Unified Manager

SANtricity 11.8

NetApp
January 31, 2025

Table of Contents

Multiple array management with Unified Manager 6

Main interface

Unified Manager interface overview

Unified Manager is a web-based interface that allows you to manage multiple storage arrays in a single view.

Main page

When you log in to Unified Manager, the main page opens to **Manage - All**. From this page, you can scroll through a list of discovered storage arrays in your network, view their status, and perform operations on a single array or on a group of arrays.

Navigation sidebar

You can access Unified Manager features and functions from the navigation sidebar.

Area	Description
Manage	Discover storage arrays in your network, launch SANtricity System Manager for an array, import settings from one array to multiple arrays, and manage array groups. Select the check boxes next to the array names to perform operations on them, such as importing settings and creating array groups. The ellipses at the end of each row provides an in-line menu for operations on a single array, such as renaming it.
Operations	View the progress of batch operations, such as importing settings from one array to another. ⓘ Some operations are not available when a storage array has a non-optimal status.
Certificate Management	Manage certificates to authenticate between browsers and clients.
Access Management	Establish user authentication for the Unified Manager interface.
Support	View technical support options, resources, and contacts.

Interface settings and help

At the top right of the interface, you can access Help and other documentation. You can also access administration options, which are available from the drop-down next to your login name.

User logins and passwords

The current user logged into the system is shown in the upper right of the interface.

For further information on users and passwords, see:

- Set admin password protection
- Change the admin password
- Change passwords for local user profiles

Supported browsers

Unified Manager can be accessed from several types of browsers.

The following browsers and versions are supported.

Browser	Minimum version
Google Chrome	89
Mozilla Firefox	80
Safari	14
Microsoft Edge	90

ⓘ The Web Services Proxy must be installed and available to the browser.

Set admin password protection

You must configure Unified Manager with an administrator password to protect it from unauthorized access.

Admin password and user profiles

When you start Unified Manager for the first time, you are prompted to set an administrator password. Any user who has the admin password can make configuration changes to the storage arrays.

In addition to the admin password, the Unified Manager interface includes pre-configured user profiles with one or more roles mapped to them. For more information, see How Access Management works.

The users and mappings cannot be changed. Only passwords can be modified. To change passwords, see:

- Change the admin password
- Change passwords for local user profiles

Session timeouts

The software prompts you for the password only once during a single management session. A session times out after 30 minutes of inactivity by default, at which time, you must enter the password again. If another user accesses the software from another management client and changes the password while your session is in progress, you are prompted for a password the next time you attempt a configuration operation or a view operation.

For security reasons, you can attempt to enter a password only five times before the software enters a "lockout" state. In this state, the software rejects subsequent password attempts. You must wait 10 minutes to reset to a "normal" state before you try to enter a password again.

You can adjust session timeouts or you can disable session timeouts altogether. For more information, see Manage session timeouts.

Change the admin password

You can change the admin password used for accessing Unified Manager.

Before you begin

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

About this task

Keep these guidelines in mind when choosing a password:

- 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 **Settings › Access Management**.
2. Select the **Local User Roles** tab.
3. Select the **admin** 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, select the checkbox to require the user to enter a password to access the system.
6. Enter the new password in the two fields.
7. Enter your local administrator password to confirm this operation, and then click **Change**.

Manage session timeouts

You can configure timeouts for Unified Manager, so that users inactive sessions are disconnected after a specified time.

About this task

By default, the session timeout for Unified Manager is 30 minutes. You can adjust that time or you can disable session timeouts altogether.

> If Access Management is configured using the Security Assertion Markup Language (SAML) capabilities embedded in the array, a session timeout might occur when the user’s SSO session reaches its maximum limit. This might occur before the System Manager session timeout.

Steps

1. From the menu bar, select the drop-down arrow next to your user login name.
2. Select **Enable/Disable session timeout**.

   The Enable/Disable Session Timeout dialog box opens.

3. Use the spinner controls to increase or decrease the time in minutes.

   The minimum timeout you can set is 15 minutes.

   > To disable session timeouts, clear the **Set the length of time…** checkbox.

4. Click **Save**.

Storage arrays

Discovery overview

To manage storage resources, you must first discover the storage arrays in the network.

How do I discover arrays?

Use the Add/Discover page to find and add the storage arrays you want to manage in your organization’s network. You can discover multiple arrays or you can discover a single array. To do this, you enter network IP addresses, and then Unified Manager attempts individual connections to each IP address in that range.

Learn more:

- Considerations for discovering arrays
- Discover multiple storage arrays
- Discover single array

How do I manage arrays?

After you discover arrays, go to the **Manage - All** page. From this page, you can scroll through a list of discovered storage arrays in your network, view their status, and perform operations on a single array or on a group of arrays.

If you want to manage a single array, you can select it and open System Manager.

Learn more:

- Considerations for accessing System Manager
- Manage an individual storage array

- View storage array status

Concepts

Considerations for discovering arrays

Before Unified Manager can display and manage storage resources, it must discover the storage arrays you want to manage in your organization’s network. You can discover multiple arrays or you can discover a single array.

Discovering multiple storage arrays

If you choose to discover multiple arrays, you enter a network IP address range and then Unified Manager attempts individual connections to each IP address in that range. Any storage array successfully reached appears on the Discover page and may be added to your management domain.

