Access management

SANtricity 11.5

NetApp
January 31, 2025

Table of Contents

Access management

Concepts

How Access Management works

Access Management is a method of establishing user authentication in SANtricity System Manager. Authentication requires users to log in to these systems with their assigned credentials.

Access Management configuration and user authentication works as follows:

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

   > 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.

2. The administrator navigates to Access Management in the user interface. The storage array is pre-configured to use local user roles, which 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 enforced in the storage array. Local user roles include pre-defined user profiles 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 embedded in the storage array.
   - **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 System Manager.
5. Users log in to the system by entering their credentials.

   > If authentication is managed with SAML and an SSO (single sign-on), the system might bypass the System Manager login dialog.

   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 tasks in the user interface.
   - Displays the user name in the upper right of the interface.

Tasks available in System Manager

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

- **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.

An unavailable task is either grayed out or does not display in the user interface. For example, a user with the Monitor role can view all information about volumes, but cannot access functions for modifying that volume. The tabs for features such as **Copy Services** and **Add to Workload** will be grayed out; only View/Edit Settings is available.

User access to SANtricity Storage Manager

When local user roles and directory services are configured, users must enter credentials before performing any of the following functions in the Enterprise Management Window (EMW):

- Renaming the storage array
- Upgrading controller firmware
- Loading a storage array configuration
- Executing a script
- Attempting to perform an active operation when an unused session has timed out

If SAML is configured for a storage array, users cannot use the EMW to discover or manage storage for that array.

Access Management terminology

Learn how the Access Management terms apply to your storage array.

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.

Term	Description
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.
IdP	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.
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. RBAC controls are enforced on the storage array and include 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.
SP	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.

Term	Description
SSO	Single sign-on (SSO) is an authentication service that allows for one set of login credentials to access multiple applications.

Permissions for mapped roles

The RBAC (role-based access control) capabilities enforced on the storage array include pre-defined user profiles with one or more roles mapped to them. Each role includes permissions for accessing tasks in SANtricity System Manager.

User profiles and mapped roles are accessible from **Settings › Access Management › Local User Roles** in the user interface of either System Manager.

The roles provide user access to tasks, as follows:

- **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.

If a user does not have permissions for a certain task, that task is either grayed out or does not display in the user interface.

Access Management with local user roles

For Access Management, administrators can use RBAC (role-based access control) capabilities enforced in the storage array. These capabilities are referred to as "local user roles."

Configuration workflow

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

1. An administrator logs in to SANtricity System 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

For Access Management, 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 SANtricity System 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 storage array.
4. After the server connection is established, the administrator maps the user groups to the storage array's roles. These roles are predefined and cannot be modified.
5. The administrator tests the connection between the LDAP server and the storage array.
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.

Access Management with SAML

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 System 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 System 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 System Manager to export a Service Provider metadata file for each controller. From the IdP system, the administrator then imports those metadata files 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 System 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 System 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, 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

How tos

View local user roles

From the Local User Roles tab, you can view the mappings of the user profiles to the default roles. These mappings are part of the RBAC (role-based access controls) enforced in the storage array.

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 user profiles and mappings cannot be changed. Only passwords can be modified.

Steps

1. Select **Settings › Access Management**.
2. Select the **Local User Roles** tab.

   The user profiles are shown in the table:

   - **Root admin** (admin) — Super administrator who has access to all functions in the system. This user profile includes all roles.
   - **Storage admin** (storage) — The administrator responsible for all storage provisioning. This user profile includes the following roles: Storage Admin, Support Admin, and Monitor.
   - **Security admin** (security) — The user responsible for security configuration, including access management, certificate management, and secure-enabled drive functions. This user profile includes the following roles: Security Admin and Monitor.
   - **Support admin** (support) — The user responsible for hardware resources, failure data, and firmware upgrades. This user profile includes the following roles: Support Admin and Monitor.
   - **Monitor** (monitor) — A user with read-only access to the system. This user profile includes only the Monitor role.

Change passwords

You can change the user passwords for each user profile 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 stripped 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.

> Changing the password in System Manager also changes it in the command line interface (CLI). In addition, password changes cause the user's active session to terminate.

Steps

1. Select **Settings › 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 check the box to require the selected user to enter a password to access the storage array, and then you can type the new password for the selected user.
6. Enter your local administrator password, and then click **Change**.

Result

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

Change local user password settings

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

Steps

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

2. Select the **Local User Roles** tab.
3. Select the **View/Edit Settings** button.

   The **Local User Password Settings** dialog box opens.

4. Do one of the following:
   - To allow local users to access the storage array *without* entering a password, uncheck the "Require all local user passwords to be at least" checkbox.
   - To set a minimum password length for all local user passwords, check 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**.

