Technical Report

Access Management for E-Series Storage Systems

Jolie Gallagher, NetApp

July 2020 | TR-4853

Abstract

This document describes how to configure Access Management, including role-based access control (RBAC), Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML), in NetApp® E-Series SANtricity® applications.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 Overview

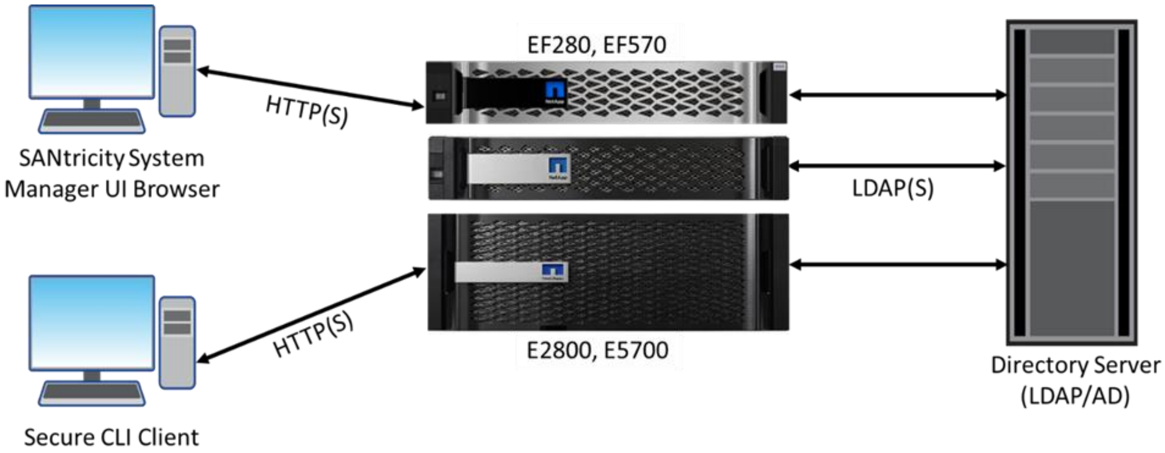
Access Management is a method of establishing user authentication for NetApp® SANtricity® applications and NetApp E-Series storage systems. Authentication can be configured by using one or more of the following methods:

- **Local user roles** (pre-configured) – Authentication is managed through role-based access control (RBAC) capabilities, which include hard-coded user profiles with specific access permissions. Administrators can use these local user roles as the single method of authentication or use them in combination with a directory service.
- **Directory service** – Authentication is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory.
- **Multifactor authentication** (System Manager only) – Authentication is managed through an identity provider (IdP) using Security Assertion Markup Language (SAML) 2.0.

After you configure an Access Management method, SANtricity users log in with their assigned user profiles. They can then perform management tasks according to their assigned roles. For example, one type of user might have access to security functions but not storage management functions. Another type of user might only have view-only permissions.

The following figure shows the logical connections between the management clients running SANtricity applications, the storage systems, and a directory server.

Figure 1) NetApp E-Series systems, integrating a directory server and RBAC.


EF280, EF570
HTTP(S)
SANtricity System Manager UI Browser
LDAP(S)
HTTP(S)
E2800, E5700
Directory Server (LDAP/AD)
Secure CLI Client

1.1 Document Scope

The information in this document applies to the following SANtricity versions and controller models:

- SANtricity applications:
  - System Manager, OS 11.40 and later
  - Unified Manager and Web Services Proxy 3.0 and later
- Controller models:
  - EF280 and E2800 storage systems
  - EF570 and E5700 storage systems
  - EF600 storage systems

Note: This document does **not** describe older SANtricity versions, older controller models, or other types of SANtricity management applications (such as CLI or API). For detailed information about access management with these other products and methods, see TR-4712 - NetApp SANtricity Management Security.

2 Local User Roles (RBAC)

For quick and simple user authentication, E-Series storage systems include preconfigured RBAC capabilities. RBAC is a method of regulating access to computer or network resources based on the roles of individual users. In SANtricity applications, these RBAC capabilities are referred to as “local user roles.”

2.1 User Profiles and Permissions

Local user roles include user profiles with varying levels of permissions. For example, a Storage Admin can provision volumes and disk pools but cannot make changes to the security configuration. See the following tables for descriptions of the profiles and the roles assigned to each.

Note: The user profiles and roles are hard-coded in E-Series systems. You cannot add, delete, or modify the local user roles. You can only change their passwords.

Table 1) Local user profiles.

User	Login	Roles	Description
Root Admin	admin	(all roles)	Super administrator with access to all functions.
Storage Admin	storage	• Storage Admin • Support Admin • Monitor	Administrator responsible for all storage provisioning with full read/write access to the storage objects (for example, volumes and disk pools).
Security Admin	security	• Security Admin • Monitor	User responsible for security configuration, including access management, certificate management, and secure-enabled drive functions.
Support Admin	support	• Support Admin • Monitor	User responsible for hardware resources, failure data, and firmware upgrades.
Monitor	monitor	• Monitor	User with read-only access to the system.
rw (read/write)	rw	• Storage Admin • Support Admin • Monitor	Legacy user shown in Unified Manager that provides read-and-write access to the system. It is not supported on newer storage systems.
ro (read only	ro	• Monitor	Legacy user shown in Unified Manager that provides read-only access to the system. It is not supported on newer storage systems.

Table 2) Role descriptions.

Role	Description
Storage Admin	Full read/write access to the storage objects (for example, volumes and disk pools). No access to the security configuration.
Security Admin	Access to the security configuration in access management, certificate management, audit log management, and the legacy management interface (SYMbol) in System Manager.
Support Admin	Access to all hardware resources, failure data, event log events, and controller firmware upgrades. No access to storage objects or the security configuration.

Role	Description
Monitor	Read-only access to view storage related data. No access to the security configuration.

2.2 Manage Passwords

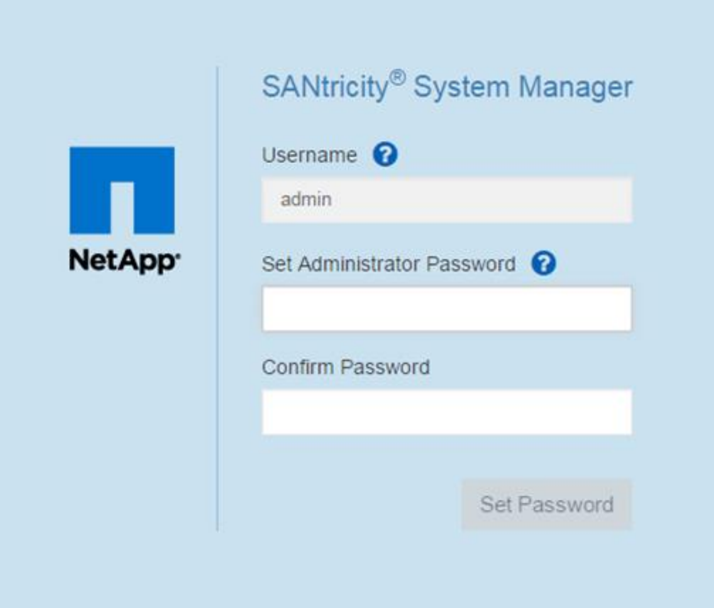
Local user roles require no configuration, except for setting the admin password. Setting passwords for other users is optional.

