Abstract
NetApp® E-Series and EF-Series arrays provide a secure, role-based access controlled, and auditable management interface for multiple users through a collection of management security features that were introduced in NetApp SANtricity® OS 11.40 and enhanced in later SANtricity OS releases. This report provides detailed information about these new SANtricity System Manager and SANtricity Storage Manager security features for NetApp E-Series E2800, E5700, EF280, and EF570 storage arrays.
LIST OF FIGURES

Figure 1) NetApp E-Series management security feature, integrating directory server and RBAC. .........................5
Figure 2) Technical components of the NetApp E-Series management security feature. ..........................................6
Figure 3) Set admin local password on initial power-up. .........................................................................................6
Figure 4) SANtricity Unified Manager local account password management. ........................................................8
Figure 5) SANtricity System Manager access management (local user roles) settings. ............................................8
Figure 6) SANtricity System Manager directory server configuration settings ....................................................10
Figure 7) SANtricity System Manager directory server role mapping settings .....................................................10
Figure 8) Technical components of secure SMcli operating against a storage array. ...........................................11
Figure 9) Navigation to change the management interface security mode ..........................................................12
Figure 10) Change the management interface mode by using the SANtricity System Manager GUI. ......................12
Figure 11) SANtricity System Manager page to view the audit log ......................................................................15
Figure 12) SANtricity System Manager dialog box to export the audit log ............................................................16
Figure 13) SANtricity System Manager page to configure the audit log settings ................................................16
Figure 14) EMW with the Web Services Certificate Management feature ........................................................19
Figure 15) Completed CSR form to request a signed certificate. .................................................................19
Figure 16) EMW navigation to import root/intermediate certificates and server certificates ............................20
Figure 17) Import Root/Intermediate CA Certificates dialog box ......................................................................21
Figure 18) Import a signed CA-generated server certificate dialog box .............................................................21
Figure 19) EMW with the Array Certificate Management feature ........................................................................24
Figure 20) Dialog box to import the storage array’s CA root/intermediate certificate .......................................25
Figure 21) Automatically generated controller untrusted certificates ..............................................................26
Figure 22) Dialog box to temporarily or permanently trust the self-signed controller certificate ........................26
Figure 23) Options when there is no trusted certificate for the requested active operation ................................27
Figure 24) Communications between management clients and Web Services proxy installed on a server ..........28
Figure 25) The Web Services proxy security certificate is not working and the connection is not secure ..........34
Figure 26) SANtricity System Manager navigation to manage certificates. .........................................................55
Figure 27) Dialog box in which the user can accept the self-signed certificate .................................................56
Figure 28) Default controller certificate status after the alternate controller self-signed certificate is accepted ....56
Figure 29) Option to upload the LDAP server’s CA root certificate to the array truststore ..............................62
Figure 30) Option in SANtricity System Manager to complete a CSR, and to import the storage array’s signed client certificate and KMIP server’s SSL certificate .................................................................63
Figure 31) How SAML integrates into E-Series products ....................................................................................64
Figure 32) Overview of login request using SAML .............................................................................................65
Figure 33) Overview of IdP-initiated logout using SAML ..................................................................................65
Figure 34) The SAML tab in SANtricity System Manager when no configuration is present ............................66
Figure 35) Common ways to configure roles in SANtricity System Manager ....................................................67
1 SANtricity Security Features

The NetApp SANtricity OS software for the latest NetApp E-Series and EF-Series arrays (E2800, E5700, EF280, EF570) supports secure, web-based storage management for individual arrays. In addition to this array-level management security, NetApp has now released enterprise-level secure management in SANtricity Unified Manager and SANtricity Web Services Proxy (WSP) 3.0, enabling secure, centralized management of hundreds of arrays.

By using the embedded Web Services management infrastructure or the new SANtricity Unified Manager and SANtricity WSP 3.0 (or later versions), administrators can manage storage arrays from a networked browser client with IP access to E-Series controller management ports and the WSP web server. Because web-based storage management exposes the managed devices to private and public networks, E-Series and EF-Series arrays and SANtricity WSP 3.0 and later releases support appropriate security schemes at various levels, including the transport layer protocol, access methods, and access control, incorporating authentication and authorization aspects.

SANtricity OS 11.40 introduced the concept of multiuser management to securely perform storage setup and management functions on individual arrays by using the SANtricity System Manager GUI, the secure CLI (secure SMcli), and API access methods. SANtricity WSP 3.0 and SANtricity Unified Manager provide this same level of security.

Note: SANtricity Unified Manager does not currently support SMcli or the individual array script editor. To use these features, you must still install the latest version of SANtricity Storage Manager management station software on a local server with IP access to the storage arrays just like you do for legacy E-Series array models today.

Users who intend to perform storage or system management functions are authenticated first, either locally or with a directory server using Lightweight Directory Access Protocol (LDAP). Upon successful authentication, they can perform management tasks according to their assigned role (role-based access control [RBAC]). When using LDAP, a user’s role is based on the user’s group settings in the directory server. For local users, access roles are hardcoded as part of the management access authorization workflow, and passwords are managed by the admin user.

Security is further enhanced by using SANtricity System Manager and SANtricity WSP 3.0 and Unified Manager by requiring administrators to set up certificates of trust (web server and CA root or intermediate certificates) between the multiple client-server relationships supported by the arrays and WSP:

- SANtricity Storage Manager Enterprise Management Window (EMW)
- SANtricity WSP 3.0 and SANtricity Unified Manager
- LDAPS servers
- Key Management Interoperability Protocol (KMIP) compliant external encryption key manager servers
- New E-Series and EF-Series arrays managed by either method such that user credentials (user ID and password) for active operations are always transferred to a trusted entity using a secure connection, directly to a browser or through another method listed

By streaming the built-in audit log to a log server, you can track events on the array and adjust the level of logging to meet your requirements.

Finally, when using SANtricity OS 11.40.2 or later, you can use multifactor authentication with Security Assertion Markup Language (SAML) 2.0 to secure the management interface for individual arrays. SANtricity WSP and SANtricity Unified Manager do not support SAML and cannot discover and manage arrays by using SAML. If you use multifactor authentication instead of directory services, only the SANtricity System Manager GUI can be used to manage the storage array. All other management interfaces are disabled, including all API access.

These management security features are available beginning in SANtricity OS 11.40 on the E2800, E5700, EF280, and EF570 systems. The enhanced security features are not available on systems that
use SANtricity Storage Manager Array Management Window (AMW), the desktop thick client, to manage the arrays.

2 RBAC and Directory Services

To support multiple users with varying privilege levels, SANtricity OS 11.40 introduced embedded directory services integration and RBAC on the E2800, E5700, EF280, and EF570 storage systems (now extended to SANtricity WSP 3.0 and SANtricity Unified Manager). The implementation applies to the SANtricity System Manager GUI, the EMW for secure SMcli, and the WSP API.

The RBAC scheme associates a specific set of permissions to perform system management tasks with system-defined roles. Users who are expected to perform these tasks are mapped to appropriate system-defined roles. When a user is authenticated, the associated authorization is applied, allowing that user to have specific permissions with their access to the management application or API.

Users are defined by using the built-in roles; or they can be members of a directory server that uses LDAP, such as 389 Directory Server for Linux or Windows Active Directory (AD).

**Note:** For user roles on the local system, there is a fixed set of user accounts and associated roles that cannot be changed.

The new management security feature also includes a configuration option to toggle between the legacy SYMbol API interface and the new HTTPS API interface. (SYMbol is an Open Network Computing RPC interface for managing NetApp E-Series storage systems.) Disabling the SYMbol interface blocks access to an array that uses nonsecure access methods. When the security feature is activated, the Web Services API that is using HTTPS acts as the underlying infrastructure element to provide seamless system configuration options by using directory services and RBAC.

The array audit log captures user activity on the storage array through the System Manager GUI, SMcli, Web Services API, and support shell.

**Note:** Activity through the traditional SYMbol access method is not captured in the audit log. (SYMbol is an Open Network Computing RPC interface for managing legacy NetApp E-Series storage systems.)

Figure 1 shows the logical connection relationship between E-Series arrays, management clients, and directory servers.

**Figure 1)** NetApp E-Series management security feature, integrating directory server and RBAC.

![Figure 1](https://via.placeholder.com/150)

Figure 2 shows the logical breakout of authentication workflows in the E-Series controllers.
2.1 Local User Passwords

When the storage array is installed, and the user opens the SANtricity System Manager GUI for the first time, the user is prompted to set the local administrator password. For simplicity, the Username field defaults to Admin, but the user must enter and validate a password, as shown in Figure 3. SANtricity System Manager also sets the SYMbol API password to the same password used for the admin account. If there is an upgrade from SANtricity OS 11.30, the local administrator user account inherits the existing SYMbol password and the user is not prompted to set another password.