Discovering a single storage array

If you choose to discover a single array, you enter the single IP address for one of the controllers in the storage array and then the individual storage array is added.

> ⓘ Unified Manager discovers and displays only the single IP address or IP address within a range assigned to a controller. If there are alternate controllers or IP addresses assigned to these controllers that fall outside of this single IP address or IP address range, then Unified Manager will not discover or display them. However, once you add the storage array, all associated IP addresses will be discovered and displayed in the Manage view.

User credentials

As part of the discovery process, you must supply the administrator password for each storage array you want to add.

Web services certificates

As part of the discovery process, Unified Manager verifies that the discovered storage arrays are using certificates by a trusted source. Unified Manager uses two types of certificate-based authentication for all connections that it establishes with the browser:

- **Trusted certificates**

  For arrays discovered by Unified Manager, you might need to install additional trusted certificates supplied by the Certificate Authority.

  Use the **Import** button to import these certificates. If you have connected to this array before, one or both controller certificates are either expired, revoked, or missing a root certificate or intermediate certificate in its certificate chain. You must replace the expired or revoked certificate or add the missing root certificate or intermediate certificate before managing the storage array.

- **Self-signed certificates**

  Self-signed certificates can also be used. If the administrator attempts to discover arrays without importing signed certificates, Unified Manager displays an error dialog box that allows the administrator to accept the self-signed certificate. The storage array’s self-signed certificate will be marked as trusted and the storage array will be added to Unified Manager.

If you do not trust the connections to the storage array, select **Cancel** and validate the storage array's security certificate strategy before adding the storage array to Unified Manager.

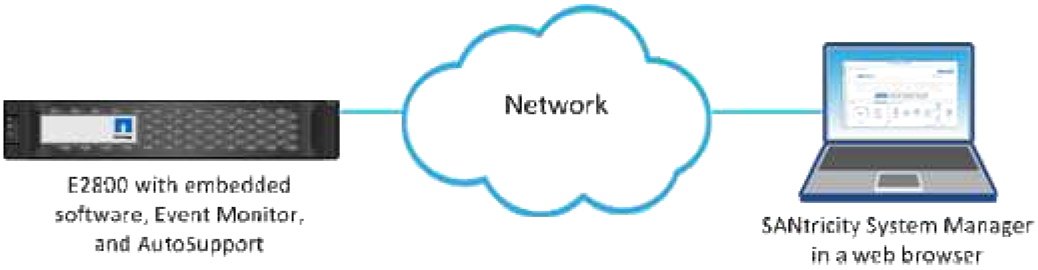
Considerations for accessing System Manager

You select one or more storage arrays and use the Launch option to open System Manager when you want to configure and manage storage arrays.

System Manager is an embedded application on the controllers, which is connected to the network through an Ethernet management port. It includes all array-based functions.

To access System Manager, you must have:

- One of the array models listed here: E-Series hardware overview
- An out-of-band connection to a network management client with a web browser.


Network
E2800 with embedded software, Event Monitor, and AutoSupport
SANtricity System Manager in a web browser

Discover arrays

Discover multiple storage arrays

You discover multiple arrays to detect all storage arrays across the subnet where the management server resides and to automatically add the discovered arrays to your management domain.

Before you begin

- You must be logged in with a user profile that includes Security Admin permissions.
- The storage array must be correctly set up and configured.
- Storage array passwords must be set up using System Manager's Access Management tile.
- To resolve untrusted certificates, you must have trusted certificate files from a Certificate Authority (CA), and the certificate files are available on your local system.

Discovering arrays is a multi-step procedure.

Step 1: Enter network address

You enter a network address range to search across the local sub-network. Any storage array successfully reached appears on the Discover page and might be added to your management domain.

If you need to stop the discovery operation for any reason, click **Stop Discovery**.

Steps

1. From the Manage page, select **Add/Discover**.

The Add/Discover dialog box appears.

2. Select the **Discover all storage arrays within a network range** radio button.
3. Enter the starting network address and ending network address to search across your local sub-network, and then click **Start Discovery**.

   The discovery process starts. This discovery process can take several minutes to complete. The table on the Discover page is populated as the storage arrays are discovered.

   > If no manageable arrays are discovered, verify that the storage arrays are properly connected to your network and their assigned addresses are within range. Click **New Discovery Parameters** to return to the Add/Discover page.

4. Review the list of discovered storage arrays.
5. Select the checkbox next to any storage array that you want to add to your management domain, and then click **Next**.

   Unified Manager performs a credential check on each array you are adding to the management domain. You might need to resolve any self-signed certificates and untrusted certificates associated with that array.

6. Click **Next** to proceed to the next step in the wizard.

Step 2: Resolve self-signed certificates during discovery

As part of the discovery process, the system verifies that the storage arrays are using certificates by a trusted source.

Steps

1. Do one of the following:
   - If you trust the connections to the discovered storage arrays, continue to the next card in the wizard. The self-signed certificates will be marked as trusted and the storage arrays will be added to Unified Manager.
   - If you do not trust the connections to the storage arrays, select **Cancel** and validate each storage array’s security certificate strategy before adding any of them to Unified Manager.
2. Click **Next** to proceed to the next step in the wizard.

