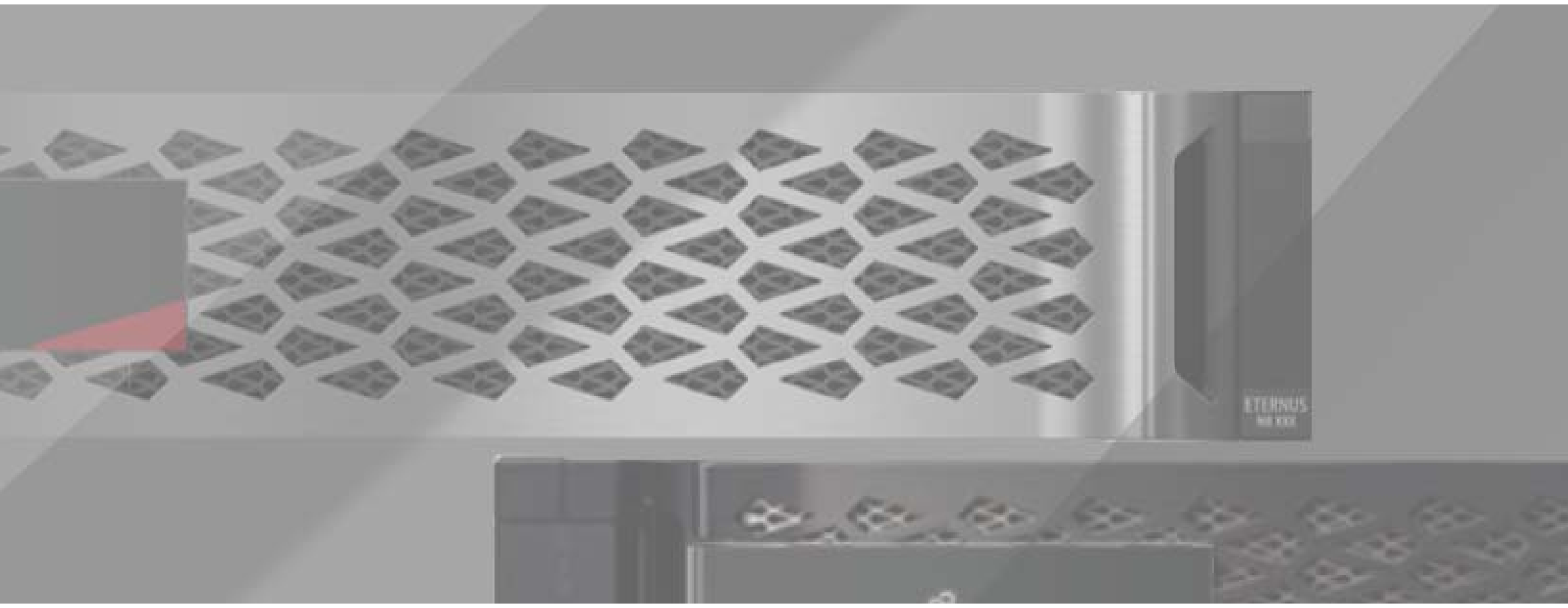
P3AG-6052-01ENZ0

FUJITSU Storage
ETERNUS AB series All-Flash Arrays,
ETERNUS HB series Hybrid Arrays

SANtricity Management Security



Feature Details and Configuration Guide

FUJITSU

Table of Contents

List of Figures

List of Tables

Preface

FUJITSU Storage ETERNUS AB/HB series storage systems 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 SANtricity OS 11.60 and enhanced in later SANtricity OS releases. This report provides detailed information about these SANtricity System Manager security features for the ETERNUS AB2100/AB5100/AB6100 and ETERNUS HB1000/HB2000/HB5000 storage systems. This report also provides management security updates introduced in SANtricity OS 11.60.

First Edition
June 2021

Trademarks

Third-party trademark information related to this product is available at:
https://www.fujitsu.com/global/products/computing/storage/eternus/trademarks.html

Trademark symbols such as ™ and ® are omitted in this document.

About This Manual

Intended Audience

This manual is intended for system administrators who configure and manage operations of the ETERNUS AB/HB, or field engineers who perform maintenance. Refer to this manual as required.

Related Information and Documents

The latest information for the ETERNUS AB/HB is available at:
https://www.fujitsu.com/global/support/products/computing/storage/manuals-list.html

Document Conventions

■ Notice Symbols

The following notice symbols are used in this manual:

Caution	Indicates information that you need to observe when using the ETERNUS AB/HB. Make sure to read the information.
Note	Indicates information and suggestions that supplement the descriptions included in this manual.

1. SANtricity Security Features

The SANtricity OS software for the ETERNUS AB2100/AB5100/AB6100 and the ETERNUS HB1000/HB2000/HB5000 supports secure, web-based storage management for individual systems. In addition to this array-level management security, Fujitsu also supports enterprise-level secure management in SANtricity Unified Manager and SANtricity Web Services Proxy (WSP), enabling secure, centralized management of hundreds of systems.

By using the embedded Web Services management infrastructure or SANtricity Unified Manager and SANtricity WSP, administrators can manage storage systems from a networked browser client with IP access to the ETERNUS AB/HB series controller management ports and the WSP web server. Because web-based storage management exposes the managed devices to private and public networks, the ETERNUS AB/HB series systems and SANtricity WSP support appropriate security schemes at various levels, including the transport layer protocol, access methods, and access control, incorporating authentication and authorization aspects.

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

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, SANtricity WSP 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 systems and WSP:

- SANtricity WSP and SANtricity Unified Manager
- LDAPS servers
- Key Management Interoperability Protocol (KMIP) compliant external encryption key manager servers
- The ETERNUS AB/HB series systems 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, you can use multifactor authentication with Security Assertion Markup Language (SAML) 2.0 to secure the management interface for individual systems. SANtricity WSP and SANtricity Unified Manager do not support SAML and cannot discover and manage systems 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 on storage systems running SANtricity OS 11.60 and later.

2. RBAC and Directory Services

To support multiple users with varying privilege levels, Fujitsu introduced the embedded directory services integration and RBAC on storage systems running SANtricity OS 11.60 and later (also extended to SANtricity WSP and SANtricity Unified Manager). The implementation applies to the SANtricity System Manager GUI 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).

Caution

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 HTTPS API interface (SYMbol is an Open Network Computing RPC interface for managing the ETERNUS AB/HB series storage systems). Disabling the SYMbol interface blocks access to an array that uses non-secure 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.

Caution

Activity through the traditional SYMbol access method is not captured in the audit log.

Figure 1 shows the logical connection relationship between the ETERNUS AB/HB series systems, management clients, and directory servers.

Figure 1 The ETERNUS AB/HB series management security feature, integrating directory server and RBAC

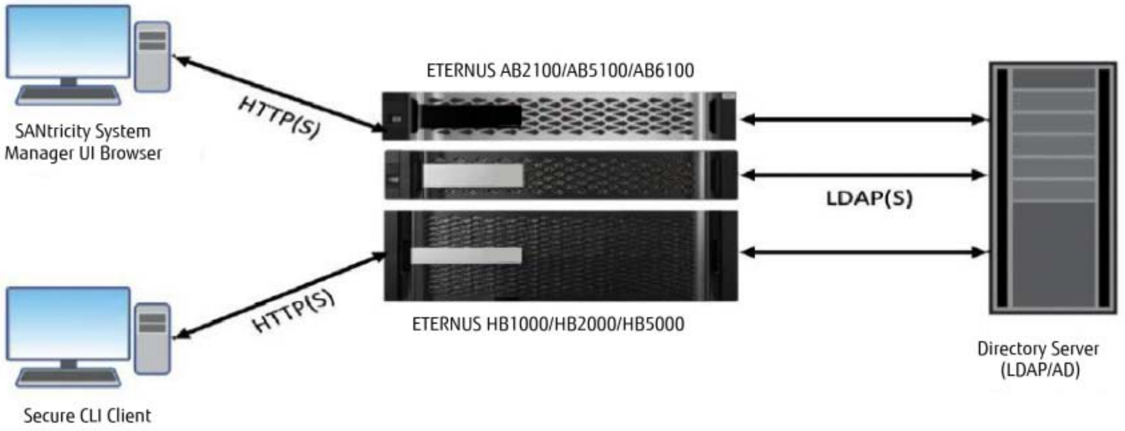
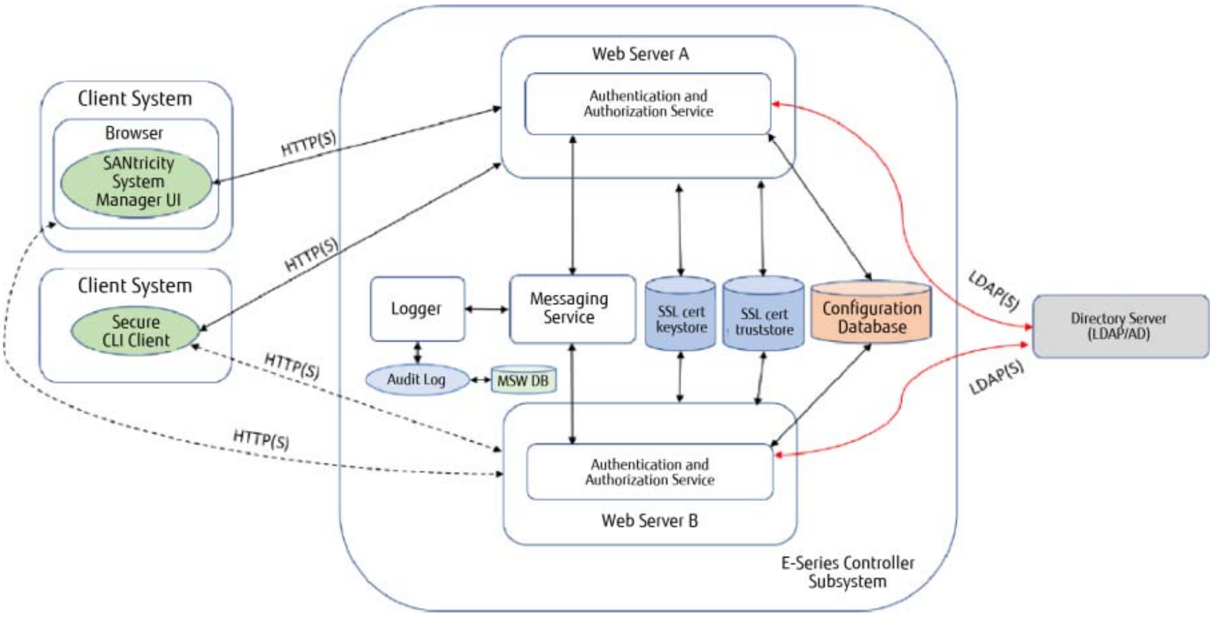

SANtricity System Manager UI Browser
HTTP(S)
ETERNUS AB2100/AB5100/AB6100
LDAP(S)
HTTP(S)
ETERNUS HB1000/HB2000/HB5000
Directory Server (LDAP/AD)
Secure CLI Client

Figure 2 shows the logical breakout of authentication workflows in the ETERNUS AB/HB series controllers.

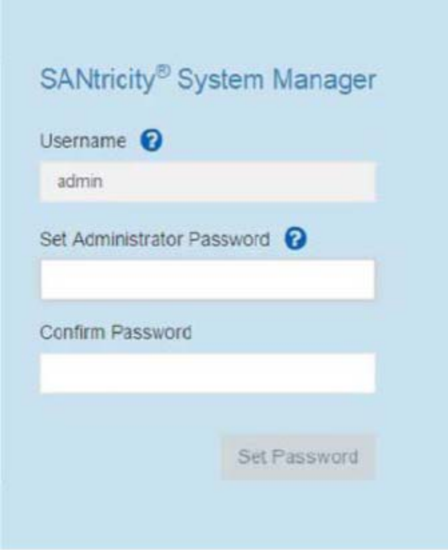
Figure 2 Technical components of the ETERNUS AB/HB series management security feature



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. The password is stored as salted and SHA-256 hashed.

Figure 3 Set admin local password on initial power-up



For SANtricity WSP 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.

Caution

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

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.

  Caution

  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.

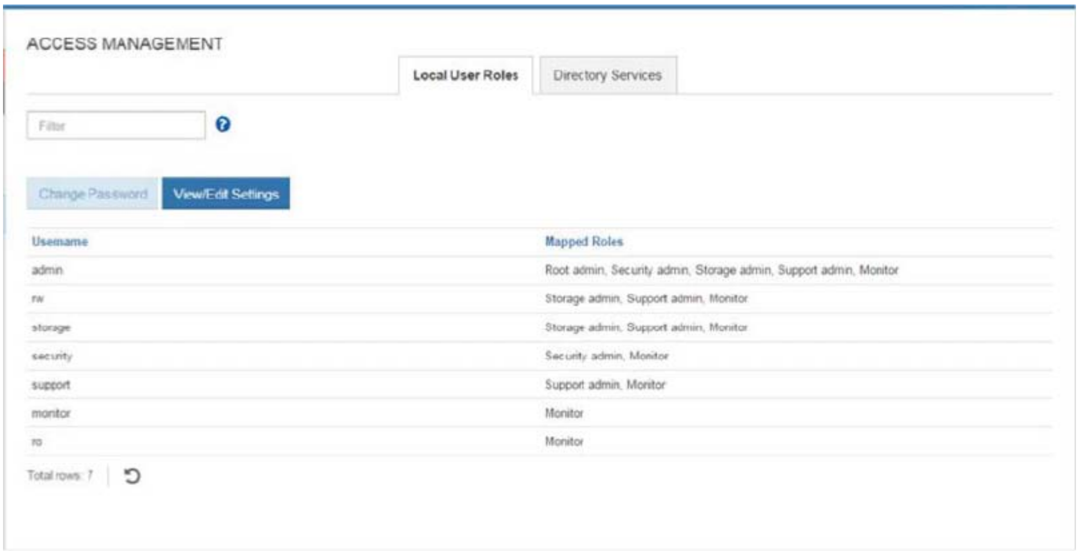
  Caution

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

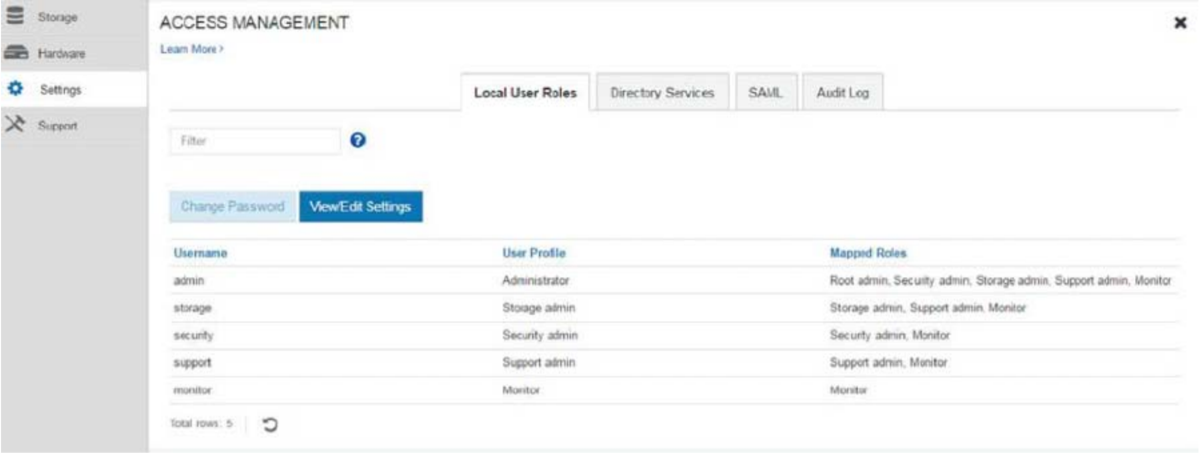
Figure 4 and Figure 5 show the user accounts and mapped roles in the SANtricity Unified Manager and SANtricity System Manager GUIs.
To view the individual user accounts in SANtricity Unified Manager, navigate directly to the Access Management tab. To see the accounts for individual systems by using SANtricity System Manager, navigate to Settings, open the Access Management tile, and click the Local User Roles tab.

Figure 4 SANtricity Unified Manager local account password management



Username	Mapped Roles
admin	Root admin, Security admin, Storage admin, Support admin, Monitor
rw	Storage admin, Support admin, Monitor
storage	Storage admin, Support admin, Monitor
security	Security admin, Monitor
support	Support admin, Monitor
monitor	Monitor
ro	Monitor

Figure 5 SANtricity System Manager access management (local user roles) settings



Username	User Profile	Mapped Roles
admin	Administrator	Root admin, Security admin, Storage admin, Support admin, Monitor
storage	Storage admin	Storage admin, Support admin, Monitor
security	Security admin	Security admin, Monitor
support	Support admin	Support admin, Monitor
monitor	Monitor	Monitor

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.

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 "Certificate Management for SANtricity System Manager Controller" (page 45) to set up certificates for LDAP with Secure Sockets Layer (SSL).

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

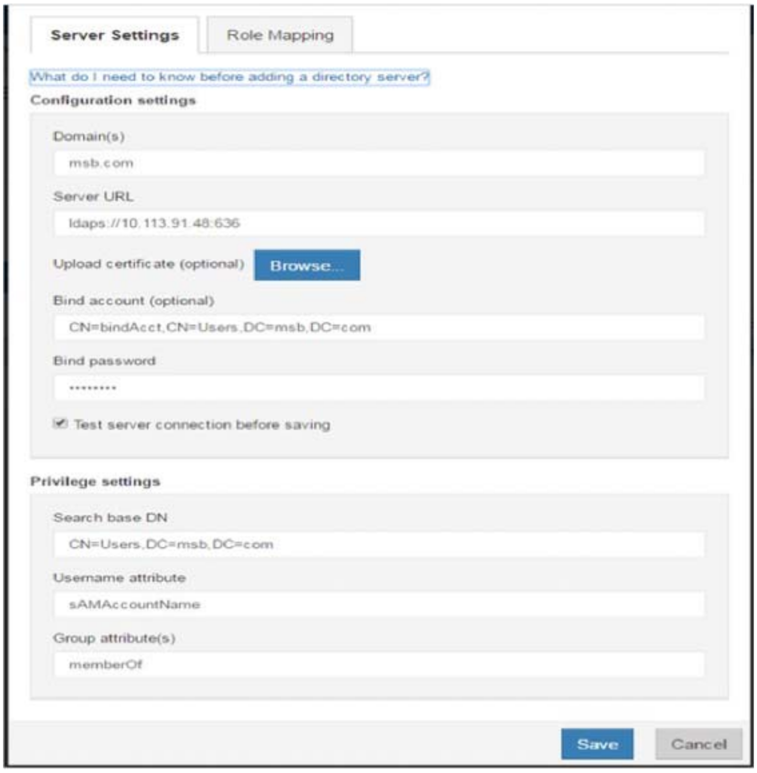
Name	Description
Domain name	Valid DNS names that contain only the ASCII letters a through z (not case sensitive), the digits 0 through 9, and the hyphen (-), but cannot start with a hyphen. Per RFCs 3629 and 4514, conversion of string representation associated with distinguished name from ASN.1 to UTF-8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

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.

Caution

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



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

Configuration settings

Domain(s): msb.com

Server URL: ldaps://10.113.91.48:636

Upload certificate (optional)

Bind account (optional): CN=bindAcct,CN=Users,DC=msb,DC=com

Bind password: ••••••••

☑ Test server connection before saving

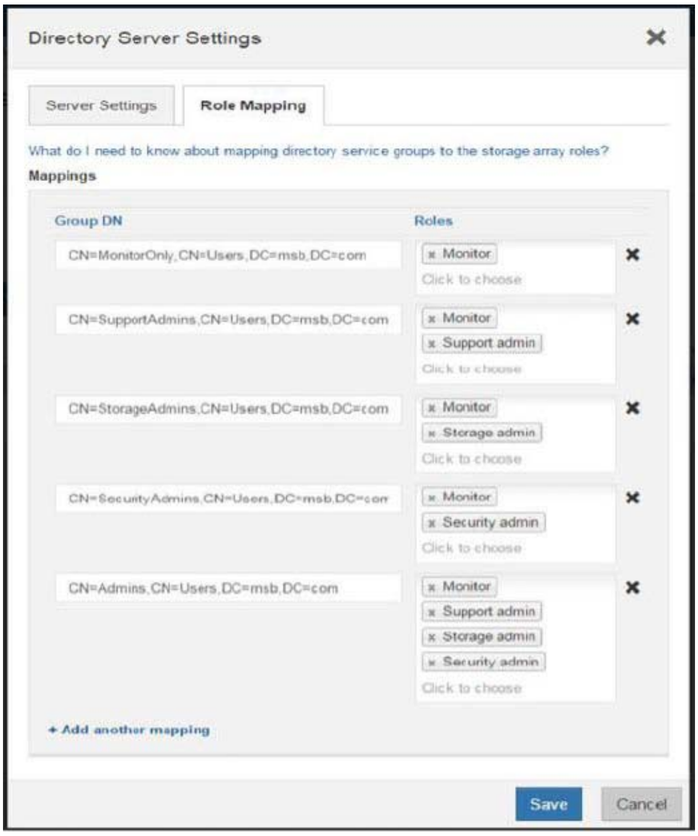
Privilege settings

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

Username attribute: sAMAccountName

Group attribute(s): memberOf

Figure 7 SANtricity System Manager directory server role mapping settings



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

Mappings

Group DN	Roles
CN=MonitorOnly,CN=Users,DC=msb,DC=com	Monitor Click to choose
CN=SupportAdmins,CN=Users,DC=msb,DC=com	Monitor Support admin Click to choose
CN=StorageAdmins,CN=Users,DC=msb,DC=com	Monitor Storage admin Click to choose
CN=SecurityAdmins,CN=Users,DC=msb,DC=cor	Monitor Security admin Click to choose
CN=Admins,CN=Users,DC=msb,DC=com	Monitor Support admin Storage admin Security admin Click to choose

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.