For SANtricity WSP 3.0 and SANtricity Unified Manager, the administrator account is set for a factory default password (user = admin / password = admin). When an administrator logs in for the first time, the admin password can be changed.
The admin user can set a password for each of the local users. Figure 4 shows the screen shot from SANtricity Unified Manager where passwords are set. Figure 5 shows the same view from SANtricity System Manager. If the passwords for the other local user accounts are not configured, a user attempting to log in to those local user accounts is denied access. If there are no plans to use the other local user accounts, the storage array can function without the other user account passwords being set.

**Note:** The admin user is the only user with the root admin role who has permission to set or change any local user’s password.

### 2.2 Built-In Roles and Local User Accounts

The new security model enforces the implementation of RBAC. This means that all users are assigned a set of permissions that define what they are authorized to do with respect to the managed array’s setup and administration functions. In other words, users are preassigned to one or more of the system-defined roles that give them access to the set of allowed operations mandated by the given roles. The role object is defined to incorporate commonly used LDAP attributes to easily derive this information from LDAP-accessible user and group directories.

The following roles are implemented in this feature:

- **Monitor.** This role gives read-only access to all storage array properties. This user cannot view the security configuration.
  
  **Note:** All users must have the monitor role to log in to a storage array. Other roles define what users can do after they are authenticated.

- **Root admin.** This is the only role that allows the user to change the passwords of any local users and run any command supported by the array. Combined with the monitor role, the root admin role allows access to all functions on the array.
  
  **Note:** The root admin user name is “admin” rather than “root.” The other user names are security, storage, support, and monitor.

- **Security admin.** This role allows the user to modify the security configuration on the array, including the ability to view audit logs, configure a secure syslog server, set LDAP/LDAPS server connections, and manage certificates. This role does not provide write access to storage array properties like pool and volume creation/deletion, but it does have read access. It also has privileges to enable/disable SYMbol access to the array.

- **Storage admin.** This role has full read/write access to the storage array properties, but with no access to perform any security configuration functions.

- **Support admin.** This role has access to all hardware resources on the array, failure data, MEL/audit log, and CFW upgrades.

- **rw.** This is a legacy WSP account with read/write permissions. It is not supported on new-generation storage arrays

- **ro.** This is a legacy WSP account with read-only permissions. It is not supported on new-generation storage arrays

Figure 4 and Figure 5 show the new user accounts and mapped roles in the SANtricity Unified Manager and SANtricity System Manager GUIs introduced with SANtricity OS 11.40 and WSP 3.0. To view the individual user accounts in SANtricity Unified Manager, navigate directly to the Access Management tab. To see the accounts for individual arrays by using SANtricity System Manager, navigate to Settings, open the Access Management tile, and click the Local User Roles tab.
Local or directory users with privileges to access certain storage management functionality based on their role assignment can perform the allowed set of operations through their choice of user interface (System Manager GUI, secure SMcli, or REST API).

The minimum set of privileges required for a user to manage the array is mapped to the monitor role. All users who need to manage an array must have at least the monitor role assigned to them. When assigning roles for specific groups in a directory server, the monitor role is assigned automatically. Other permission levels can be added by the admin or security user.

This feature supports the defined set of local user accounts. Administrators cannot add new local user accounts to the array beyond the predefined accounts, and the predefined local user accounts cannot be changed.

### 2.3 LDAP User and Group Account Mapping

LDAP is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. A common use of LDAP is to provide a
central place to store user names and passwords, allowing many different applications and services to connect to the LDAP server to validate users. For more information about LDAP, refer to the LDAP Wikipedia topic.

For SANtricity OS to validate users through LDAP, it must be configured to authenticate with the Microsoft AD, Linux 389, or some other directory server. The configuration scheme allows multiple instances of directory server configurations to support multiple LDAP domains. Each LDAP domain has a name that is presumed to match the DNS domain for the LDAP server, but it is not required. See section 5.3, Certificate Management for SANtricity System Manager Controller, to set up certificates for LDAP with Secure Sockets Layer (SSL) [LDAPS].

Domains can be named anything if they are valid DNS names that contain only ASCII letters. In addition to the domain name, Table 1 shows attributes that are supported as part of the directory server configuration.

Table 1) LDAP configuration parameters.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name</td>
<td>Valid DNS names that contain only the ASCII letters a through z (not case sensitive), the digits 0 through 9, and the hyphen (-), but cannot start with a hyphen. Per RFCs 3629 and 4514, conversion of string representation associated with distinguished name from ASN.1 to UTF-8 encoded Unicode representation is allowed.</td>
</tr>
<tr>
<td>LDAP URL</td>
<td>The URL to access the LDAP server in the form of ldap[s]://host:port.</td>
</tr>
<tr>
<td>User bind attribute (filter base)</td>
<td>The attribute to which the user ID is bound to authenticate the user in the form of attribute=%s, where %s is replaced by the user name. This allows a large amount of flexibility.</td>
</tr>
<tr>
<td>Search base</td>
<td>The LDAP context to search for users. Usually in the form of: CN=Users, DC=cpoc, DC=local.</td>
</tr>
<tr>
<td>Group attribute</td>
<td>A list of group attributes on the user that is searched for group-to-role mapping.</td>
</tr>
<tr>
<td>Group to role mapping</td>
<td>A list of regular expression patterns to match to the user's group attributes to match to roles.</td>
</tr>
<tr>
<td>Bind account user ID</td>
<td>Requires a read-only user account for search queries against the LDAP server and/or for searching within the scope of groups.</td>
</tr>
<tr>
<td>Bind account password</td>
<td>The password associated with the read-only account for search queries against the LDAP server and/or for searching within the scope of groups.</td>
</tr>
</tbody>
</table>

Figure 6 shows the directory server setup wizard, and Figure 7 shows the Role Mapping tab, where users and groups defined in the directory service server are assigned access privileges on the array.

Note: SANtricity System Manager screenshots are shown in the figures, but the SANtricity Unified Manager uses the same setup wizard for directory servers.
Figure 6) SANtricity System Manager directory server configuration settings.

Figure 7) SANtricity System Manager directory server role mapping settings.
When a directory user attempts to log in, the user ID and the domain provided by the user are the criteria that determine the search scope.

The format of the user ID is expected to be one of the following:

- **Standard email address pattern**: user@domainname
- **Domain name\user**, where domain name is the name associated with the domain in the LDAP configuration
- **Local**

The format is required to distinctly identify which user base to use for validating a given user and to determine which domain to use for forwarding the authentication request. Groups within the directory server must be created, and user names must be placed in them.

**Note:** Auto searching for user names in the directory is not supported.

The domain name local is reserved to reference the local user account database. If no directory services are configured, the user ID is checked against the local user account database. When directory services are configured, the user ID of form user@local initiates validation against the local user account database.

### 3 Secure SMcli

The secure SMcli allows an SMcli client to interact with a storage array through a secure HTTPS channel. It provides a thin HTTPS client that allows customers to interoperate with storage arrays by using traditional SMcli grammar and command semantics, but with a secure protocol.

**Note:** SMcli is supported with SANtricity Storage Manager EMW, but not with WSP or Unified Manager.

Instead of the client providing parsing logic and executing commands against an array, the secure SMcli provides a lightweight wrapper that interacts with the storage array where most of the command processing takes place.

#### 3.1 Secure SMcli Logical Architecture

When the secure SMcli interacts directly with the E2800, E5700, EF280, or EF570 array, it can communicate with the storage array by using the legacy SYMbol interface or the HTTPS protocol, depending on how the array interface is set. Figure 8 shows the logical connectivity from an SMcli host to an E-Series array that is managed by SANtricity System Manager.

**Figure 8**) Technical components of secure SMcli operating against a storage array.
**Note:** By default, E2800, E5700, EF280, and EF570 arrays all have the legacy SYMbol interface active from the factory. To change the array to a secure interface, you must install the appropriate CA root, intermediate, and signed server certificates on both storage array controllers. Also, the array management interface must be changed to the secure mode by using the SANtricity System Manager GUI. The GUI navigation is Settings > System > Additional Settings, and then Change Management Interface, as shown in Figure 9 and Figure 10.

Figure 9) Navigation to change the management interface security mode.

Select Settings then System and scroll to bottom.

![Image of GUI settings navigation](image)

Figure 10) Change the management interface mode by using the SANtricity System Manager GUI.