Set the Admin Password

When you access System Manager or Unified Manager for the first time, the interface prompts you to set the password for the root admin.

To set the admin password in System Manager, complete the following steps:

1. From your browser, enter `https://` followed by the domain name or IP address of a storage system controller.
   `https://<DomainName or IPAddress>`
2. Enter a password for the admin in the two fields, and then click Set Password. The password can include up to 30 characters.



Username: admin

To set the admin password in Unified Manager, complete the following steps:

1. Open a browser and enter `https://` followed by the IP address or FQDN of the server on which the Web Services Proxy is installed, the listening port number (defaults to 8080 for HTTP or 8443 for HTTPS), and then `/um`.

   ```
   http[s]://<server>:<port>/um
   ```

   The Unified Manager login page opens, which looks similar to the System Manager login page shown above.
2. Enter a password for the admin in the two fields, and then click Set Password. The password can include up to 30 characters.

Set Passwords for Other Users

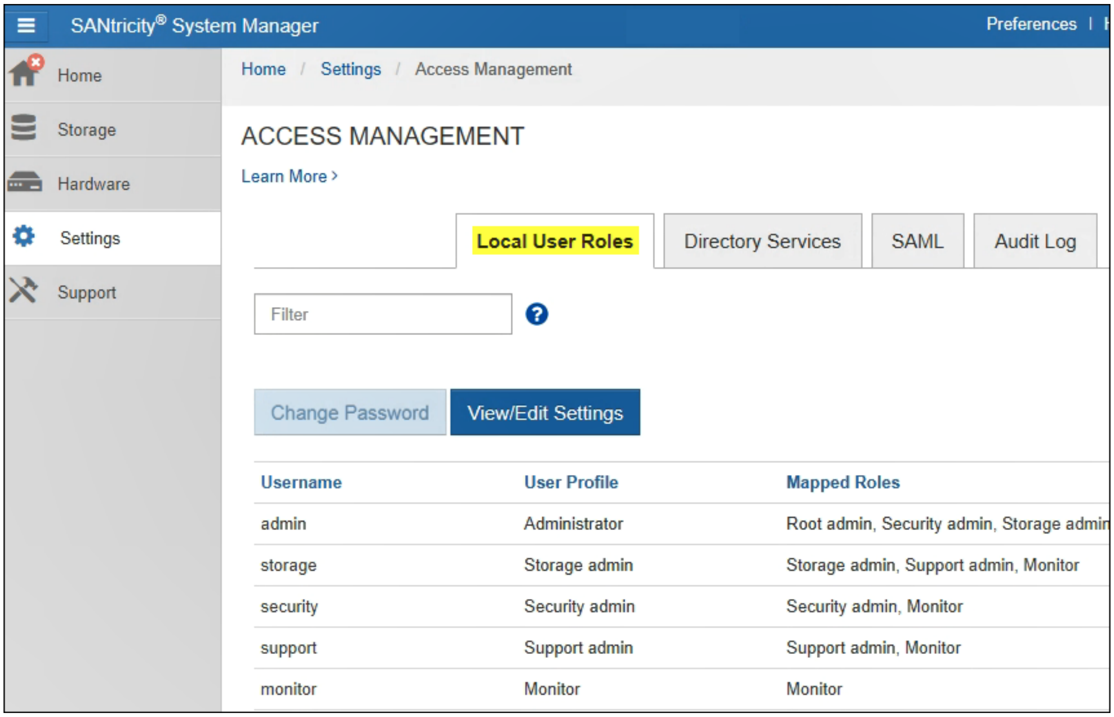
Optionally, you can set passwords for other user profiles in both System Manager and Unified Manager.

Note: You must be logged in as Admin to modify passwords.

To set passwords, complete the following steps:

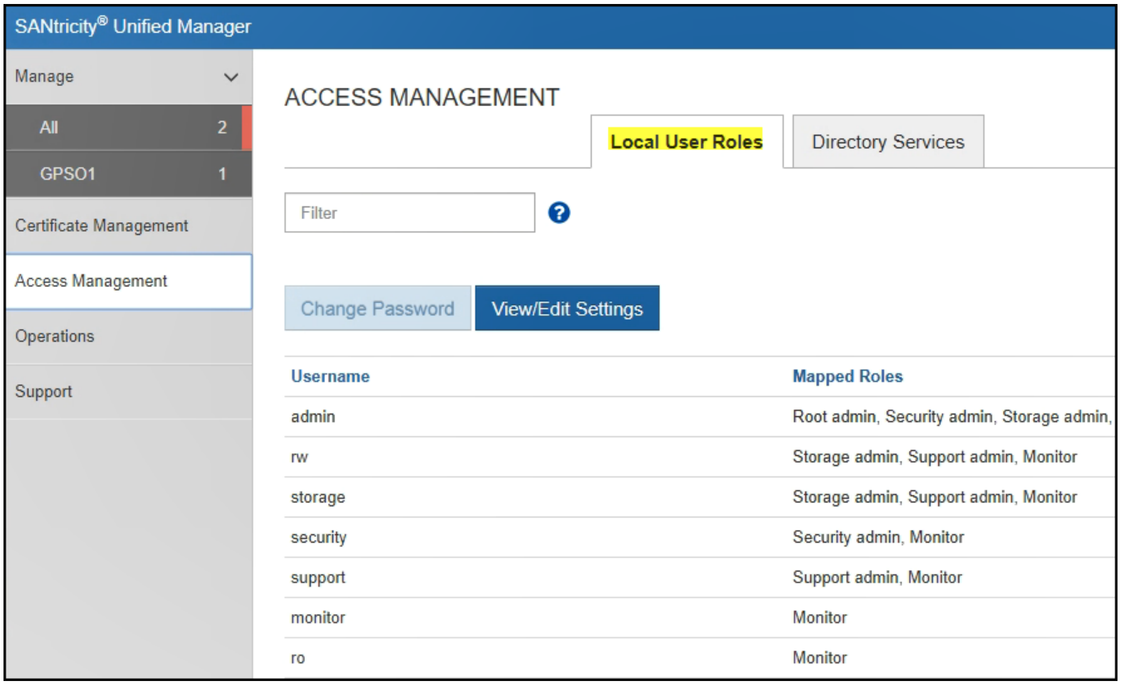
1. Go to the Local User Roles page.