Step 3: Resolve untrusted certificates during discovery

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

You may 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 the check box next to any storage array that you want to resolve untrusted certificates for, and then select the **Import** button.

   A dialog box opens for importing the trusted certificate files.

2. Click **Browse** to select the certificate files for the storage arrays.

   The file names display in the dialog box.

3. Click **Import**.

   The files are uploaded and validated.

   > ⓘ Any storage array with untrusted certificate issues that are unresolved will not be added to Unified Manager.

4. Click **Next** to proceed to the next step in the wizard.

Step 4: Provide passwords

You must enter the passwords for the storage arrays that you want to add to your management domain.

Steps

1. Enter the password for each storage array you want to add to Unified Manager.
2. **Optional:** Associate storage arrays to a group: From the drop-down list, select the desired group to associate with the selected storage arrays.
3. Click **Finish**.

After you finish

The storage arrays are added to your management domain and associated with the selected group (if specified).

> ⓘ It can take several minutes for Unified Manager to connect to the specified storage arrays.

Discover single array

Use the Add/Discover Single Storage Array option to manually discover and add a single storage array to your organization’s network.

Before you begin

- The storage array must be correctly set up and configured.
- Storage array passwords must be set up using System Manager’s Access Management tile.

Steps

1. From the Manage page, select **Add/Discover**.

   The Add/Discover dialog box appears.

2. Select the **Discover a single storage array** radio button.
3. Enter the IP address for one of the controllers in the storage array, and then click **Start Discovery**.

It can take several minutes for Unified Manager to connect to the specified storage array.

> The Storage Array Not Accessible message appears when the connection to the IP address of the specified controller is unsuccessful.

4. If prompted, resolve any self-signed certificates.

   As part of the discovery process, the system verifies that the discovered storage arrays are using certificates by a trusted source. If it cannot locate a digital certificate for a storage array, it prompts you to resolve the certificate that is not signed by a recognized certificate authority (CA) by adding a security exception.

5. If prompted, resolve any untrusted certificates.

   Untrusted certificates occur when a storage array attempts to establish a secure connection to Unified Manager, but the connection fails to confirm as secure. Resolve untrusted certificates by importing a certificate authority (CA) certificate that has been issued by a trusted third party.

6. Click **Next**.
7. **Optional:** Associate the discovered storage array to a group: From the drop-down list, select the desired group to associate with the storage array.

   The "All" group is selected by default.

8. Enter the administrator password for the storage array that you want to add to your management domain, and then click **OK**.

After you finish

The storage array is added to Unified Manager and, if specified, it is also added to the group you selected.

If automatic support data collection is enabled, support data is automatically collected for a storage array that you add.

Manage arrays

View storage array status

Unified Manager displays the status of each storage array that has been discovered.

Go to the **Manage - All** page. From this page, you can view the status of the connection between the Web Services Proxy and that storage array.

Status indicators are described in the following table.

Status	Indicates
Optimal	The storage array is in an optimal state. There are no certificate issues and the password is valid.
Invalid Password	An invalid storage array password was provided.

Status	Indicates
Untrusted Certificate	One or more connections with the storage array is untrusted because the HTTPS certificate is either self-signed and has not been imported, or the certificate is CA-signed and the root and intermediate CA certificates have not been imported.
Needs Attention	There is a problem with the storage array that requires your intervention to correct it.
Lockdown	The storage array is in a locked-down state.
Unknown	The storage array has never been contacted. This can happen when the Web Services Proxy is starting up and has not yet made contact with the storage array, or the storage array is offline and has never been contacted since the Web Services Proxy was started.
Offline	The Web Services Proxy had previously contacted the storage array, but now has lost all connection to it.

Manage an individual storage array

You can use the Launch option to open the browser-based System Manager for one or more storage arrays when you want to perform management operations.

Steps

1. From the Manage page, select one or more storage arrays that you want to manage.
2. Click **Launch**.

   The system opens a new window and displays the System Manager login page.
3. Enter your username and password, and then click **Log in**.

Change storage array passwords

You can update the passwords used for viewing and accessing storage arrays in Unified Manager.

Before you begin

- You must be logged in with a user profile that includes Storage admin permissions.
- You must know the current password for the storage array, which is set in System Manager.

About this task

In this task, you enter the current password for a storage array so you can access it in Unified Manager. This might be necessary if the array password was changed in System Manager and now it must also be changed in Unified Manager.

Steps

1. From the Manage page, select one or more storage arrays.
2. Select **Uncommon Tasks › Provide Storage Array Passwords**.

3. Enter the password or passwords for each storage array, and then click **Save**.

Remove storage arrays from SANtricity Unified Manager

You can remove one or more storage arrays if you no longer want to manage it from Unified Manager.

About this task

You cannot access any of the storage arrays you remove. You can, however, establish a connection to any of the removed storage arrays by pointing a browser directly to its IP address or host name.

Removing a storage array does not affect the storage array or its data in any way. If a storage array is accidentally removed, it can be added again.

Steps

1. Select the **Manage** page.
2. Select one or more storage arrays that you want to remove.
3. Select **Uncommon Tasks › Remove storage array**.

   The storage array is removed from all the views in SANtricity Unified Manager.