Select Change Management Interface

![Image of GUI settings](image)

**Note:** See section 5, Certificate Management, for a full explanation of how to configure the array management interfaces to enable secure communications.
3.2 Formatting Secure SMcli Commands

To establish a secure SMcli connection, the user invokes both a user name and a password on the command line for a given command or session. For example, to change the name of a storage array by using the secure SMcli, open a command prompt from a management station with IP access to the array management ports. The secure SMcli uses the management path to controller A or controller B based on the host names or IP addresses supplied in the SMcli command strings for one or both controllers.

**Note:** You must install SANtricity Storage Manager 11.40 or later on the management station to use SMcli, whether in legacy or secure mode. For Windows, the installation directory is usually C:\Program Files\StorageManager\client.

After you are in the Windows directory with the SMcli.exe file, you can run a secure or nonsecure command to change the storage array name.

```
C:\Program Files\StorageManager\client>SMcli <Array management IP> -u <root admin or storage admin username> -p <password> -c "set storageArray userLabel="EF570_All_Flash_Array"";
Performing syntax check...
Syntax check complete.
Executing script...
Script execution complete.
SMcli completed successfully.
```

**Note:** The backslash before and after the new array name is used for Windows SMcli. The slashes are not necessary when using a Linux-based command line.

Using `-u <username>` in SMcli command strings indicates that you want to use HTTPS if a secure connection is available. If a secure connection is not available, SMcli uses SYMbol instead. If an array has the management interface set for secure, it accepts only SMcli commands that include a valid username and password. Table 2 describes the command line interaction with different array models and security modes.

<table>
<thead>
<tr>
<th>Command Syntax</th>
<th>E2800, E5700, EF280, and EF570; Legacy SYMbol - On</th>
<th>E2800, E5700, EF280, and EF570; HTTPS - On</th>
<th>E2700, E5600, EF560; Legacy SYMbol - On</th>
</tr>
</thead>
<tbody>
<tr>
<td>...&gt; SMcli &lt;IP Address&gt; -u &lt;username&gt; -p &lt;Password&gt; -c &quot;command=&quot;argument&quot;&quot;;</td>
<td>SMcli uses a legacy SYMbol connection to the array</td>
<td>SMcli uses a secure HTTPS connection to the array</td>
<td>SMcli uses a legacy SYMbol connection to the array</td>
</tr>
<tr>
<td>...&gt; SMcli &lt;IP Address&gt; -p &lt;Password&gt; -c &quot;command=&quot;argument&quot;&quot;;</td>
<td>SMcli uses a legacy SYMbol connection to the array</td>
<td>Command fails, indicating that network errors were detected</td>
<td>SMcli uses a legacy SYMbol connection to the array</td>
</tr>
</tbody>
</table>

The `-p` | `-P` parameter allows the following uses:

- `-p "password"`
- `-P <file-name>` | `-`

When the form `-p` is used, the password is specified directly on the command line in clear text, which is consistent with existing behavior. The form `-P <file-name>` allows the password to be read from a file. `-P` allows the password to be read from standard input.
The user name is specified as `-u <user-name>`. The user name can be specified in any of the following forms:

- `user-name@domain-name`. Provides the domain name that should be used to resolve the user’s credentials after the @ sign.
- `domain-name\user-name`. Provides the domain name before the \; this is traditional Microsoft Active Directory style naming.
- `user-name`. Allows a bare user name to be specified. If the user name matches one of the local account names, it is used. Otherwise, the default directory services domain name is used to attempt to log in. If both fail, the login attempt fails.

As a prerequisite to executing a secure SMcli command against a storage array, an HTTPS login must have taken place. The user is authenticated, and authorization permissions are retrieved from either the local account information or from a directory server. In either case, a set of roles is known for the logged-in user.

All SMcli commands have a set of roles that are permitted to run those commands. An incoming SMcli request against an array causes a role check to be performed before the command is run. If the user has insufficient permissions to run the command, an error is returned and command execution is terminated. The SMcli-to-role mappings are set and cannot be modified by the user.

**Note:** See the [SMcli User Guide](#) on the E-Series and SANtricity 11 Resources page for an alphabetical list of available commands.

Finally, if you want to run a secure SMcli command before you have installed CA-signed certificates on the array, you can use the `-k` option following the IP address in the command string. This tells SMcli not to check certificates as part of setting up an HTTPS connection. This is the same condition as connecting with a browser by using HTTPS and accepting the security warning that the connection is not secure. This is the case when the controllers still have self-signed certificates instead of CA-signed certificates.

**Note:** The CA root certificate used on the array controllers must also be installed in the EMW truststore. In rare cases, the CA intermediate certificate might also be required in the EMW truststore.

## 4 Audit Log

One new feature introduced in SANtricity OS 11.40 is the ability to track user activity through an audit trail log. An entry is posted to the log when a user initiates an action or a command through any of the secure access methods that results in a security event. Users attempting login, authentication, and authorization activities also constitute security events.

The audit log scope extends to all user-accessible secure access interfaces (System Manager GUI, secure SMcli, support shell interface, and Web Services API), but it does not log activity by using the SYMbol API. User access through this interface can be disabled when directory services authentication is configured on the array.

Table 3 describes the scope of the audit log across various access methods.

<table>
<thead>
<tr>
<th>Management Access Interface</th>
<th>Audit Log Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Manager GUI</td>
<td>All user activities, including login and logout, session establishment and termination, invoked actions and requests, and their respective outcomes.</td>
</tr>
<tr>
<td>Secure SMcli</td>
<td>All user activities, including login and logout, session establishment and termination, invoked request and endpoint, along with the SMcli commands, command context, and their respective outcomes.</td>
</tr>
<tr>
<td>Management Access Interface</td>
<td>Audit Log Scope</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Web Services API</td>
<td>All user activities, including login and logout, session establishment and termination, invoked actions and requests, and their respective outcomes.</td>
</tr>
<tr>
<td>Support Shell Interface</td>
<td>SSH session establishment and termination, user login and logout activities. Types of user-initiated actions and commands and their respective outcomes are not tracked for this access method.</td>
</tr>
</tbody>
</table>

The logs are persisted on the storage array in the nonvolatile storage region for access by both controllers. A user who has security administrative privileges can use any of the access methods to view and retrieve the logs or export them into a CSV file format.

**Figure 11** shows the audit log in SANtricity System Manager under Settings > Access Management > Audit Log.

**Figure 11)** SANtricity System Manager page to view the audit log.

The file export operation supports exporting audit log records through a timestamp range or a record ID range request through the System Manager GUI, Secure SMcli, or API access method. **Figure 12** shows the Export Table dialog box.
Audit logs are intended to continuously capture user actions throughout the lifecycle of an array that supports this feature. Therefore, an appropriate set of rules must be defined concerning the control action when the log file size reaches certain criteria, based on either file size or number of log entry records. Figure 13 shows the page where the audit log settings are managed.

Figure 13) SANtricity System Manager page to configure the audit log settings.
5 Certificate Management

In cryptography, a certificate authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This certification allows others to rely on signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted by both the owner of the certificate and the party relying on the certificate. The format of these certificates is specified by the International Telecommunications Union's Standardization (ITU-T) X.509 international standard.

A common use for certificate authorities is to sign certificates used in HTTPS, the secure browsing protocol for the World Wide Web. In the SANtricity OS 11.30 release, NetApp introduced the CA certificate management feature in the SANtricity EMW to allow a secure browsing protocol between SANtricity System Manager sessions and the EMW to support configuring remote mirroring. Beginning with SANtricity OS 11.40, the CA Certificate Management feature was renamed Web Services Certificate Management to more accurately describe what the feature does. With SANtricity OS 11.50, this functionality on the Web Services proxy is elevated to the SANtricity Unified Manager GUI. The certificate management in WSP is still available and is supported directly by using API commands (endpoints) defined in the API Swagger doc. The following workflows are described later in this section:

- WSP certificates using WSP 2.1 API endpoints
- WSP certificates using WSP 3.0 API endpoints
- WSP 3.0 certificates using SANtricity Unified Manager

In SANtricity OS 11.40, NetApp introduced the array certificate management feature in the EMW for the E2800, E5700, EF280, and EF570 arrays to ensure that the communication between the EMW and the storage array is done on a path with a secure connection. There are a few operations that the EMW can perform on the storage array where the user ID and password are required. To prevent sensitive information from being compromised by a man-in-the-middle attack, EMW makes it possible to establish trust between the two parties with the use of certificates.