   For System Manager, select Settings > Access Management > Local User Roles.



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

   For Unified Manager, select Access Management > Local User Roles.

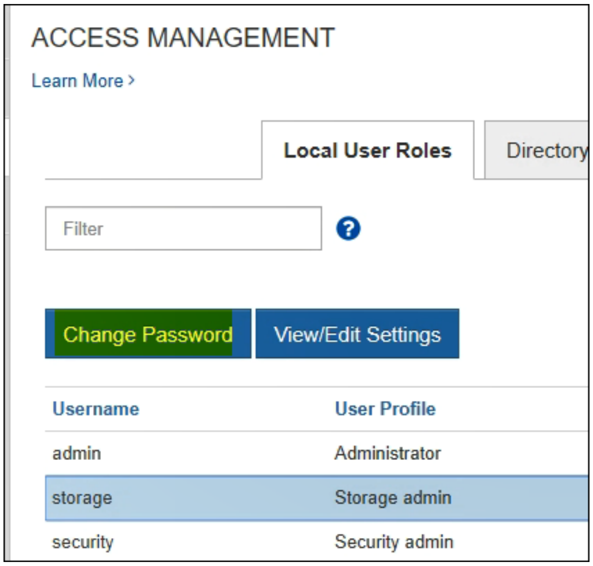


Username	Mapped Roles
admin	Root admin, Security admin, Storage admin,
rw	Storage admin, Support admin, Monitor
storage	Storage admin, Support admin, Monitor
security	Security admin, Monitor
support	Support admin, Monitor
monitor	Monitor
ro	Monitor

2. From the table, select the user for which you want to manage passwords.

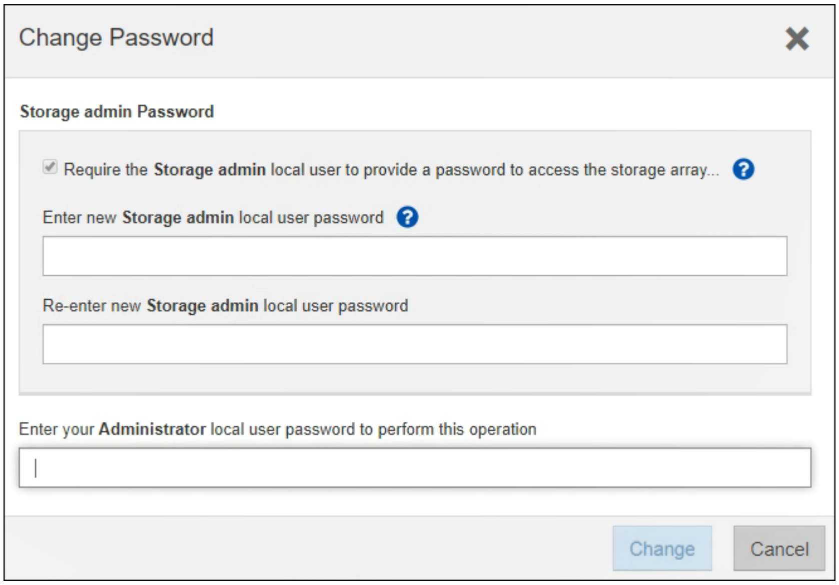
   The Change Password button becomes available.

3. Select Change Password.



Username	User Profile
admin	Administrator
storage	Storage admin
security	Security admin

4. In the Change Password dialog box, do the following:
   a. Keep the checkbox selected if you want to force this user to enter a password before accessing the storage system.
   b. Type the new password for the selected user. Passwords are case sensitive and can include up to 30 characters.
   c. Enter your administrator password to confirm this operation, and then click Change.



Change Password

Storage admin Password

☑ Require the **Storage admin** local user to provide a password to access the storage array...

Enter new **Storage admin** local user password

Re-enter new **Storage admin** local user password

Enter your **Administrator** local user password to perform this operation

Removing Password Requirements for Users

If you want to remove password requirements for users, follow these steps:

1. From the Local Users tab, select the user from the table, and then select View/Edit Settings.
2. In the Local User Password Settings dialog box, deselect the box for requiring a minimum password, and then click Save.

3 Directory Services (LDAP)

For user authentication in E-Series systems, you can configure an LDAP server and a directory service, such as Active Directory. LDAP is a vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. This protocol allows many different applications and services to connect to the LDAP server for validating users.

To enable LDAP to work with SANtricity applications, you establish communications between the storage system and an LDAP server, and then map the LDAP user groups to the storage system's predefined roles.

Note: SANtricity applications allow you to configure multiple instances of directory servers.

3.1 LDAP Setup

Before you begin configuration in System Manager or Unified Manager, do the following:

- Define user groups in your directory service.
- Install the LDAP server's certificate chain on your local machine (required only for LDAP servers using a secure protocol).
- Ensure that the LDAP server is using Transport Layer Security (TLS) 1.2 (minimum supported version).
- Gather the following LDAP server credentials and attributes:
  - Domain name of the LDAP server used in the login (username@domain)
  - Server URL
  - Bind account credentials (if used) for search queries against the LDAP server

3.2 Adding a Directory Server and Mapping Roles

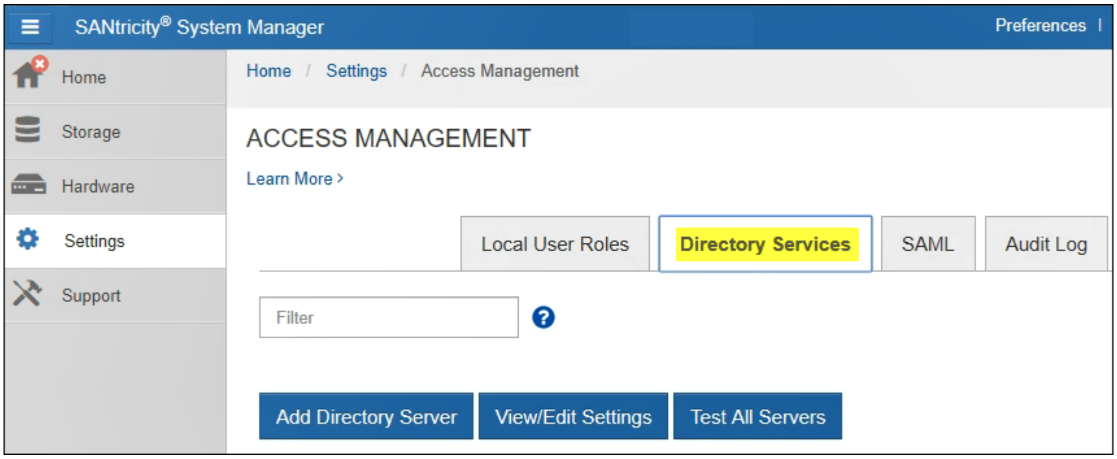
LDAP configuration is a two-step process. First, you enter the domain name and URL of the directory server. Next, you map the LDAP server's user groups to the storage system's predefined roles.

