Access management

SANtricity software

NetApp
November 03, 2025

Table of Contents

Access management

Learn about SANtricity Unified Manager access management

Access Management is a method of configuring user authentication in SANtricity Unified Manager.

What authentication methods are available?

The following authentication methods are available:

- **Local user roles** — Authentication is managed through RBAC (role-based access control) capabilities. Local user roles include pre-defined user profiles and roles with specific access permissions.
- **Directory services** — Authentication is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory.
- **SAML** — Authentication is managed through an Identity Provider (IdP) using SAML 2.0.

Learn more:

- How Access Management works
- Access Management terminology
- Permissions for mapped roles
- SAML

How do I configure Access Management?

The SANtricity software is pre-configured to use local user roles. If you want to use LDAP, you can configure it under the Access Management page.

Learn more:

- Access Management with local user roles
- Access Management with directory services
- Configure SAML

Concepts

How access management works in SANtricity Unified Manager

Use Access Management to establish user authentication in SANtricity Unified Manager.

Configuration workflow

Access Management configuration works as follows:

1. An administrator logs in to Unified Manager with a user profile that includes Security admin permissions.

> (i) For first-time login, the username `admin` is automatically displayed and cannot be changed. The `admin` user has full access to all functions in the system. The password must be set on first-time login.

2. The administrator navigates to Access Management in the user interface, which includes pre-configured local user roles. These roles are an implementation of RBAC (role-based access control) capabilities.

3. The administrator configures one or more of the following authentication methods:

   - **Local user roles** — Authentication is managed through RBAC capabilities. Local user roles include pre-defined users and roles 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. No configuration is necessary, other than setting passwords for users.

   - **Directory services** — Authentication is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory. An administrator connects to the LDAP server, and then maps the LDAP users to the local user roles.

   - **SAML** — Authentication is managed through an Identity Provider (IdP) using the Security Assertion Markup Language (SAML) 2.0. An administrator establishes communication between the IdP system and the storage array, and then maps IdP users to the local user roles embedded in the storage array.

4. The administrator provides users with login credentials for Unified Manager.

5. Users log in to the system by entering their credentials. During login, the system performs the following background tasks:

   - Authenticates the user name and password against the user account.

   - Determines the user's permissions based on the assigned roles.

   - Provides the user with access to functions in the user interface.

   - Displays the user name in the top banner.

Functions available in Unified Manager

Access to functions depends on a user's assigned roles, which include the following:

- **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 arrays, 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.

An unavailable function is either grayed out or does not display in the user interface.

Learn about SANtricity Unified Manager access management terminology

Learn how the Access Management terms apply to SANtricity Unified Manager.

Term	Description
Active Directory	Active Directory (AD) is a Microsoft directory service that uses LDAP for Windows domain networks.
Binding	Bind operations are used to authenticate clients to the directory server. Binding usually requires account and password credentials, but some servers allow for anonymous bind operations.
CA	A certificate authority (CA) is a trusted entity that issues electronic documents, called digital certificates, for Internet security. These certificates identify website owners, which allows for secure connections between clients and servers.
Certificate	A certificate identifies the owner of a site for security purposes, which prevents attackers from impersonating the site. The certificate contains information about the site owner and the identity of the trusted entity who certifies (signs) this information.
LDAP	Lightweight Directory Access Protocol (LDAP) is an application protocol for accessing and maintaining distributed directory information services. This protocol allows many different applications and services to connect to the LDAP server for validating users.
RBAC	Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users. Unified Manager includes predefined roles.
SAML	Security Assertion Markup Language (SAML) is an XML-based standard for authentication and authorization between two entities. SAML allows for multi-factor authentication, in which users must provide two or more items for proving their identity (for example, a password and fingerprint). The storage array's embedded SAML feature is SAML2.0 compliant for identity assertion, authentication, and authorization.
SSO	Single sign-on (SSO) is an authentication service that allows for one set of login credentials to access multiple applications.
Web Services Proxy	The Web Services Proxy, which provides access through standard HTTPS mechanisms, allows administrators to configure management services for storage arrays. The proxy can be installed on Windows or Linux hosts. The Unified Manager interface is available with the Web Services Proxy.