Settings import

Settings import overview

The Import Settings feature allows you to perform a batch operation for importing the settings from one array to multiple arrays. This feature saves time when you need to configure multiple arrays in the network.

What settings can be imported?

You can import alerting methods, AutoSupport configurations, Directory Services configurations, storage configurations (such as volume groups and pools), and system settings (such as automatic load balancing).

Learn more:

- How Import Settings works
- Requirements for replicating storage configurations

How do I perform a batch import?

On a storage array to be used as the source, open System Manager and configure the desired settings. Then from Unified Manager, go to the Manage page and import the settings to one or more arrays.

Learn more:

- Import alert settings
- Import AutoSupport settings
- Import directory services settings

- Import storage configuration settings
- Import system settings

Concepts

How Import Settings works

You can use Unified Manager to import settings from one storage array to multiple storage arrays. The Import Settings feature is a batch operation that saves time when you need to configure multiple arrays in the network.

Settings available for import

The following configurations can be imported to multiple arrays:

- **Alerts** — Alerting methods to send important events to administrators, using email, a syslog server, or an SNMP server.
- **AutoSupport** — A feature that monitors the health of a storage array and sends automatic dispatches to technical support.
- **Directory services** — A method of user authentication that is managed through an LDAP (Lightweight Directory Access Protocol) server and directory service, such as Microsoft's Active Directory.
- **Storage configuration** — Configurations relating to the following:
  - Volumes (thick and non-repository volumes only)
  - Volume groups and pools
  - Hot spare drive assignments
- **System settings** — Configurations relating to the following:
  - Media scan settings for a volume
  - SSD settings
  - Automatic load balancing (does not include host connectivity reporting)

Configuration workflow

To import settings, follow this workflow:

1. On a storage array to be used as the source, configure the settings using System Manager.
2. On the storage arrays to be used as the targets, back up their configuration using System Manager.
3. From Unified Manager, go to the **Manage** page and import the settings.
4. From the **Operations** page, review the results of the Import Settings operation.

Requirements for replicating storage configurations

Before importing a storage configuration from one storage array to another, review the requirements and guidelines.

Shelves

- The shelves where the controllers reside must be identical on the source and target arrays.
- Shelf IDs must be identical on the source and target arrays.
- Expansion shelves must be populated in the same slots with the same drive types (if the drive is used in the configuration, the location of unused drives does not matter).

Controllers

- The controller type can be different between the source and target arrays (for example, importing from an E2800 to an E5700), but the RBOD enclosure type must be identical.
- The HICs, including the DA capabilities of the host, must be identical between the source and target arrays.
- Importing from a duplex to simplex configuration is not supported; however, importing from simplex to duplex is allowed.
- FDE settings are not included in the import process.

Status

- The target arrays must be in Optimal status.
- The source array does not need to be in Optimal status.

Storage

- Drive capacity may vary between the source and target arrays, as long as the volume capacity on the target is larger than the source. (A target array might have newer, larger capacity drives that would not be fully configured into volumes by the replication operation.)
- Disk pool volumes 64 TB or larger on the source array will prevent the import process on the targets.
- Thin volumes are not included in the import process.

Use batch imports

Import alert settings

You can import alert configurations from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- Alerts are configured in System Manager for the storage array you want to use as the source (**Settings › Alerts**).
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

You can select email, SNMP, or syslog alerts for the import operation. The imported settings include:

- **Email alerts** — A mail server address and the email addresses of the alert recipients.
- **Syslog alerts** — A syslog server address and a UDP port.
- **SNMP alerts** — A community name and IP address for the SNMP server.

Steps

1. From the Manage page, click **Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog box, select either **Email alerts**, **SNMP alerts**, or **Syslog alerts**, and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog box, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog box, select one or more arrays to receive the new settings.

   ⓘ Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog box if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured to send alerts to administrators through email, SNMP, or syslog.

Import AutoSupport settings

You can import an AutoSupport configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- AutoSupport is configured in System Manager for the storage array you want to use as the source (**Support › Support Center**).
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

Imported settings include the separate features (Basic AutoSupport, AutoSupport OnDemand, and Remote Diagnostics), the maintenance window, delivery method, and dispatch schedule.

Steps

1. From the Manage page, click **Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog box, select **AutoSupport** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog box, select the array with the settings you want to import, and then click **Next**.

4. In the Select Targets dialog box, select one or more arrays to receive the new settings.

   > ⓘ Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog box if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same AutoSupport settings as the source array.

Import directory services settings

You can import a directory services configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- Directory services are configured in System Manager for the storage array you want to use as the source (**Settings › Access Management**).
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

Imported settings include the domain name and URL of an LDAP (Lightweight Directory Access Protocol) server, along with the mappings for the LDAP server's user groups to the storage array's predefined roles.

Steps

1. From the Manage page, click **Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog box, select **Directory services** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog box, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog box, select one or more arrays to receive the new settings.

   > ⓘ Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog box if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same directory services as the source array.

Import system settings

You can import the system configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- System settings are configured in System Manager for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).

About this task

Imported settings include media scan settings for a volume, SSD settings for controllers, and automatic load balancing (does not include host connectivity reporting).

Steps

1. From the Manage page, click **Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog box, select **System** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog box, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog box, select one or more arrays to receive the new settings.

   > Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog box if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same system settings as the source array.

Import storage configuration settings

You can import the storage configuration from one storage array to other storage arrays. This batch operation saves time when you need to configure multiple arrays in the network.

Before you begin

- Storage is configured in SANtricity System Manager for the storage array you want to use as the source.
- The existing configuration for the target storage arrays are backed up in System Manager (**Settings › System › Save Storage Array Configuration**).
- The source and target arrays must meet these requirements:
  - The shelves where the controllers reside must be identical.
  - Shelf IDs must be identical.
  - Expansion shelves must be populated in the same slots with the same drive types.
  - The RBOD enclosure type must be identical.
  - The HICs, including the Data Assurance capabilities of the host, must be identical.
  - The target arrays must be in Optimal status.
  - The volume capacity on the target array is larger than the source array’s capacity.
- You understand the following restrictions:
  - Importing from a duplex to simplex configuration is not supported; however, importing from simplex to duplex is allowed.
  - Disk pool volumes 64 TB or larger on the source array will prevent the import process on the targets.
  - Thin volumes are not included in the import process.

About this task

Imported settings include configured volumes (thick and non-repository volumes only), volume groups, pools, and hot spare drive assignments.

Steps

1. From the Manage page, click **Import Settings**.

   The Import Settings wizard opens.

2. In the Select Settings dialog box, select **Storage configuration** and then click **Next**.

   A dialog box opens for selecting the source array.

3. In the Select Source dialog box, select the array with the settings you want to import, and then click **Next**.
4. In the Select Targets dialog box, select one or more arrays to receive the new settings.

   > ⓘ Storage arrays with firmware below 8.50 are not available for selection. In addition, an array does not appear in this dialog box if Unified Manager cannot communicate with that array (for example, if it is offline or if it has certificate, password, or networking problems).

5. Click **Finish**.

   The Operations page displays the results of the import operation. If the operation fails, you can click on its row to see more information.

Results

The target storage arrays are now configured with the same storage configuration as the source array.

FAQs

What settings will be imported?

The Import Settings feature is a batch operation that loads configurations from one storage array to multiple storage arrays. The settings that are imported during this operation depend on how the source storage array is configured in System Manager.

The following settings can be imported to multiple storage arrays:

- **Email alerts** — Settings include a mail server address and the email addresses of the alert recipients.
- **Syslog alerts** — Settings include a syslog server address and a UDP port.
- **SNMP alerts** — Settings include a community name and IP address for the SNMP server.
- **AutoSupport** — Settings include the separate features (Basic AutoSupport, AutoSupport OnDemand, and Remote Diagnostics), the maintenance window, delivery method, and dispatch schedule.
- **Directory services** — Configuration includes the domain name and URL of an LDAP (Lightweight Directory Access Protocol) server, along with the mappings for the LDAP server’s user groups to the storage array’s predefined roles.
- **Storage configuration** — Configurations include volumes (only thick and only non-repository volumes), volume groups, pools, and hot spare drive assignments.
- **System settings** — Configurations include media scan settings for a volume, SSD cache for controllers, and automatic load balancing (does not include host connectivity reporting).

Why don’t I see all of my storage arrays?

During the Import Settings operation, some of your storage arrays might not be available in the target selection dialog box.

Storage arrays might not appear for the following reasons:

- The firmware version is below 8.50.
- The storage array is offline.
- The system cannot communicate with that array (for example, the array has certificate, password, or networking problems).

Array groups

Groups overview

From the Manage Groups page, you can create a set of storage array groups for easier management.

What are array groups?

You can manage your physical and virtualized infrastructure by grouping a set of storage arrays. You might want to group storage arrays to make it easier to run monitoring or reporting jobs.

There are two types of groups:

- **All group** — The All group is the default group and includes all the storage arrays discovered in your organization. The All group can be accessed from the main view.
- **User-created group** — A user-created group includes the storage arrays that you manually select to add to that group. User-created groups can be accessed from the main view.

How do I configure groups?

From the Manage Groups page, you can create a group and then add arrays to that group.

Learn more:

- Configure storage array group

Configure storage array group

You create storage groups, and then add storage arrays to the groups.

Configuring groups is a two-step procedure.

Step 1: Create group

You first create a group. The storage group defines which drives provide the storage that makes up the volume.

Steps

1. From the Manage page, select **Manage Groups › Create storage array group**.
2. In the **Name** field, type a name for the new group.
3. Select the storage arrays that you want to add to the new group.
4. Click **Create**.

Step 2: Add storage array to group

You can add one or more storage arrays to a user-created group.

Steps

1. From the main view, select **Manage**, and then select the group that you want to add storage arrays to.
2. Select **Manage Groups › Add storage arrays to group**.
3. Select the storage arrays that you want to add to the group.
4. Click **Add.**

Remove storage arrays from group

You can remove one or more managed storage arrays from a group if you no longer want to manage it from a specific storage group.

About this task

Removing storage arrays from a group does not affect the storage array or its data in any way. If your storage array is managed by System Manager, you can still manage it using your browser. If a storage array is accidentally removed from a group, it can be added again.