Caution

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.

In August 2019 (updated March 2020), Microsoft published a Security Advisory (ADV190023) to guide users to enable LDAP Channel Binding and LDAP Signing. Microsoft has acknowledged that the current default configurations for LDAP channel binding and LDAP signing exist on Active Directory domain controllers that let LDAP clients communicate with them without enforcing LDAP channel binding and LDAP signing.

Caution

Since SANtricity OS does not support both LDAP channel binding and LDAP signing, Fujitsu strongly recommends users to harden their LDAP environment by implementing LDAP over SSL/TLS (LDAPS) instead of LDAP until SANtricity OS supports these two features in the future release.

Microsoft made two changes in the March 10, 2020 update, as follows:

- Change #1:
  Microsoft recommended to manually set the LDAP signing group policy to Require Signing and monitor the Directory Services event log for LDAP signing failures. The mapping between the LDAP Signing Policy setting and the registry setting is as follows:

  - Policy Setting: "Domain controller: LDAP server signing requirements"
  - Registry Setting: LDAPServerIntegrity
  - DataType: DWORD
  - Registry Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

Group Policy Heading	Registry Setting
Off	0
None	1 (default)
Require Signing	2

  Caution

  Fujitsu recommends that this registry setting be set to either "0" (Off) or "1" (None) until we support LDAP Signing in a future release ,unless the user is configured for LDAPS.

- Change #2:
  Microsoft added a new Domain controller: LDAP server channel binding token requirements group policy to configure LDAP channel binding on supported devices. The mapping between the LDAP Channel Binding Policy setting and the registry setting is as follows:

  - Policy Setting: "Domain controller: LDAP server channel binding token requirements"
  - Registry Setting: LdapEnforceChannelBinding
  - DataType: DWORD
  - Registry Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

Group Policy Heading	Registry Setting
Never	0
When Supported	1 (default)
Always	2

Caution

Fujitsu recommends that this registry setting be set to either "0" (Never) or "1" (When Supported) until we support LDAP Channel Binding in a future release

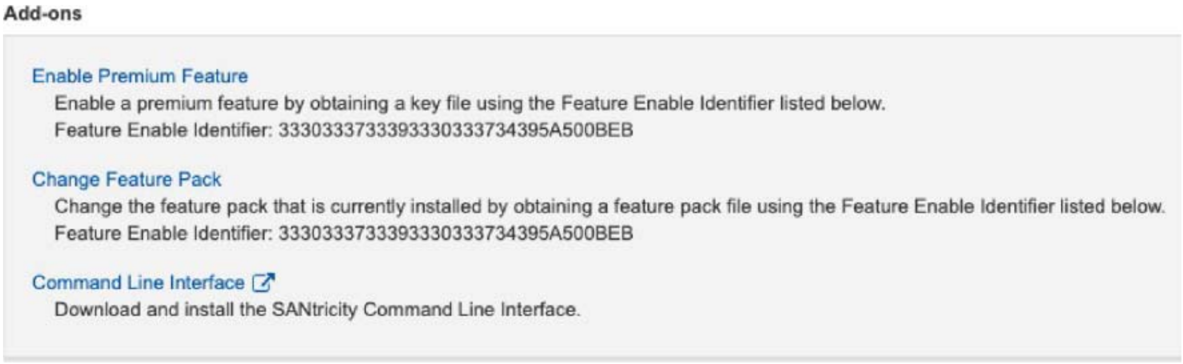
3. Secure SMcli

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 systems by using traditional SMcli grammar and command semantics, but with a secure protocol.

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.

Secure SMcli package can be downloaded via the System Manager. It can be found under Settings > System > Add-ons section, as shown in Figure 8.

Figure 8 Location to download the SMcli via the System Manager



Add-ons

Enable Premium Feature

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

Feature Enable Identifier: 3330333733393330333734395A500BEB

Change Feature Pack

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

Feature Enable Identifier: 3330333733393330333734395A500BEB

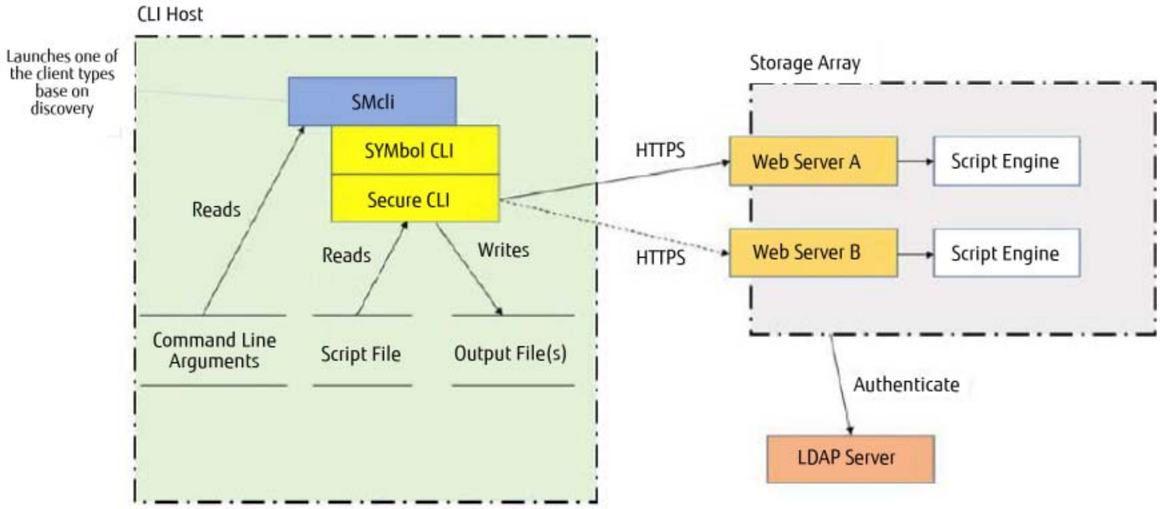
Command Line Interface

Download and install the SANtricity Command Line Interface.

Secure SMcli Logical Architecture

When the secure SMcli interacts directly with the storage systems, it can communicate with the storage system by using the legacy SYMbol interface or the HTTPS protocol, depending on how the array interface is set. Figure 9 shows the logical connectivity from an SMcli host to an ETERNUS AB/HB series array that is managed by SANtricity System Manager.

Figure 9 Technical components of secure SMcli operating against a storage array

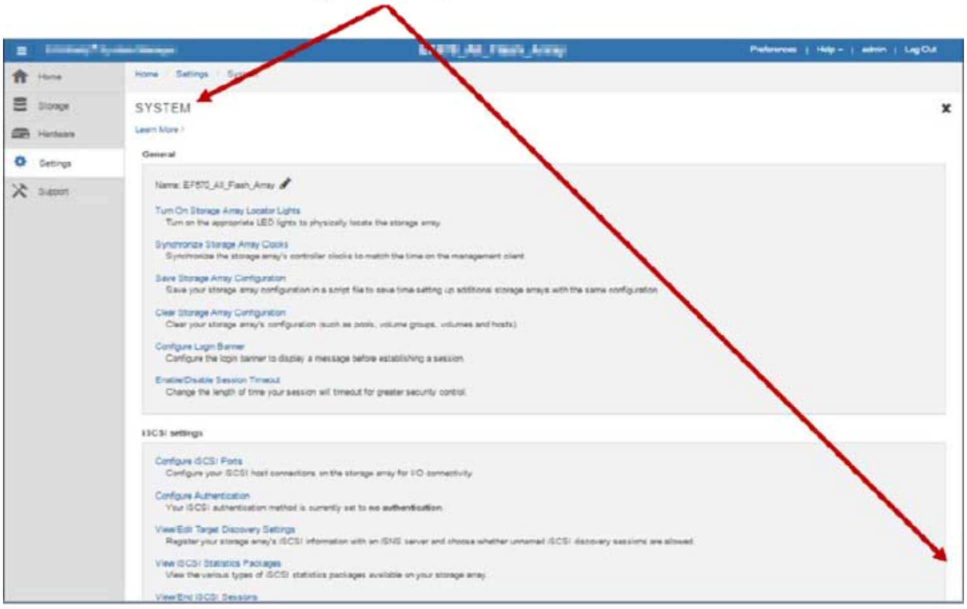


Caution

By default, the storage systems 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 10 and Figure 11.

Figure 10 Navigation to change the management interface security mode

Select Settings then System and scroll to buttom.



SYSTEM

Learn More ›

General

Name: EF570_All_Flash_Array

Turn On Storage Array Locator Lights
Turn on the appropriate LED lights to physically locate the storage array.

Synchronize Storage Array Clocks
Synchronize the storage array's controller clocks to match the time on the management client.

Save Storage Array Configuration
Save your storage array configuration in a script file to save time setting up additional storage arrays with the same configuration.

Clear Storage Array Configuration
Clear your storage array's configuration (such as pools, volume groups, volumes and hosts).

Configure Login Banner
Configure the login banner to display a message before establishing a session.

Enable/Disable Session Timeout
Change the length of time your session will timeout for greater security control.

iSCSI settings

Configure iSCSI Ports
Configure your iSCSI host connections on the storage array for I/O connectivity.

Configure Authentication
Your iSCSI authentication method is currently set to **no authentication**.

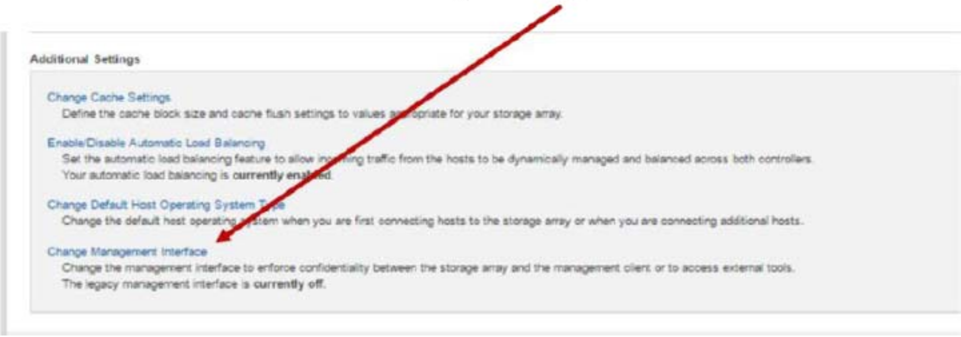
View/Edit Target Discovery Settings
Register your storage array's iSCSI information with an iSNS server and choose whether unnamed iSCSI discovery sessions are allowed.

View iSCSI Statistics Packages
View the various types of iSCSI statistics packages available on your storage array.

View/End iSCSI Sessions

Figure 11 Change the management interface mode by using the SANtricity System Manager GUI

Select Change Management Interface



Additional Settings

Change Cache Settings
Define the cache block size and cache flush settings to values appropriate for your storage array.

Enable/Disable Automatic Load Balancing
Set the automatic load balancing feature to allow incoming traffic from the hosts to be dynamically managed and balanced across both controllers.
Your automatic load balancing is **currently enabled**.

Change Default Host Operating System Type
Change the default host operating system when you are first connecting hosts to the storage array or when you are connecting additional hosts.

Change Management Interface
Change the management interface to enforce confidentiality between the storage array and the management client or to access external tools.
The legacy management interface is **currently off**.

Caution

See "5. Certificate Management" (page 24) for a full explanation of how to configure the array management interfaces to enable secure communications.

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.

Caution

You must install SANtricity System Manager 11.60 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\SystemManager\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\SystemManager\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.