Permissions for mapped roles

The RBAC (role-based access control) capabilities include pre-defined users with one or more roles mapped to them. Each role includes permissions for accessing tasks in SANtricity Unified Manager.

The roles provide user access to tasks, as follows:

- **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 arrays, 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.

If a user does not have permissions for a certain function, that function is either unavailable for selection or does not display in the user interface.

Access management with local user roles in SANtricity Unified Manager

Administrators can use RBAC (role-based access control) capabilities enforced in SANtricity Unified Manager. These capabilities are referred to as "local user roles."

Configuration workflow

Local user roles are pre-configured in the system. To use local user roles for authentication, administrators can do the following:

1. An administrator logs in to Unified Manager with a user profile that includes Security admin permissions.

   > ⓘ The `admin` user has full access to all functions in the system.

2. An administrator reviews the user profiles, which are predefined and cannot be modified.
3. Optionally, the administrator assigns new passwords for each user profile.
4. Users log in to the system with their assigned credentials.

Management

When using only local user roles for authentication, administrators can perform the following management tasks:

- Change passwords.
- Set a minimum length for passwords.
- Allow users to log in without passwords.

Access management with directory services in SANtricity Unified Manager

Administrators can use an LDAP (Lightweight Directory Access Protocol) server and a directory service, such as Microsoft's Active Directory.

Configuration workflow

If an LDAP server and directory service are used in the network, configuration works as follows:

1. An administrator logs in to Unified Manager with a user profile that includes Security admin permissions.

> ⓘ   The `admin` user has full access to all functions in the system.

2. The administrator enters the configuration settings for the LDAP server. Settings include the domain name, URL, and Bind account information.

3. If the LDAP server uses a secure protocol (LDAPS), the administrator uploads a certificate authority (CA) certificate chain for authentication between the LDAP server and the host system where the Web Services Proxy is installed.

4. After the server connection is established, the administrator maps the user groups to the local user roles. These roles are predefined and cannot be modified.

5. The administrator tests the connection between the LDAP server and the Web Services Proxy.

6. Users log in to the system with their assigned LDAP/Directory Services credentials.

Management

When using directory services for authentication, administrators can perform the following management tasks:

- Add a directory server.
- Edit directory server settings.
- Map LDAP users to local user roles.
- Remove a directory server.
- Change passwords.
- Set a minimum length for passwords.
- Allow users to log in without passwords.

Access management with SAML in SANtricity Unified Manager

For Access Management, administrators can use the Security Assertion Markup Language (SAML) 2.0 capabilities embedded in the array.

Configuration workflow

SAML configuration works as follows:

1. An administrator logs in to Unified Manager with a user profile that includes Security Admin permissions.

> ⓘ   The `admin` user has full access to all functions in System Manager.

2. The administrator goes to the **SAML** tab under Access Management.

3. An administrator configures communications with the Identity Provider (IdP). An IdP is an external system used to request credentials from a user and determine if the user is successfully authenticated. To configure communications with the storage array, the administrator downloads the IdP metadata file from the IdP system, and then uses Unified Manager to upload the file to the storage array.

4. An administrator establishes a trust relationship between the Service Provider and the IdP. A Service Provider controls user authorization; in this case, the controller in the storage array acts as the Service Provider. To configure communications, the administrator uses Unified Manager to export a Service Provider metadata file for the controller. From the IdP system, the administrator then imports the metadata file to the IdP.

	Administrators should also make sure that the IdP supports the ability to return a Name ID on authentication.

5. The administrator maps the storage array's roles to user attributes defined in the IdP. To do this, the administrator uses Unified Manager to create the mappings.

6. The administrator tests the SSO login to the IdP URL. This test ensures the storage array and IdP can communicate.

	Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance.