The SANtricity OS 11.40 release also introduced a certificate management feature in SANtricity System Manager to:

- Support CA certificates on each controller in the storage array
- Trust LDAPS or other server certificates
- Support embedded key management server certificate

Finally, support for certificate management was added to the SANtricity WSP to enable secure communications between a server running the Web Services proxy software and E2800, EF280, E5700, and EF570 arrays that are managed and monitored by the proxy. Beginning with SANtricity WSP 3.0 and SANtricity Unified Manager, there are new options for customers who only have new-generation E-Series and EF-Series arrays running SANtricity OS 11.40 or later. This extends to customers who want to manage their new arrays by using the advanced security features, and still manage older generation arrays by using SANtricity Storage Manager EMW.

The decision about which interface to use depends on your need for security versus the desire to use certain features. Table 4 describes considerations to help make that decision.
<table>
<thead>
<tr>
<th>Management Client</th>
<th>Mirroring Feature</th>
<th>SMcli</th>
<th>Script Editor</th>
<th>Importing Settings from One Array to Other Arrays</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANtricity Storage Manager</td>
<td>Supports mirroring for legacy and new-generation E-Series and EF-Series arrays</td>
<td>Supports standard and secure SMcli</td>
<td>Supported for both legacy and new-generation arrays with the legacy SYMbol API interface enabled</td>
<td>Not supported</td>
</tr>
<tr>
<td>SANtricity WSP 3.0 and Unified Manager</td>
<td>Supports mirroring only for new-generation E-Series and EF-Series arrays</td>
<td>Not supported</td>
<td>Not supported</td>
<td>New feature to automate deploying new arrays that use common settings (alerts, ASUP, storage configuration, and more)</td>
</tr>
</tbody>
</table>

### 5.1 Certificate Management for Remote Mirroring

Storage arrays managed by the browser-based SANtricity System Manager (version 11.30 and later) require that a trusted certificate be used to establish secure communications between arrays when administrators want to use secure management interfaces. This is accomplished by using security certificates imported to the WSP or the EMW to allow the array controllers to authenticate through the WSP 3.0 or the EMW Web Services or to facilitate remote mirroring configuration. This capability enables secure communications to both the primary and the secondary storage arrays. The operations that use the secure communications path are asynchronous mirror group creation, asynchronous mirrored pair creation, and synchronous mirrored pair creation.

**Note:** These operations are not supported from SANtricity System Manager when either the primary or secondary storage array has the external SYMbol port disabled. The recommended workaround is to temporarily enable SYMbol on each SYMbol-disabled array, perform the operation, and then disable SYMbol again on the temporarily enabled arrays. By default, the SYMbol port is enabled. It gets disabled when configuring for user access control with a directory server, such as LDAP, or when multifactor authentication is used.

### Setting Up EMW Certificates

The EMW Web Services proxy is an application used by the EMW to send commands to the storage array controllers. If an attempt is made to perform remote mirroring without first importing a trusted certificate, a warning message opens in the EMW to indicate that the certificate is not signed by a validated CA.

To load a signed server certificate on the EMW web server, generate a certificate signing request (CSR file) for the computer where the EMW is installed by using the wizard in the EMW, as shown in Figure 14 and Figure 15.
Figure 14) SANtricity EMW with the Web Services Certificate Management feature.

Figure 15) Completed CSR form to request a signed certificate.
The CSR form is prefilled with the Common Name, Alternate IP Address, and Alternate DNS Name information. Be sure that the common name and alternate DNS include the fully qualified domain name (FQDN), and the alternate IP address must have the IP address of the management station where SANtricity Storage Manager was installed.

**Note:** When the CSR form is generated, a private key is created for the EMW web server. The private key is embedded in the CSR and stored locally. When the new security key is imported from the CA, the local server confirms that the private key used to create the CSR matches the private key embedded in the CA security certificate. Therefore, you must not generate a new CSR after one is submitted to the CA. If you do, the EMW generates a new private key, and the certificate you receive from the CA does not work because the private embedded key in the CA certificate no longer matches the private key stored at the EMW. If this occurs, you must repeat the process of purchasing a new certificate from a CA.

When the CSR form is complete, send the CSR file with the embedded private key to a CA such as VeriSign, DigiCert, or GoDaddy. If the certificates from the CA are individual certificates (for example, a root certificate, intermediate certificate, and the CA-signed server certificate), import the certificates directly to the EMW where the CSR was created.

**Note:** The root and intermediate certificates must be imported before the server certificate because EMW checks the validity of the server certificate before installing it. This is required only when the root and intermediate certificates for your CA are not included in the preinstalled certificate key store.

Figure 16, Figure 17, and Figure 18 show the Import Root/Intermediate and Server CA Certificates wizards used to import new CA certificates.

**Figure 16**) EMW navigation to import root/intermediate certificates and server certificates.

![EMW navigation](image)

**Note:** When browsing to select the certificate files, use the Ctrl key to select all intermediate certificate and root certificate files so that all certificates are imported at the same time.
If the CA provides a chained certificate instead of individual certificates, follow these steps to break up the certificate chain.

1. To open the chained certificate, use the Windows certmgr utility and double-click the .p7b – PKCS #7 certificate file (Windows will recognize the file type).

2. Expand the Certificates tree to display the certificates in the right pane by using the Windows Cert Manager.
3. Export each of the certificates in the certificate chain.

4. Follow the wizard to export each certificate in the chain to a local directory on the host where SANtricity Storage Manager is installed and the CSR was generated.

   **Note:** Be sure to select the desired cert file type—typically base-64 encoded format, because it is easy to validate keys by using common decoder software.
5. After the exports are complete, a file is created for each of the individual certificates in the certificate chain. In the following example, `certnew_chain_VED_EMW` is a certificate chain file, and the other files are `.cer` security certificate files.

**EMW Certificate Management for Active Operations**

SANtricity Storage Manager 11.40 EMW enables the user to perform all active operations on the E2800, E5700, EF280, and EF570 arrays and all E-Series and EF-Series storage arrays that use SANtricity controller firmware 8.10 or later. These operations include firmware upgrade, storage array rename, load storage array configuration, and script editor. For SANtricity OS 11.40, these operations can be performed only on storage arrays with trusted certificates. Active operations require a user to be authenticated with the storage array.

For nonactive operations, the EMW can connect to storage arrays even when the certificates for the controllers are not trusted. This ability supports the existing discovery and read-only functionality without
requiring a login or certificate validation. To ensure that the user’s credentials are not sent to untrusted systems, the EMW does not allow logging in to a controller until the certificate for the controller is trusted, either temporarily or permanently.

With a storage array that contains two controllers, it is possible for only one of the controllers to be trusted. In that case, it is acceptable to perform the login only to the trusted controller. The untrusted controller will not be usable for commands that require authentication until the trust issue is resolved. Figure 19 shows the navigation in SANtricity Storage Manager to manage certificates.

Figure 19) SANtricity EMW with the Array Certificate Management feature.

CA Signed Controller Certificates and the EMW

SANtricity Storage Manager 11.40 EMW is a Java-based application, and the Java Runtime Environment (JRE) shipped with the EMW contains a set of preinstalled CA root certificates in the EMW truststore. These certificates are considered trusted by the EMW, so any certificate signed with one of these CA root certificates is trusted without any additional user intervention. The truststore is shared with the Web Services proxy embedded in the EMW so that trusting can be accomplished in one place.

CA-signed controller certificates are certificates installed on array controllers where the subject and issuer of the certificate are not the same. These certificates are not explicitly trusted by the user and might require the user to have both the intermediate certificate and the root certificate from the CA installed in their truststore. In other implementations, certificates of this type are trusted if only the root certificate is trusted. NetApp’s implementation is the latter; having a trusted root certificate is sufficient to build the trust relationship between the EMW and the storage array. If the user has their controller certificates signed by one of the CA certificates contained in the preinstalled CA certificates file, then no further action is required on their part. If the user chooses to use an internal CA certificate or some other CA certificate not provided by the preinstalled CA certificates on their controllers, then they need to manually import any of the root CA certificates needed for full trust of the installed controller certificate. When a root CA certificate is imported, the certificate is added to the user-managed EMW truststore, allowing the trust to persist across EMW sessions. Figure 20 shows the import Root/Intermediate CA Certificates dialog box opened from the EMW.
The EMW enables users to view the certificates they have trusted and to view the preinstalled certificates. This view is not comprehensive, and an export capability is provided so that users can view the details of the certificates with a third-party certificate viewer. The export can save a single self-signed certificate, root certificate, or intermediate certificate.

The EMW also provides a way for users to remove trust for a self-signed certificate or any certificates signed by a CA certificate that they imported. This is done by removing the specified certificate from the user-managed truststore. The change is applicable to all new connections, but it does not affect existing connections.

**Note:** Removing a single root certificate can potentially impact multiple arrays if the associated controller security certificates are all signed by the same root certificate.