Note: The procedures for LDAP configuration are basically the same for System Manager and Unified Manager. Follow the steps below for either application.

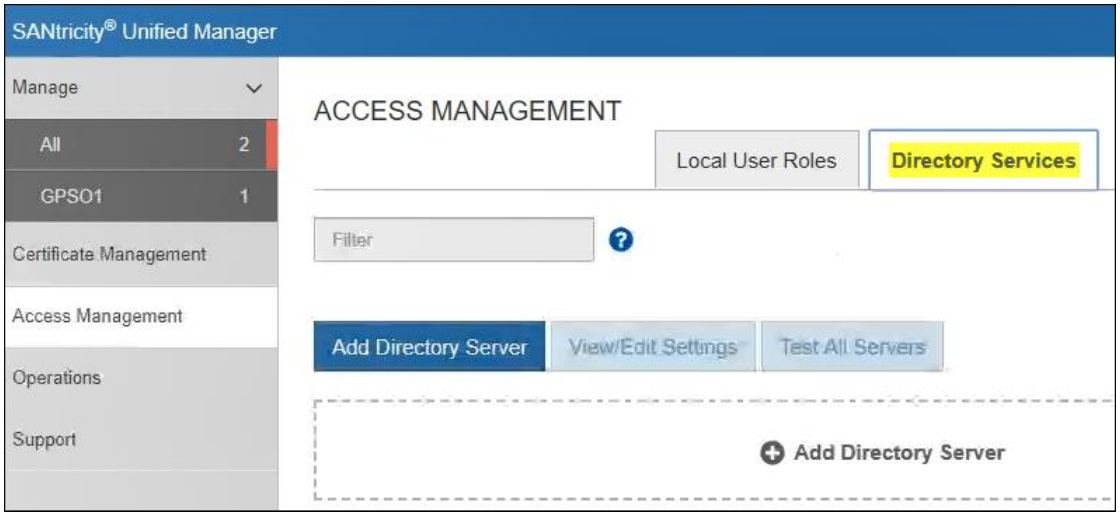
To configure a directory server, follow these steps:

1. Log in to System Manager or Unified Manager with a user profile that includes Security Admin permissions.
2. Go to the Directory Services page.

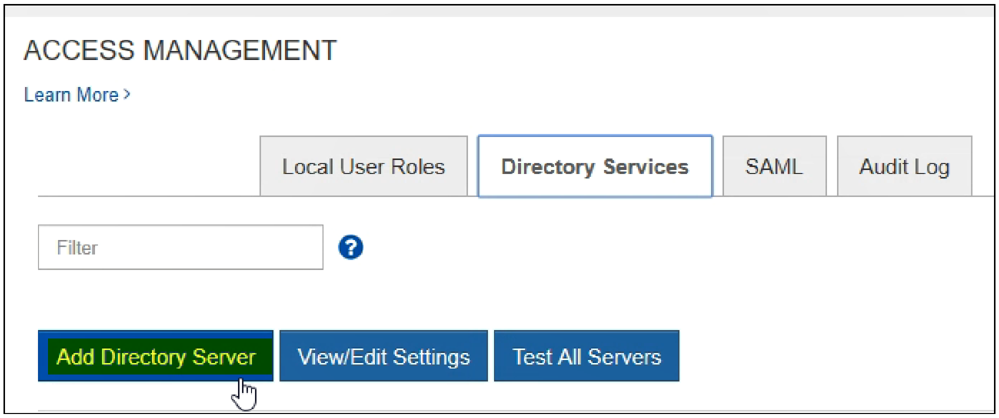
   For System Manager, select Settings > Access Management > Directory Services.



   For Unified Manager, select Access Management > Directory Services.