C:\Program Files\SystemManager\client>
```

Caution

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 2 Connection behavior when using -u <username> in SMcli commands

Command Syntax	ETERNUS AB2100/AB5100/AB6100 and ETERNUS HB1000/HB2000/HB5000; Legacy SYMbol- On	ETERNUS AB2100/AB5100/AB6100 and ETERNUS HB1000/HB2000/HB5000; HTTPS - On
...> SMcli <IP Address> -u <username> -p <Password> -c <"command=\"argument\">";	SMcli uses a legacy SYMbol connection to the system	SMcli uses a secure HTTPS connection to the system
...> SMcli <IP Address> -p <Password> -c <"command=\"argument\">";	SMcli uses a legacy SYMbol connection to the system	Command fails, indicating that network errors were detected

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 system, 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 the command execution is terminated. The SMcli-to-role mappings are set and cannot be modified by the user.

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.

4. Audit Log

SANtricity OS has 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 storage system.

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

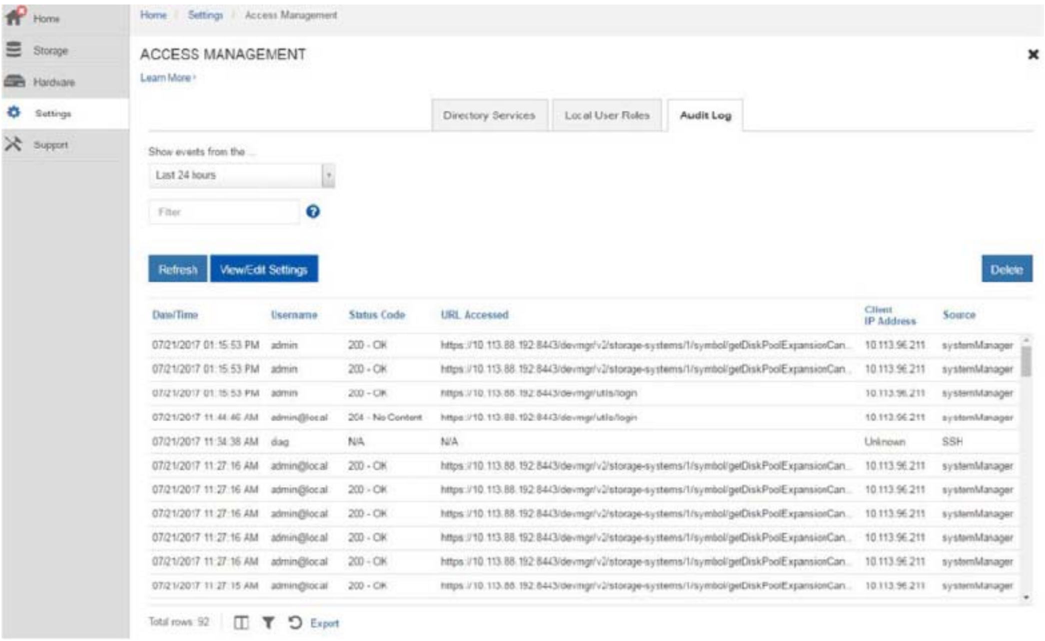
Table 3 Audit Log Scope

Management Access Interface	Audit Log Scope
System Manager GUI	All user activities, including login and logout, session establishment and termination, invoked actions and requests, and their respective outcomes.
Secure SMcli	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.
Web Services API	All user activities, including login and logout, session establishment and termination, invoked actions and requests, and their respective outcomes.
Support Shell Interface	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.

The logs are persisted on the storage system in the non-volatile 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 12 shows the audit log in SANtricity System Manager under Settings > Access Management > Audit Log.

Figure 12 SANtricity System Manager page to view the audit log



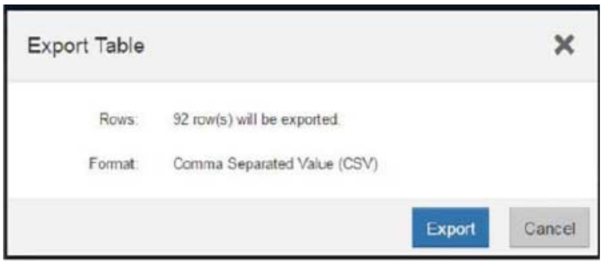
Show events from the ...
Last 24 hours

Date/Time	Username	Status Code	URL Accessed	Client IP Address	Source
07/21/2017 01:15:53 PM	admin	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 01:15:53 PM	admin	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 01:15:53 PM	admin	200 - OK	https://10.113.88.192:8443/devmgr/utils/login	10.113.96.211	systemManager
07/21/2017 11:44:46 AM	admin@local	204 - No Content	https://10.113.88.192:8443/devmgr/utils/login	10.113.96.211	systemManager
07/21/2017 11:34:38 AM	diag	N/A	N/A	Unknown	SSH
07/21/2017 11:27:16 AM	admin@local	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 11:27:16 AM	admin@local	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 11:27:16 AM	admin@local	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 11:27:16 AM	admin@local	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 11:27:16 AM	admin@local	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager
07/21/2017 11:27:15 AM	admin@local	200 - OK	https://10.113.88.192:8443/devmgr/v2/storage-systems/1/symbol/getDiskPoolExpansionCan...	10.113.96.211	systemManager

Total rows: 92

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 13 shows the Export Table dialog box.

Figure 13 SANtricity System Manager dialog box to export the audit log



Export Table

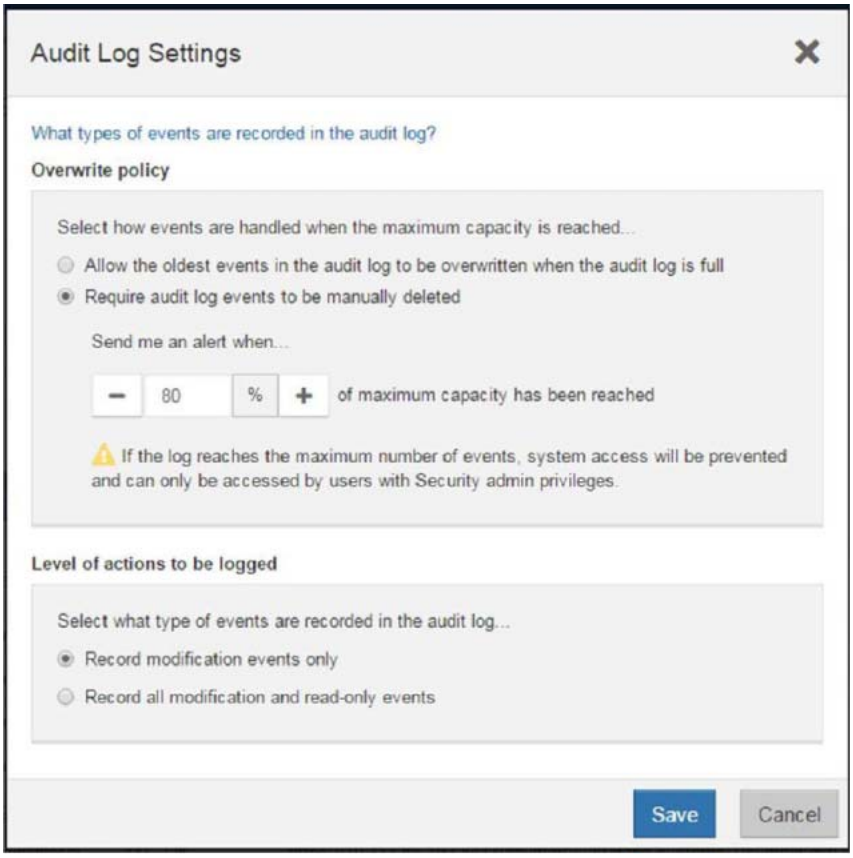
Rows: 92 row(s) will be exported.

Format: Comma Separated Value (CSV)

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 14 shows the page where the audit log settings are managed.

Figure 14 SANtricity System Manager page to configure the audit log settings



Audit Log Settings

What types of events are recorded in the audit log?

Overwrite policy

Select how events are handled when the maximum capacity is reached...

○ Allow the oldest events in the audit log to be overwritten when the audit log is full

● Require audit log events to be manually deleted

Send me an alert when...

− 80 % + of maximum capacity has been reached

⚠ If the log reaches the maximum number of events, system access will be prevented and can only be accessed by users with Security admin privileges.

Level of actions to be logged

Select what type of events are recorded in the audit log...

● Record modification events only

○ Record all modification and read-only events

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. The following workflows are described later in this section:

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

The certificate management feature is introduced in SANtricity System Manager to:

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

SANtricity WSP supports certificate management to enable secure communications between a server running the Web Services proxy software and the supported storage systems that are managed and monitored by the proxy.

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 4 Supported management features of the different management clients

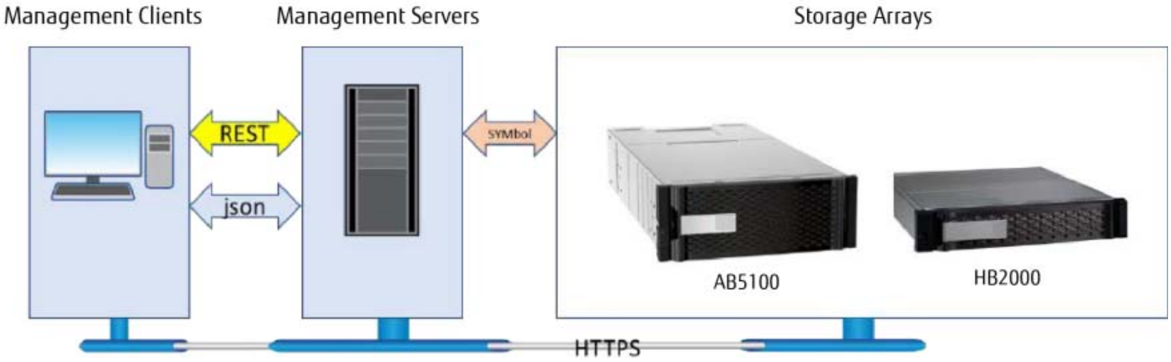
Management Client	Mirroring Feature	SMcli	Script Editor	Importing Settings from One System to Other Systems
SANtricity Web Services Proxy and Unified Manager	Mirroring is supported only for the ETERNUS AB/HB series systems	Not supported	Not supported	New feature to automate deploying new systems that use common settings (alerts, ASUP, storage configuration, and more)

Certificate Management for Web Services Proxy

Fujitsu Web Services are used in three areas. The Web Services Proxy resides on the server where the SANtricity software is installed. The 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 Web Services Proxy, a standalone Fujitsu SANtricity WSP can be installed on a Windows or Linux server. This proxy provides Web Services APIs to configure, manage, and monitor the ETERNUS AB/HB series systems. The proxy provides access to a collection of REST-style interfaces to access services defined for storage systems. Figure 15 is a high-level overview of the communications between client machines, the Web Services Proxy running on a server, and the ETERNUS AB/HB series systems.

Figure 15 Communications between management clients and Web Services Proxy installed on a server



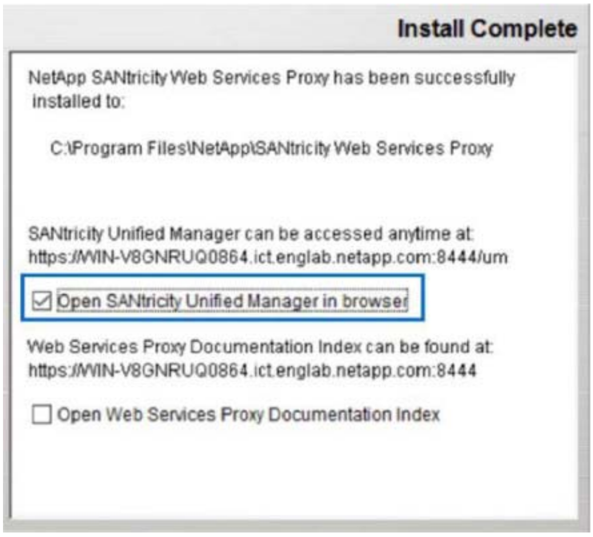
The third Web Services implementation is the SANtricity System Manager Web Services, the embedded version residing on the array controller. Similarly, clients access the Web Services through standard HTTPS mechanisms. As the Web Services satisfy the client request through collecting data or executing configuration change requests to the storage system, the Web Services module issues SYMbol requests to the storage systems.

WSP Certificate Management Using SANtricity Unified Manager

Included with SANtricity WSP 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 systems.

Procedure ▶▶▶

1 Open SANtricity Unified Manager from the WSP installation wizard or by navigating to https://<WSP Server FQDN>:<Secure Port #>/um.



Install Complete

NetApp SANtricity Web Services Proxy has been successfully installed to:

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

SANtricity Unified Manager can be accessed anytime at:
https://WIN-V8GNRUQ0864.ict.englab.netapp.com:8444/um

☑ Open SANtricity Unified Manager in browser

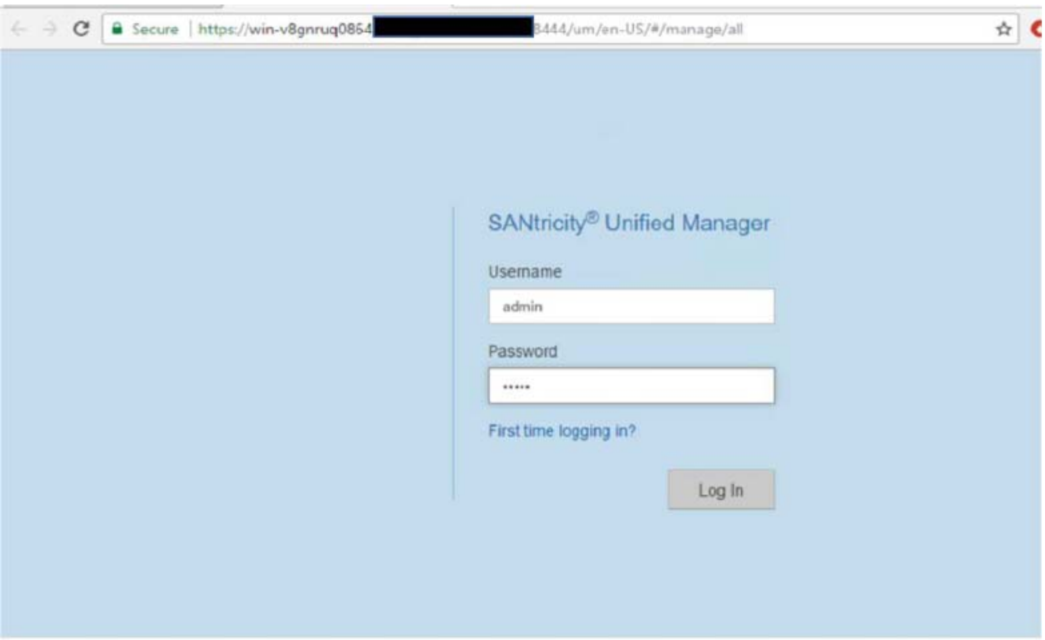
Web Services Proxy Documentation Index can be found at:
https://WIN-V8GNRUQ0864.ict.englab.netapp.com:8444

☐ Open Web Services Proxy Documentation Index

2 Log in as user = admin and password = admin.

Caution

If you have changed the default admin account password, log in with that new password.



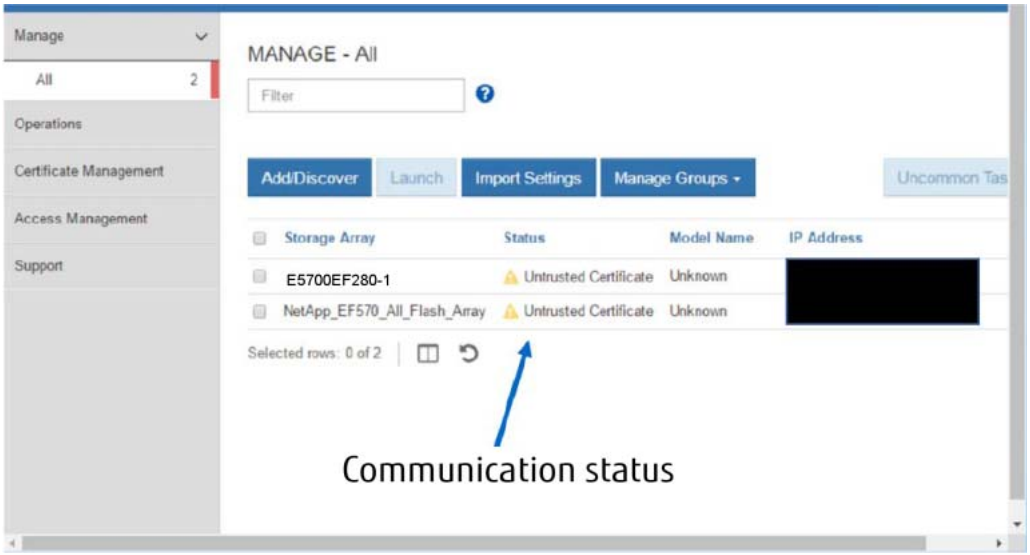
Secure | https://win-v8gnruq0864[redacted]444/um/en-US/#/manage/all

SANtricity® Unified Manager

Username: admin

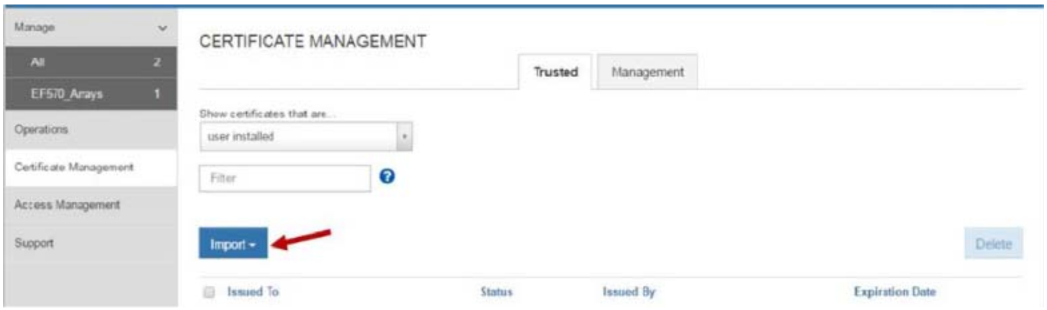
Password: •••••

Discovered systems are displayed on the landing page, including the communication status to each array.



Storage Array	Status	Model Name	IP Address
E5700EF280-1	⚠ Untrusted Certificate	Unknown	[redacted]
NetApp_EF570_All_Flash_Array	⚠ Untrusted Certificate	Unknown	[redacted]

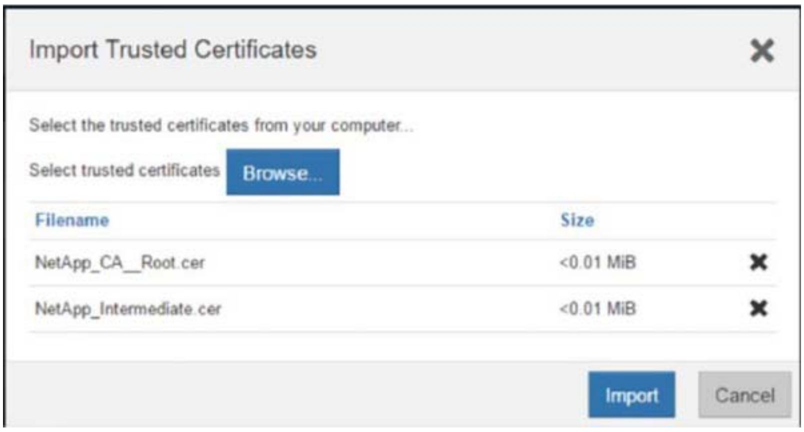
3 Navigate to the Certificate Management tab and select Import.



Show certificates that are... user installed

Issued To	Status	Issued By	Expiration Date

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.

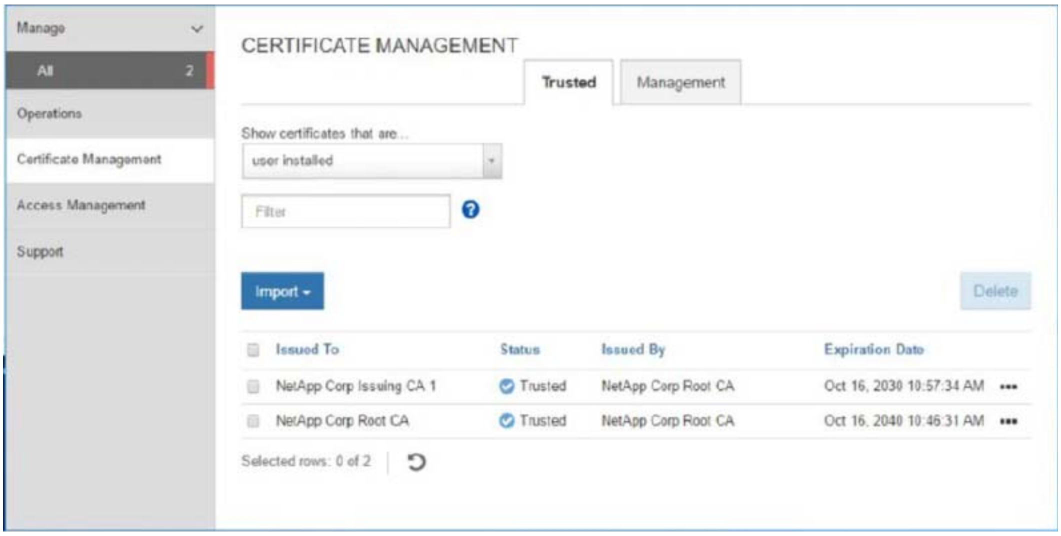


Select the trusted certificates from your computer...

Select trusted certificates

Filename	Size
NetApp_CA__Root.cer	<0.01 MiB
NetApp_Intermediate.cer	<0.01 MiB

The newly imported certificates are displayed in the Certificate Management pane.



CERTIFICATE MANAGEMENT

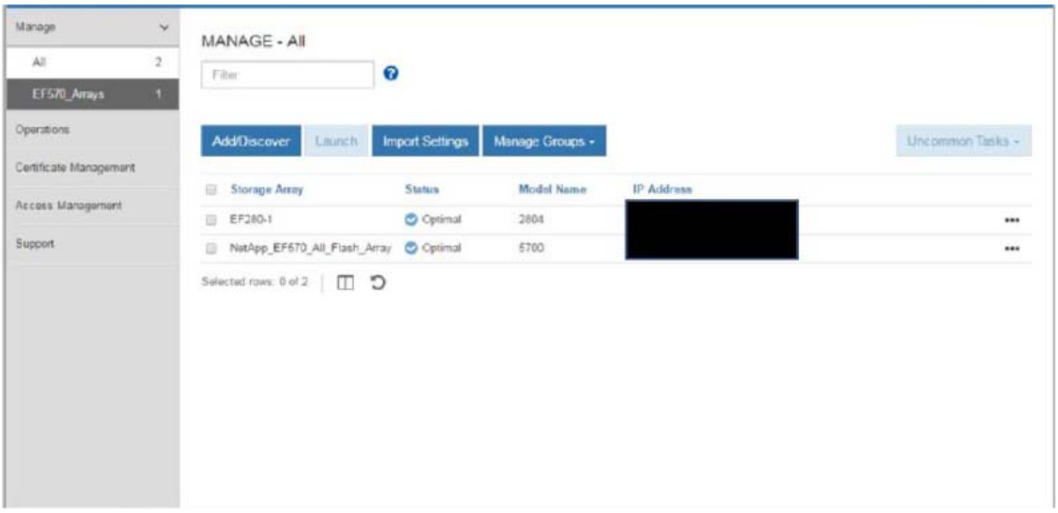
Show certificates that are...

user installed

□	Issued To	Status	Issued By	Expiration Date	
□	NetApp Corp Issuing CA 1	✓ Trusted	NetApp Corp Root CA	Oct 16, 2030 10:57:34 AM	•••
□	NetApp Corp Root CA	✓ Trusted	NetApp Corp Root CA	Oct 16, 2040 10:46:31 AM	•••

Selected rows: 0 of 2

This resolves certificate issues with systems that have a CA certificate installed.



MANAGE - All

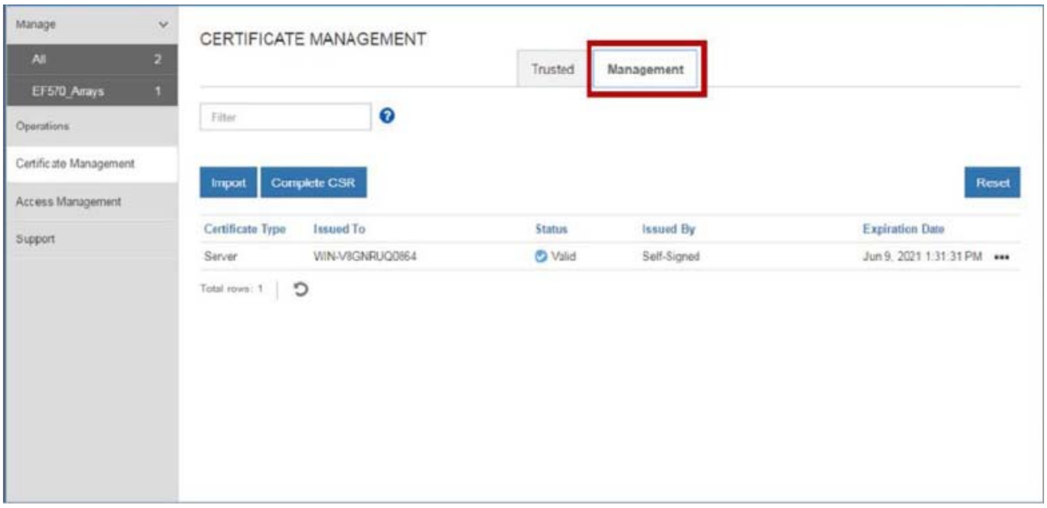
□	Storage Array	Status	Model Name	IP Address	
□	EF280-1	✓ Optimal	2804	[redacted]	•••
□	NetApp_EF570_All_Flash_Array	✓ Optimal	5700	[redacted]	•••

Selected rows: 0 of 2

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.

5 Navigate to the Certificate Management tab, click Management, and execute a Reset to regenerate a new self-signed certificate on the web server.

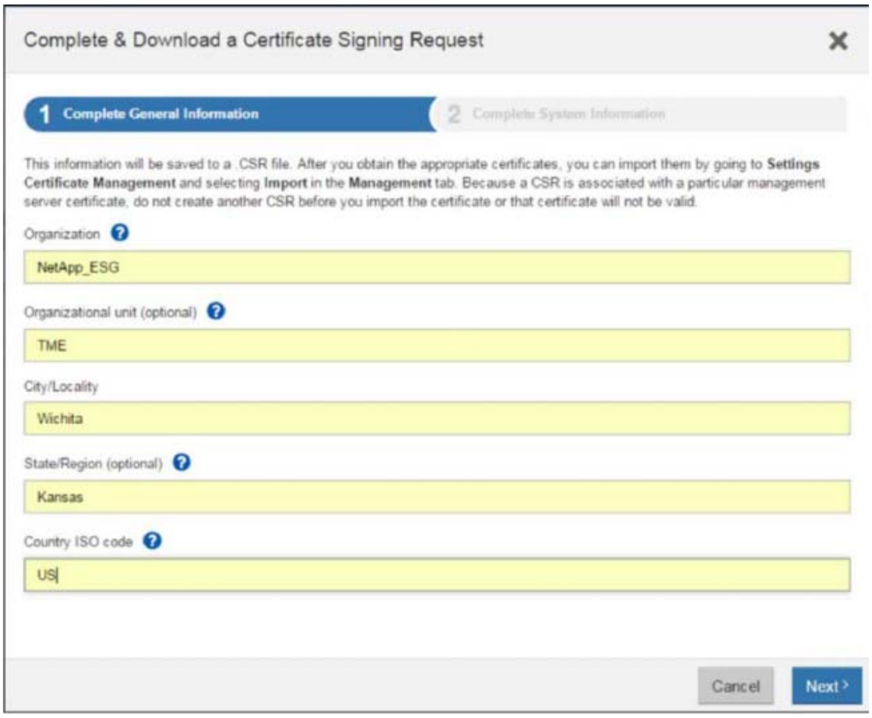
After your browser refreshes, the browser might block access to the destination site and report that the site is using HTTP Strict Transport Security. This condition arises when you switch back to self-signed certificates. To clear the condition that is blocking access to the destination, you must clear the browsing data from the browser.



CERTIFICATE MANAGEMENT

Certificate Type	Issued To	Status	Issued By	Expiration Date
Server	WIN-V8GNRUQ0864	✓ Valid	Self-Signed	Jun 9, 2021 1:31:31 PM

6 Select the Complete CSR tab and follow the wizard to complete the CSR.



Complete & Download a Certificate Signing Request

This information will be saved to a .CSR file. After you obtain the appropriate certificates, you can import them by going to **Settings Certificate Management** and selecting **Import** in the **Management** tab. Because a CSR is associated with a particular management server certificate, do not create another CSR before you import the certificate or that certificate will not be valid.

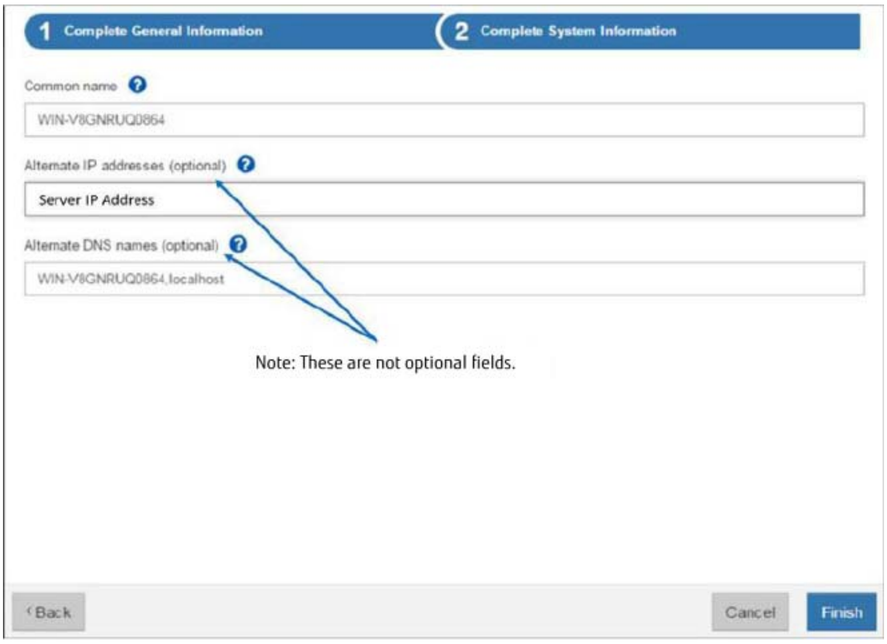
Organization: NetApp_ESG

Organizational unit (optional): TME

City/Locality: Wichita

State/Region (optional): Kansas

Country ISO code: US



Common name
WIN-V8GNRUQ0864

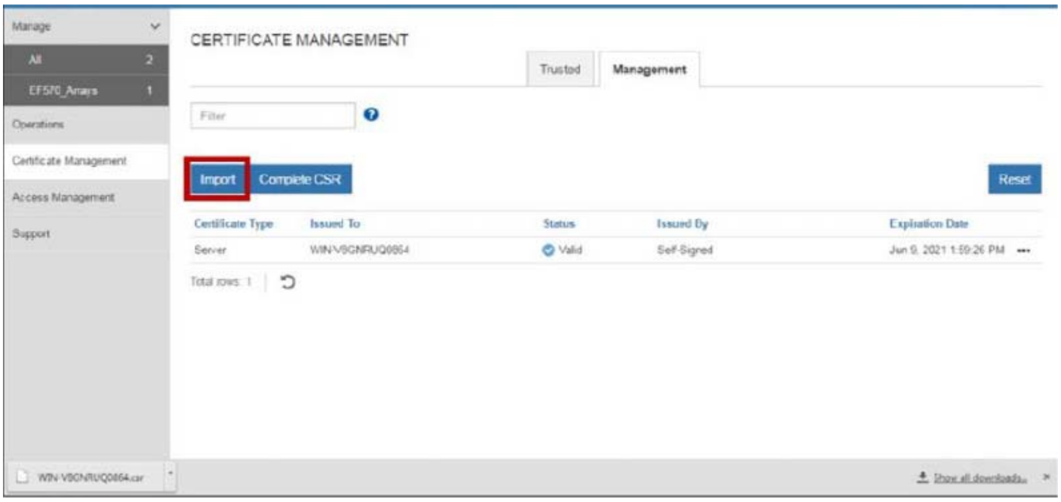
Alternate IP addresses (optional)
Server IP Address

Alternate DNS names (optional)
WIN-V8GNRUQ0864,localhost

Note: These are not optional fields.

7 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).

8 Import the new certificates by using the Import wizard.

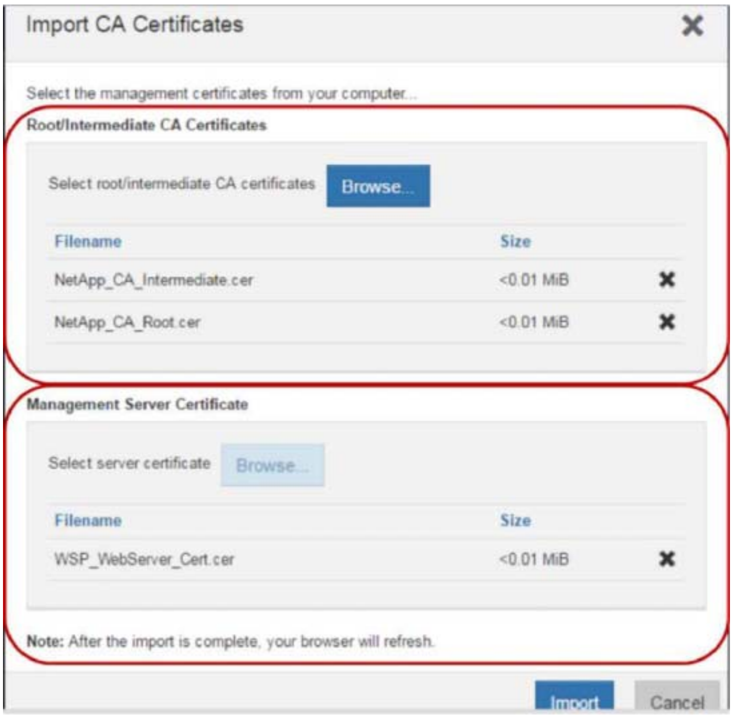


CERTIFICATE MANAGEMENT

Certificate Type	Issued To	Status	Issued By	Expiration Date
Server	WIN-V8GNRUQ0864	Valid	Self-Signed	Jun 9, 2021 1:59:26 PM

Total rows: 1

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



Import CA Certificates

Select the management certificates from your computer...

Root/Intermediate CA Certificates

Select root/intermediate CA certificates

Filename	Size
NetApp_CA_Intermediate.cer	<0.01 MiB
NetApp_CA_Root.cer	<0.01 MiB

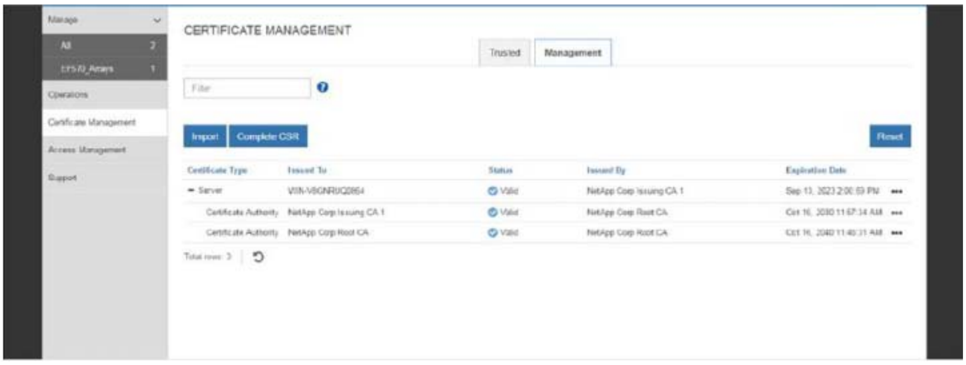
Management Server Certificate

Select server certificate

Filename	Size
WSP_WebServer_Cert.cer	<0.01 MiB

Note: After the import is complete, your browser will refresh.

10 After the web server is imported it restarts, the browser window resets, and the browser session is secure. Start a new browser session.



CERTIFICATE MANAGEMENT

Certificate Type	Issued To	Status	Issued By	Expiration Date
Server	VIIN-V8GNRUQ0854	Valid	NetApp Corp Issuing CA 1	Sep 13, 2023 2:00:59 PM
Certificate Authority	NetApp Corp Issuing CA 1	Valid	NetApp Corp Root CA	Oct 16, 2030 11:57:14 AM
Certificate Authority	NetApp Corp Root CA	Valid	NetApp Corp Root CA	Oct 16, 2040 11:40:31 AM

Total rows: 3

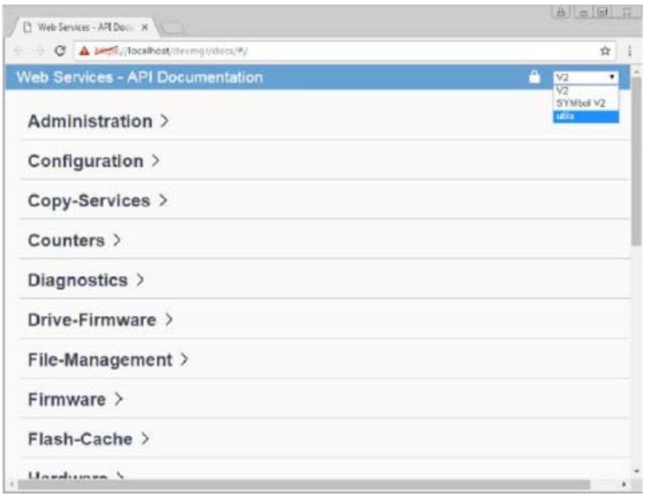
Accessing the Web Services REST API

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 16 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/#/.

Caution

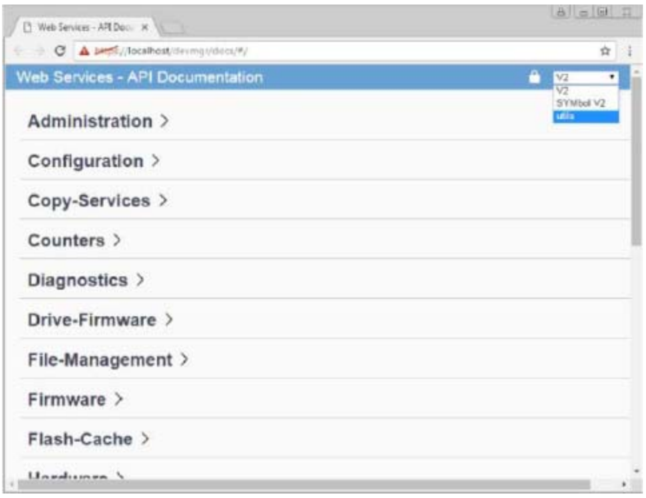
The default secure port is 8443, but depending on the server where SANtricity WSP is installed, the proxy might switch to a different port number. As a result, the port for this application could be different in your environment.

Logging in to the Web Services Proxy as Admin

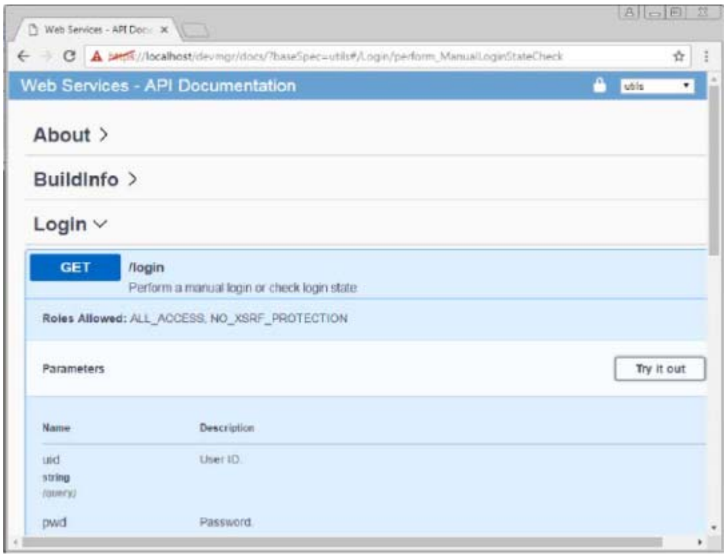
To confirm that you can log in to the target web server, including the access permissions associated with the security admin role, follow these steps.

Procedure ▶▶▶

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



2 Expand the Login commands and select the Get:/ login command.


Web Services - API Doc
~~https~~://localhost/devmgr/docs/?baseSpec=utils#/Login/perform_ManualLoginStateCheck
Web Services - API Documentation
utils
About >
BuildInfo >
Login ∨
GET
/login

Perform a manual login or check login state

Roles Allowed: ALL_ACCESS, NO_XSRF_PROTECTION

Parameters

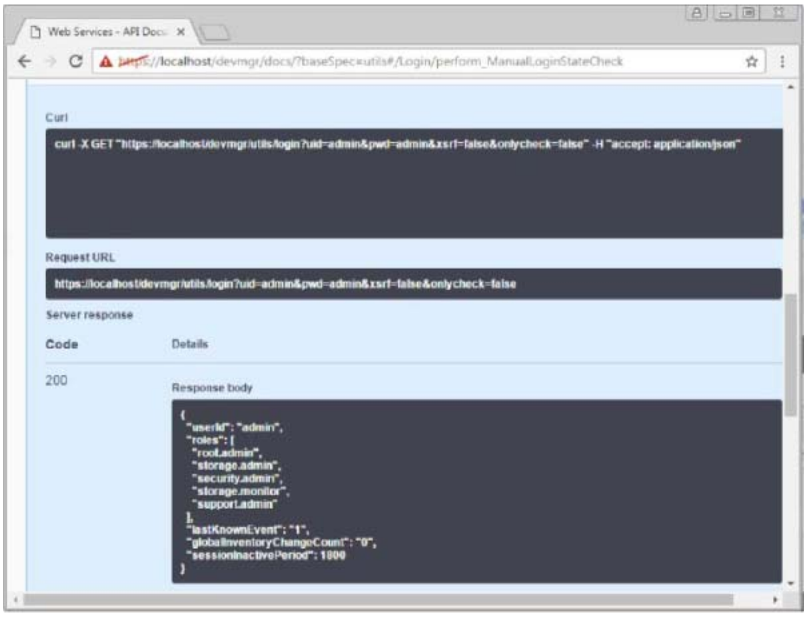
Try it out

Name	Description
uid string (query)	User ID.
pwd	Password.

3 Click Try It Out, edit the user ID and password to be user = admin / password = admin, and click Execute.

Caution

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.


Web Services - API Docu
~~https~~://localhost/devmgr/docs/?baseSpec=utils#/Login/perform_ManualLoginStateCheck

Curl

