Certificates and authentication

SANtricity 11.6

NetApp
June 11, 2024

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity-116/um-certificates/how-certificates-work-unified.html on June 11, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Certificates and authentication

Certificate Management

Concepts

How certificates work

Certificates are digital files that identify online entities, such as websites and servers, for secure communications on the internet.

Signed certificates

Certificates ensure that web communications are transmitted in encrypted form, privately and unaltered, only between the specified server and client. Using Unified Manager, you can manage certificates for the browser on a host management system and the controllers in the discovered storage arrays.

A certificate can be signed by a trusted authority, or it can be self-signed. "Signing" simply means that someone validated the owner's identity and determined that their devices can be trusted. Storage arrays ship with an automatically generated self-signed certificate on each controller. You can continue to use the self-signed certificates, or you can obtain CA-signed certificates for a more secure connection between the controllers and the host systems.

Although CA-signed certificates provide better security protection (for example, preventing man-in-the-middle attacks), they also require fees that can be expensive if you have a large network. In contrast, self-signed certificates are less secure, but they are free. Therefore, self-signed certificates are most often used for internal testing environments, not in production environments.

A signed certificate is validated by a certificate authority (CA), which is a trusted third-party organization. Signed certificates include details about the owner of the entity (typically, a server or website), date of certificate issue and expiration, valid domains for the entity, and a digital signature composed of letters and numbers.

When you open a browser and enter a web address, your system performs a certificate-checking process in the background to determine if you are connecting to a website that includes a valid, CA-signed certificate. Generally, a site that is secured with a signed certificate includes a padlock icon and an https designation in the address. If you attempt to connect to a website that does not contain a CA-signed certificate, your browser displays a warning that the site is not secure.

The CA takes steps to verify your identity during the application process. They might send an email to your registered business, verify your business address, and perform an HTTP or DNS verification. When the application process is complete, the CA sends you digital files to load on a host management system. Typically, these files include a chain of trust, as follows:

- **Root** — At the top of the hierarchy is the root certificate, which contains a private key used to sign other certificates. The root identifies a particular CA organization. If you use the same CA for all your network devices, you need only one root certificate.
- **Intermediate** — Branching off from the root are the intermediate certificates. The CA issues one or more intermediate certificates to act as middlemen between a protected root and server certificates.
- **Server** — At the bottom of the chain is the server certificate, which identifies your specific entity, such as a

website or other device. Each controller in an storage array requires a separate server certificate.

Self-signed certificates

Each controller in the storage array includes a pre-installed, self-signed certificate. A self-signed certificate is similar to a CA-signed certificate, except that it is validated by the owner of the entity instead of a third party. Like a CA-signed certificate, a self-signed certificate contains its own private key, and also ensures that data is encrypted and sent over an HTTPS connection between a server and client.

Self-signed certificates are not “trusted” by browsers. Each time you attempt to connect to a website that contains only a self-signed certificate, the browser displays a warning message. You must click a link in the warning message that allows you to proceed to the website; by doing so, you are essentially accepting the self-signed certificate.

Certificates for Unified Manager

The Unified Manager interface is installed with the Web Services Proxy on a host system. When you open a browser and try connecting to Unified Manager, the browser attempts to verify that the host is a trusted source by checking for a digital certificate. If the browser does not locate a CA-signed certificate for the server, it opens a warning message. From there, you can continue to the website to accept the self-signed certificate for that session. Or, you can obtain signed, digital certificates from a CA so you no longer see the warning message.

Certificates for controllers

During a Unified Manager session, you might see additional security messages when you attempt to access a controller that does not have a CA-signed certificate. In this event, you can permanently trust the self-signed certificate or you can import the CA-signed certificates for the controllers so the Web Services Proxy server can authenticate incoming client requests from these controllers.

Certificate terminology

The following terms apply to certificate management.

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.
CSR	A certificate signing request (CSR) is a message that is sent from an applicant to a certificate authority (CA). The CSR validates the information the CA requires to issue a certificate.
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.
Certificate chain	A hierarchy of files that adds a layer of security to the certificates. Typically, the chain includes one root certificate at the top of the hierarchy, one or more intermediate certificates, and the server certificates that identify the entities.