3. Select Add Directory Server.

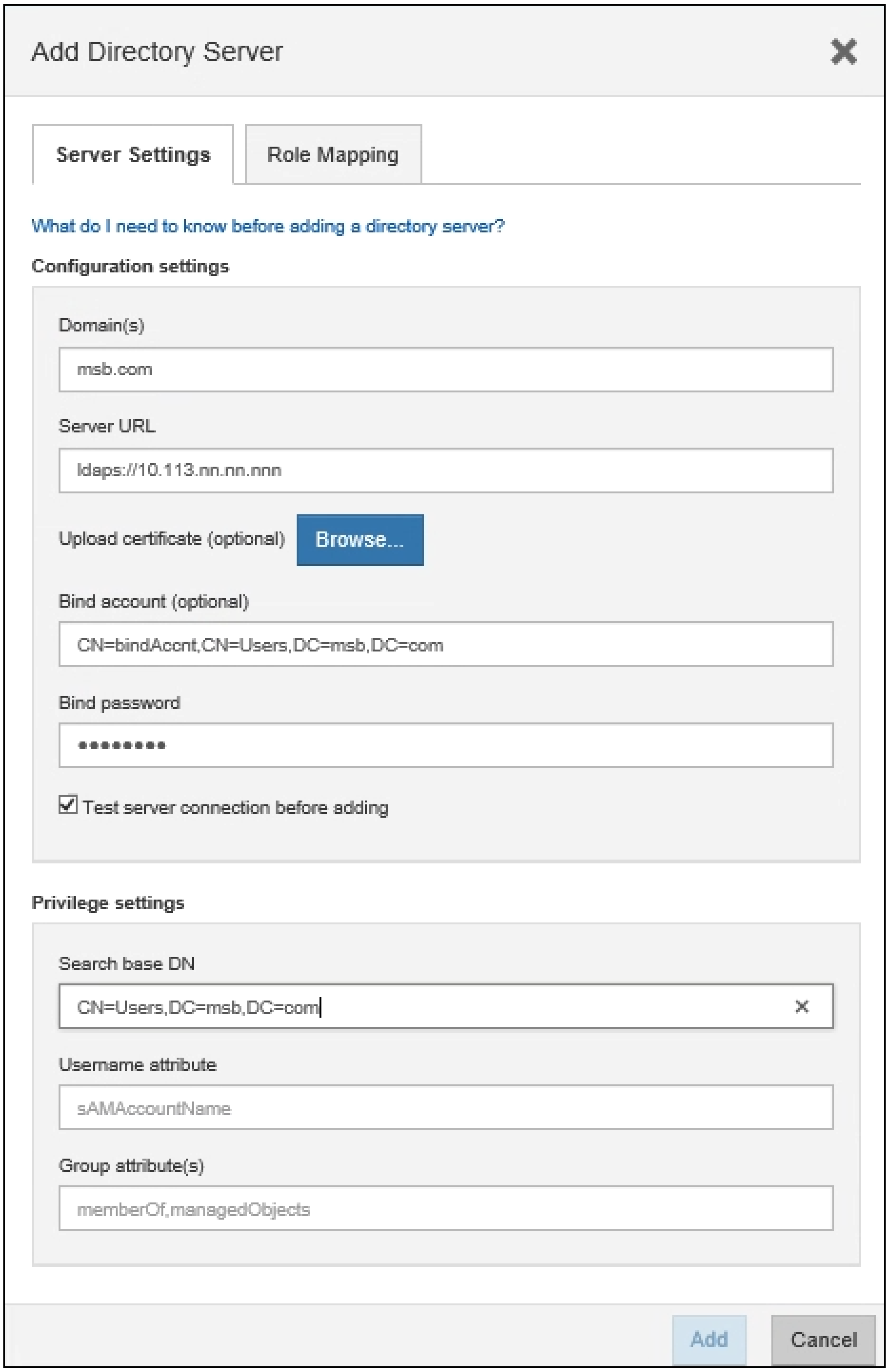


4. In the Server Settings tab, enter the credentials for the LDAP server as described in the following table.

Field	Description
Domain Name	Enter the domain name of the LDAP server. For multiple domains, enter the domains in a comma separated list. The domain name is used in the login (username@domain) to specify which directory server to authenticate against. Valid DNS names can contain only: tASCII letters **a** through **z** (not case sensitive), digits **0** through **9**, and a hyphen (**-**), but cannot start with a hyphen. **Note:** Auto searching for user names in the directory is not supported.
Server URL	Enter the URL for accessing the LDAP server in the form of `ldap[s]://host:port`.
Upload certificate	**Note:** This field appears only if an LDAP protocol is specified in the Server URL field above. Click Browse and select a CA certificate to upload. This is the trusted certificate or certificate chain used for authenticating the LDAP server.
Bind account / Bind password	If a bind account is used, enter a read-only user account for search queries against the LDAP server and for searching within the groups. Enter the account name in an LDAP-type format. For example, if the bind user is called "bindacct," then you might enter a value such as: `CN=bindacct,CN=Users,DC=cpoc,DC=local` In addition, you must enter the password for the bind account.
Test server connection before adding	Select this checkbox if you want to make sure that the system can communicate with the LDAP server configuration you entered. The test occurs after you click Add at the bottom of the dialog box. If this checkbox is selected and the test fails, the configuration is not added. You must resolve the error or de-select the checkbox to skip the testing and add the configuration. See Table 3 for more information.
Search base DN	Enter the LDAP context to search for users, typically in the form of: `CN=Users, DC=cpoc, DC=local`
Username attribute	Enter the attribute that is bound to the user ID for authentication. For example: `sAMAccountName`

Field	Description
Group attribute	Enter a list of group attributes on the user, which is used for group-to-role mapping. For example: `memberOf, managedObjects`

See the following screen shot for an example.



Configuration settings

Domain(s): msb.com

Server URL: ldaps://10.113.nn.nn.nnn

Upload certificate (optional)

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

Bind password: ●●●●●●●●

☑ Test server connection before adding

Privilege settings

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

Username attribute: sAMAccountName

Group attribute(s): memberOf,managedObjects

5. If you want to check the server settings before adding role mapping, click Add at the bottom of the dialog box.

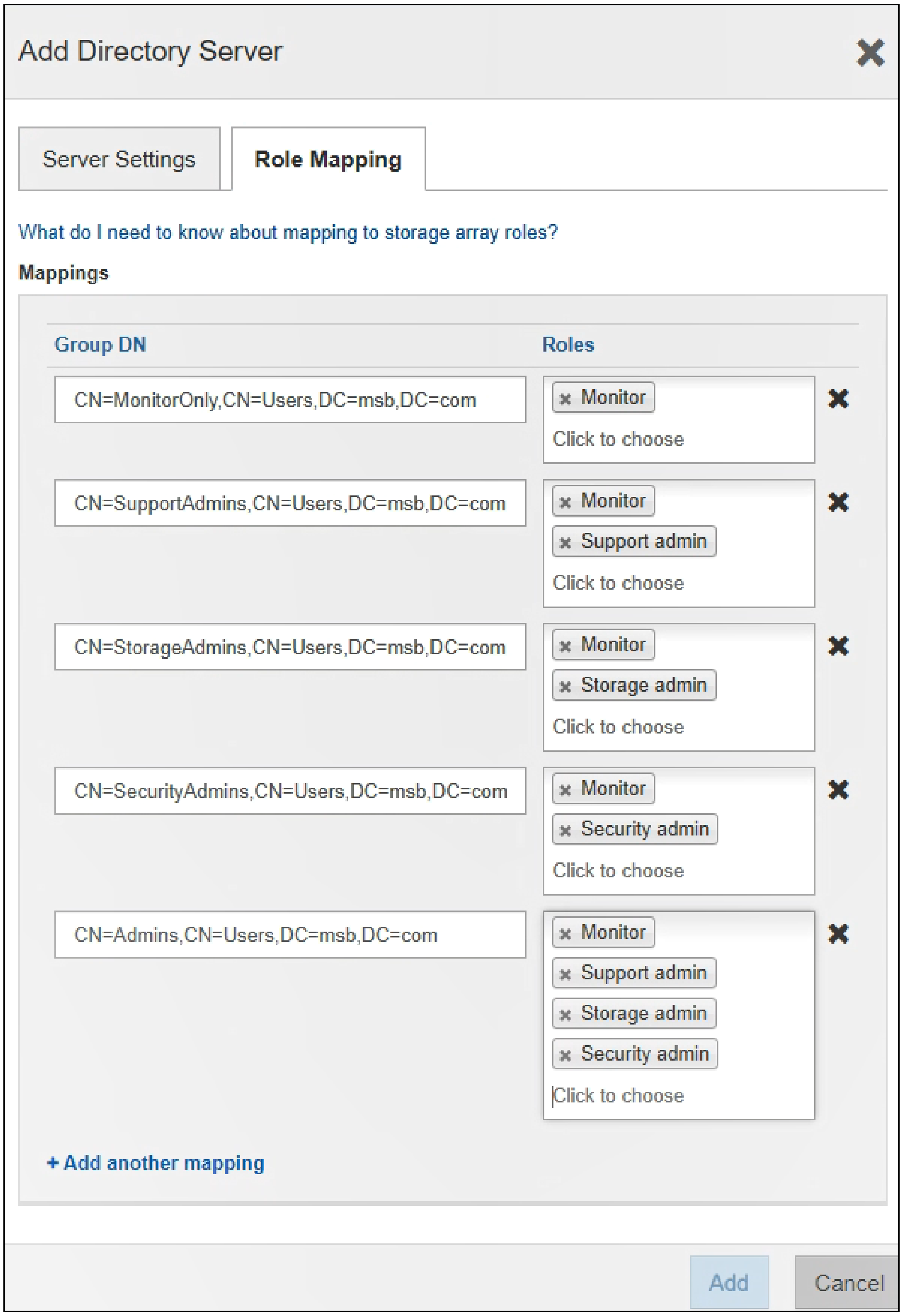
   The system performs a validation, making sure that the storage system and LDAP server can communicate. If you see an error message, refer to Table 3.

