANtricity 11.40
Version 2.0	May 2018	Updates for SANtricity OS 11.40.1 and SANtricity OS 11.40.2

© 2018 NetApp, Inc. All rights reserved.

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

Copyright Information

Copyright © 2017–2018 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark Information

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

TR-4631-0518