7. From Unified Manager, the administrator enables SAML for the storage array.

8. Users log in to the system with their SSO credentials.

Management

When using SAML for authentication, administrators can perform the following management tasks:

- Modify or create new role mappings
- Export Service Provider files

Access restrictions

When SAML is enabled, users cannot discover or manage storage for that array from the legacy Storage Manager interface.

In addition, the following clients cannot access storage array services and resources:

- Enterprise Management Window (EMW)
- Command-line interface (CLI)
- Software Developer Kits (SDK) clients
- In-band clients
- HTTP Basic Authentication REST API clients
- Login using standard REST API endpoint

Use local user roles

View local user roles

From the Local User Roles tab, you can view the mappings of the users to the default roles. These mappings are part of the RBAC (role-based access controls) enforced in the Web Services Proxy for SANtricity Unified Manager.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

About this task

The users and mappings cannot be changed. Only passwords can be modified.

Steps

1. Select **Access Management**.

2. Select the **Local User Roles** tab.

   The users are shown in the table:

   - **admin** — Super administrator who has access to all functions in the system. This user includes all roles.

   - **storage** — The administrator responsible for all storage provisioning. This user includes the following roles: Storage Admin, Support Admin, and Monitor.

   - **security** — The user responsible for security configuration, including Access Management and Certificate Management. This user includes the following roles: Security Admin and Monitor.

   - **support** — The user responsible for hardware resources, failure data, and firmware upgrades. This user includes the following roles: Support Admin and Monitor.

   - **monitor** — A user with read-only access to the system. This user includes only the Monitor role.

   - **rw** (read/write) — This user includes the following roles: Storage Admin, Support Admin, and Monitor.

   - **ro** (read only) — This user includes only the Monitor role.

Change passwords for local user profiles in SANtricity Unified Manager

You can change the user passwords for each user in Access Management.

Before you begin

- You must be logged in as the local administrator, which includes Root admin permissions.

- You must know the local administrator password.

About this task

Keep these guidelines in mind when choosing a password:

- Any new local user passwords must meet or exceed the current setting for a minimum password (in View/Edit Settings).

- Passwords are case sensitive.

- Trailing spaces are not removed from passwords when they are set. Be careful to include spaces if they were included in the password.

- For increased security, use at least 15 alphanumeric characters and change the password frequently.

Steps

1. Select **Access Management**.

2. Select the **Local User Roles** tab.

3. Select a user from the table.

   The Change Password button becomes available.

4. Select **Change Password**.

The Change Password dialog box opens.

5. If no minimum password length is set for local user passwords, you can select the checkbox to require the user to enter a password to access the system.

6. Enter the new password for the selected user in the two fields.

7. Enter your local administrator password to confirm this operation, and then click **Change**.

Results

If the user is currently logged in, the password change causes the user's active session to terminate.

Change local user password settings in SANtricity Unified Manager

You can set the minimum required length for all new or updated local user passwords. You also can allow local users to access the system without entering a password.

Before you begin

You must be logged in as the local administrator, which includes Root admin permissions.

About this task

Keep these guidelines in mind when setting the minimum length for local user passwords:

- Setting changes do not affect existing local user passwords.
- The minimum required length setting for local user passwords must be between 0 and 30 characters.
- Any new local user passwords must meet or exceed the current minimum length setting.
- Do not set a minimum length for the password if you want local users to access the system without entering a password.

Steps

1. Select **Access Management**.

2. Select the **Local User Roles** tab.

3. Select **View/Edit Settings**.

   The Local User Password Settings dialog box opens.

4. Do one of the following:

   ○ To allow local users to access the system *without* entering a password, clear the "Require all local user passwords to be at least" checkbox.

   ○ To set a minimum password length for all local user passwords, select the "Require all local user passwords to be at least" checkbox and then use the spinner box to set the minimum required length for all local user passwords.

   Any new local user passwords must meet or exceed the current setting.

5. Click **Save**.

Use directory services

Add directory server in SANtricity Unified Manager

To configure authentication for Access Management, you establish communications between an LDAP server and the host running the Web Services Proxy for SANtricity Unified Manager. You then map the LDAP user groups to the local user roles.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

- User groups must be defined in your directory service.