```
curl -X GET "https://localhost/devmgr/utils/login?uid=admin&pwd=admin&xsrf=false&onlycheck=false" -H "accept: application/json"
```

Request URL

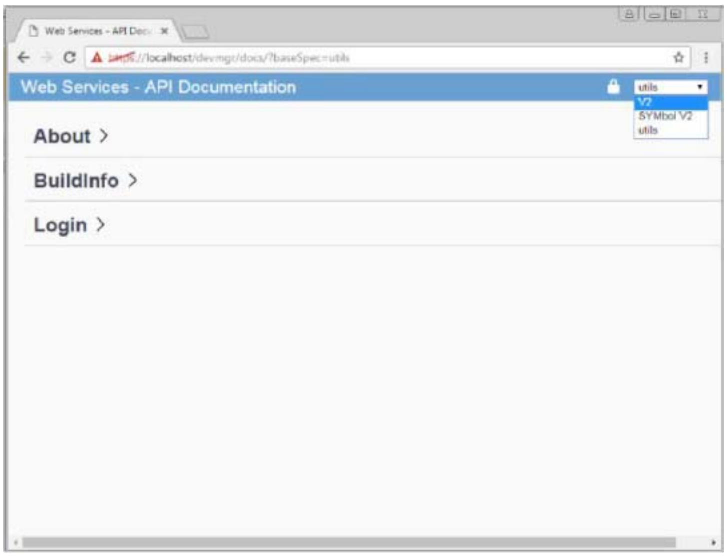
```
https://localhost/devmgr/utils/login?uid=admin&pwd=admin&xsrf=false&onlycheck=false
```

Server response

Code	Details
200	Response body

```
{
  "userId": "admin",
  "roles": [
    "root.admin",
    "storage.admin",
    "security.admin",
    "storage.monitor",
    "support.admin"
  ],
  "lastKnownEvent": "1",
  "globalInventoryChangeCount": "0",
  "sessionInactivePeriod": 1800
}
```

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

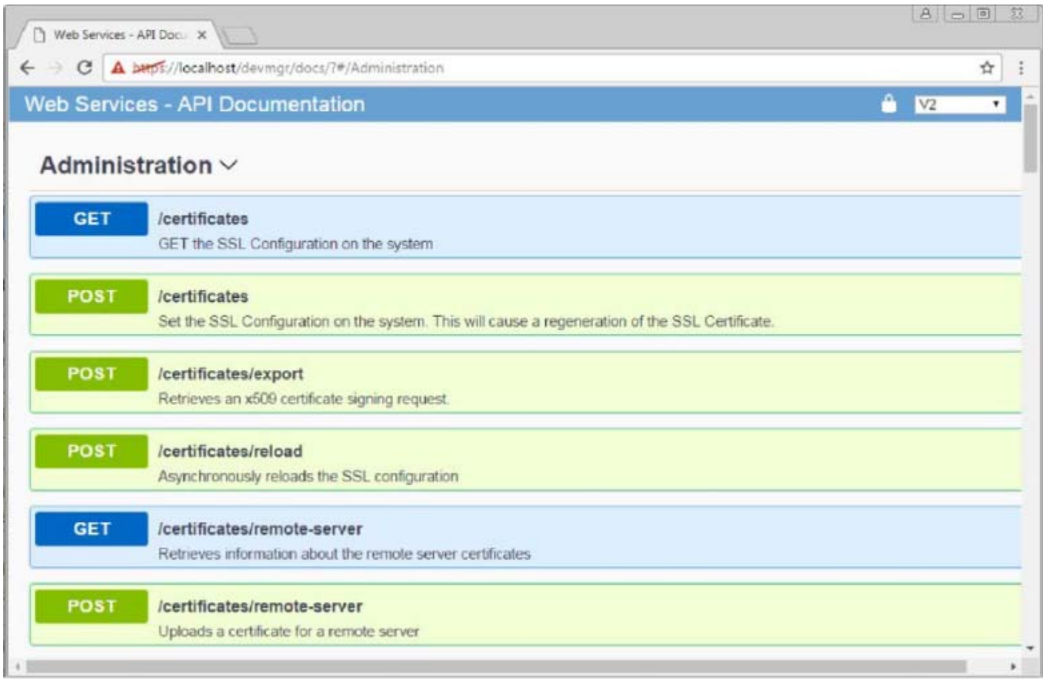

Web Services - API Docu
~~https~~://localhost/devmgr/docs/?baseSpec=utils
Web Services - API Documentation
utils
V2
SYMbol V2
utils
About >
BuildInfo >
Login >

Installing Web Services Proxy Security Certificates by Using WSP

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

Procedure ▶▶▶

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



Web Services - API Documentation

Administration

GET /certificates
GET the SSL Configuration on the system

POST /certificates
Set the SSL Configuration on the system. This will cause a regeneration of the SSL Certificate.

POST /certificates/export
Retrieves an x509 certificate signing request.

POST /certificates/reload
Asynchronously reloads the SSL configuration

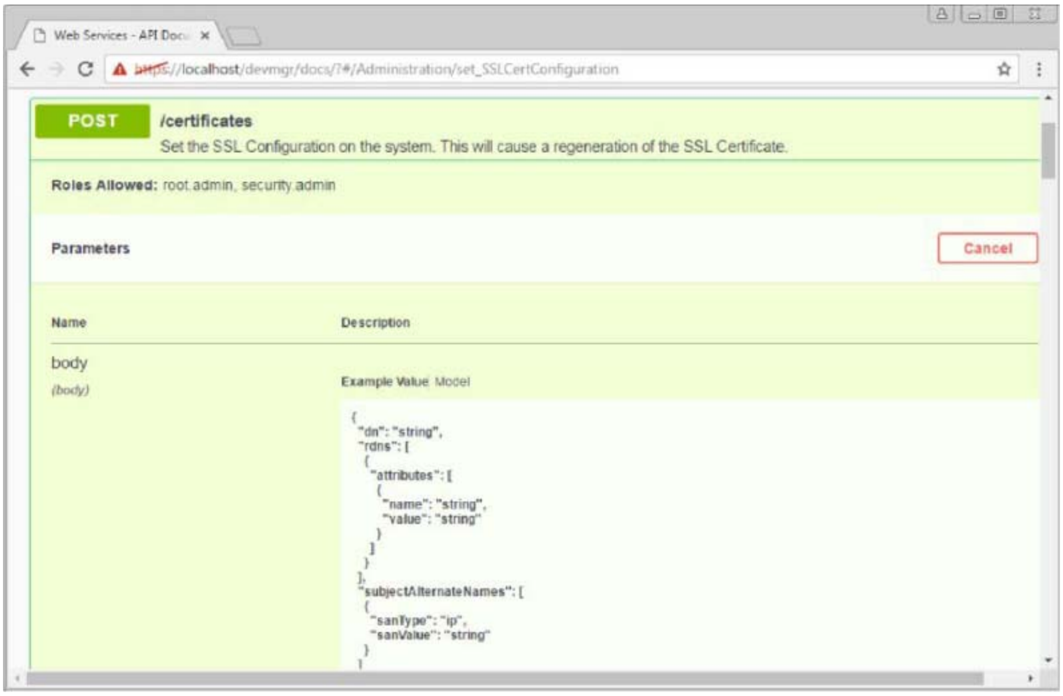
GET /certificates/remote-server
Retrieves information about the remote server certificates

POST /certificates/remote-server
Uploads a certificate for a remote server

2 Select POST:/certificates and then click Try It Out.

Caution

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.



https://localhost/devmgr/docs/?#/Administration/set_SSLCertConfiguration

/certificates

Set the SSL Configuration on the system. This will cause a regeneration of the SSL Certificate.

Roles Allowed: root.admin, security.admin

Parameters

Name	Description
body *(body)*	**Example Value** Model

```
{
  "dn": "string",
  "rdns": [
    {
      "attributes": [
        {
          "name": "string",
          "value": "string"
        }
      ]
    }
  ],
  "subjectAlternateNames": [
    {
      "sanType": "ip",
      "sanValue": "string"
    }
  ]
```

3 Add the required information in the Example values pane to generate a valid CA certificate and then run the commands.

Caution

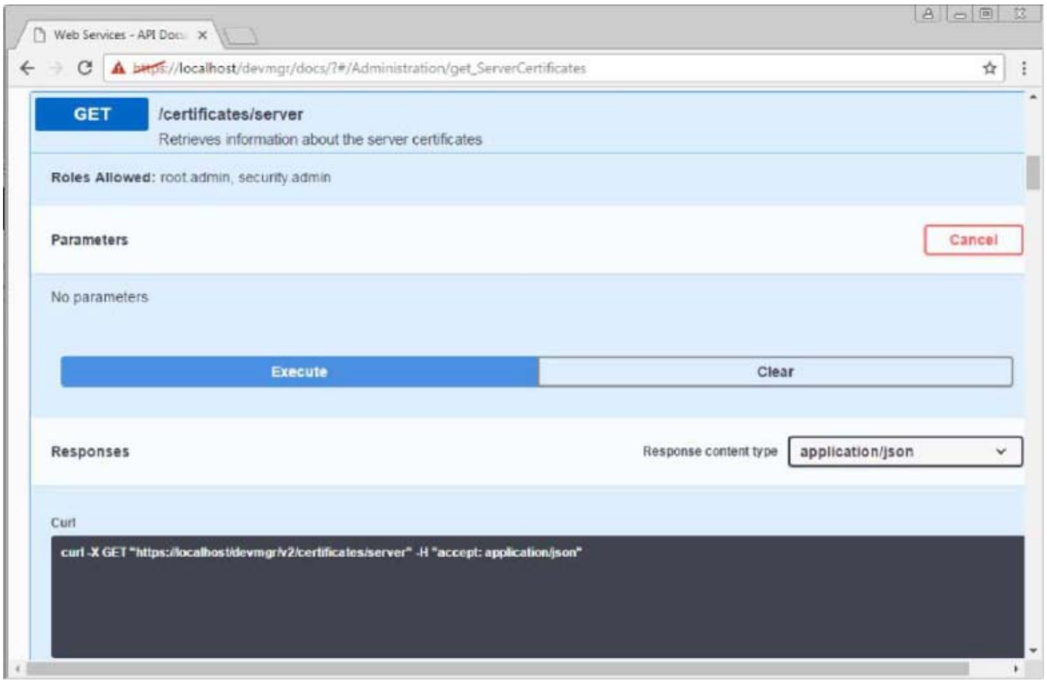
To find the valid DN attributes, refer to https://www.ietf.org/rfc/rfc2253.txt. This example is for customers who are based in the United States.