Term	Description
Intermediate certificate	One or more intermediate certificates branch off from the root in the certificate chain. The CA issues one or more intermediate certificates to act as middlemen between a protected root and server certificates.
Keystore	A keystore is a repository on your host management system that contains private keys, along with their corresponding public keys and certificates. These keys and certificates identify your own entities, such as the controllers.
Root certificate	The root certificate is at the top of the hierarchy in the certificate chain, and contains a private key used to sign other certificates. The root identifies a particular CA organization. If you use the same CA for all your network devices, you need only one root certificate.
Signed certificate	A certificate that is validated by a certificate authority (CA). This data file contains a private key and ensures that data is sent in encrypted form between a server and a client over an HTTPS connection. In addition, a signed certificate includes details about the owner of the entity (typically, a server or website) and a digital signature composed of letters and numbers. A signed certificate uses a chain of trust, and therefore is most often used in production environments. Also referred to as a "CA-signed certificate" or a "management certificate."
Self-signed certificate	A self-signed certificate is validated by the owner of the entity. This data file contains a private key and ensures that data is sent in encrypted form between a server and a client over an HTTPS connection. It also includes a digital signature composed of letters and numbers. A self-signed certificate does not use the same chain of trust as a CA-signed certificate, and therefore is most often used in test environments. Also referred to as a "preinstalled" certificate.
Server certificate	The server certificate is at the bottom of the certificate chain. It identifies your specific entity, such as a website or other device. Each controller in a storage system requires a separate server certificate.
Truststore	A truststore is a repository that contains certificates from trusted third parties, such as CAs.
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 bundled with the Web Services Proxy.

How tos

Use CA-signed certificates

You can obtain and import CA-signed certificates for secure access to the management system hosting Unified Manager.

Before you begin

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

About this task

Using CA-signed certificates is a two-step procedure.

Step 1: Complete and submit a CSR

You must first generate a certificate signing request (CSR) file and send it to the CA.

Before you begin

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

About this task

This task describes how to generate the CSR file that you send to a CA to receive signed, management certificates for the system hosting Unified Manager and the Web Services Proxy. You must provide information about your organization, plus the IP address or DNS name of the host system.

Do not generate a new CSR after submission to the CA. When you generate a CSR, the system creates a private and public key pair. The public key is part of the CSR, while the private key is kept in the keystore. When you receive the signed certificates and import them into the keystore, the system ensures that both the private and public keys are the original pair. Therefore, you must not generate a new CSR after submitting one to the CA. If you do, the controllers generate new keys, and the certificates you receive from the CA will not work.

Steps

1. Select **Certificate Management**.
2. From the **Management** tab, select **Complete CSR**.
3. Enter the following information, and then click **Next**:
   - **Organization** — The full, legal name of your company or organization. Include suffixes, such as Inc. or Corp.
   - **Organizational unit (optional)** — The division of your organization that is handling the certificate.
   - **City/Locality** — The city where your host system or business is located.
   - **State/Region (optional)** — The state or region where your host system or business is located.
   - **Country ISO code** — Your country's two-digit ISO (International Organization for Standardization) code, such as US.
4. Enter the following information about the host system:
   - **Common name** — The IP address or DNS name of the host system where the Web Services Proxy is installed. Make sure this address is correct; it must match exactly what you enter to access Unified Manager in the browser. Do not include http:// or https://.
   - **Alternate IP addresses** — If the common name is an IP address, you can optionally enter any additional IP addresses or aliases for the host system. For multiple entries, use a comma-delimited format.
   - **Alternate DNS names** — If the common name is a DNS name, enter any additional DNS names for the host system. For multiple entries, use a comma-delimited format. If there are no alternate DNS names, but you entered a DNS name in the first field, copy that name here.

5. Click **Finish**.

   A CSR file is downloaded to your local system. The folder location of the download depends on your browser.

6. Submit the CSR file to a CA and request signed certificates in PEM or DER format.

After you finish

Wait for the CA to return the certificate files, and then go to Step 2: Import management certificates.

Step 2: Import management certificates

After you receive signed certificates, import the certificate chain for the host system where the Unified Manager interface is installed.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- You have generated a certificate signing request (.CSR file) and sent it to the CA.
- The CA returned trusted certificate files.
- The certificate files are installed on your local system.
- If the CA provided a chained certificate (for example, a .p7b file), you must unpack the chained file into individual files: the root certificate, one or more intermediate certificates, and the server certificate. You can use the Windows `certmgr` utility to unpack the files (right-click and select **All Tasks › Export**). When the exports are complete, a CER file is shown for each certificate file in the chain.

Steps

1. Select **Certificate Management**.
2. From the **Management** tab, select **Import**.

   A dialog box opens for importing the certificate files.

3. Click **Browse** to first select the root and intermediate files, and then select the server certificate.

   The filenames are displayed in the dialog box.

4. Click **Import**.

Results

The files are uploaded and validated. The certificate information displays on the Certificate Management page.

Reset management certificates

You can revert the management certificate to the original, factory self-signed state.

Before you begin

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

About this task

This task deletes the current management certificate from the host system where the Web Services Proxy and

SANtricity Unified Manager are installed. After the certificate is reset, the host system reverts to using the self-signed certificate.