Steps

1. From the Manage page, select **Manage Groups › Remove storage arrays from group**.
2. From the drop-down, select the group that contains the storage arrays you want to remove, and then click the check box next to each storage array that you want to remove from the group.
3. Click **Remove**.

Delete storage array group

You can remove one or more storage array groups that are no longer needed.

About this task

This operation deletes only the storage array group. Storage arrays associated with the deleted group remain accessible through the Manage All view or any other group it is associated with.

Steps

1. From the Manage page, select **Manage Groups › Delete storage array group**.
2. Select one or more storage array groups that you want to delete.
3. Click **Delete**.

Rename storage array group

You can change the name of a storage array group when the current name is no longer meaningful or applicable.

About this task

Keep these guidelines in mind.

- A name can consist of letters, numbers, and the special characters underscore (_), hyphen (-), and pound (#). If you choose any other characters, an error message appears. You are prompted to choose another name.
- Limit the name to 30 characters. Any leading and trailing spaces in the name are deleted.
- Use a unique, meaningful name that is easy to understand and remember.
- Avoid arbitrary names or names that would quickly lose their meaning in the future.

Steps

1. From the main view, select **Manage**, and then select the storage array group you want to rename.
2. Select **Manage Groups › Rename storage array group**.
3. In the **Group Name** field, type a new name for the group.
4. Click **Rename.**

Upgrades

Upgrade Center overview

From the Upgrade Center, you can manage SANtricity OS software and NVSRAM upgrades for multiple storage arrays.

How do upgrades work?

You download the latest OS software and then upgrade one or more arrays.

Upgrade workflow

The following steps provide a high-level workflow for performing software upgrades.

1. You download the latest SANtricity OS software file from the Support site (a link is available from Unified Manager in the Support page). Save the file on the management host system (the host where you access Unified Manager in a browser), and then unzip the file.
2. In Unified Manager, you load the SANtricity OS software file and the NVSRAM file into the repository (an area of the Web Services Proxy server where files are stored). You can add files either from **Upgrade Center › Upgrade SANtricity OS Software or from Upgrade Center › Manage Software Repository**.
3. After the files are loaded in the repository, you can then select the file to be used in the upgrade. From the Upgrade SANtricity OS software page (**Upgrade Center › Upgrade SANtricity OS software**), you select the SANtricity OS software file and the NVSRAM file. After you select a software file, a list of compatible storage arrays appear on this page. You then select the storage arrays that you want to upgrade with the new software. (You cannot select incompatible arrays.)
4. You can then begin an immediate software transfer and activation, or you can choose to stage the files for activation at a later time. During the upgrade process, Unified Manager performs the following tasks:
   a. Performs a health check on the storage arrays to determine if any conditions exist that might prevent the upgrade from completing. If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.
   b. Transfers the upgrade files to each controller.
   c. Reboots the controllers and activates the new SANtricity OS software, one controller at a time. During activation, the existing SANtricity OS file is replaced with the new file.

   > ⓘ You can also specify that the software is activated at a later time.

Immediate or staged upgrade

You can activate the upgrade immediately or stage it for a later time. You might choose to activate later for these reasons:

- **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. Depending on the I/O load and cache size, a controller upgrade can typically take between 15 to 25 minutes to complete. The controllers reboot and fail over during activation so performance might be lower than usual until the upgrade completes.
- **Type of package** — You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

To activate staged software, go to **Support › Upgrade Center** and click **Activate** in the area labeled SANtricity OS Controller Software upgrade.

Health check

A health check runs as part of the upgrade process, but you can also run a health check separately before you begin (go to **Upgrade Center › Pre-Upgrade Health Check**).

The health check assesses all storage system components to make sure that the upgrade can proceed. The following conditions might prevent the upgrade:

- Failed assigned drives
- Hot spares in use
- Incomplete volume groups
- Exclusive operations running
- Missing volumes
- Controller in Non-optimal status
- Excess number of event log events
- Configuration database validation failure
- Drives with old versions of DACstore

What do I need to know before upgrading?

Before you upgrade multiple storage arrays, review the key considerations as part of your planning.

Current versions

You can view the current SANtricity OS software versions from the Manage page of Unified Manager for each discovered storage array. The version is shown in the SANtricity OS Software column. The controller firmware and NVSRAM information is available in a pop-up dialog box when you click on the SANtricity OS version in each row.

Other components requiring upgrade

As part of the upgrade process, you might also need to upgrade the host's multipath/failover driver or the HBA driver so that the host can interact with the controllers correctly.

For compatibility information, refer to the NetApp Interoperability Matrix. Also, see the procedures in the Express Guides for your operating system. Express Guides are available from the E-Series and SANtricity documentation.

Dual controllers

If a storage array contains two controllers and you have a multipath driver installed, the storage array can continue to process I/O while the upgrade occurs. During the upgrade, the following process occurs:

1. Controller A fails over all its LUNs to controller B.
2. Upgrade occurs on controller A.
3. Controller A takes back its LUNs and all of controller B's LUNs.
4. Upgrade occurs on controller B.

After the upgrade completes, you might need to manually redistribute volumes between the controllers to ensure volumes return to the correct owning controller.

Upgrade software and firmware

Perform pre-upgrade health check

A health check runs as part of the upgrade process, but you also can run a health check separately before you begin. The health check assesses components of the storage array to make sure that the upgrade can proceed.

Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Pre-Upgrade Health Check**.

   The Pre-Upgrade Health Check dialog box opens and lists all the discovered storage systems.

2. If needed, filter or sort the storage systems in the list, so you can view all systems that are not currently in the Optimal state.
3. Select the check boxes for the storage systems that you want to run through the health check.
4. Click **Start**.

   The progress is shown in the dialog box while the health check is performed.

5. When the health check completes, you can click on the ellipses (…) to the right of each row to view more information and perform other tasks.

   > ⓘ If any arrays fail the health check, you can skip that particular array and continue the upgrade for the others, or you can stop the entire process and troubleshoot the arrays that did not pass.

Upgrade SANtricity OS

Upgrade one or more storage arrays with the latest software and NVSRAM to make sure that you have all the latest features and bug fixes. Controller NVSRAM is a controller file that specifies the default settings for the controllers.

Before you begin

- The latest SANtricity OS files are available on the host system where the SANtricity Web Services Proxy and Unified Manager are running.
- You know whether you want to activate your software upgrade now or later.

  You might choose to activate later for these reasons:

  - **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers fail over during activation, so performance might be lower than usual until the upgrade completes.
  - **Type of package** — You might want to test the new OS software on one storage array before you upgrade the files on other storage arrays.

> ⓘ Systems must be running SANtricity OS 11.70.5 to upgrade to 11.80.x or later.

About this task

> ⓘ Risk of data loss or risk of damage to the storage array - Do not make changes to the storage array while the upgrade is occurring. Maintain power to the storage array.

Steps

1. If your storage array contains only one controller or a multipath driver is not in use, stop I/O activity to the storage array to prevent application errors. If your storage array has two controllers and you have a multipath driver installed, you do not need to stop I/O activity.
2. From the main view, select **Manage**, and then select one or more storage arrays that you want to upgrade.
3. Select **Upgrade Center › Upgrade SANtricity OS Software**.

   The Upgrade SANtricity OS software page appears.

4. Download the latest SANtricity OS software package from the NetApp support site to your local machine.
   a. Click **Add new file to software repository**.
   b. Click the link for finding the latest **SANtricity OS Downloads**.
   c. Click the **Download Latest Release** link.
   d. Follow the remaining instructions to download the SANtricity OS file and the NVSRAM file to your local machine.

   > ⓘ Digitally signed firmware is required in version 8.42 and above. If you attempt to download unsigned firmware, an error is displayed and the download is aborted.

5. Select the OS software file and the NVSRAM file that you want to use to upgrade the controllers:
   a. From the **Select a SANtricity OS software file** drop-down, select the OS file that you downloaded to your local machine.

      If there are multiple files available, the files are sorted from newest date to oldest date.

      > ⓘ The software repository lists all software files associated with the Web Services Proxy. If you do not see the file that you want to use, you can click the link, **Add new file to software repository**, to browse to the location where the OS file that you want to add resides.

   b. From the **Select an NVSRAM file** drop-down, select the controller file that you want to use.

      If there are multiple files, the files are sorted from newest date to oldest date.

6. In the Compatible Storage Array table, review the storage arrays that are compatible with the OS software file that you selected, and then select the arrays you want to upgrade.
   - The storage arrays that you selected in the Manage view and that are compatible with the selected firmware file are selected by default in the Compatible Storage Array table.
   - The storage arrays that cannot be updated with the selected firmware file are not selectable in the Compatible Storage Array table as indicated by the status **Incompatible**.
7. **Optional:** To transfer the software file to the storage arrays without activating them, select the **Transfer the OS software to the storage arrays, mark it as staged, and activate at a later time** check box.
8. Click **Start**.
9. Depending on whether you chose to activate now or later, do one of the following:

  - Type **TRANSFER** to confirm that you want to transfer the proposed OS software versions on the arrays you selected to upgrade, and then click **Transfer**.

    To activate the transferred software, select **Upgrade Center › Activate Staged OS Software**.

  - Type **UPGRADE** to confirm that you want to transfer and activate the proposed OS software versions on the arrays you selected to upgrade, and then click **Upgrade**.

    The system transfers the software file to each storage array you selected to upgrade and then activates that file by initiating a reboot.

  The following actions occur during the upgrade operation:

  - A pre-upgrade health check runs as part of the upgrade process. The pre-upgrade health check assesses all storage array components to make sure that the upgrade can proceed.
  - If any health check fails for a storage array, the upgrade stops. You can click the ellipsis (…) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the upgrade.
  - You can cancel the upgrade operation after the pre-upgrade health check.

10. **Optional:** Once the upgrade has completed, you can see a list of what was upgraded for a specific storage array by clicking the ellipsis (…) and then selecting **Save Log**.

    The file is saved in the Downloads folder for your browser with the name `upgrade_log-<date>.json`.

Activate staged OS software

You can choose to activate the software file immediately or wait until a more convenient time. This procedure assumes you chose to activate the software file at a later time.

About this task

You can transfer the firmware files without activating them. You might choose to activate later for these reasons:

- **Time of day** — Activating the software can take a long time, so you might want to wait until I/O loads are lighter. The controllers reboot and fail over during activation so performance might be lower than usual until the upgrade completes.
- **Type of package** — You might want to test the new software and firmware on one storage array before upgrading the files on other storage arrays.