Add directory server

To configure authentication for Access Management, you can establish communications between the storage array and an LDAP server, and then map the LDAP user groups to the 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.
- 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 must also 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 can also enter your user account name and password. Next, you map the LDAP server's user groups to the storage array's predefined roles.

> During the procedure to add an LDAP server, the legacy management interface will be disabled. The legacy management interface (SYMbol) is a method of communication between the storage array and the management client. When disabled, the storage array and management client use a more secure method of communication (REST API over https).

Steps

1. Select **Settings › 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 above. Enter the password for the bind account.
Test server connection before adding	Select this checkbox if you want to make sure the storage array 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	

Setting	Description
Search base DN	Enter the LDAP context to search for users, typically in the form of `CN=Users, DC=copc, 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.
Roles	Click in the field and select one of the storage array's 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 System Manager. 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. System Manager will not operate correctly for any user without the Monitor role present.

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

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 **Settings › 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.

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 storage array can communicate with the LDAP server configuration. The test occurs after you click Save at the bottom of the dialog box. If this checkbox is selected and the test fails, the configuration is not changed. You must resolve the error or de-select the checkbox to skip the testing and re-edit the configuration.

Setting	Description
Privilege settings	
Search base DN	The LDAP context to search for users, typically in the form of `CN=Users, DC=copc, 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.

Setting	Description
Mappings	
Group DN	The domain name for the LDAP user group to be mapped.
Roles	The storage array's 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 System Manager. The storage array's roles include the following: • **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. System Manager will not operate correctly for any user without the Monitor role present.

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

Result

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 storage array, 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 **Settings › 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.

Configure SAML

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.

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 System 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
- Step 2: Export Service Provider files
- Step 3: Map roles
- Step 4: Test SSO login
- Step 5: Enable SAML

Step 1: Upload the IdP metadata file

To provide the storage array with IdP connection information, you import IdP metadata into System 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.
- 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 clocks are 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 System Manager.

About this task

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 array, even if there are two controllers.

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 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.

Before you begin

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

About this task

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.

Steps

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: Map roles

To provide users with authorization and access to System 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 System Manager.
- A Service Provider metadata file for each controller is imported into the IdP system for the trust relationship.

About this task

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

Steps

1. Click the link for mapping System 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.
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 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. System 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 System Manager.
- A Service Provider metadata file for each controller is imported into the IdP system for the trust relationship.

Steps

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.

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 addresses in the SP metadata files are correct.

Step 5: Enable SAML

Your final step is to enable SAML user authentication.

Before you begin

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

About this task

This task describes how 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.

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 opens.

2. Type `enable`, and then click **Enable**.
3. Enter user credentials for an SSO login test.

Result

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

Change SAML role mappings

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 System 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 System 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.

The Monitor role is required for all users, including the administrator. System 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**.

Result

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

Export SAML Service Provider files

If necessary, you can export Service Provider metadata for the storage array and re-import the file(s) 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 controllers (one file for each controller). The IdP needs this metadata to establish a trust relationship with the controllers 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 opens.

4. For each controller, click **Export** to save the metadata file to your local system.

   The domain name fields for each controller are read-only.

   Make a note of where the file is stored.

5. From the local system, locate the Service Provider metadata file(s) you exported.

   There is one XML-formatted file for each controller.

6. From the IdP server, import the Service Provider metadata file(s). You can either import the files directly or you can manually enter the controller information from them.
7. Click **Close**.

View audit log activity

By viewing audit logs, users with Security Admin permissions can monitor user actions, authentication failures, invalid login attempts, and the user session lifespan.

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.

Steps

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

2. Select the **Audit Log** tab.

   Audit log activity appears in tabular format, which includes the following columns of information:

   - **Date/Time** — Timestamp of when the storage array detected the event (in GMT).
   - **Username** — The user name associated with the event. For any non-authenticated actions on the storage array, "N/A" appears as the user name. Non-authenticated actions might be triggered by the internal proxy or some other mechanism.
   - **Status Code** — HTTP status code of the operation (200, 400, etc.) and descriptive text associated with the event.
   - **URL Accessed** — Full URL (including host) and query string.
   - **Client IP Address** — IP address of the client associated with the event.
   - **Source** — Logging source associated with the event, which can be System Manager, CLI, Web Services, or Support Shell.