6. Click the Role Mapping tab.

7. Assign LDAP groups to the predefined roles as described in the following table. A group can have multiple assigned roles.

Field	Description
Group DN	Specify the group distinguished name (DN) for the LDAP user group to be mapped. **Note:** Nested groups are not supported.
Roles	Click in the field and select one of the local user roles to be mapped to the Group DN. You must individually select each role you want to include for this group. **Note:** The Monitor role is required in combination with the other roles to log in to the SANtricity application. The mapped roles include the following permissions: • **Storage admin** – Full read/write access to storage objects on the storage systems, but no access to the security configuration. • **Security admin** – Access to the security configuration in access management and certificate management. • **Support admin** – Access to all hardware resources on storage systems, failure data, and MEL events. No access to storage objects or the security configuration. • **Monitor** – Read-only access to all storage objects, but no access to the security configuration.

See the following screen shot for an example.



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=com	Monitor Security admin Click to choose
CN=Admins,CN=Users,DC=msb,DC=com	Monitor Support admin Storage admin Security admin Click to choose

8. If desired, click +Add Another Mapping to enter more group-to-role mappings.
9. When you are finished, click Add.

The system performs a validation making sure that the storage system and LDAP server can communicate. If you see an error message, such as `Service server connection failed`, or `Failed connection … (Web Server 422)`, see the following table to troubleshoot the issue.

Table 3) Common LDAP connection problems and solutions.

Problem	Solution
LDAP server settings are incorrect.	The connection will fail if the LDAP server settings are incorrect. Go to the Server Settings tab and make sure there are no errors in the domain name or URL of the directory server or extra spaces in the values. The domain name must be specified as `username@domain`. Valid DNS names can contain only: ASCII letters **a** through **z** (not case sensitive), digits **0** through **9**, and a hyphen (**-**), but cannot start with a hyphen. The URL must be specified as `ldap[s]://host:port`.
Search base DN and Group DN settings are incorrect.	If your Group DN for the role mapping is not within the search base DN, the connection status will report Pass, but when you try to log in to System Manager, a Login Failed error occurs. In the audit logs, the HTTP Return status will be 401 Unauthorized. Go to the Server Settings tab and verify that the Search base DN is correct. This field specifies the LDAP context to search for users, and is typically in the form of: `CN=Users, DC=cpoc, DC=local` The CN= should be your group name, not an individual user name. Next, go to the Role Mappings tab and make sure the Group DN is correct. This is the group distinguished name (DN) for the LDAP user group to be mapped. Make sure that there are no extra spaces or special characters in the values.
Bind account information is missing	If your server configuration requires a binding account for search queries, you must enter binding account information. Go to the Server Settings tab and enter the account name in an LDAP-type format. For example, if the bind user is called "bindacct," then you might enter a value such as: `CN=bindacct,CN=Users,DC=cpoc,DC=local` In addition, you must enter the password for the bind account.
LDAP server is using TLS 1.2 or below	TLS 1.0 and 1.1 were deprecated starting in the 11.50 controller firmware. Enable TLS 1.2 on the LDAP server.
NTP server is not configured	The storage array and the LDAP server might be experiencing a time-drift issue. To resolve this problem, you can configure a connection to the Network Time Protocol (NTP) server. Go to the Hardware page, and then click the controller you want to configure. From the controller's context menu, select Configure NTP Server.
LDAP server is using nested groups	Nested groups are not supported in SANtricity applications. Enter a single group in the Group DN field.
LDAP is using the wrong port	Use port 639 for Secure SSL.

4 Security Assertion Markup Language (SAML)

For user authentication in System Manager, you can use SAML 2.0 capabilities, which are embedded in the E-Series storage system (SANtricity OS 11.40.2 and later). 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.

Note: Authentication with SAML is only available in System Manager. For detailed information about its implementation, see TR-4712 - NetApp SANtricity Management Security.

To configure SAML, you must establish a connection between an IdP and the storage provider:

- An IdP is an external system used to request credentials from a user and to determine if that user is successfully authenticated. The IdP can be configured to provide multi-factor authentication and to use any user database, such as Active Directory. Your security team is responsible for maintaining the IdP.
- A service provider is a system that controls user authentication and access. When you configure SAML, the storage system acts as the service provider for requesting authentication from the IdP. To establish a trust relationship between the IdP and storage system, you share metadata files between these two entities. Next, you map the IdP user entities to the embedded roles. Finally, you test the connection and SSO logins before enabling SAML.

Note: After SAML is enabled, you **cannot** disable it through the UI or edit the IdP settings. SAML cannot be disabled without having physical access to the hardware. To disable SAML, you must have serial shell access to a controller. Contact NetApp technical support for instructions.

4.1 Requirements for Using SAML

A security administrator must configure an IdP in your network. NetApp supports Shibboleth and Microsoft ADFS as IdPs.

Before you begin configuration in System Manager, confirm that the IdP administrator has performed the following tasks:

- Configured user attributes and groups in the IdP system.
- Verified that the IdP supports the ability to return a Name ID on authentication.
- Verified that the IdP server and controller clocks are synchronized (either through an NTP server or by adjusting the controller clock settings).
- Downloaded an IdP metadata file from the IdP system and copied it to the local system used for accessing System Manager.

  Note: The IdP must provide attributes so that System Manager can 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 IdP. Refer to the official documentation for those products to understand how to set up attributes to be returned to System Manager during authentication.

In addition, you must meet the following prerequisites:

- Your system is using SANtricity OS 11.40.2 and later.
- You know the IP address or domain name of each controller in the storage system.

4.2 Restrictions when Using SAML

When using SAML, be aware of the following restrictions:

- Once SAML is enabled, you cannot disable it through the UI or edit the IdP settings. If you need to disable or edit the SAML configuration, contact NetApp technical support for assistance. We recommend that you test the single sign-on (SSO) logins before you enable SAML in the final configuration step. (The system also performs an SSO login test before enabling SAML.)
- If you must disable SAML in the future, the system automatically restores the previous authentication configuration (for example, Local User Roles and/or Directory Services).
- If Directory Services (LDAP) is currently configured for user authentication, SAML overrides that configuration.