Steps

1. Select **Certificate Management**.
2. From the **Management** tab, select **Reset**.

   A **Confirm Reset Management Certificate** dialog box opens.

3. Type `reset` in the field, and then click **Reset**.

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

Results

The system reverts to using the self-signed certificate from the server. As a result, the system prompts users to manually accept the self-signed certificate for their sessions.

Import certificates for arrays

If necessary, you can import certificates for the storage arrays so they can authenticate with the system hosting SANtricity Unified Manager. Certificates can be signed by a certificate authority (CA) or can be self-signed.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, certificate functions do not appear.
- If you are importing trusted certificates, the certificates must be imported for the storage array controllers using SANtricity System Manager.

Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.

   This page shows all certificates reported for the storage arrays.

3. Select either **Import › Certificates** to import a CA certificate or **Import › Self-signed storage array certificates** to import a self-signed certificate.

   To limit the view, you can use the **Show certificates that are…** filtering field or you can sort the certificate rows by clicking one of the column heads.

4. In the dialog box, select the certificate and then click **Import**.

   The certificate is uploaded and validated.

View certificates

You can view summary information for a certificate, which includes the organization using

the certificate, the authority that issued the certificate, the period of validity, and the fingerprints (unique identifiers).

Before you begin

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

Steps

1. Select **Certificate Management**.
2. Select one of the following tabs:
   - **Management** — Shows the certificate for the system hosting the Web Services Proxy. A management certificate can be self-signed or approved by a certificate authority (CA). It allows secure access to Unified Manager.
   - **Trusted** — Shows certificates that Unified Manager can access for storage arrays and other remote servers, such as an LDAP server. The certificates can be issued from a certificate authority (CA) or can be self-signed.
3. To see more information about a certificate, select its row, select the ellipses at the end of the row, and then click **View** or **Export**.

Export certificates

You can export a certificate to view its complete details.

Before you begin

To open the exported file, you must have a certificate viewer application.

Steps

1. Select **Certificate Management**.
2. Select one of the following tabs:
   - **Management** — Shows the certificate for the system hosting the Web Services Proxy. A management certificate can be self-signed or approved by a certificate authority (CA). It allows secure access to Unified Manager.
   - **Trusted** — Shows certificates that Unified Manager can access for storage arrays and other remote servers, such as an LDAP server. The certificates can be issued from a certificate authority (CA) or can be self-signed.
3. Select a certificate from the page, and then click the ellipses at the end of the row.
4. Click **Export**, and then save the certificate file.
5. Open the file in your certificate viewer application.

Delete trusted certificates

You can delete one or more certificates that are no longer needed, such as an expired certificate.

Before you begin

Import the new certificate before deleting the old one.

Be aware that deleting a root or intermediate certificate can impact multiple storage arrays, since these arrays can share the same certificate files.

Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.
3. Select one or more certificates in the table, and then click **Delete**.

   The **Delete** function is not available for pre-installed certificates.

   The Confirm Delete Trusted Certificate dialog box opens.

4. Confirm the deletion, and then click **Delete**.

   The certificate is removed from the table.

Resolve untrusted certificates

Untrusted certificates occur when a storage array attempts to establish a secure connection to SANtricity Unified Manager, but the connection fails to confirm as secure. From the Certificate page, you can resolve untrusted certificates by importing a self-signed certificate from the storage array or by importing a certificate authority (CA) certificate that has been issued by a trusted third party.

Before you begin

- You must be logged in with a user profile that includes Security Admin permissions.
- If you plan to import a CA-signed certificate:
  - You have generated a certificate signing request (.CSR file) for each controller in the storage array and sent it to the CA.
  - The CA returned trusted certificate files.
  - The certificate files are available on your local system.

About this task

You might need to install additional trusted CA certificates if any of the following are true:

- You recently added a storage array.
- One or both certificates are expired.
- One or both certificates are revoked.
- One or both certificates are missing a root or intermediate certificate.

Steps

1. Select **Certificate Management**.
2. Select the **Trusted** tab.

   This page shows all certificates reported for the storage arrays.

3. Select either **Import › Certificates**. to import a CA certificate or **Import › Self-signed storage array certificates** to import a self-signed certificate.

   To limit the view, you can use the **Show certificates that are…** filtering field or you can sort the certificate rows by clicking one of the column heads.

4. In the dialog box, select the certificate, and then click **Import**.

   The certificate is uploaded and validated.

Access Management

Concepts

How Access Management works

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.

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

Term	Description
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

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. **Optional:** 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 SANtricity 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.

How tos

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

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**.

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 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=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 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.

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=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 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 to SANtricity Unified Manager, review these possible causes.

Login errors to Unified 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.

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, 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

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.