3. Use the selections on the Audit Log page to view and manage events.

Selection Details

Selection	Description
Show events from the…	Limit events shown by date range (last 24 hours, last 7 days, last 30 days, or a custom date range).
Filter	Limit events shown by the characters entered in the field. Use quotes ("") for an exact word match, enter `OR` to return one or more words, or enter a dash (--) to omit words.
Refresh	Select **Refresh** to update the page to the most current events.
View/Edit Settings	Select **View/Edit Settings** to open a dialog box that allows you to specify a full log policy and level of actions to be logged.
Delete events	Select **Delete** to open a dialog box that allows you to remove old events from the page.
Show/hide columns	Click the **Show/Hide** column icon  to select additional columns for display in the table. Additional columns include: • **Method** — The HTTP method (for example, POST, GET, DELETE, etc.). • **CLI Command Executed** — The CLI command (grammar) executed for Secure CLI requests. • **CLI Return Status** — A CLI status code or a request for input files from the client. • **SYMbol Procedure** — The SYMbol procedure executed. • **SSH Event Type** — Secure Shell (SSH) events type, such as login, logout, and login_fail. • **SSH Session PID** — Process ID number of the SSH session. • **SSH Session Duration(s)** — The number of seconds the user was logged in.
Toggle column filters	Click the **Toggle** icon  to open filtering fields for each column. Enter characters within a column field to limit events shown by those characters. Click the icon again to close the filtering fields.
Undo changes	Click the **Undo** icon  to return the table to the default configuration.
Export	Click **Export** to save the table data to a comma separated value (CSV) file.

Define audit log policies

You can change the overwrite policy and the types of events recorded in the audit log.

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

This task describes how to change the audit log settings, which include the policy for overwriting old events and the policy for recording event types.

Steps

1. Select **Settings › Access Management**.
2. Select the **Audit Log** tab.
3. Select **View/Edit Settings**.

   The **Audit Log Settings** dialog box opens.

4. Change the overwrite policy or types of events recorded.

Field Details

Setting	Description
Overwrite policy	Determines the policy for overwriting old events when the maximum capacity is reached: • **Allow the oldest events in the audit log to be overwritten when the audit log is full** — Overwrites the old events when the audit log reaches 50,000 records. • **Require audit log events to be manually deleted** — Specifies that events will not be automatically deleted; instead, a threshold warning appears at the set percentage. Events must be deleted manually. ⓘ If the overwrite policy is disabled and the audit log entries reach the maximum limit, access to System Manager is denied to users without Security Admin permissions. To restore system access to users without Security Admin permissions, a user assigned to the Security Admin role must delete the old event records. ⓘ Overwrite policies do not apply if a syslog server is configured for archiving audit logs.
Level of actions to be logged	Determines types of events to be logged: • **Record modification events only** — Shows only the events where a user action involves making a change in the system. • **Record all modification and read-only events** — Shows all events, including a user action that involves reading or downloading information.

5. Click **Save**.

Delete events from the audit log

You can clear the audit log of old events, which makes searching through events more

manageable. You have the option of saving old events to a CSV (comma-separated values) file upon deletion.

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

This task describes how to remove old events from the audit log.

Steps

1. Select **Settings › Access Management**.
2. Select the **Audit Log** tab.
3. Select **Delete**.

   The **Delete Audit Log dialog** box opens.
4. Select or enter the number of oldest events that you want to delete.
5. If you want to export the deleted events to a CSV file (recommended), keep the checkbox selected. You will be prompted to enter a file name and location when you click **Delete** in the next step. Otherwise, if you do not want to save events to a CSV file, click the checkbox to deselect it.
6. Click **Delete**.

   A confirmation dialog box opens.
7. Type `delete` in the field, and then click **Delete**.

   The oldest events are removed from the Audit Log page.

Configure syslog server for audit logs

If you want to archive audit logs onto an external syslog server, you can configure communications between that server and the storage array. After the connection is established, audit logs are automatically saved to the syslog server.

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.
- The syslog server address, protocol, and port number must be available. The server address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- If your server uses a secure protocol (for example, TLS), a Certificate Authority (CA) certificate must be available on your local system. CA certificates identify website owners for secure connections between servers and clients.

Steps

1. Select **Settings › Access Management**.
2. From the **Audit Log** tab, select **Configure Syslog Servers**.

   The **Configure Syslog Servers** dialog box opens.

3. Click **Add**.

   The **Add Syslog Server** dialog box opens.

4. Enter information for the server, and then click **Add**.
   - Server address — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
   - Protocol — Select a protocol from the drop-down list (for example, TLS, UDP, or TCP).
   - Upload certificate (optional) — If you selected the TLS protocol and have not yet uploaded a signed CA certificate, click Browse to upload a certificate file. Audit logs are not archived to a syslog server without a trusted certificate.

     > If the certificate becomes invalid later, the TLS handshake will fail. As a result, an error message is posted to the audit log and messages are no longer sent to the syslog server. To resolve this issue, you must fix the certificate on the syslog server and then go to **Settings › Audit Log › Configure Syslog Servers › Test All**.