- When SAML is configured, it is the only method used to authenticate users for access to System Manager. Other forms of management no longer work because they cannot authenticate. As a result, the following SANtricity clients cannot access storage system resources:
  - Enterprise Management Window (EMW), for older model arrays
  - CLI
  - Software development kit (SDK)
  - In-band
  - HTTP Basic Authentication REST API
  - Login using standard REST API endpoint

4.3 Previous LDAP Configurations

If you enable SAML when Directory Services is configured as the authentication method, SAML supersedes Directory Services in System Manager. If you disable SAML later, the Directory Services configuration returns to its previous configuration.

4.4 Configuring SAML with System Manager

Configuring SAML authentication is a multi-step procedure:

- Step 1: Upload the IdP metadata file
- Step 2: Export service provider files
- Step 3: Map roles
- Step 4: Test SSO login
- Step 5: Enable SAML

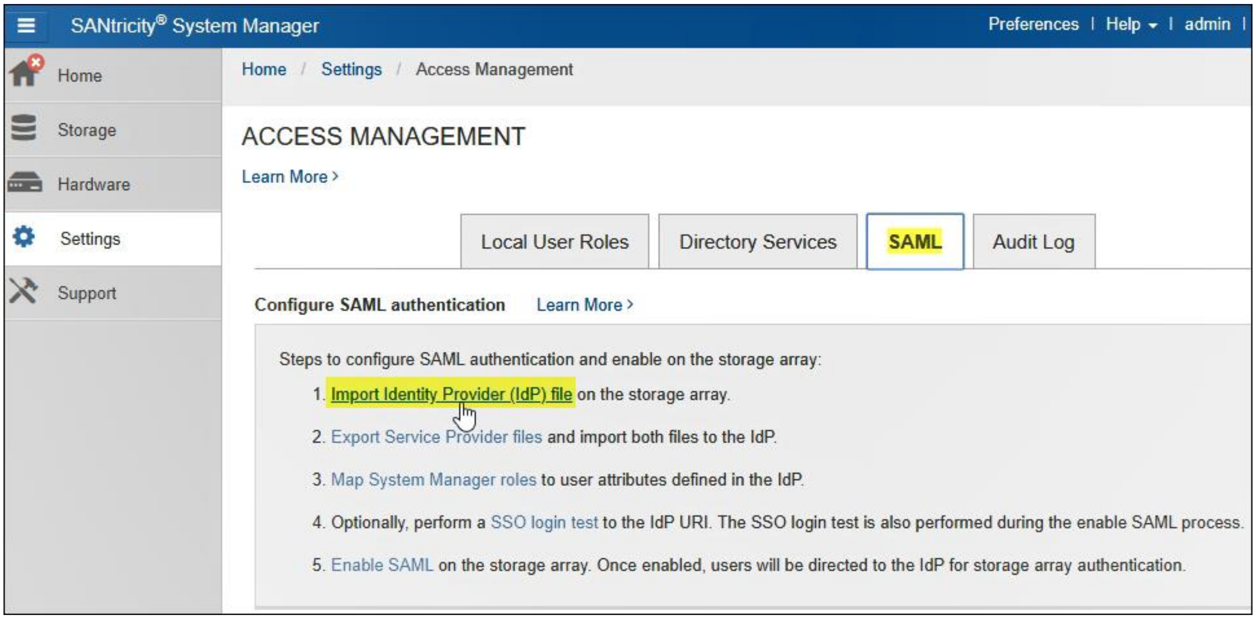
Step 1: Uploading the IdP Metadata File

In this task, you upload a metadata file from the IdP into System Manager. The IdP system needs this metadata to redirect authentication requests to the correct URL and to validate responses received. You only need to upload one metadata file for the storage system, even if there are two controllers.

To provide the storage system with IdP connection information, complete the following steps:

1. Log into System Manager with a user profile that includes Security Admin permissions. Otherwise, the Access Management functions do not appear.
2. Select Settings > Access Management.
3. Select the SAML tab.

   The page displays an overview of configuration steps.
4. Click the Import Identity Provider (IdP) File link.



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.

The Import Identity Provider File dialog box opens.

5. Click Browse to select and upload the IdP metadata file you copied to your local system.

   After you select the file, the IdP Entity ID is displayed.

6. Click Import.

Step 2: Exporting Service Provider Files

In this task, you export metadata from the controllers (one file for each controller). The IdP needs this metadata to establish a trust relationship with the controllers and to process authorization requests. The file includes information such as the controller domain name or IP address, so that the IdP can communicate with the service providers.

1. Click the Export Service Provider Files link.

   The Export Service Provider Files dialog opens.

2. Enter the controller IP address or DNS name in the Controller A field, and then click Export to save the metadata file to your local system. If the storage array includes two controllers, repeat this step for the second controller in the Controller B field.

   After you click Export, the service provider metadata is downloaded to your local system. Make a note of where the file is stored.

3. From the local system, locate the service provider metadata file(s) you exported.

   There is one XML-formatted file for each controller.

4. From the IdP server, import the service provider metadata file(s) to establish the trust relationship. You can either import the files directly or you can manually enter the controller information from the files.

Step 3: Mapping Roles

In this task, you use System Manager to map IdP groups to local user roles.

