Access management

SANtricity 11.7

NetApp
February 12, 2024

Table of Contents

Access management

Access Management overview

Access Management is a method of configuring user authentication in 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.

Learn more:

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

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

Concepts

How Access Management works

Use Access Management to establish user authentication in 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.

   > ⓘ 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.
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.

Access Management terminology

Learn how the Access Management terms apply to 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.

Term	Description
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.
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 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

Administrators can use RBAC (role-based access control) capabilities enforced in 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

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.

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 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

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

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

To configure authentication for Access Management, you establish communications between an LDAP server and the host running the Web Services Proxy for 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.

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

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.

FAQs

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.

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.

> ⓘ 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.

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.

Copyright information

Trademark information