- LDAP server credentials must be available, including the domain name, server URL, and optionally the bind account user name and password.

- For LDAPS servers using a secure protocol, the LDAP server's certificate chain must be installed on your local machine.

About this task

Adding a directory server is a two-step process. First you enter the domain name and URL. If your server uses a secure protocol, you also must upload a CA certificate for authentication if it is signed by a non-standard signing authority. If you have credentials for a bind account, you also can enter your user account name and password. Next, you map the LDAP server's user groups to local user roles.

Steps

1. Select **Access Management**.

2. From the **Directory Services** tab, select **Add Directory Server**.

   The Add Directory Server dialog box opens.

3. In the **Server Settings** tab, enter the credentials for the LDAP server.

Field details

Setting	Description
Configuration settings	
Domain(s)	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.
Server URL	Enter the URL for accessing the LDAP server in the form of `ldap[s]://`**`host:*port*`**.
Upload certificate (optional)	ⓘ This field appears only if an LDAPS 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 (optional)	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`.
Bind password (optional)	ⓘ This field appears when you enter a bind account. Enter the password for the bind account.
Test server connection before adding	Select this checkbox if you want to make sure 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.
Privilege settings	
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`.
Group attribute(s)	Enter a list of group attributes on the user, which is used for group-to-role mapping. For example: `memberOf, managedObjects`.

4. Click the **Role Mapping** tab.

5. Assign LDAP groups to the predefined roles. A group can have multiple assigned roles.

Field details

Setting	Description
Mappings	
Group DN	Specify the group distinguished name (DN) for the LDAP user group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern: \.[]{}()<>*+-=!?^$|
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. The Monitor role is required in combination with the other roles to log in to SANtricity Unified Manager. 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 arrays, 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.

> ℹ️ The Monitor role is required for all users, including the administrator.

6. If desired, click **Add another mapping** to enter more group-to-role mappings.

7. When you are finished with the mappings, click **Add**.

The system performs a validation, making sure that the storage array and LDAP server can communicate. If an error message appears, check the credentials entered in the dialog box and re-enter the information if necessary.

Edit directory server settings and role mappings in SANtricity Unified Manager

If you previously configured a directory server in Access Management, you can change its settings at any time. Settings include the server connection information and the group-to-role mappings.

Before you begin

• You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access

Management functions do not appear.

- A directory server must be defined.

Steps

1. Select **Access Management**.
2. Select the **Directory Services** tab.
3. If more than one server is defined, select the server you want to edit from the table.
4. Select **View/Edit Settings**.

   The Directory Server Settings dialog box opens.

5. In the **Server Settings** tab, change the desired settings.

Field details

Setting	Description
Configuration settings	
Domain(s)	The domain name(s) of the LDAP server(s). 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.
Server URL	The URL for accessing the LDAP server in the form of `ldap[s]://host:port`.
Bind account (optional)	The read-only user account for search queries against the LDAP server and for searching within the groups.
Bind password (optional)	The password for the bind account. (This field appears when a bind account is entered.)
Test server connection before saving	Checks that the system can communicate with the LDAP server configuration. The test occurs after you click **Save**. If this checkbox is selected and the test fails, the configuration is not changed. You must resolve the error or clear the checkbox to skip the testing and re-edit the configuration.
Privilege settings	
Search base DN	The LDAP context to search for users, typically in the form of `CN=Users, DC=cpoc, DC=local`.
Username attribute	The attribute that is bound to the user ID for authentication. For example: `sAMAccountName`.
Group attribute(s)	A list of group attributes on the user, which is used for group-to-role mapping. For example: `memberOf, managedObjects`.

6. In the **Role Mapping** tab, change the desired mapping.

Field details

Setting	Description
Mappings	
Group DN	The domain name for the LDAP user group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern: \.[]{}()<>*+-=!?^$|
Roles	The roles to be mapped to the Group DN. You must individually select each role you want to include for this group. The Monitor role is required in combination with the other roles to log in to SANtricity Unified Manager. The roles include the following: • **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 arrays, 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.