```
{
  "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_Origianization_Unit"
       },
       {
         "name": "L",
         "value": "Enter_Location"
       },
       {
         "name": "ST",
         "value": "Enter_State"
       },
       {
         "name": "C",
         "value": "US"
       }
      ]
     }
    ],
    "subjectAlternateNames": [
      {
       "sanType": "dns",
       "sanValue": "Enter_server_FQDN"
     },
     {
       "sanType": "ip",
       "sanValue": "Enter_server_IP"
     }
    ]
}
```

Caution

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.



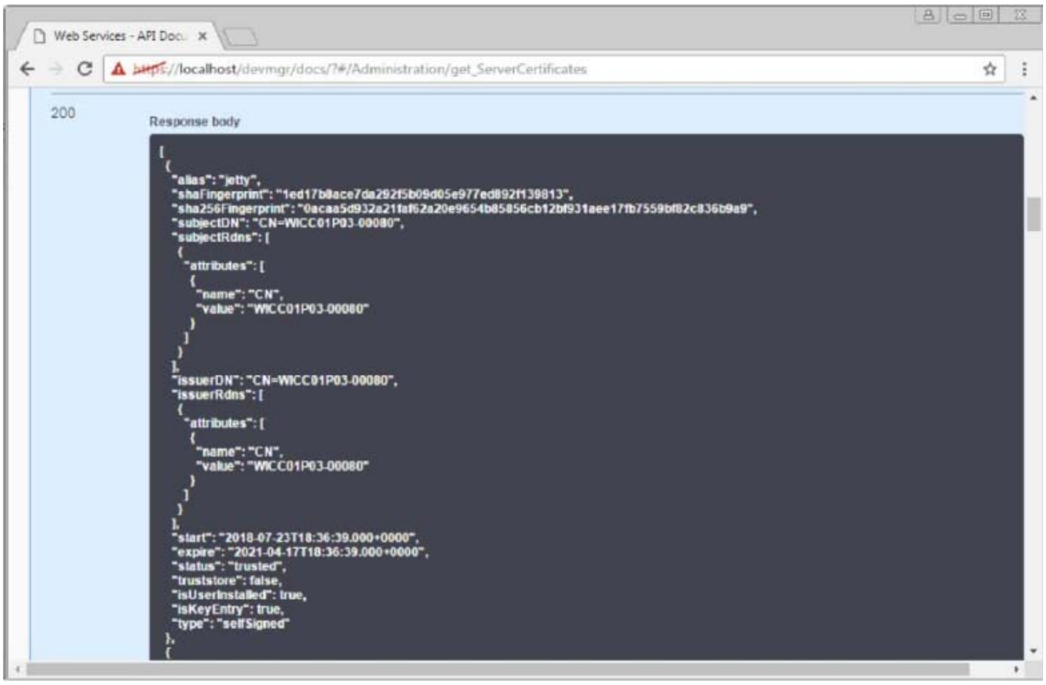
/certificates/server

Retrieves information about the server certificates

Roles Allowed: root.admin, security.admin

No parameters

```
curl -X GET "https://localhost/devmgr/v2/certificates/server" -H "accept: application/json"
```

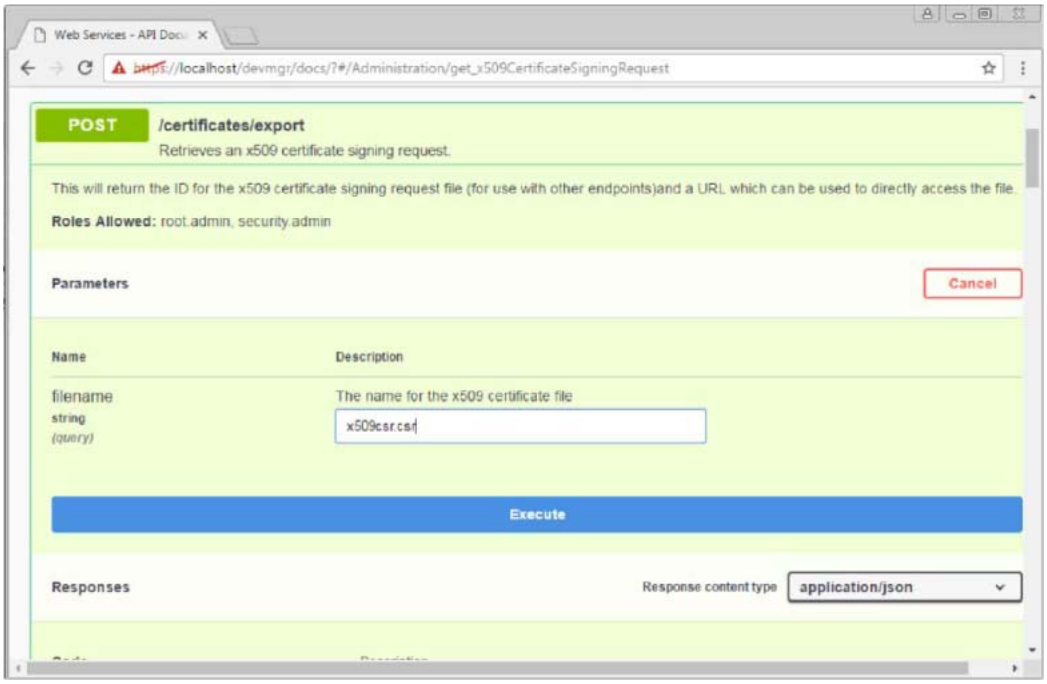

Web Services - API Doc
https://localhost/devmgr/docs/?#/Administration/get_ServerCertificates
200
Response body

```
[
 {
  "alias": "jetty",
  "shaFingerprint": "1ed17b8ace7da292f5b09d05e977ed892f139813",
  "sha256Fingerprint": "0acaa5d932a21faf62a20e9654b85856cb12bf931aee17fb7559bf82c836b9a9",
  "subjectDN": "CN=WICC01P03-00080",
  "subjectRdns": [
   {
    "attributes": [
     {
      "name": "CN",
      "value": "WICC01P03-00080"
     }
    ]
   }
  ],
  "issuerDN": "CN=WICC01P03-00080",
  "issuerRdns": [
   {
    "attributes": [
     {
      "name": "CN",
      "value": "WICC01P03-00080"
     }
    ]
   }
  ],
  "start": "2018-07-23T18:36:39.000+0000",
  "expire": "2021-04-17T18:36:39.000+0000",
  "status": "trusted",
  "truststore": false,
  "isUserInstalled": true,
  "isKeyEntry": true,
  "type": "selfSigned"
 },
 {
```

Caution

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.



Web Services - API Doc
https://localhost/devmgr/docs/?#/Administration/get_x509CertificateSigningRequest
POST
Cancel
Execute
application/json

/certificates/export

Retrieves an x509 certificate signing request.

This will return the ID for the x509 certificate signing request file (for use with other endpoints)and a URL which can be used to directly access the file.

Roles Allowed: root.admin, security.admin

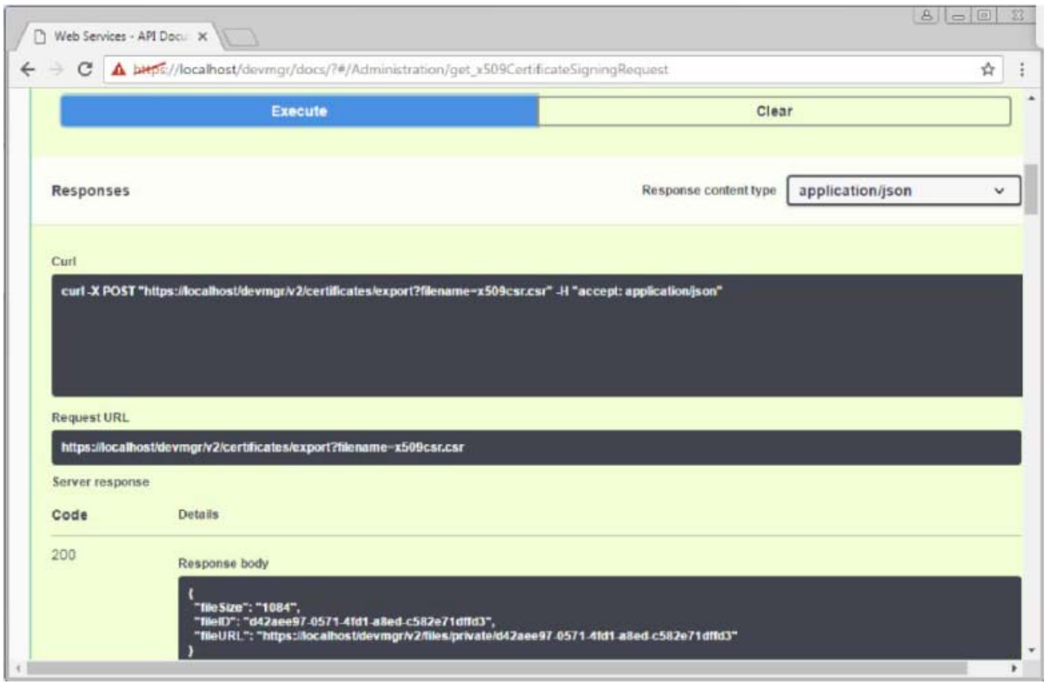
Parameters

Name	Description
filename string *(query)*	The name for the x509 certificate file x509csr.csr

Responses

Response content type: application/json

6 Copy and paste the file URL into a new browser tab to download the CSR file.



Web Services - API Doc
https://localhost/devmgr/docs/?#/Administration/get_x509CertificateSigningRequest
Execute
Clear
application/json

Responses

Response content type: application/json

Curl

```
curl -X POST "https://localhost/devmgr/v2/certificates/export?filename=x509csr.csr" -H "accept: application/json"
```

Request URL

```
https://localhost/devmgr/v2/certificates/export?filename=x509csr.csr
```

Server response

Code	Details
200	Response body

```
{
 "fileSize": "1084",
 "fileID": "d42aee97-0571-4fd1-a8ed-c582e71dffd3",
 "fileURL": "https://localhost/devmgr/v2/files/private/d42aee97-0571-4fd1-a8ed-c582e71dffd3"
}
```

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.

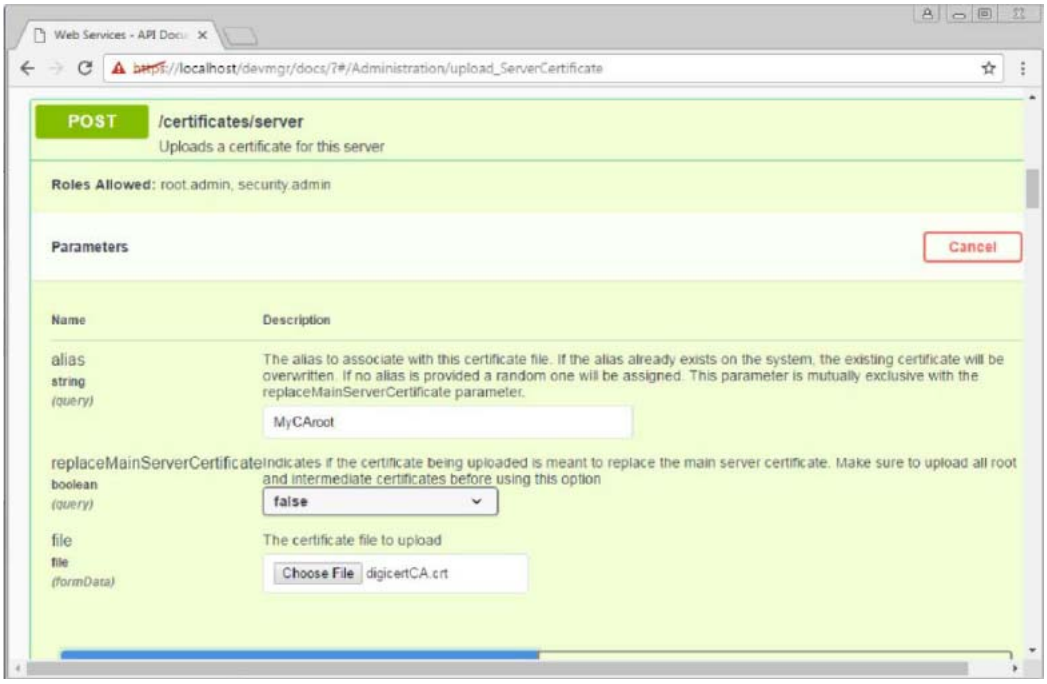
9-1 Expand the POST:/sslconfig/server endpoint and click Try It Out.

9-2 Enter a name for the CA root certificate in the alias field.

9-3 Select false in the replaceMainServerCertificate field.

9-4 Browse to and select the new CA root certificate.

9-5 Click Execute.



~~https~~://localhost/devmgr/docs/?#/Administration/upload_ServerCertificate

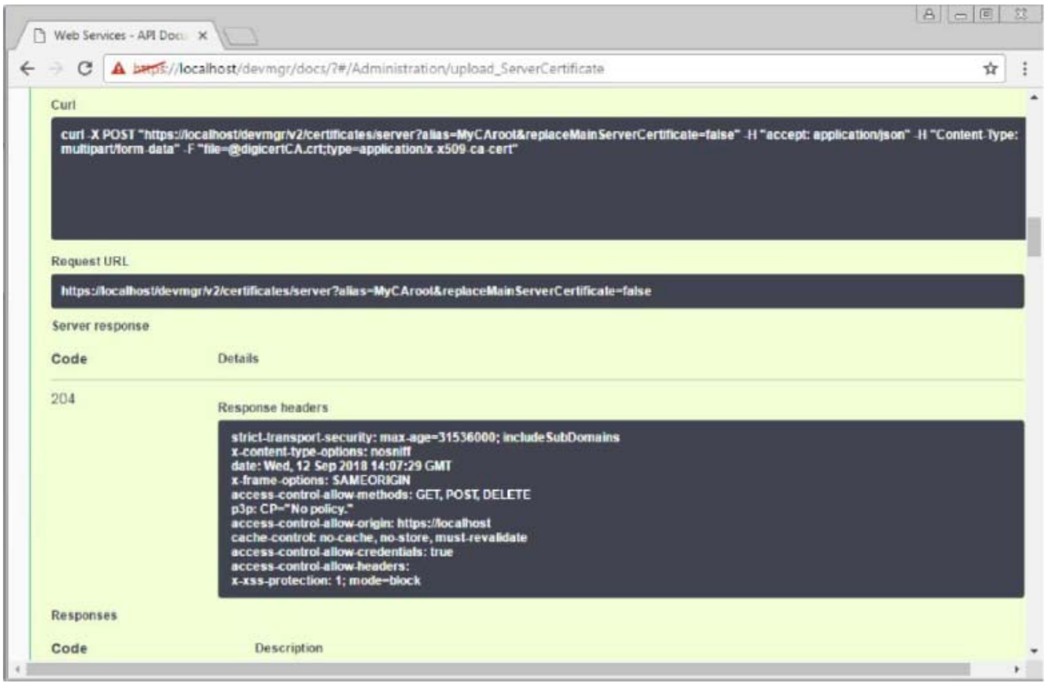
/certificates/server
Uploads a certificate for this server

Roles Allowed: root.admin, security.admin

Parameters

Name	Description
alias string *(query)*	The alias to associate with this certificate file. If the alias already exists on the system, the existing certificate will be overwritten. If no alias is provided a random one will be assigned. This parameter is mutually exclusive with the replaceMainServerCertificate parameter. MyCAroot
replaceMainServerCertificate boolean *(query)*	Indicates if the certificate being uploaded is meant to replace the main server certificate. Make sure to upload all root and intermediate certificates before using this option false
file file *(formData)*	The certificate file to upload digicertCA.crt

9-6 Confirm that the certificate upload was successful.



Web Services - API Doc
~~https~~://localhost/devmgr/docs/?#/Administration/upload_ServerCertificate

Curl

```
curl -X POST "https://localhost/devmgr/v2/certificates/server?alias=MyCAroot&replaceMainServerCertificate=false" -H "accept: application/json" -H "Content-Type:
multipart/form-data" -F "file=@digicertCA.crt;type=application/x-x509-ca-cert"
```

Request URL

```
https://localhost/devmgr/v2/certificates/server?alias=MyCAroot&replaceMainServerCertificate=false
```

Server response

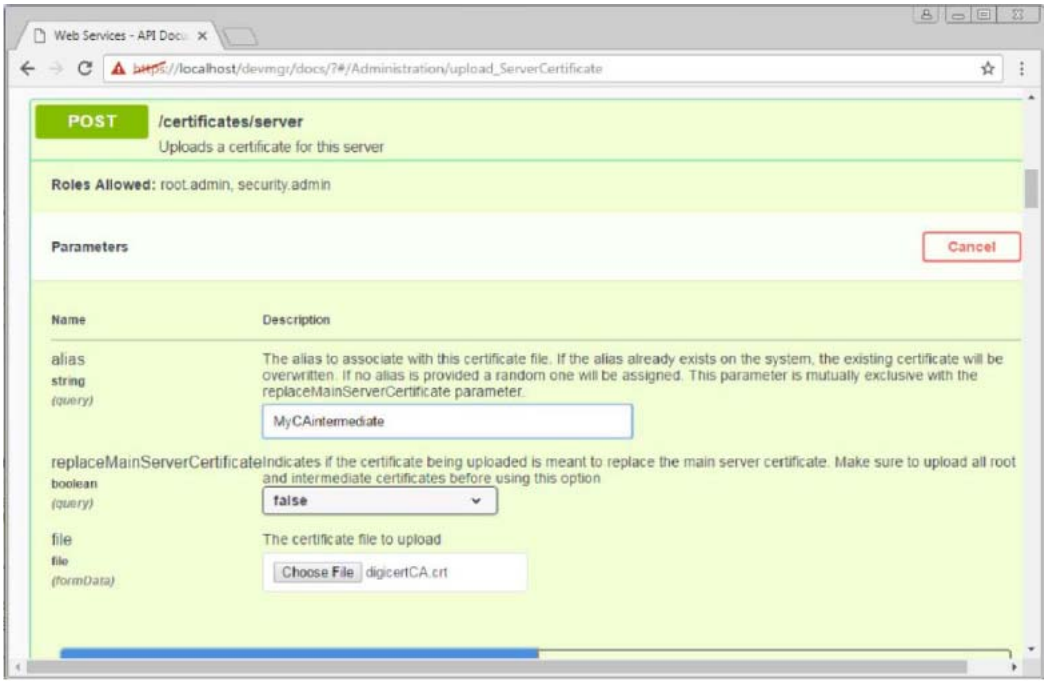
Code	Details
204	Response headers