**Self-Signed Controller Certificates and the EMW**

The E2800, E5700, EF280, and EF570 controllers ship with an automatically generated self-signed certificate on each controller. When a user requests to perform any active operation against arrays with self-signed certificates, and there are no trusted certificates in the EMW truststore, the EMW provides an option to temporarily trust the self-signed certificate or to permanently trust it. When the user temporarily trusts a self-signed certificate, it is persisted in memory only, so the trust is valid only for the current EMW session. On the other hand, when a self-signed certificate is permanently trusted in the EMW by the user, the certificate is written to the user-managed truststore file. This allows the trust to persist across EMW sessions. Figure 21 and Figure 22 show the wizard that allows users to temporarily or permanently accept self-signed certificates.
Figure 21) Automatically generated controller untrusted certificates.

![Automatically generated controller untrusted certificates](image)

Figure 22) Dialog box to temporarily or permanently trust the self-signed controller certificate.

![Dialog box to temporarily or permanently trust the self-signed controller certificate](image)

When there are no trusted certificates, active operation requests are rejected with the dialog box shown in Figure 23.
5.2 Certificate Management for Web Services Proxy

NetApp Web Services are used in three areas. As described in section 5.1, Certificate Management for Remote Mirroring, the EMW Web Services proxy resides on the server where the SANtricity EMW software is installed. The EMW Web Services proxy is a restricted proxy that is used solely by the SANtricity System Manager running on the same server to communicate with the alternate array to facilitate remote mirroring configuration.

In addition to the EMW Web Services proxy, a standalone NetApp SANtricity WSP can be installed on a Windows or Linux server. This proxy provides Web Services APIs to configure, manage, and monitor E-Series and EF-Series arrays. The proxy provides access to a collection of REST-style interfaces to access services defined for storage arrays. Figure 24 is a high-level overview of the communications between client machines, the Web Services proxy running on a server, and the E-Series arrays.
The third Web Services implementation is the SANtricity System Manager Web Services, the embedded version residing on the array controller. Similarly, clients access the Web Services through standard HTTPS mechanisms. As the Web Services satisfy the client request through collecting data or executing configuration change requests to the storage system, the Web Services module issues SYMbol requests to the storage systems.

**WSP 3.0 Certificate Management Using SANtricity Unified Manager**

New with SANtricity WSP 3.0 is SANtricity Unified Manager, and one of the embedded features is the ability to manage WSP security certificates from the Unified Manager GUI. The following procedures show the workflows required to manage WSP certificates. The first procedure is to import CA root and intermediate certificates to the WSP that the WSP server will use to authenticate incoming client requests from arrays.

1. Open SANtricity Unified Manager from the WSP installation wizard or by navigating to
   [https://<WSP Server FQDN>:<Secure Port #>/um](https://<WSP Server FQDN>:<Secure Port #>/um).
2. Log in as user = admin and password = admin.
   
   **Note:** If you have changed the default admin account password, log in with that new password.

Discovered arrays are displayed on the landing page, including the communication status to each array.
3. Navigate to the Certificate Management tab and select Import.

4. When prompted by the Certificates wizard, browse to the CA root and intermediate certificates files and select the files to import; use the Ctrl key to select multiple files.

The newly imported certificates are displayed in the Certificate Management pane.
This resolves certificate issues with arrays that have a CA certificate installed.

To generate and install a new SANtricity WSP web server certificate (the server certificate the WSP presents to clients contacting the WSP), you must generate a CSR and submit the CSR files to a CA authority. After you receive your new certificates, you then import them in a manner similar to the previous procedure.

1. Navigate to the Certificate Management tab, click Management, and execute a Reset to regenerate a new self-signed certificate on the web server.
2. Select the Complete CSR tab and follow the wizard to complete the CSR.

Note: These are not optional fields.
3. Click Finish, download the CSR file, and send the CSR file to your CA authority to request a new web server certificate (this usually comes in a certificate chain with the root and intermediate certificates).

4. Import the new certificates by using the Import wizard.

5. Select the root and intermediate certificates and the new web server certificate to be imported.

6. After the web server is imported it restarts, the browser window resets, and the browser session is secure. Start a new browser session.
Accessing the Web Services REST API

To reach the REST API by using a web browser on the host where the proxy is installed, go to https://localhost/devmgr/docs/#/.

If this is the first time you are accessing the REST API, each type of browser displays the following:

- Chrome displays Your Connection is Not Private. Click Advanced to proceed to the website.
- Internet Explorer displays There is a Problem with This Website’s Security Certificate. Click Continue to This Website (Not Recommended) to proceed to the website.
- Firefox displays Your Connection is Not Secure. Click the Advanced button and add an exception for the certificate to proceed to the website.

Figure 25) The Web Services proxy security certificate is not working and the connection is not secure.

The Web Services proxy can also be accessed remotely by using a supported browser to access https://<Web_Proxy_host_server_FQDN_or_IP>:<secure port ID>/devmgr/docs/#/.
**Note:** The default secure port is 8443, but depending on the server where SANtricity WSP is installed, the proxy might switch to a different port number. As a result, the port for this application could be different in your environment.

Logging In to the Web Services Proxy as Admin

To confirm that you can log in to the target web server, including the access permissions associated with the security admin role, follow these steps.

1. Select **Utils** from the drop-down menu to access the **Utilities page**.

2. Expand the **Login commands** and select the **Get:/login** command.
3. Click Try It Out, edit the user ID and password to be user = admin / password = admin, and click Execute.  
   **Note:** The Responses section shows the command set and indicates the status of the command, including returning any associated information. In this example, the roles assigned to the admin user are listed.

   ![Response Image](image)

   ![Response Details](image)

4. Select V2 from the drop-down menu to return to the V2 page and execute the procedure to generate and install CA certificates.

   ![Select V2](image)
Installing Web Services Proxy Security Certificates by Using WSP 3.0

The following procedure is based on the example endpoints available with Web Services Proxy 3.0.

1. Expand the Administration line and scroll down to the /certificates endpoints.

2. Select POST:/certificates and then click Try It Out.
   
   **Note:** This step causes the web server to regenerate a self-signed certificate and allows you to enter information in several fields to define the common name, organization, organization unit, alternate ID, and other information used to generate the CSR.
3. Add the required information in the Example values pane to generate a valid CA certificate and then run the commands.

**Note:** To find the valid DN attributes, refer to [https://www.ietf.org/rfc/rfc2253.txt](https://www.ietf.org/rfc/rfc2253.txt). This example is for customers who are based in the United States.

```json
{
    "dn": "CN=Enter_server_FQDN,O=Company_Name,OU=Organization_Unit,L=Location,ST=State,C=US",
    "rdns": [
        {
            "attributes": [
                {
                    "name": "CN",
                    "value": "Enter_server_FQDN"
                },
                {
                    "name": "O",
                    "value": "Enter_Company_Name"
                },
                {
                    "name": "OU",
                    "value": "Enter_Organization_Unit"
                },
                {
                    "name": "L",
                    "value": "Enter_Location"
                },
                {
                    "name": "ST",
                    "value": "Enter_State"
                },
                {
                    "name": "C",
                    "value": "US"
                }
            ]
        }
    ]
}
```
Note: Do not call POST:/certificates or POST:/certificates/reset again or you will need to regenerate the CSR. When you call POST:/certificates or POST:/certificates/reset you are generating a new self-signed certificate with a new private key. If you send a CSR that was generated before the last reset of the private key on the server, the new security certificate won't work. You will need to generate a new CSR and request a new CA certificate.

4. Execute the GET:/certificates/server endpoint to confirm that the current certificate status is the self-signed certificate with the information added from the POST:/certificates command.
Note: The server certificate (denoted by the alias jetty) is still self-signed at this point.

5. Expand the POST:/certificates/export endpoint, click Try It Out, enter a file name for the CSR file, and click Execute.
6. Copy and paste the file URL into a new browser tab to download the CSR file.
7. Send the CSR to a valid CA and request a new web server certificate chain.
8. When the CA issues a new certificate chain, use the certificate manager tool to break out the root, intermediate, and web server certificates.
9. When the individual certificate files are available, import them to the Web Services proxy server.
   a. Expand the POST:/sslconfig/server endpoint and click Try It Out.
   b. Enter a name for the CA root certificate in the alias field.
   c. Select false in the replaceMainServerCertificate field.
   d. Browse to and select the new CA root certificate.
   e. Click Execute.
   f. Confirm that the certificate upload was successful.
g. Repeat the CA certificate upload procedure for the CA intermediate certificate.
h. Repeat the certificate upload procedure for the new web server security certificate file. Select True from the replaceMainServerCertificate drop-down menu.

i. Confirm that the web server security certificate import was successful.
j. To confirm that the new root, intermediate, and web server certificates are now available in the keystore, run GET:/certificates/server.