> ⓘ The Monitor role is required for all users, including the administrator.

7. If desired, click **Add another mapping** to enter more group-to-role mappings.

8. Click **Save**.

Results

After you complete this task, any active user sessions are terminated. Only your current user session is retained.

Remove directory server

To break the connection between a directory server and the Web Services Proxy, you can remove the server information from the Access Management page. You might want to perform this task if you configured a new server, and then want to remove the old one.

Before you begin

You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

About this task

After you complete this task, any active user sessions are terminated. Only your current user session is retained.

Steps

1. Select **Access Management**.

2. Select the **Directory Services** tab.

3. From the list, select the directory server you want to delete.

4. Click **Remove**.

   The Remove Directory Server dialog box opens.

5. Type `remove` in the field, and then click **Remove**.

   The directory server configuration settings, privilege settings, and role mappings are removed. Users can no longer log in with credentials from this server.

Use SAML

Configure SAML in SANtricity Unified Manager

To configure authentication for Access Management, you can use the Security Assertion Markup Language (SAML) capabilities embedded in the storage array. This configuration establishes a connection between an Identity Provider and the Storage Provider.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

- You must know the IP address or domain name the controller in the storage array.

- An IdP administrator has configured an IdP system.

- An IdP administrator has ensured that the IdP supports the ability to return a Name ID on authentication.

- An administrator has ensured that the IdP server and controller clock is synchronized (either through an NTP server or by adjusting the controller clock settings).

- An IdP metadata file is downloaded from the IdP system and is available on the local system used for accessing Unified Manager.

About this task

An Identity Provider (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 (SP) is a system that controls user authentication and access. When Access Management is configured with SAML, the storage array acts as the Service Provider for requesting authentication from the Identity Provider. To establish a connection between the IdP and storage array, you share metadata files between these two entities. Next, you map the IdP user entities to the storage array roles. And finally, you test the connection and SSO logins before enabling SAML.

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

> ⚠️ **Editing and Disabling.** Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance.

Configuring SAML authentication is a multi-step procedure.

Step 1: Upload the IdP metadata file

To provide the storage array with IdP connection information, you import IdP metadata into Unified Manager. The IdP system needs this metadata to redirect authentication requests to the correct URL and to validate responses received.

Steps

1. Select **Settings › Access Management**.

2. Select the **SAML** tab.

   The page displays an overview of configuration steps.

3. Click the **Import Identity Provider (IdP) file** link.

   The Import Identity Provider File dialog box opens.

4. 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.

5. Click **Import**.

Step 2: Export Service Provider files

To establish a trust relationship between the IdP and the storage array, you import the Service Provider metadata into the IdP. The IdP needs this metadata to establish a trust relationship with the controller 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.

Steps

1. Click the **Export Service Provider files** link.

   The Export Service Provider Files dialog box 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.

   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 XML-formatted Service Provider metadata file you exported.

4. From the IdP server, import the Service Provider metadata file to establish the trust relationship. You can either import the file directly or you can manually enter the controller information from the file.

Step 3: Map roles

To provide users with authorization and access to Unified Manager, you must map the IdP user attributes and

group memberships to the storage array's predefined roles.

Before you begin

- An IdP administrator has configured user attributes and group membership in the IdP system.
- The IdP metadata file is imported into Unified Manager.
- A Service Provider metadata file for the controller is imported into the IdP system for the trust relationship.

Steps

1. Click the link for **mapping Unified Manager** roles.

   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 details

Setting	Description
Mappings	
User Attribute	Specify the attribute (for example, "member of") for the SAML group to be mapped.
Attribute Value	Specify the attribute value for the group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern: \.[]{}()<>*+-=!?^$|
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 Unified 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 the storage objects (for example, volumes and disk pools), but no access to the security configuration. • **Security admin** — Access to the security configuration in Access Management, certificate management, audit log management, and the ability to turn the legacy management interface (SYMbol) on or off. • **Support admin** — Access to all hardware resources on the storage array, failure data, MEL events, and controller firmware upgrades. No access to storage objects or the security configuration. • **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

> **ⓘ** The Monitor role is required for all users, including the administrator. Unified Manager will not operate correctly for any user without the Monitor role present.