```
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
date: Wed, 12 Sep 2018 14:07:29 GMT
x-frame-options: SAMEORIGIN
access-control-allow-methods: GET, POST, DELETE
p3p: CP="No policy."
access-control-allow-origin: https://localhost
cache-control: no-cache, no-store, must-revalidate
access-control-allow-credentials: true
access-control-allow-headers:
x-xss-protection: 1; mode=block
```

Responses

Code	Description

9-7 Repeat the CA certificate upload procedure for the CA intermediate certificate.



Web Services - API Doc
~~https~~://localhost/devmgr/docs/?#/Administration/upload_ServerCertificate
POST
Cancel
Choose File

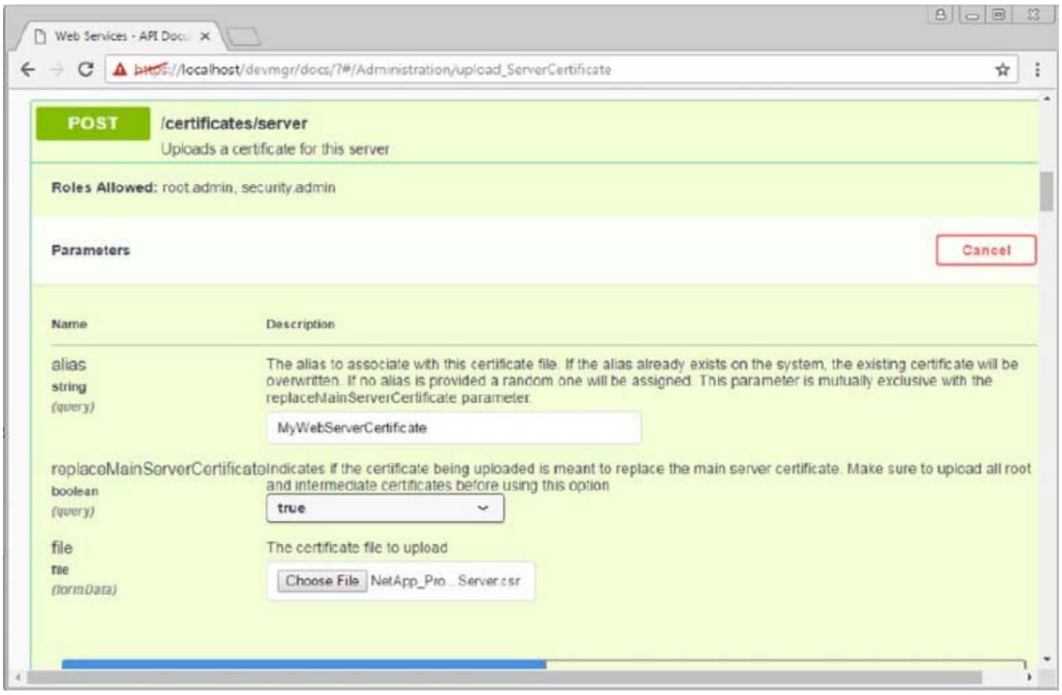
/certificates/server
Uploads a certificate for this server

Roles Allowed: root.admin, security.admin

Parameters

Name	Description
alias string *(query)*	The alias to associate with this certificate file. If the alias already exists on the system, the existing certificate will be overwritten. If no alias is provided a random one will be assigned. This parameter is mutually exclusive with the replaceMainServerCertificate parameter. MyCAintermediate
replaceMainServerCertificate boolean *(query)*	Indicates if the certificate being uploaded is meant to replace the main server certificate. Make sure to upload all root and intermediate certificates before using this option false
file file *(formData)*	The certificate file to upload Choose File digicertCA.crt

9-8 Repeat the certificate upload procedure for the new web server security certificate file. Select True from the replaceMainServerCertificate drop-down menu.


Web Services - API Docu
https://localhost/devmgr/docs/?#/Administration/upload_ServerCertificate
POST
Cancel
Choose File

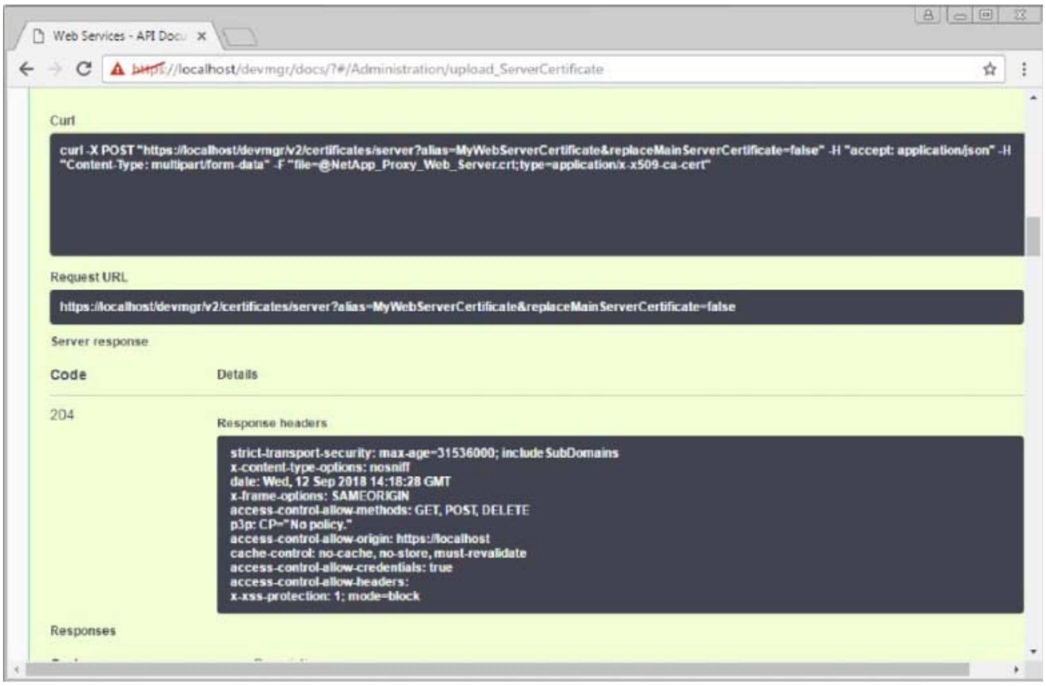
/certificates/server
Uploads a certificate for this server

Roles Allowed: root.admin, security.admin

Parameters

Name	Description
alias string *(query)*	The alias to associate with this certificate file. If the alias already exists on the system, the existing certificate will be overwritten. If no alias is provided a random one will be assigned. This parameter is mutually exclusive with the replaceMainServerCertificate parameter. MyWebServerCertificate
replaceMainServerCertificate boolean *(query)*	Indicates if the certificate being uploaded is meant to replace the main server certificate. Make sure to upload all root and intermediate certificates before using this option true
file file *(formData)*	The certificate file to upload NetApp_Pro...Server.csr

9-9 Confirm that the web server security certificate import was successful.


Web Services - API Docu
https://localhost/devmgr/docs/?#/Administration/upload_ServerCertificate

Curl

```
curl -X POST "https://localhost/devmgr/v2/certificates/server?alias=MyWebServerCertificate&replaceMainServerCertificate=false" -H "accept: application/json" -H
"Content-Type: multipart/form-data" -F "file=@NetApp_Proxy_Web_Server.crt;type=application/x-x509-ca-cert"
```

Request URL

```
https://localhost/devmgr/v2/certificates/server?alias=MyWebServerCertificate&replaceMainServerCertificate=false
```

Server response

Code: 204

Details

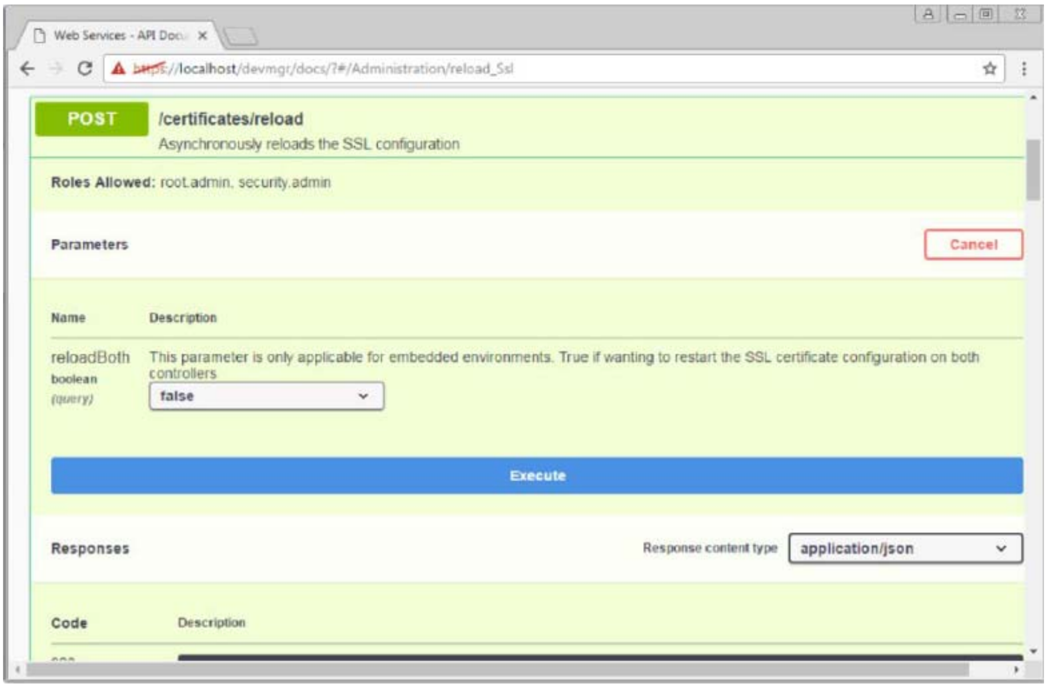
Response headers

```
strict-transport-security: max-age=31536000; includeSubDomains
x-content-type-options: nosniff
date: Wed, 12 Sep 2018 14:18:28 GMT
x-frame-options: SAMEORIGIN
access-control-allow-methods: GET, POST, DELETE
p3p: CP="No policy."
access-control-allow-origin: https://localhost
cache-control: no-cache, no-store, must-revalidate
access-control-allow-credentials: true
access-control-allow-headers:
x-xss-protection: 1; mode=block
```

Responses

9-10 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.



Web Services - API Doc
~~https~~://localhost/devmgr/docs/?#/Administration/reload_Ssl
POST
Cancel
Execute

/certificates/reload

Asynchronously reloads the SSL configuration

Roles Allowed: root.admin, security.admin

Parameters

Name	Description
reloadBoth boolean *(query)*	This parameter is only applicable for embedded environments. True if wanting to restart the SSL certificate configuration on both controllers false

Responses

Response content type: application/json

Code	Description

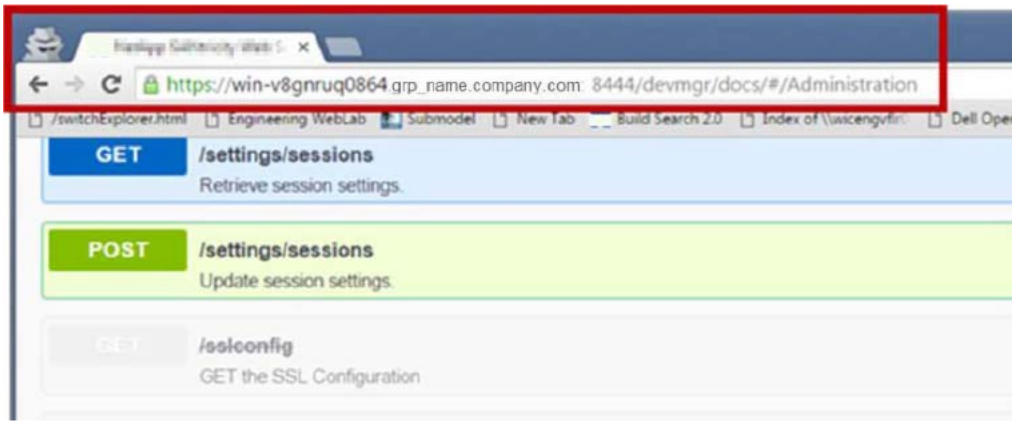
Caution

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.

Caution

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.



/settings/sessions
Retrieve session settings.

/settings/sessions
Update session settings.

/sslconfig
GET the SSL Configuration

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.

Caution

You can now use an external tool such as OpenSSL to generate a Certificate Signing Request (CSR), which also requires you to import a private key file along with the signed certificate.

Figure 17 shows the default controller web server certificate status where HTTPS connections are not secure.

Figure 17 SANtricity System Manager navigation to manage certificates

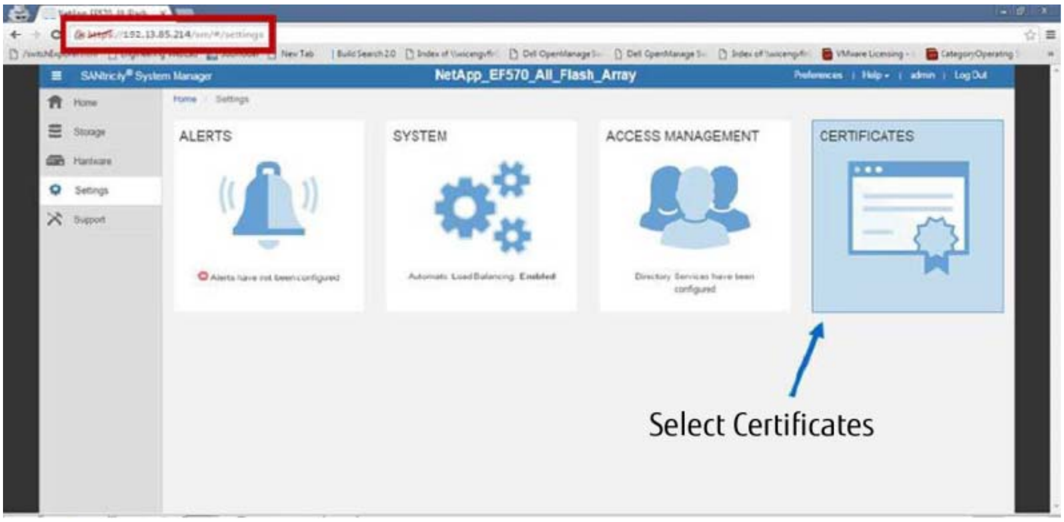
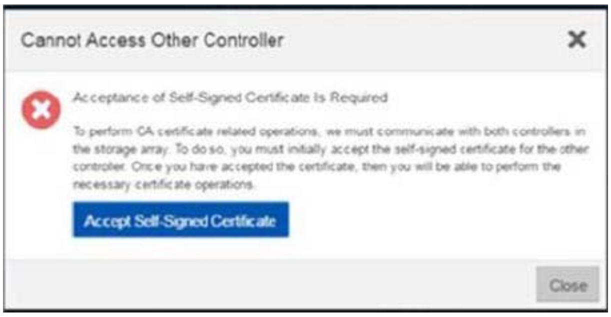


Figure 18 shows the dialog box in which you are asked to accept the self-signed certificate of the alternate controller.

Figure 18 Dialog box in which the user can accept the self-signed certificate

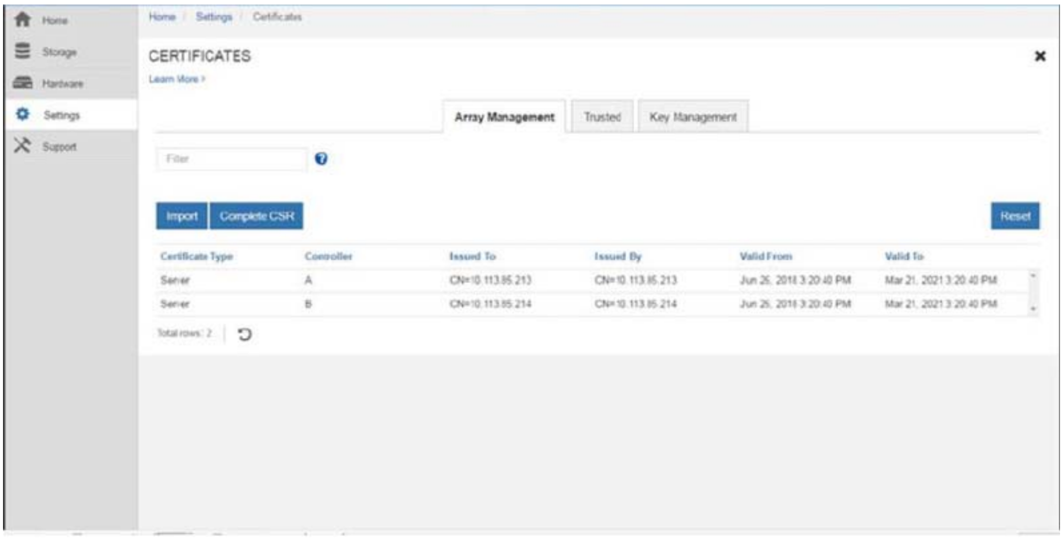

Cannot Access Other Controller

Acceptance of Self-Signed Certificate Is Required

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

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 19.

Figure 19 Default controller certificate status after the alternate controller self-signed certificate is accepted



Certificate Type	Controller	Issued To	Issued By	Valid From	Valid To
Server	A	CN=10.113.85.213	CN=10.113.85.213	Jun 26, 2018 3:20:40 PM	Mar 21, 2021 3:20:40 PM
Server	B	CN=10.113.85.214	CN=10.113.85.214	Jun 26, 2018 3:20:40 PM	Mar 21, 2021 3:20:40 PM

Total rows: 2

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

Procedure ▶▶▶

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.

> **Caution**
>
> After your browser refreshes, the browser might block access to the destination site and report that the site is using HTTP Strict Transport Security. This condition arises when you switch back to self-signed certificates. To clear the condition that is blocking access to the destination, you must clear the browser cache data from the browser.

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

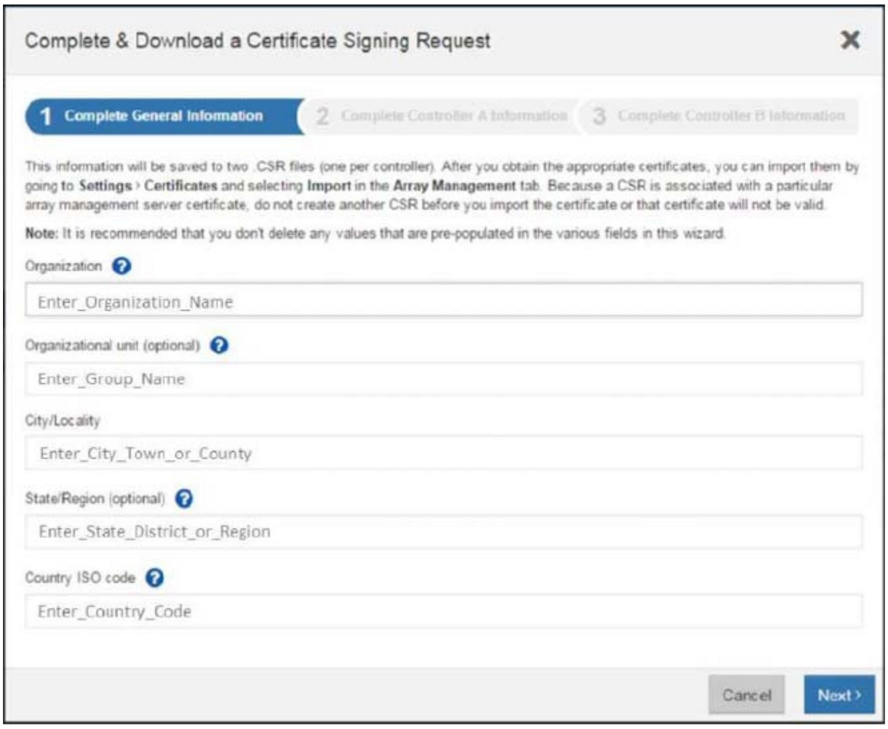
```
C:\Users\admin>nslookup 192.13.85.213
Server: DNS1.location.group.company.com
Address: 192.11.102.130