10. Select and expand the POST:/certificates/reload endpoint and click Try It Out. When prompted whether you want to restart both controllers, select False (True applies only in the case of dual-array controllers). Click Execute.

![POST /certificates/reload endpoint screenshot](image)

**Note:** The /certificates/reload endpoint usually returns a successful http 202 response. However, the reload of the web server truststore and keystore certificates does create a race condition between the API process and the web server certificate reload process. In rare cases, the web server certificate reload can beat the API processing. In this case, the reload appears to fail even though it completed successfully. If this occurs, continue to the next step anyway. If the reload actually fails, the next step will not succeed.

11. Close the current browser session to the Web Services proxy, open a new browser session, and confirm that a new secure browser connection to the Web Services proxy can be established.

**Note:** Using an incognito or in-private browsing session allows you to open a connection to the server without using any saved data from previous browsing sessions.
Installing Web Services Proxy Security Certificates by Using WSP 2.3

The procedure described in this section is based on the example endpoints available with SANtricity WSP 2.3. All certificate management endpoints are displayed as deprecated and are grayed out. All the endpoints still work as they did in the previous proxy release and are used in the following procedure. These endpoints will be replaced by new endpoints in a future release.

**Note:** If you use the on-board Web Services proxy from an E-Series controller running SANtricity OS 11.40.0 to 11.40.2 instead of the SANtricity System manager GUI to set up the array security certificates, you will notice that the /sslconfig endpoints are not deprecated and grayed out. The /ssl endpoints will be changed to /certificates endpoints consistent with the host-based Web Services proxy in a future release.

1. Expand the Administration list and scroll down to the grayed-out /ssl endpoints.
2. Select Post:/ssl config and then click Try It Out.

   **Note:** This step causes the web server to regenerate a self-signed certificate and allows you to enter information in several fields to define the common name, organization, organization unit, alternate ID, and other information used to generate the CSR.
3. Add the required information in the Example values pane to generate a valid CA certificate and then run the commands.

**Note:** To find the valid DN attributes, refer to [https://www.ietf.org/rfc/rfc2253.txt](https://www.ietf.org/rfc/rfc2253.txt). This example is intended for customers who are based in the United States.

```json
{
  "dn": "CN=Enter_server_FQDN,O=Company_Name,OU=Organization_Unit,L=Location,ST=State,C=US",
  "rdns": [
    {
      "attributes": [
        {
          "name": "CN",
          "value": "Enter_server_FQDN"
        },
        {
          "name": "O",
          "value": "Enter_Company_Name"
        },
        {
          "name": "OU",
          "value": "Enter_Organization_Unit"
        },
        {
          "name": "L",
          "value": "Enter_Location"
        },
        {
          "name": "ST",
          "value": "Enter_State"
        },
        {
          "name": "C",
          "value": "US"
        }
      ]
    }
  ]
}```
Note: Do not call POST: /sslconfig or Post: /sslconfig/reset again or you will need to regenerate the CSR. When you call POST: /sslconfig or Post: /sslconfig/reset, you are generating a new self-signed certificate with a new private key. If you send a CSR that was generated before the last reset of the private key on the server, the new security certificate won't work. You will need to generate a new CSR and request a new CA certificate.

4. Execute the Get: /sslconfig endpoint to confirm that the current certificate status is the self-signed certificate with the information added from the Post: /sslconfig command.
Note: The server certificate (denoted by the alias jetty) is still self-signed at this point.

5. Expand the Get: /sslcfg/export endpoint, click Try It Out, enter a file name for the CSR file, and click Execute.

6. Use the download link to download the new CSR file.
7. Send the CSR to a valid CA and request a new web server certificate chain.
8. When the CA issues a new certificate chain, use the certificate manager tool to break out the root, intermediate, and web server certificates.
9. When the individual certificate files are available, import them to the Web Services proxy server.
   a. Expand the Post:/sslconfig/ca endpoint and click Try It Out.
   b. Select False to upload the CA certificates to the keystore where the web server security certificate will be installed.
   c. Enter a name for the CA root certificate, browse to the new CA root certificate, and click Execute.
   d. Confirm that the certificate upload was successful.
e. Repeat the CA certificate upload procedure to the keystore for the CA intermediate certificate.

f. Select and expand the Post: /sslconfig/import endpoint, browse to the new web server security certificate file, and click Execute.
g. Confirm that the web server security certificate import was successful.

h. To confirm that the new root, intermediate, and web server certificates are now available in the keystore, run Get: /sslconfig/ca and select False to view certificates in the keystore instead of the truststore.
10. Select and expand the Post: /sslconfig/reload endpoint and click Try It Out. When prompted whether you want to restart both controllers, select False (True applies only in the case of dual-array controllers). Click Execute.

Note: The /sslconfig/reload endpoint usually returns a successful http 202 response. However, the reload of the web server truststore and keystore certificates does create a race condition between the API process and the web server certificate reload process. In rare cases, the web server certificate reload can beat the API processing. In this case, the reload appears to fail even though it completed successfully. If this occurs, continue to the next step anyway. If the reload actually failed, the next step will not succeed.
11. Close the current browser session to the Web Services proxy, open a new browser session, and confirm that a new secure browser connection to the Web Services proxy can be established.

   **Note:** Using an incognito or in-private browsing session allows you to open a connection to the server without using any saved data from previous browsing sessions.

5.3 Certificate Management for SANtricity System Manager Controller

When an administrator uses SANtricity System Manager to set up certificates on an array for the first time, the default status is for the web servers on the controllers not to trust each other, because both have a default self-signed certificate. SANtricity System Manager needs to physically access only one of the two controllers, so when you navigate to Settings > Certificates for the first time, a dialog box opens asking if you want to accept the other controller’s self-signed certificate. Figure 26 shows the default controller web server certificate status where HTTPS connections are not secure.

Figure 26) SANtricity System Manager navigation to manage certificates.

Figure 27 shows the dialog box in which you are asked to accept the self-signed certificate of the alternate controller.
Accept the self-signed certificate for the alternate controller to manage the controller certificates. After you accept the certificate, the Certificates window is displayed, as shown in Figure 28.

The following procedure describes the SANtricity System Manager GUI controller CSR process.

1. Run the `Reset` command in the Certificates pane to reset and regenerate the controller self-signed certificates. This command restarts the process in a clean state following the array installation.

2. Run the `nslookup` command from a server command prompt in the array’s management network to obtain the controller’s FQDN.