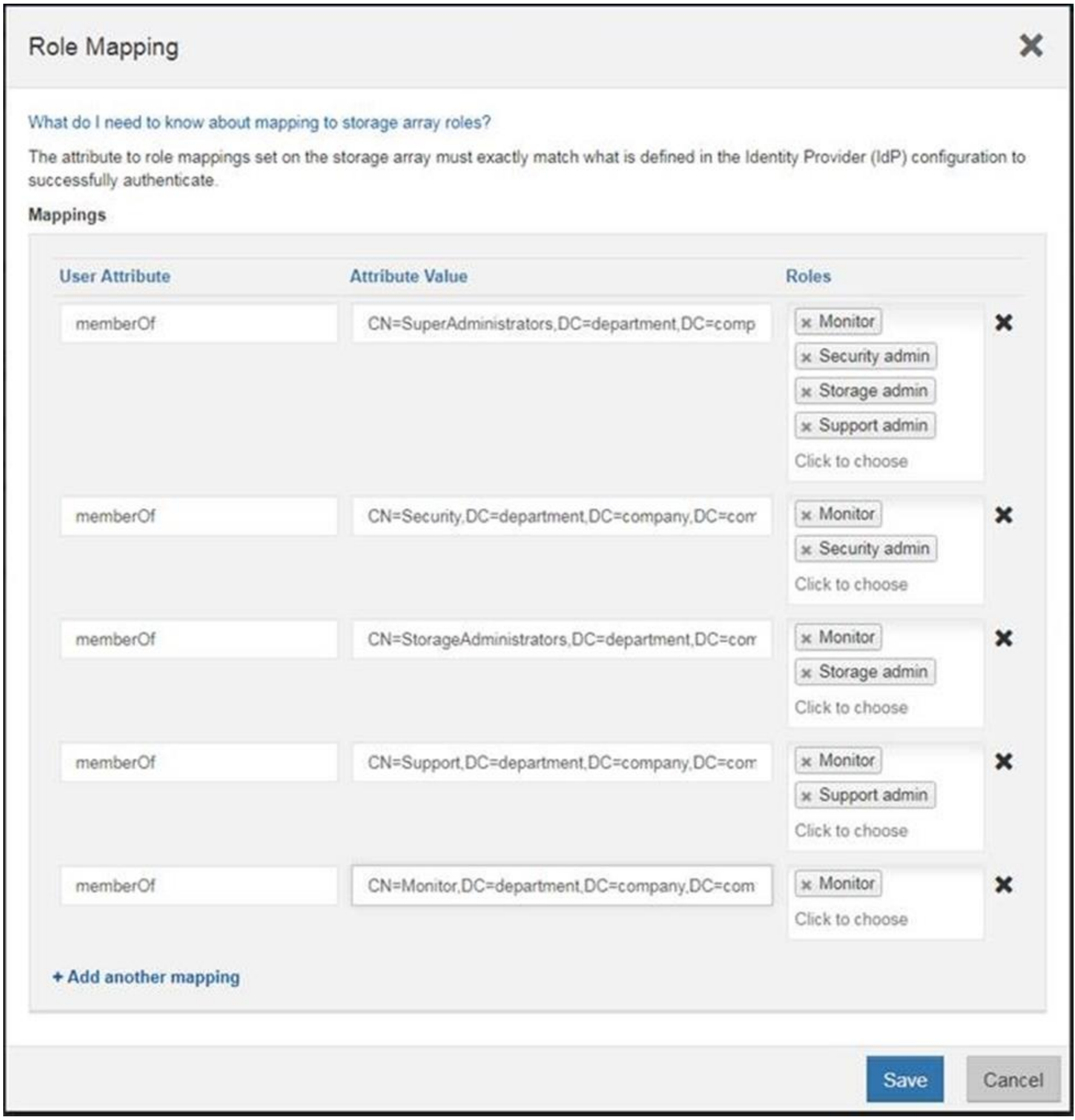
1. Click the Map System Manager Roles link.

   The Role Mapping dialog box opens.

2. Assign IdP user attributes and groups to the predefined roles. A group can have multiple assigned roles.

Field	Description
User Attribute	Specify the attribute (for example, "member of") for the SAML group to be mapped. **Note:** In addition to user attributes, the IdP needs to return a valid NameID for 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 System Manager.
Attribute Value	Specify the attribute value for the group to be mapped.
Roles	Click in the field and select one of the storage array's roles to be mapped to the attribute. You must individually select each role you want to include. The Monitor role is required in combination with the other roles to log in to System Manager. The Security Admin role is also required for at least one group. The mapped roles include the following permissions: • **Storage admin** – Full read/write access to storage objects on the arrays, but no access to the security configuration. • **Security admin** – Access to the security configuration in access management and certificate management. • **Support admin** – Access to all hardware resources on storage systems, failure data, and event log events. No access to storage objects or the security configuration. • **Monitor** – Read-only access to all storage objects, but no access to the security configuration.

See the following screen shot for an example.



What do I need to know about mapping to storage array roles?

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=cor	× Monitor × Security admin Click to choose
memberOf	CN=StorageAdministrators,DC=department,DC=cor	× Monitor × Storage admin Click to choose
memberOf	CN=Support,DC=department,DC=company,DC=cor	× Monitor × Support admin Click to choose
memberOf	CN=Monitor,DC=department,DC=company,DC=com	× Monitor Click to choose

If

3. If desired, click +Add Another Mapping to enter more group-to-role mappings.

   Note: System Manager allows you to change role mappings later, even after SAML is enabled.

4. When you are finished with the mappings, click Save.

Step 4: Testing the SSO Login

To ensure that the IdP system and storage array can communicate, you should test an SSO login. This test is also performed during the final step for enabling SAML.

1. Select the Test SSO Login link.

   A dialog opens for entering SSO credentials.

2. Enter login credentials for a user with both Security Admin permissions and Monitor permissions.

A dialog opens while the system tests the login with your configured IdP. This test redirects the user to the IdP login page and validates that the user was properly authenticated and authorized using all configured settings.

3. Look for a Test Successful message.
4. If the test completes successfully, go to the next step for enabling SAML.

   If the test does **not** complete successfully, an error message appears with further information. Verify the following and then try the test again:

   – The user belongs to a group with permissions for Security Admin and Monitor.

   – The metadata you uploaded for the IdP server is correct.

   – The controller addresses in the SP metadata files are correct.

   If you still see an error, see the following table to review possible issues with the IdP configuration.

Table 4) Common SAML configuration issues.

Issue	Description
Storage array 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 array and IdP clocks are more than 5 minutes apart, SAML authentication in System Manager fails.
Expired IdP certificates	If the IdP certificates have expired, all SAML authentication in System Manager fails. In that case, you must disable SAML with the help of a NetApp technical support engineer, make a serial connection to the storage array, and reimport their IdP metadata files with valid x509 certificates embedded in the metadata.
Unable to map roles	If the SSO login test continuously fails with the error that it was unable to map proper roles, the identity provider or System Manager might not be configured properly to map attributes to roles. This can also occur because the security admin and storage monitor roles are required for a successful test.
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 System Manager identifying the user with a randomly generated ID. Refer to the IdP documentation to configure a NameID to be sent to System Manager.

Step 5: Enabling SAML

Your final step is to enable SAML user authentication. During this process, the system also prompts you to test an SSO login. The SSO login test process is described in the previous step.

Note: Once SAML is enabled, you **cannot** disable it through the UI or edit the IdP settings. If you need to disable or edit the SAML configuration, contact technical support for assistance.

1. From the SAML tab, select the Enable SAML link.

   The Confirm Enable SAML dialog opens.
2. Type `enable`, and then click Enable.
3. Enter user credentials for an SSO login test.

   After the system enables SAML, it terminates all active sessions and begins authenticating users through SAML.

Where to Find Additional Information

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

- NetApp SANtricity Management Security configuration guide:
  TR-4712- NetApp SANtricity Management Security
- NetApp Product Documentation:
  https://docs.netapp.com

Version History

Version	Date	Document Version History
Version 1.0	July 2020	Initial release.

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

Copyright Information

Trademark Information