3. If desired, click **Add another mapping** to enter more group-to-role mappings.

> **ⓘ** Role mappings can be modified after SAML is enabled.

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

Step 4: Test SSO login

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

Before you begin

- The IdP metadata file is imported into Unified Manager.
- A Service Provider metadata file for the controller is imported into the IdP system for the trust relationship.

Steps

1. Select the **Test SSO Login** link.

   A dialog box opens for entering SSO credentials.

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

   A dialog box opens while the system tests the login.

3. Look for a Test Successful message. 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. Make sure that:

   - 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 address in the SP metadata files is correct.

Step 5: Enable SAML

Your final step is to finish the SAML configuration for 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.

Before you begin

- The IdP metadata file is imported into Unified Manager.
- A Service Provider metadata file for the controller is imported into the IdP system for the trust relationship.
- At least one Monitor and one Security Admin role mapping is configured.

> **⚠** **Editing and Disabling.** Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance.

Steps

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

   The Confirm Enable SAML dialog box opens.

2. Type `enable`, and then click **Enable**.

3. Enter user credentials for an SSO login test.

Results

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

Change SAML role mappings in SANtricity Unified Manager

If you previously configured SAML for Access Management, you can change the role mappings between the IdP groups and the storage array's predefined roles.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.
- An IdP administrator has configured user attributes and group membership in the IdP system.
- SAML is configured and enabled.

Steps

1. Select **Settings › Access Management**.

2. Select the **SAML** tab.

3. Select **Role Mapping**.

   The Role Mapping dialog box opens.

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

   > ⚠ Be careful that you do not remove your permissions while SAML is enabled, or you will lose access to Unified Manager.

Field details

Setting	Description
Mappings	
User Attribute	Specify the attribute (for example, "member of") for the SAML group to be mapped.
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 for this group. The Monitor role is required in combination with the other roles to log in to Unified Manager. A Security Admin role must be assigned to at least one group. The mapped roles include the following permissions: • **Storage admin** — Full read/write access to the storage objects (for example, volumes and disk pools), but no access to the security configuration. • **Security admin** — Access to the security configuration in Access Management, certificate management, audit log management, and the ability to turn the legacy management interface (SYMbol) on or off. • **Support admin** — Access to all hardware resources on the storage array, failure data, MEL events, and controller firmware upgrades. No access to storage objects or the security configuration. • **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

> (i) The Monitor role is required for all users, including the administrator. Unified Manager will not operate correctly for any user without the Monitor role present.

5. Optionally, click **Add another mapping** to enter more group-to-role mappings.

6. Click **Save**.

Results

After you complete this task, any active user sessions are terminated. Only your current user session is retained.

Export SAML Service Provider files in SANtricity Unified Manager

If necessary, you can export Service Provider metadata for the storage array and re-import the file into the Identity Provider (IdP) system.

Before you begin

• You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.

- SAML is configured and enabled.

About this task

In this task, you export metadata from the controller. The IdP needs this metadata to establish a trust relationship with the controller and to process authentication requests. The file includes information such as the controller domain name or IP address that the IdP can use for sending requests.

Steps

1. Select **Settings › Access Management**.

2. Select the **SAML** tab.

3. Select **Export**.

   The Export Service Provider Files dialog box opens.

4. Click **Export** to save the metadata file to your local system.

   > (i)   The domain name field is read-only.

   Make a note of where the file is stored.

5. From the local system, locate the XML-formatted Service Provider metadata file you exported.

6. From the IdP server, import the Service Provider metadata file. You can either import the file directly or you can manually enter the controller information.

7. Click **Close**.

User access management FAQ for SANtricity Unified Manager

This FAQ can help if you're just looking for a quick answer to a question.