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
```

Caution

If you are not using a DNS server, you can skip the `nslookup` step. Instead, use the autopopulated primary controller IP address as the common name and the same autopopulated 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.

3-1 Enter the information to identify the organization and location.



Complete & Download a Certificate Signing Request

✕
1 Complete General Information
2 Complete Controller A Information
3 Complete Controller B Information

This information will be saved to two .CSR files (one per controller). After you obtain the appropriate certificates, you can import them by going to **Settings** › **Certificates** and selecting **Import** in the **Array Management** tab. Because a CSR is associated with a particular array management server certificate, do not create another CSR before you import the certificate or that certificate will not be valid.

Note: It is recommended that you don't delete any values that are pre-populated in the various fields in this wizard.

Organization ?
Enter_Organization_Name

Organizational unit (optional) ?
Enter_Group_Name

City/Locality
Enter_City_Town_or_County

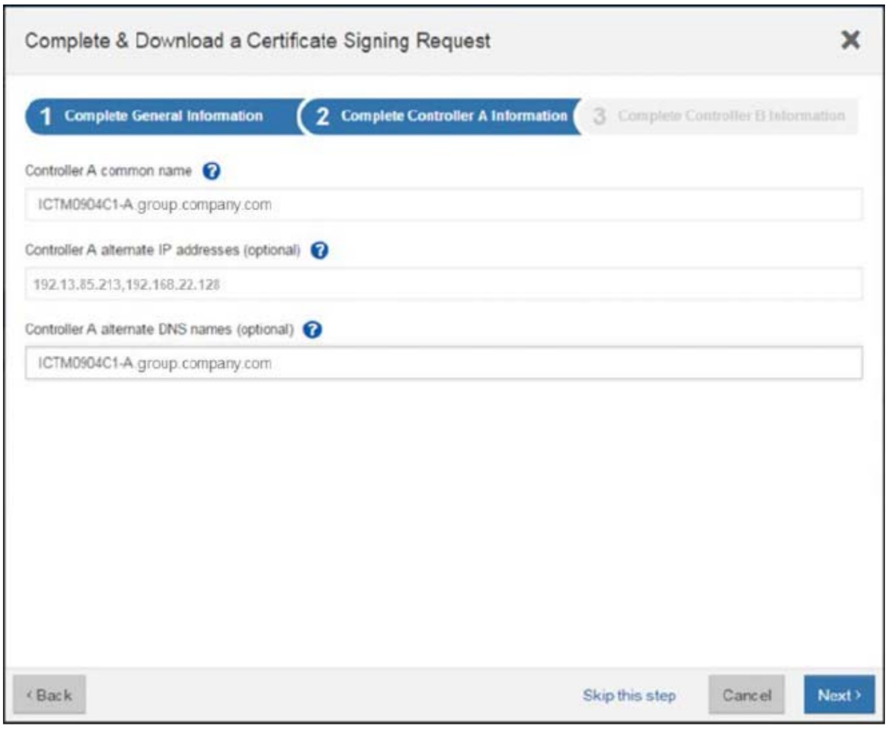
State/Region (optional) ?
Enter_State_District_or_Region

Country ISO code ?
Enter_Country_Code

3-2 Use the FQDN for controller A to change or fill in the information for controller A.

Caution

When a DNS is not used, do not change the autopopulated 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.



Complete & Download a Certificate Signing Request

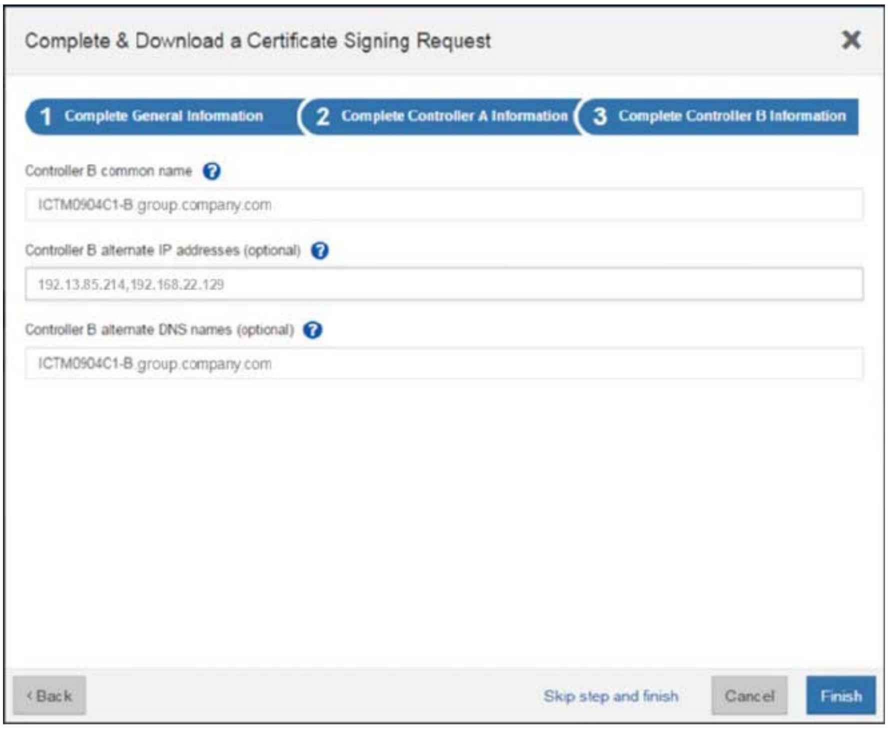
Controller A common name: ICTM0904C1-A.group.company.com

Controller A alternate IP addresses (optional): 192.13.85.213,192.168.22.128

Controller A alternate DNS names (optional): ICTM0904C1-A.group.company.com

1 Complete General Information
2 Complete Controller A Information
3 Complete Controller B Information
‹ Back
Skip this step
Cancel
Next ›

3-3 Use the FQDN for controller B to change or fill in the information for controller B.



Complete & Download a Certificate Signing Request

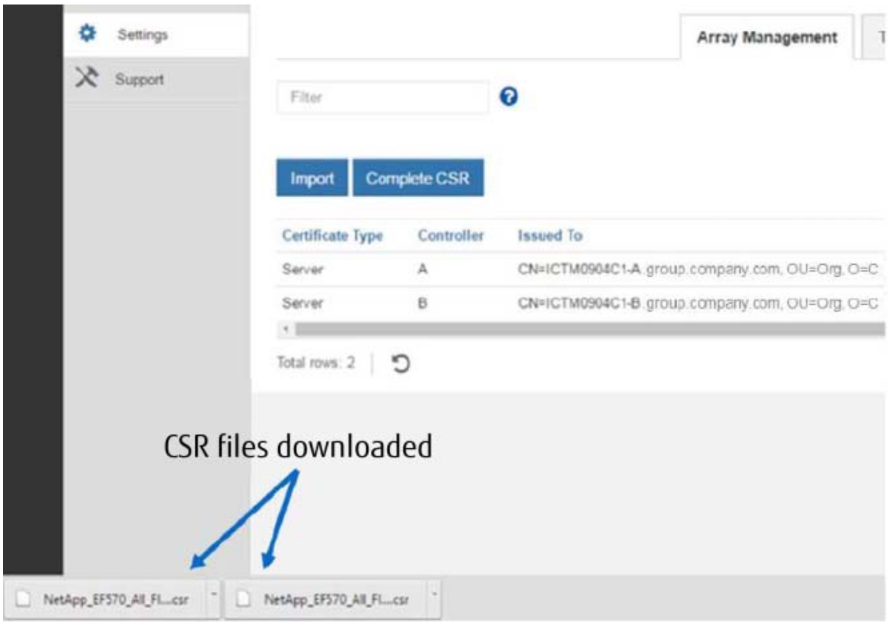
Controller B common name: ICTM0904C1-B.group.company.com

Controller B alternate IP addresses (optional): 192.13.85.214,192.168.22.129

Controller B alternate DNS names (optional): ICTM0904C1-B.group.company.com

1 Complete General Information
2 Complete Controller A Information
3 Complete Controller B Information
‹ Back
Skip step and finish
Cancel
Finish

3-4 Click Finish to generate two CSR files, one for controller A and one for controller B.



Certificate Type	Controller	Issued To
Server	A	CN=ICTM0904C1-A.group.company.com, OU=Org, O=C
Server	B	CN=ICTM0904C1-B.group.company.com, OU=Org, O=C

Total rows: 2

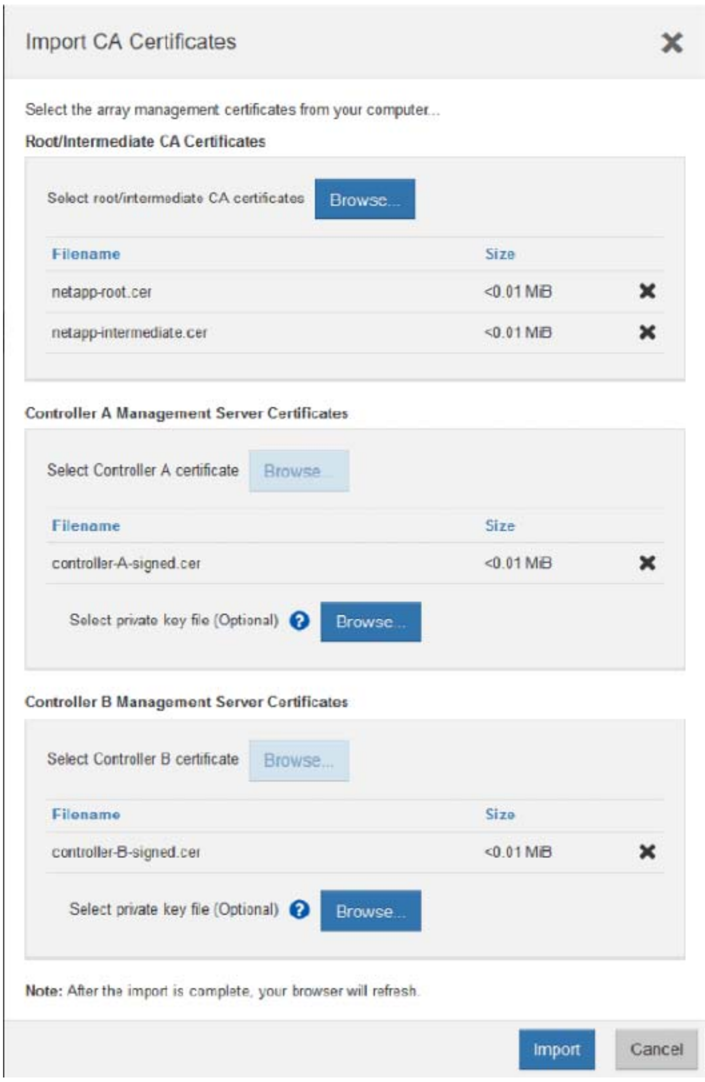
CSR files downloaded

4 Submit the CSR files to a CA and request one or more new signed security certificates (for example, Verisign or DigiCert), and request signed certificates in PEM format.

> **Caution**
>
> - The ETERNUS AB/HB series systems require PEM format (Base64 ASCII encoding) for signed certificates, which includes the following file types: pem, .crt, .cer, or .key.
> - After you submit a CSR file to the CA, do NOT regenerate another CSR file. Whenever you generate a CSR, the system creates a private and public key pair. The public key is part of the CSR, while the private key is kept in the system's keystore. When you receive the signed certificates and import them, the system ensures that both the private and public keys are the original pair. If the keys do not match, the signed certificates will not work and you must request new certificates from the CA.

5 After the certificate files are received from the CA, they must be imported by using the SANtricity System Manager Import Certificates wizard. These files include the root certificate, one or more intermediate certificates, and the server certificates.

> **Caution**
>
> - 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. Be sure to use base-64 encoding when breaking up the cert chain.
> - If the CA provided a chained certificate file (for example, a .p7b file), you must unpack the chained file into individual files: the root certificate, one or more intermediate certificates, and the server certificates that identify the controllers. You can use the Windows certmgr utility to unpack the files (right-click and select All Tasks > Export). Base-64 encoding is recommended. When the exports are complete, a CER file is shown for each certificate file in the chain.



Import CA Certificates

Select the array management certificates from your computer...

Root/Intermediate CA Certificates

Select root/intermediate CA certificates

Filename	Size
netapp-root.cer	<0.01 MiB
netapp-intermediate.cer	<0.01 MiB

Controller A Management Server Certificates

Select Controller A certificate

Filename	Size
controller-A-signed.cer	<0.01 MiB

Select private key file (Optional)

Controller B Management Server Certificates

Select Controller B certificate

Filename	Size
controller-B-signed.cer	<0.01 MiB

Select private key file (Optional)

Note: After the import is complete, your browser will refresh.

6 Select Settings > Certificates.

7 From the Array Management tab, select Import. A dialog box opens for importing the certificate file(s).

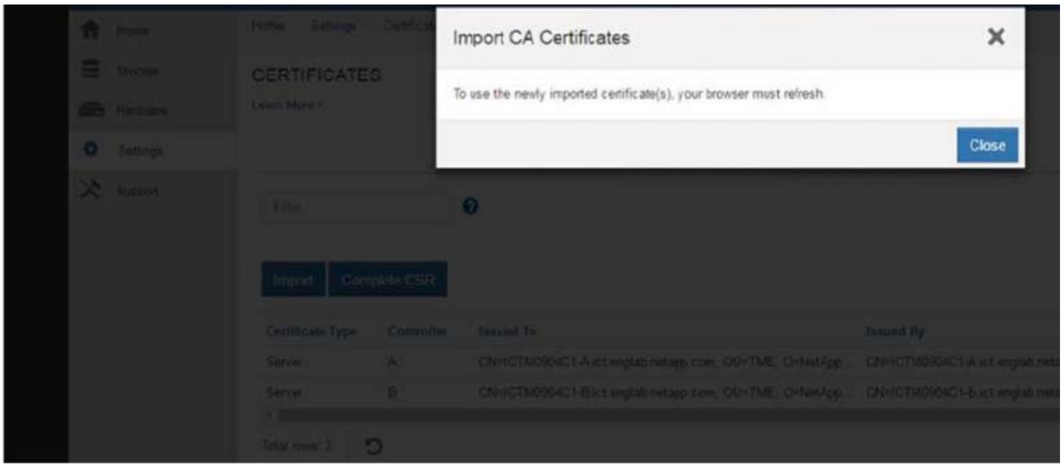
8 Click the Browse buttons to first select the root and intermediate certificate files, and then select each server certificate for the controllers.

The root and intermediate files are the same for both controllers. Only the server certificates are unique for each controller. If you generated the CSR from an external tool, you must also import the private key file that was created along with the CSR.

9 The file names are displayed in the dialog box. Click Import.

10 The files are uploaded and validated. 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.

The session is automatically terminated. You must log in again for the certificates to take effect. When you log in again, the new CA-signed certificates are used for your session. When the import process is complete, the browser displays a message to refresh the browser session.



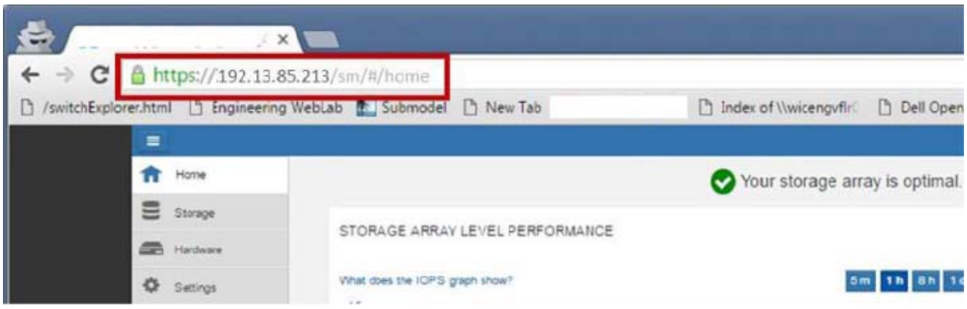
Import CA Certificates

To use the newly imported certificate(s), your browser must refresh.

Close

Certificate Type	Controller	Issued To	Issued By
Server	A	CN=ICTM0904C1-A.ict.englab.netapp.com, OU=TME, O=NetApp ...	CN=ICTM0904C1-A.ict.englab.neta
Server	B	CN=ICTM0904C1-B.ict.englab.netapp.com, OU=TME, O=NetApp ...	CN=ICTM0904C1-B.ict.englab.neta

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



https://192.13.85.213/sm/#/home

Your storage array is optimal.

STORAGE ARRAY LEVEL PERFORMANCE

What does the IOPS graph show?

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 (user name 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:

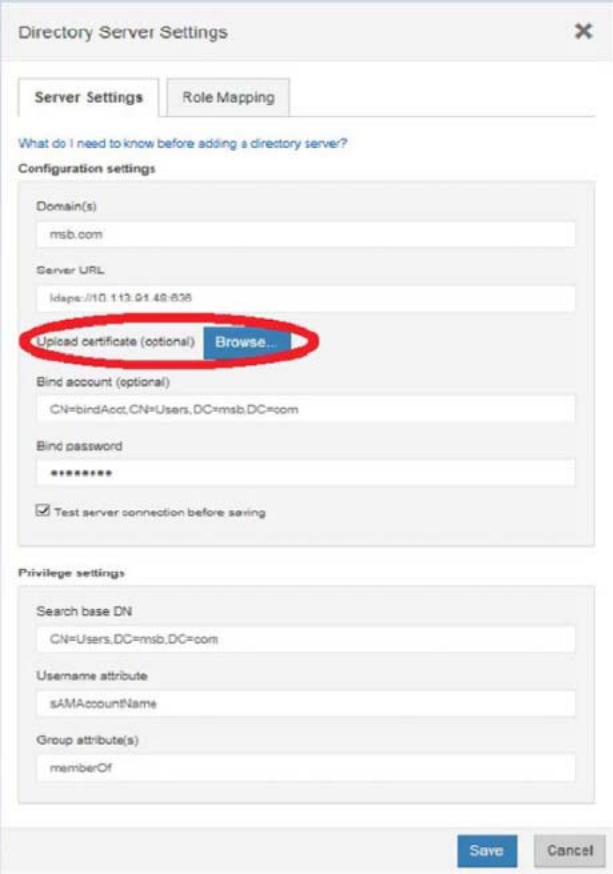
- Some Windows applications authenticate with Active Directory Domain Services (AD DS) through simple bind. Because simple bind exposes the users' credentials in clear text, use of Kerberos is preferred. If simple bind is necessary, Fujitsu strongly recommends using SSL/TLS to encrypt the authentication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

LDAPS is supported and can be configured using the SANtricity System Manager GUI, as shown in Figure 21. 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.

Caution

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 20 Option to upload the LDAP server’s CA root certificate to the array truststore


Directory Server Settings
✕
Server Settings
Role Mapping
What do I need to know before adding a directory server?
Browse...
Save
Cancel

Configuration settings

Domain(s): msb.com

Server URL: ldaps://10.113.91.48:636

Upload certificate (optional)

Bind account (optional): CN=bindAcct,CN=Users,DC=msb,DC=com

Bind password: ********

☑ Test server connection before saving

Privilege settings

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

Username attribute: sAMAccountName

Group attribute(s): memberOf

Certificate Management for Embedded External Key Management Server

The full disk encryption (FDE) feature is enhanced 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 available on all storage systems running SANtricity OS 11.60 and 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 both a secure connection and authentication between the storage system and the key management server. SANtricity System Manager provides an interface to walk the administrator through the process of generating a Certificate Signing Request (CSR) for the storage system controller and installing both the storage system's signed client certificate and the EKMS server's SSL certificate. This process can also be performed through SMcli.

Caution

The following steps are appropriate for the Gemalto Key Management Server. Other sequences may be required for other Key Management Server products.

Steps to Enable External Key Management

There are several configuration steps that must be taken on the external key management server (EKMS) itself. This guide will not go in depth on those steps, but rather make references to artifacts that are obtained from the EKMS.

Procedure ▶▶▶

1. During the process of setting up you EKMS server you may choose what type of authentication to use for client requests. It is recommended to select `SSL session and username` as the most secure type.

   During this configuration step, you may choose what field in the client's certificate to use as the username. This allows a username to be passed in the client certificate to provide authentication.

2. Use SANtricity System Manager to generate a new CSR. In the CSR request dialog, you will want to designate a username in the same field you designated in step 1.

   See "Figure 22 Certificate Signing Request Dialog" (page 55).

3. Take the CSR information to the EKMS server and go through the certificate signing process.

   You will generate a new client certificate, which should be downloaded to your local system.

4. Use SANtricity System Manager to configure a connection to your EKMS server.