   - Port — Enter the port number for the syslog receiver. After you click **Add**, the **Configure Syslog Servers** dialog box opens and displays your configured syslog server on the page.
5. To test the server connection with the storage array, select **Test All**.

Result

After configuration, all new audit logs are sent to the syslog server. Previous logs are not transferred.

Edit syslog server settings for audit log records

You can change the settings for the syslog server used for archiving audit logs, and also upload a new Certificate Authority (CA) certificate for the server.

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.
- The syslog server address, protocol, and port number must be available. The server address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- If you are uploading a new CA certificate, the certificate must be available on your local system.

Steps

1. Select **Settings › Access Management**.
2. From the **Audit Log** tab, select **Configure Syslog Servers**.

   Configured syslog servers are displayed on the page.

3. To edit the server information, select the **Edit** (pencil) icon to the right of the server name, and then make desired changes in the following fields:
   - Server Address — Enter a fully qualified domain name, an IPv4 address, or an IPv6 address.
   - Protocol — Select a protocol from the drop-down list (for example, TLS, UDP, or TCP).
   - Port — Enter the port number for the syslog receiver.
4. If you changed the protocol to the secure TLS protocol (from either UDP or TCP), click **Import Trusted Certificate** to upload a CA certificate.

5. To test the new connection with the storage array, select **Test All**.

Result

After configuration, all new audit logs are sent to the syslog server. Previous logs are not transferred.

FAQs

Why can’t I log in?

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

Login errors to System Manager might occur for one of these reasons:

- You entered an incorrect username or password.
- You have insufficient privileges.
- The directory server (if configured) might be unavailable. If this is the case, try logging in with a local user role.
- You attempted to log in unsuccessfully multiple times, which triggered the lockout mode. Wait 10 minutes to re-login.
- A lockout condition was triggered and your audit log might be full. Go to Access Management and delete old events from the audit log.
- SAML authentication is enabled. Refresh your browser to log in.

Login errors to a remote storage array for mirroring tasks might occur for one of these reasons:

- You have entered an incorrect password.
- You attempted to log in unsuccessfully multiple times, which triggered the lockout mode. Wait 10 minutes to log in again.
- The maximum number of client connections used on the controller has been reached. Check for multiple users or clients.

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

Before adding a directory server in Access Management, make sure you meet the following 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 following guidelines.

The storage array’s embedded RBAC (role-based access control) capabilities include the following roles:

- **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.

Directory Services

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

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

Which external management tools may be affected by this change?

When you make certain changes in System Manager, such as switching the management interface or using SAML for an authentication method, some external tools and features might be restricted from use.

Management interface

Tools that communicate directly with the legacy management interface (SYMbol), such as the SANtricity SMI-S Provider or OnCommand Insight (OCI), do not work unless the Legacy Management Interface setting is enabled. In addition, you cannot use legacy CLI commands or perform mirroring operations if this setting is disabled.

Contact technical support for more information.

SAML authentication

When SAML is enabled, 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

Contact technical support for more information.

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 clocks are 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 System Manager.
- You know the IP address or domain name of each 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 types of events are recorded in the audit log?

The audit log can record modification events, or both modification and read-only events.

Depending on the policy settings, the following types of events are shown:

- **Modification events** — User actions from within System Manager that involve changes to the system, such as provisioning storage.
- **Modification and read-only events** — User actions that involve changes to the system, as well as events that involve viewing or downloading information, such as viewing volume assignments.

What do I need to know before configuring a syslog server?

You can archive audit logs onto an external syslog server.

Before configuring a syslog server, keep the following guidelines in mind.

- Make sure you know the server address, protocol, and port number. The server address can be a fully qualified domain name, an IPv4 address, or an IPv6 address.
- If your server uses a secure protocol (for example, TLS), a Certificate Authority (CA) certificate must be available on your local system. CA certificates identify website owners for secure connections between servers and clients.
- After configuration, all new audit logs are sent to the syslog server. Previous logs are not transferred.
- The **Overwrite Policy** settings (available from View/Edit Settings) do not affect how logs are managed with a syslog server configuration.
- Audit logs follow the RFC 5424 messaging format.

The syslog server is no longer receiving audit logs. What do I do?

If you configured a syslog server with a TLS protocol, the server cannot receive messages if the certificate becomes invalid for any reason. An error message about the invalid certificate is posted to the audit log.

To resolve this issue, you must first fix the certificate for the syslog server. Once a valid certificate chain is in place, go to **Settings › Audit Log › Configure Syslog Servers › Test All**.

Copyright information

Trademark information