Why can't I log in?

If you receive an error when attempting to log in, review these possible causes.

Login errors might occur for one of these reasons:

- You entered an incorrect user name or password.
- You have insufficient privileges.
- You attempted to log in unsuccessfully multiple times, which triggered the lockout mode. Wait 10 minutes to re-login.
- SAML authentication is enabled. Refresh your browser to log in.

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

Before adding a directory server in Access Management, you must meet certain requirements.

- User groups must be defined in your directory service.
- LDAP server credentials must be available, including the domain name, server URL, and optionally the

bind account user name and password.

- For LDAPS servers using a secure protocol, the LDAP server's certificate chain must be installed on your local machine.

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

Before mapping groups to roles, review the guidelines.

The RBAC (role-based access control) capabilities include the following roles:

- **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 arrays, 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.

> (i) The Monitor role is required for all users, including the administrator.

If you are using an LDAP (Lightweight Directory Access Protocol) server and Directory Services, make sure that:

- An administrator has defined user groups in the directory service.
- You know the group domain names for the LDAP user groups.

SAML

If you are using the Security Assertion Markup Language (SAML) capabilities embedded in the storage array, make sure that:

- An Identity Provider (IdP) administrator has configured user attributes and group membership in the IdP system.
- You know the group membership names.
- You know the attribute value for the group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern:

```
\.[]{}()<>*+-=!?^$|
```

- The Monitor role is required for all users, including the administrator. Unified Manager will not operate correctly for any user without the Monitor role present.

What do I need to know before configuring and enabling SAML?

Before configuring and enabling the Security Assertion Markup Language (SAML) capabilities for authentication, make sure you meet the following requirements and understand SAML restrictions.

Requirements

Before you begin, make sure that:

- An Identity Provider (IdP) is configured in your network. An IdP is an external system used to request credentials from a user and determine if the user is successfully authenticated. Your security team is responsible for maintaining the IdP.

- An IdP administrator has configured user attributes and groups in the IdP system.

- An IdP administrator has ensured that the IdP supports the ability to return a Name ID on authentication.

- An administrator has ensured that the IdP server and controller clock is synchronized (either through an NTP server or by adjusting the controller clock settings).

- An IdP metadata file is downloaded from the IdP system and available on the local system used for accessing Unified Manager.

- You know the IP address or domain name the controller in the storage array.

Restrictions

In addition to the requirements above, make sure you understand the following restrictions:

- Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance. We recommend that you test the SSO logins before you enable SAML in the final configuration step. (The system also performs an SSO login test before enabling SAML.)

- If you disable SAML in the future, the system automatically restores the previous configuration (Local User Roles and/or Directory Services).

- If Directory Services are currently configured for user authentication, SAML overrides that configuration.

- When SAML is configured, the following clients cannot access storage array resources:
  - Enterprise Management Window (EMW)
  - Command-line interface (CLI)
  - Software Developer Kits (SDK) clients
  - In-band clients
  - HTTP Basic Authentication REST API clients
  - Login using standard REST API endpoint

What are the local users?

Local users are predefined in the system and include specific permissions.

Local users include:

- **admin** — Super administrator who has access to all functions in the system. This user includes all roles. The password must be set on first-time login.

- **storage** — The administrator responsible for all storage provisioning. This user includes the following roles: Storage Admin, Support Admin, and Monitor. This account is disabled until a password is set.

- **security** — The user responsible for security configuration, including Access Management and Certificate Management. This user includes the following roles: Security Admin and Monitor. This account is disabled until a password is set.

- **support** — The user responsible for hardware resources, failure data, and firmware upgrades. This user includes the following roles: Support Admin and Monitor. This account is disabled until a password is set.

- **monitor** — A user with read-only access to the system. This user includes only the Monitor role. This account is disabled until a password is set.

- **rw** (read/write) — This user includes the following roles: Storage Admin, Support Admin, and Monitor. This account is disabled until a password is set.

- **ro** (read only) — This user includes only the Monitor role. This account is disabled until a password is set.