   This step requires you to provide the EKMS server's IP or host address and the port number, and to import the storage array client certificate. The EKMS server certificate must also be imported so the storage array can trust the EKMS server. Note that the EKMS server's intermediate or root certificate may also be imported. See "Figure 23 Connecting to a key management server" (page 56).

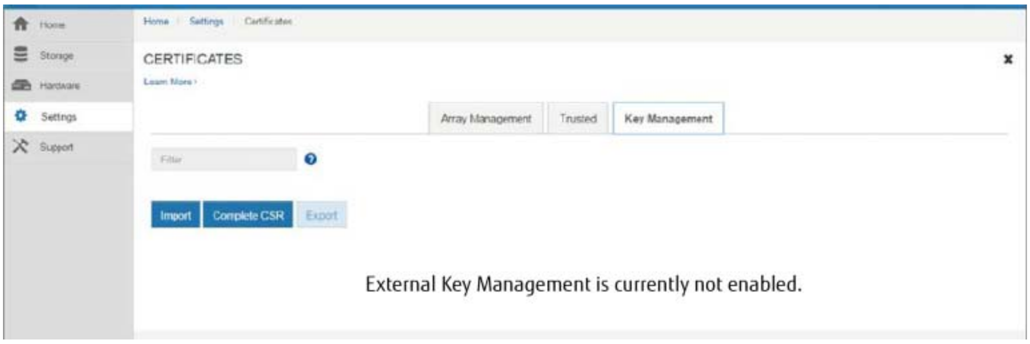
5. The next step is to optionally retrieve a backup key and finish the connection configuration.

   If the Create backup key checkbox is unchecked, then a backup key will not be downloaded.

6 Click the Finish button to complete the Create External Security Key workflow.

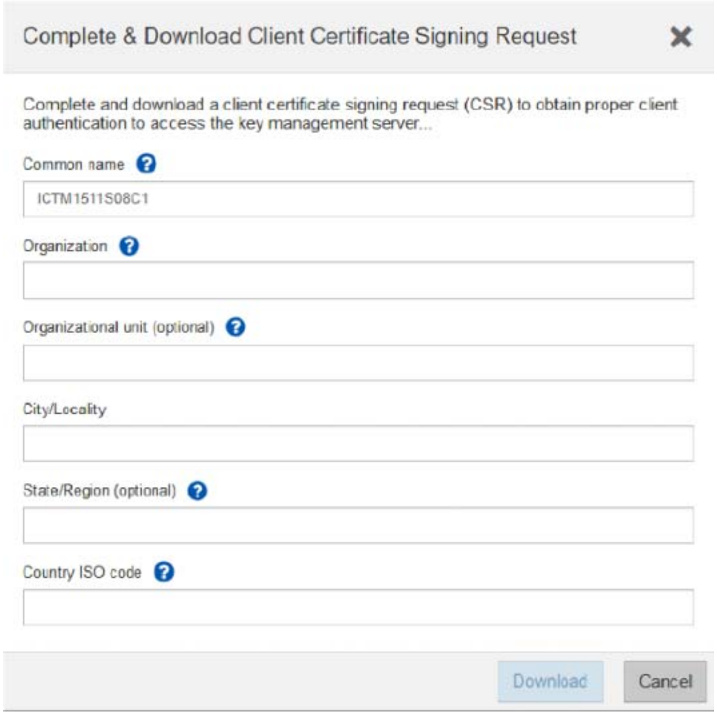
Figure 21 shows the open certificates tile in SANtricity System Manager, where the external key management server certificates are managed.

Figure 21 Option in SANtricity System Manager to complete a CSR, and to import the storage system's signed client certificate and EKMS server's SSL certificate



External Key Management is currently not enabled.

Figure 22 Certificate Signing Request Dialog



Complete & Download Client Certificate Signing Request

Complete and download a client certificate signing request (CSR) to obtain proper client authentication to access the key management server...

Common name: ICTM1511S08C1

Organization:

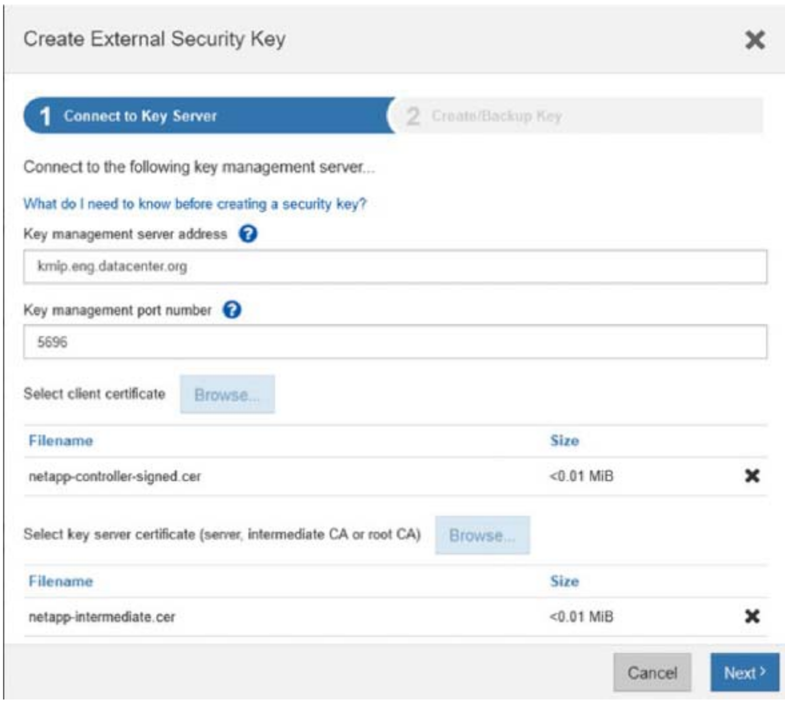
Organizational unit (optional):

City/Locality:

State/Region (optional):

Country ISO code:

Figure 23 Connecting to a key management server



Create External Security Key

Connect to the following key management server...

What do I need to know before creating a security key?

Key management server address: kmip.eng.datacenter.org

Key management port number: 5696

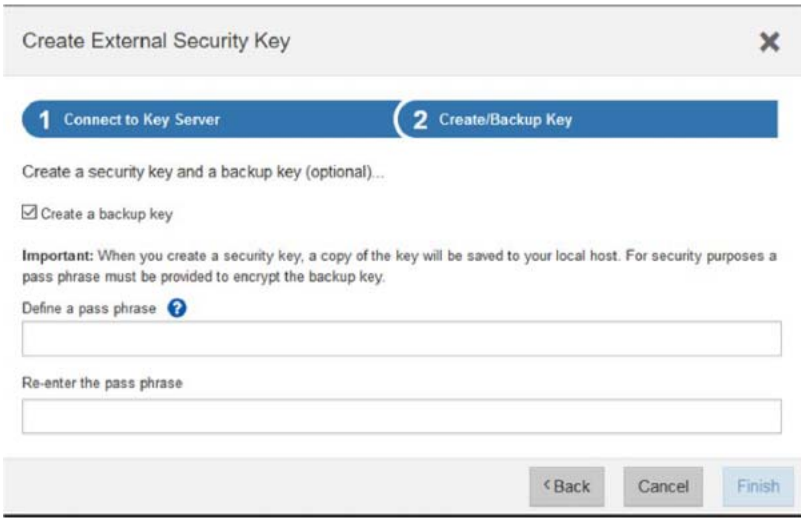
Select client certificate

Filename	Size
netapp-controller-signed.cer	<0.01 MiB

Select key server certificate (server, intermediate CA or root CA)

Filename	Size
netapp-intermediate.cer	<0.01 MiB

Figure 24 Creating an optional backup key



Create External Security Key

Create a security key and a backup key (optional)...

☑ Create a backup key

Important: When you create a security key, a copy of the key will be saved to your local host. For security purposes a pass phrase must be provided to encrypt the backup key.

Define a pass phrase

Re-enter the pass phrase

6. SAML 2.0 and MFA in SANtricity OS

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.

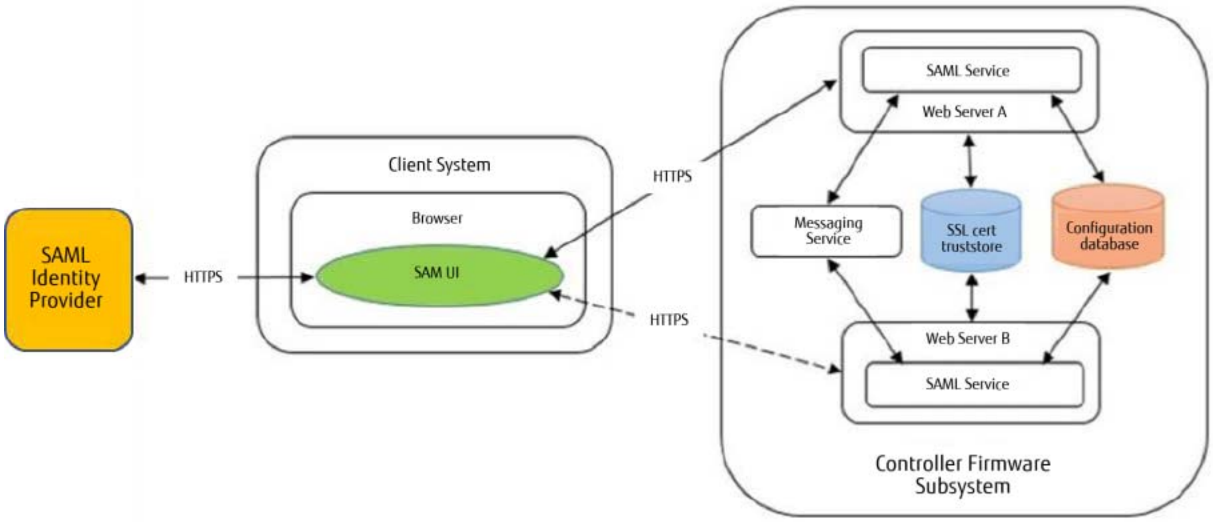
Multifactor authentication (MFA) requires the user to provide two or more items as proof of identity to be successfully authenticated. The separate pieces of evidence are typically at least two of the following types: knowledge (something the user knows, such as a password); possession (something the 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 the ETERNUS AB/HB 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.

MFA Architectural Overview

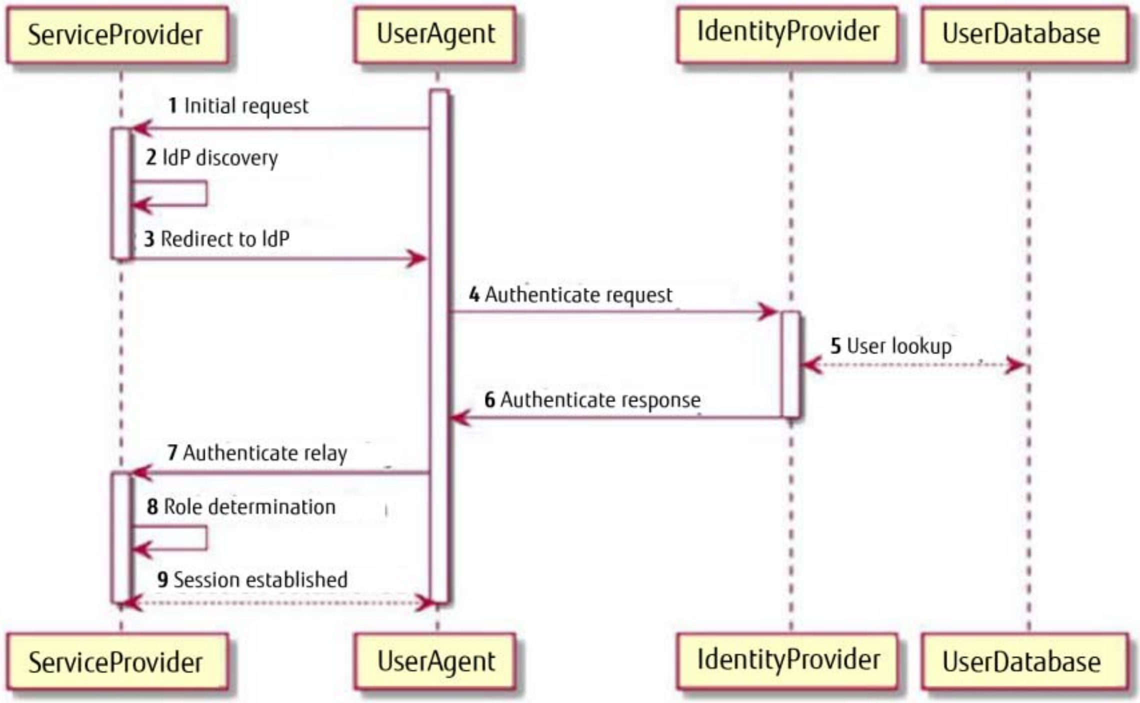
SAML is integrated into the ETERNUS AB/HB series products using version 2.0 of the standard, and Fujitsu officially supports Shibboleth and Microsoft ADFS as identity providers (IdPs). Figure 25 is a high-level overview of all components used to achieve SAML integration. Communication with the authentication 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 certificates provided by the identity provider. This enables the ETERNUS AB/HB 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 25 How SAML integrates into the ETERNUS AB/HB series products



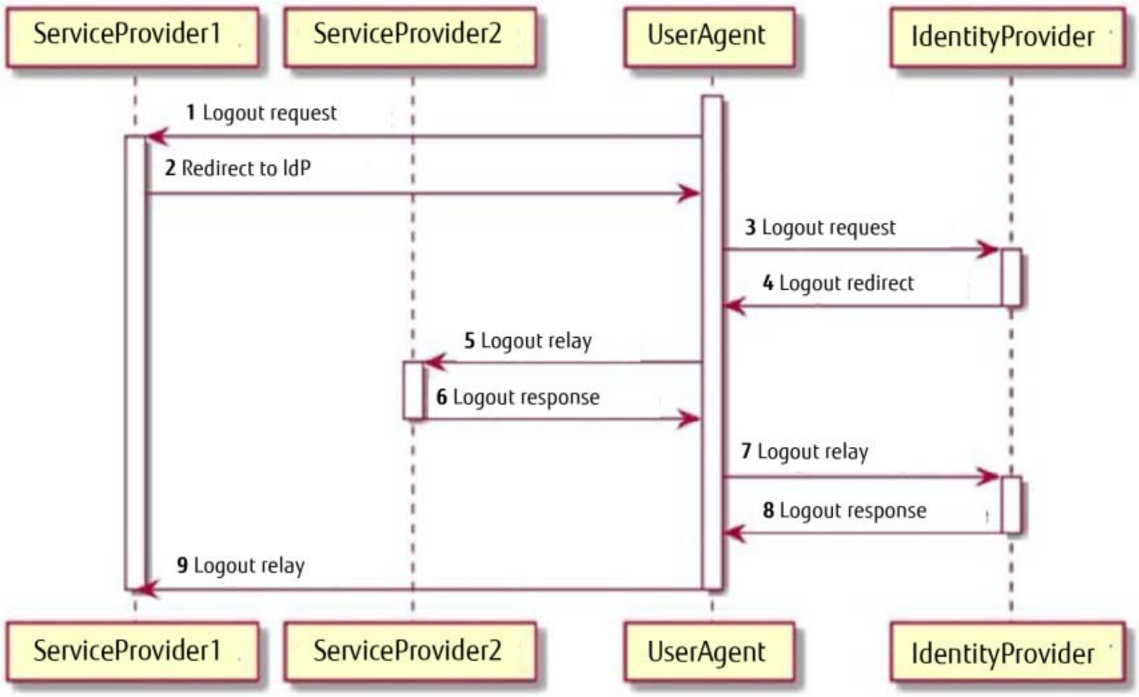
After SAML is configured on the ETERNUS AB/HB series system, logging into SANtricity System Manager is possible only through a configured IdP. When users attempt to access SANtricity System Manager, they are sent to their IdP's login page instead of to the default SANtricity System Manager login page. 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 26 shows how a login request flows through the different components of the ETERNUS AB/HB series system. The service provider represents an ETERNUS AB/HB 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.

Figure 26 Overview of login request using SAML



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 27. The SANtricity System Manager application receives this request and invalidates all sessions associated with the logout request.

Figure 27 Overview of IdP-initiated logout using SAML



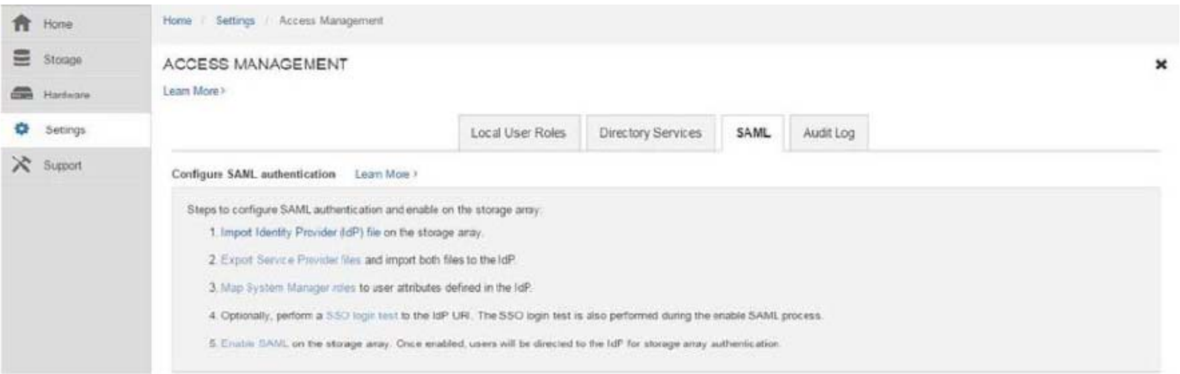
Configuring SAML

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. A SAML tab is available in SANtricity System Manager in the Settings > Access Management tile, shown in Figure 28. This tab allows the configuration of an IdP to authenticate users. After a 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 SANtricity, 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.

Caution

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 storage system and will need to contact a Fujitsu technical support engineer for instructions.

Figure 28 The SAML tab in SANtricity System Manager when no configuration is present



Steps to configure SAML authentication and enable on the storage array:

1. Import Identity Provider (IdP) file on the storage array.
2. Export Service Provider files and import both files to the IdP.
3. Map System Manager roles to user attributes defined in the IdP.
4. Optionally, perform a SSO login test to the IdP URI. The SSO login test is also performed during the enable SAML process.
5. Enable SAML on the storage array. Once enabled, users will be directed to the IdP for storage array authentication.

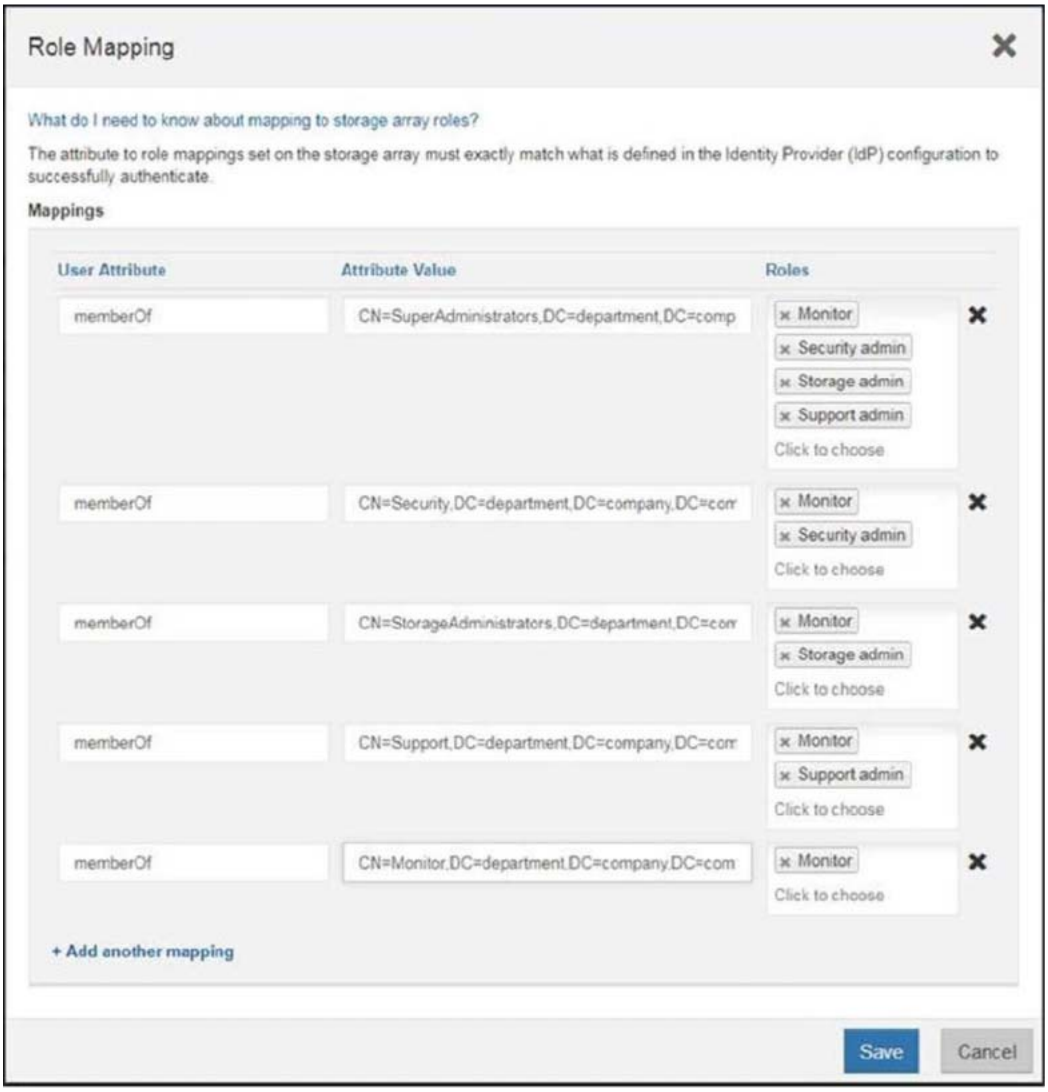
SANtricity System Manager establishes a trust relationship with an identity provider by exchanging metadata files. The customer must export the identity provider's metadata file and import it into SANtricity System Manager by using the Import Identity Provider file link on the SAML tab in Access Management. 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 system 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 ETERNUS AB/HB 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 29. This allows SANtricity System Manager to correctly map roles to users after they are authenticated through an IdP.

Figure 29 Common ways to configure roles in SANtricity System Manager


Role Mapping
What do I need to know about mapping to storage array roles?
+ Add another mapping
Save
Cancel

The attribute to role mappings set on the storage array must exactly match what is defined in the Identity Provider (IdP) configuration to successfully authenticate.

Mappings

User Attribute	Attribute Value	Roles
memberOf	CN=SuperAdministrators,DC=department,DC=comp	Monitor Security admin Storage admin Support admin Click to choose
memberOf	CN=Security,DC=department,DC=company,DC=com	Monitor Security admin Click to choose
memberOf	CN=StorageAdministrators,DC=department,DC=com	Monitor Storage admin Click to choose
memberOf	CN=Support,DC=department,DC=company,DC=com	Monitor Support admin Click to choose
memberOf	CN=Monitor,DC=department,DC=company,DC=com	Monitor Click to choose

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

Misconfiguration Issue	Description
Storage system clock and identity provider clock are out of sync	SAML uses time stamps that expire to prevent attacks that use old data. If the storage system and IdP clocks are more than 5 minutes apart, SAML authentication in SANtricity System Manager fails.
Expired IdP certificates	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 Fujitsu technical support engineer, make a serial connection to the storage system, and reimport their IdP metadata files with valid x509 certificates embedded in the metadata.
Unable to map roles	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.
User name is reported as a long unreadable list of numbers and letters	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.

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 SANtricity, 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

Fujitsu takes storage management security and security for data at rest seriously. To help address the ever-increasing threat from malicious insider activities, Fujitsu has implemented new features starting in SANtricity OS 11.60, including RBAC, directory services support, secure SMcli, certificate management, audit logs, and multifactor authentication with IdP using SAML 2.0. These feature enhancements help Fujitsu customers protect their data. The multiple interface options and security configuration choices make it easy to adopt the ETERNUS AB/HB series systems in enterprise environments where enhanced management security is a core qualifying attribute for all new storage systems.

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 storage system 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 Fujitsu Support for assistance.

What format should my certificate be in?

Answer:
It should be in PEM (base-64 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 system.

- 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.

- 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 the ETERNUS AB/HB series

This section addresses questions regarding SAML 2.0 on the ETERNUS AB/HB series.

What identity providers does the ETERNUS AB/HB series support?

Answer:
The ETERNUS AB/HB 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 system?

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 system configuration?

Answer:
Yes, the metadata generated by the ETERNUS AB/HB 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.

FUJITSU Storage
ETERNUS AB series All-Flash Arrays,
ETERNUS HB series Hybrid Arrays
SANtricity Management Security

P3AG-6052-01ENZ0

Date of issuance: June 20201
Issuance responsibility: FUJITSU LIMITED

- The content of this manual is subject to change without notice.
- This manual was prepared with the utmost attention to detail.
  However, Fujitsu shall assume no responsibility for any operational problems as the result of errors, omissions, or the use of information in this manual.
- Fujitsu assumes no liability for damages to third party copyrights or other rights arising from the use of any information in this manual.
- The content of this manual may not be reproduced or distributed in part or in its entirety without prior permission from Fujitsu.

FUJITSU