```
C:\Users\admin>nslookup 192.13.85.213
Server: DNS1.location.group.company.com
Address: 192.11.102.130
```
Name: ICTM0904C1-A.group.company.com
Address: 192.13.85.213

C:\Users\admin>nslookup 192.13.85.214
Server: DNS1.location.group.company.com
Address: 192.11.102.130
Name: ICTM0904C1-B.group.company.com
Address: 192.13.85.214

**Note:** If you are not using a DNS server, you can skip the `nslookup` step. Instead, use the autopolulated primary controller IP address as the common name and the same autopolulated IP address as the alternate IP address in the CSR form. You can add additional alternate IP addresses by using a comma-separated list, but the first alternate IP address must match the common name IP for the CA signed certificates to be imported and work properly.

3. Select the Complete CSR tab to generate a new certificate request for both controllers.
   a. Enter the information to identify the organization and location.

   ![Complete & Download a Certificate Signing Request](image)

   b. Use the FQDN for controller A to change or fill in the information for controller A.

   **Note:** When a DNS is not used, do not change the autopolulated common name or alternate IP address. You can add additional alternate IP addresses in a comma-separated list, but the common name IP and the first alternate IP address must match exactly.
c. Use the FQDN for controller B to change or fill in the information for controller B.
d. Click Finish to generate two CSR files, one for controller A and one for controller B.
4. **Submit the CSR files to a CA and request one or more new signed security certificates.**

   **Note:** When the CSR is generated, a private key is created for the web server on each controller. The private keys are embedded in the CSR files for each controller and are stored locally. When the new security certificates are imported from the CA, the controller web servers confirm that the private key used to create each CSR matches the private key embedded in the CA security certificates. Therefore, you must not generate a new CSR after one is submitted to the CA. If you do, the controllers generate new private keys, and the certificates you receive from the CA won't work because the private embedded key in the CA certificates no longer matches the private key stored on the controllers. If this occurs, you must repeat the process of purchasing new certificates from the CA.

5. **After the certificates are received from the CA, they must be imported by using the SANtricity System Manager Import Certificates wizard.**

   **Note:** If the certificates are not provided individually (root, intermediate, and security certificates), you must break up the chain by using the Windows cert manager tool, as described in section 5.1, Certificate Management for Remote Mirroring. Be sure to use base-64 encoding when breaking up the cert chain.
6. The CA root and intermediate certificates are the same for all interfaces and must be uploaded to validate the signed security certificates for each controller.

   **Note:** To complete the procedure, the system requests the admin or security admin credentials. When the import process is complete, the browser displays a message to refresh the browser session.

7. When you close your browser session and start a new SANtricity System Manager session, the new session should indicate a secure browser connection.

### 5.4 Certificate Management for LDAPS Server

By default, LDAP communications between client and server applications are not encrypted. This means that it would be possible to use a network monitoring device or software to view the communications traveling between LDAP clients and directory servers. This situation is especially problematic when an LDAP simple bind is used because credentials (username and password) are passed over the network unencrypted. This could quickly lead to the compromise of credentials.

Reasons for enabling LDAP over Secure Sockets Layer (SSL) and Transport Layer Security (TLS), also known as LDAPS, include the following:

- Some Windows applications authenticate with Active Directory Domain Services (AD DS) through simple bind. Because simple bind exposes the users' credentials in clear text, use of Kerberos is
preferred. If simple bind is necessary, NetApp strongly recommends using SSL/TLS to encrypt the authentication session.

- Use of proxy binding or password change over LDAP, which requires LDAPS.
- Some applications that integrate with LDAP servers (such as Active Directory and Active Directory Domain Controllers) require encrypted communications. To encrypt LDAP communications in a Windows network, you can enable LDAP over SSL (LDAPS).

SANtricity OS 11.40 supports LDAPS. It can be configured by using the SANtricity System Manager GUI, as shown in Figure 29. For convenience, the directory server configuration wizard allows users to upload the CA root and intermediate certificates that match the LDAPS servers’ CA signed certificate to the array truststore. This can also be accomplished by using the secure SMcli.

**Note:** In most cases, only the root certificate is required to be uploaded to the array truststore, but there are cases where both the LDAPS servers’ root and intermediate certificates must be in the array truststore.

Figure 29) Option to upload the LDAP server’s CA root certificate to the array truststore.

5.5 Certificate Management for Embedded External Key Management Server

SANtricity OS 11.40 enhances the existing full disk encryption (FDE) feature by introducing the ability for users to manage the FDE security key through a centralized key management platform like Gemalto SafeNet KeySecure Enterprise Encryption Key Management, which adheres to the Key Management Interface Protocol (KMIP) standard. This feature is in addition to the preexisting SANtricity internal
A security key management solution and is available beginning with E2800, E5700, EF280, and EF570 storage arrays running SANtricity OS 11.40 or later.

In the process of enabling the external key management feature, the administrator must install a set of certificates on the array. These certificates are used to establish a secure connection between the storage array and the key management server. SANtricity System Manager provides an interface to walk the administrator through the process of generating a CSR for the storage array controller and installing both the storage array’s signed client certificate and the KMIP server’s SSL certificate. This process can also be performed through SMcli. Figure 30 shows the open certificates tile in SANtricity System Manager, where the external key management server certificates are managed.

Figure 30) Option in SANtricity System Manager to complete a CSR, and to import the storage array’s signed client certificate and KMIP server’s SSL certificate.

6 SAML 2.0 and MFA in SANtricity OS 11.40.2

Security Assertion Markup Language (SAML) is an industry standard for sending authentication requests and user data securely between multiple systems. This standard allows many applications to use a single service to manage all user authentication and session management.

Multifactor authentication (MFA) requires the user to provide two or more items as proof of identity to be successfully authenticated. The separate pieces of evidence are typically at least two of the following types: knowledge (something the user knows, such as a password); possession (something the user has, such as a device that provides a changing code); or inherence (something the user is, such as biometrics, like a fingerprint). The specific type of evidence required is configured by the end-user organization’s security team.

The integration of SAML into E-Series products makes it possible to communicate with an external system that can authenticate a user with multiple forms of authentication and then report the success or failure of the authentication to the SANtricity System Manager application. The external system can be configured to use single-factor, two-factor, or multifactor authentication. The external system also provides the ability to support single sign-on capabilities with other applications.

6.1 MFA Architectural Overview

SAML is integrated into the E-Series products using version 2.0 of the standard, and NetApp officially supports Shibboleth and Microsoft ADFS as identity providers (IdPs). Figure 31 is a high-level overview of all components used to achieve SAML integration. Communication with the authentication server flows through the user’s web browser, so the SANtricity System Manager application never makes a direct connection. SAML allows SANtricity System Manager to pass sensitive information to the identity provider by using HTTP redirection through the user’s web browser. All information is signed and
encrypted by using x509 certificates provided by the identity provider. This enables the E-Series products to allow management by a user authenticated through a third-party IdP such as Shibboleth or Microsoft ADFS. After the SANtricity System Manager is configured, it can authorize with proper roles and associate a uniquely identifying name or ID to a user who has authenticated by using an IdP.

Figure 31) How SAML integrates into E-Series products.

After SAML is configured on the E-Series system, logging into SANtricity System Manager is possible only through a configured IdP. When users attempt to access SANtricity System Manager, they are sent to their IdP’s login page instead of to the default SANtricity System Manager login page. After entering their credentials, users are sent back to SANtricity System Manager with an authenticated session and are authorized based on attributes associated with their identity. Figure 32 shows how a login request flows through the different components of the E-Series array. The service provider represents an E-Series product; the user agent represents the user’s web browser; the identity provider is the third-party service that manages authentication, such as Microsoft ADFS or Shibboleth; and the user database is a back-end user management application, such as LDAP.
Because the identity provider manages all sessions associated with authenticated users, it might issue a request to log a user out of the system. The IdP accomplishes this task by issuing a single logout request to all applications that it supports, as shown in Figure 33. The SANtricity System Manager application receives this request and invalidates all sessions associated with the logout request.
SAML is supported in SANtricity OS 11.40.2 and later. If a customer loads an older version of the SANtricity OS on their E-Series system, SAML is not usable, and the customer must log in using the supported authentication method for that release. If the customer previously had a SAML configuration on their E-Series system and they load SANtricity OS 11.40.2 or later, the previous configuration is restored, and they are required to authenticate by using an IdP configured through SAML.

6.2 Configuring SAML

To configure SANtricity System Manager to work with a third-party identity provider, several steps need to occur, both in SANtricity System Manager and on the IdP server. As of SANtricity OS 11.40.2, a new tab, SAML, was added to SANtricity System Manager in the Settings > Access Management tile, shown in Figure 34. This tab allows the configuration of an IdP to authenticate users. After an SAML configuration is complete and validated, it can be enabled. When SAML is enabled, it is the only method used to authenticate users for access to SANtricity System Manager. Other forms of management no longer work because they cannot authenticate. This includes the EMW, SMcli client, software developer kit client, in-band management using UTM, REST API clients using HTTP basic authentication, and REST API clients using the standard login endpoint.

Note: Customers should take great care to make sure that their configuration is well tested before enabling SAML. It cannot be disabled without physical access to the hardware. To disable SAML, customers must have serial shell access to a controller on the array and will need to contact a NetApp technical support engineer for instructions.

Figure 34) The SAML tab in SANtricity System Manager when no configuration is present.

SANtricity System Manager establishes a trust relationship with an identity provider by exchanging metadata files. The customer must export the identity provider’s metadata file and import it into SANtricity System Manager by using the Import Identity Provider file link on the SAML tab in Access Management. This process registers an IdP with SANtricity System Manager so that the application knows where to send users to authenticate.

The customer then needs to export the SANtricity System Manager metadata file from all controllers in the storage array by using the Export Service Provider Files link on the SAML tab in Access Management. These files are sent to the IdP to register the E-Series system as a service provider that uses the authentication from the IdP.

The identity provider needs to provide attributes so that SANtricity System Manager can properly authorize users with various roles. In Microsoft ADFS, this is achieved by mapping LDAP attributes to claim rules that can be returned with authentication requests. In Shibboleth, various configuration XML files are used to map attributes to be returned with authentication requests for each identity provider. Refer to the official documentation for those products to understand how to set up attributes to be returned to SANtricity System Manager during authentication. After the attributes have been configured on the IdP, use the Map System Manager Roles link on the SAML tab in Access Management to map
those attributes to the various SANtricity System Manager roles. Enter the user attribute and attribute value for the roles you want matched to that combination to authorize users to access SANtricity System Manager, as shown in Figure 35. This allows SANtricity System Manager to correctly map roles to users after they are authenticated through an IdP.

Figure 35) Common ways to configure roles in SANtricity System Manager.

In addition to user attributes, the IdP needs to send back a valid NameID for SANtricity System Manager to uniquely identify the user without using a randomly generated ID. Although this is not required, it does allow better reporting of user activity through the audit log. Shibboleth and Microsoft ADFS support returning NameID with various configuration options. Refer to your IdP documentation to configure a NameID to be sent to SANtricity System Manager.
At this point, SANtricity System Manager should be ready to test a login by using a configured identity provider. This is done by using the SSO Login Test link on the SAML tab in Access Management. This test redirects the user to the IdP’s login page and validates that the user was properly authenticated and authorized using all configured settings. The test can fail for several reasons, but the most common is that roles were not properly mapped for the authenticated user. If the role mappings are valid, and it is still not possible to successfully complete a login test, refer to Table 5 to review other possible issues with the IdP configuration.

Table 5) Common configuration issues.

<table>
<thead>
<tr>
<th>Misconfiguration Issue</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage array clock and identity provider clock are out of sync</td>
<td>SAML uses time stamps that expire to prevent attacks that use old data. If the storage array and IdP clocks are more than 5 minutes apart, SAML authentication in SANtricity System Manager fails.</td>
</tr>
<tr>
<td>Expired IdP certificates</td>
<td>If the IdP certificates have expired, all SAML authentication in SANtricity System Manager fails. In that case, customers need to disable SAML with the help of a NetApp technical support engineer, make a serial connection to the storage array, and reimport their IdP metadata files with valid x509 certificates embedded in the metadata.</td>
</tr>
<tr>
<td>Unable to map roles</td>
<td>The SSO login test continuously fails with the error that it was unable to map proper roles. This can happen because the identity provider or SANtricity System Manager is not configured properly to map attributes to roles. It can also occur because the security admin and storage monitor roles are required for a successful test. Refer to the official documentation for those products to understand how to set up attributes to be returned to SANtricity System Manager during authentication.</td>
</tr>
<tr>
<td>User name is reported as a long unreadable list of numbers and letters</td>
<td>There is no configured NameID on the identity provider, which results in SANtricity System Manager identifying the user with a randomly generated ID. Refer to the IdP documentation to configure a NameID to be sent to SANtricity System Manager.</td>
</tr>
</tbody>
</table>

After a test is successfully completed, the customer can use the Enable SAML link. After SAML is enabled, it is the only method used to authenticate users for access to SANtricity System Manager. Other forms of management no longer work because they cannot authenticate. This includes the EMW, Unified Manager, SMcli client, software developer kit client, in-band management using UTM, REST API clients using HTTP basic authentication, and REST API clients using the standard login endpoint.

7 Conclusion

NetApp takes storage management security and security for data at rest seriously. To help address the ever-increasing threat from malicious insider activities, NetApp has implemented new features in SANtricity OS 11.40 and 11.40.2, including RBAC, directory services support, secure SMcli, certificate management, audit logs, and multifactor authentication with IdP using SAML 2.0. These feature enhancements help NetApp customers protect their data. The multiple interface options and security configuration choices make it easy to adopt E-Series and EF-Series arrays in enterprise environments where enhanced management security is a core qualifying attribute for all new storage arrays.
Appendix A: Frequently Asked Questions

This appendix answers common questions about the rules and functionality of the SANtricity Management security features.

LDAP, RBAC, and Certificates

This section addresses frequently asked questions about LDAP, RBAC, and certificates.

What if SYMbol API is disabled and the user has lost their LDP password (or access)?

Answer: The user can either log into the array by using a local account or access the serial shell to manually reenable SYMbol access and/or disable LDAP authentication. If it’s necessary to use the serial shell, contact NetApp Customer Success Services for assistance.

What format should my certificate be in?

Answer: It should be in either a PEM (base-64 encoded) or DER (binary encoded) format.

Why are tiles missing in SANtricity System Manager?

Answer: If a tile is not present, it is associated with a REST API endpoint that is not accessible by the user's current roles.

Why are some inputs, buttons, and other elements disabled throughout SANtricity System Manager?

Answer: An element can be disabled if the option is not supported, not applicable, or not valid for a selected object or in certain contexts. In addition, an element can be disabled if it is associated with a dialog box and/or REST API endpoint that is not accessible by the user's current roles.

Why are some storage systems and/or mirror groups not displayed in the Create Mirror Group and Create Mirrored Pair dialog boxes?

Answer: The list of remote storage systems is filtered based on whether the storage system is asynchronous or synchronous mirroring compatible with the current storage system. SYMbol can now be disabled, but it must be enabled on both storage systems to enable Create Mirror Group and Create Mirrored Pair workflows in SANtricity System Manager. The list of remote storage systems in the Create Mirror Group and Create Mirrored Pair dialog boxes, as well as the mirror groups in the Create Mirrored Pair dialog box, are filtered based on whether SYMbol is enabled on that remote storage system.

Why does my valid LDAP user name and password not authenticate?

Answer: Your LDAP configuration might be improperly configured. Double-check the settings you used, and if the issue persists, see if any error messages are being logged to the web server debug logs. Alternatively, you can run <array_ip>/devmgr/v2/storage-systems/1/ldap/test in a browser to print out any issues with your configured domains on that embedded array.

What are the local users accounts defined for an embedded system running SANtricity System Manager?

Answer: admin@local, storage@local, monitor@local, support@local, and security@local.

What is the default admin password?

Answer: The default admin password is always the storage array password. If a storage array password is not set when upgrading from SANtricity OS 11.30, the password is an empty string. When the admin password is set through SANtricity System Manager or SMcli, the storage array password is updated to match.

Why am I getting a 403 response on login?
Answer: Login is locked out for excessive attempts or insufficient permissions if your audit log is full. You can wait 10 minutes for the excessive failed login case, or attempt to sign in with security administrator privileges to clear the audit log.

Why am I getting a 403 response on requests other than login?
Answer: The user you have authenticated does not have the proper permissions for that request, your XSRF token is invalid, or your audit log is full and is restricting access.

Why was I logged out when I was actively using SANtricity System Manager?
Answer: Another user has changed security-related configurations, causing all other users to be logged out.

Why can I not specify local as an LDAP domain name?
Answer: The Rest API reserves "local" to be used for the local accounts on the system.

Why does importing a signed server certificate cause root and intermediate certificates to be removed from the keystore?
Answer: When a signed server certificate is imported, the keystore is pruned so that only root and intermediate certificates needed to validate the signed certificate chain remain.

SAML 2.0 on E-Series
This section addresses questions regarding SAML 2.0 on E-Series.

What identity providers does E-Series support?
Answer: E-Series supports ADFS 3.0 and Shibboleth IdPs.

Why is my SSO test timing out in SANtricity System Manager?
Answer: SANtricity System Manager uses dialog boxes to run the SSO test. Make sure that your browser is not blocking the dialog boxes from SANtricity System Manager.

Why was I logged out of SANtricity System Manager while I was actively managing my storage array?
Answer: The IdP specifies a time when the user’s session is no longer valid. When that time is reached, SANtricity System Manager logs the user out and requires them to authenticate again. Also, any configuration changes to SAML cause all users to be logged out.

Do I need to reconfigure my identity provider if I clear the storage array configuration?
Answer: Yes, the metadata generated by the E-Series system needs to be reexported from the controller and imported to the IdP to ensure that the correct certificate files are in place.

What browsers are supported on SANtricity System Manager for the SAML feature?
Answer: Internet Explorer, Firefox, Chrome, and Safari. The Edge browser is not currently supported with the SAML feature.
Where to Find Additional Information

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

- NetApp SANtricity System Manager online help

- NetApp SANtricity Unified Manager online help

- NetApp SANtricity Web Services Proxy 3.0 Installation Guide
  https://library.netapp.com/ecm/ecm_get_file/ECMLP2846165

- NetApp SANtricity Web Services Proxy 3.0 User Guide
  https://library.netapp.com/ecm/ecm_get_file/ECMLP2846166

- NetApp SANtricity Web Services Proxy 3.0 additional documentation
  https://mysupport.netapp.com/NOW/download/software/estheseries_webservices/3.0/

- SANtricity SMcli User Guide

- E-Series and SANtricity 11 Resources page
  https://mysupport.netapp.com/info/web/ECMP1658252.html

- NetApp Product Documentation

Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Document Version History</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 2.0</td>
<td>December 2018</td>
<td>Updates for the latest SANtricity OS software.</td>
</tr>
<tr>
<td>Version 1.0</td>
<td>August 2018</td>
<td>Initial version for SANtricity OS 11.40.2</td>
</tr>
</tbody>
</table>
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 © 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, tapping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

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

TR-4712-1218