ⓘ You cannot stop the activation process after it starts.

Steps

1. From the main view, select **Manage**. If necessary, click the Status column to sort, at the top of the page, all storage arrays with a status of "OS Upgrade (awaiting activation)."
2. Select one or more storage arrays that you want to activate software for, and then select **Upgrade Center › Activate Staged OS Software**.

   The following actions occur during the upgrade operation:

   - A pre-upgrade health check runs as part of the activate process. The pre-upgrade health check assesses all storage array components to make sure that the activation can proceed.

  - If any health check fails for a storage array, the activation stops. You can click the ellipsis (…) and select **Save Log** to review the errors. You can also choose to override the health check error and then click **Continue** to proceed with the activation.
  - You can cancel the activate operation after the pre-upgrade health check.
    On successful completion of the pre-upgrade health check, activation occurs. The time it takes to activate depends on your storage array configuration and the components that you are activating.

3. **Optional:** After the activation is complete, you can see a list of what was activated for a specific storage array by clicking the ellipsis (…) and then selecting **Save Log**.

   The file is saved in the Downloads folder for your browser with the name `activate_log-<date>.json`.

Manage software repository

The software repository lists all software files associated with the Web Services Proxy.

If you do not see the file that you want to use, you can use the Manage Software Repository option to import one or more SANtricity OS files to the host system where the Web Services Proxy and Unified Manager are running. You can also choose to delete one or more SANtricity OS files that are available in the software repository.

Before you begin

If you are adding SANtricity OS files, make sure that the OS files are available on your local system.

Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Manage Software Repository**.

   The Manage Software Repository dialog box appears.

2. Do one of the following actions:

Option	Do this….
Import	a. Click **Import.** b. Click **Browse**, and then navigate to the location where the OS files you want to add reside. OS files have a filename similar to `N2800-830000-000.dlp`. c. Select one or more OS files that you want to add, and then click **Import**.
Delete	a. Select one or more OS files that you want to remove from the software repository. b. Click **Delete**.

Results

If you selected import, the file(s) are uploaded and validated. If you selected delete, the files are removed from the software repository.

Clear staged OS software

You can remove staged OS software to ensure that a pending version is not inadvertently activated at a later time. Removing the staged OS software does not affect the current version that is running on the storage arrays.

Steps

1. From the main view, select **Manage**, and then select **Upgrade Center › Clear Staged OS Software**.

   The Clear Staged OS Software dialog box opens and lists all the discovered storage systems with pending software or NVSRAM.

2. If needed, filter or sort the storage systems in the list, so you can view all systems that have staged software.
3. Select the check boxes for the storage systems with pending software that you want cleared.
4. Click **Clear**.

   The status of the operation is shown in the dialog box.

Mirroring

Mirroring overview

Use the mirroring features to replicate data between a local storage array and a remote storage array, either asynchronously or synchronously.

> ⓘ Synchronous mirroring is not available on the EF600 or EF300 storage system.

What is mirroring?

SANtricity applications include two types of mirroring — asynchronous and synchronous. Asynchronous mirroring copies data volumes on demand or on a schedule, which minimizes or avoids downtime that might result from data corruption or loss. Synchronous mirroring replicates data volumes in real time to ensure continuous availability.

Learn more:

- How mirroring works
- Mirroring terminology

How do I configure mirroring?

You configure asynchronous or synchronous mirroring in Unified Manager, and then use System Manager to manage synchronizations.

Learn more:

- Mirroring configuration workflow
- Requirements for using mirroring

- Create asynchronous mirrored pair
- Create synchronous mirrored pair

Concepts

How mirroring works

Unified Manager includes configuration options for the SANtricity mirroring features, which enable administrators to replicate data between two storage arrays for data protection.

ⓘ Synchronous mirroring is not available on the EF600 or EF300 storage system.

Types of mirroring

SANtricity applications include two types of mirroring — asynchronous and synchronous.

Asynchronous mirroring copies data volumes on demand or on a schedule, which minimizes or avoids downtime that might result from data corruption or loss. Asynchronous mirroring captures the state of the primary volume at a particular point in time and copies just the data that has changed since the last image capture. The primary site can be updated immediately and the secondary site can be updated as bandwidth allows. The information is cached and sent later, as network resources become available. This type of mirroring is ideal for periodic processes such as backup and archive.

Synchronous mirroring replicates data volumes in real time to ensure continuous availability. The purpose is to achieve a recovery point objective (RPO) of zero lost data by having a copy of important data available if a disaster happens on one of the two storage arrays. The copy is identical to production data at every moment because each time a write is done to the primary volume, a write is done to the secondary volume. The host does not receive an acknowledgment that the write was successful until the secondary volume is updated with the changes that were made on the primary volume. This type of mirroring is ideal for business continuity purposes such as disaster recovery.

Differences between mirroring types

The following table describes the main differences between the two types of mirroring.

Attribute	Asynchronous	Synchronous
Replication method	Point-in-time — Mirroring is done on demand or automatically according to a user-defined schedule.	Continuous — Mirroring is automatically executed continuously, copying data from every host write.
Distance	Supports long distances between arrays. Typically, the distance is limited only by the capabilities of the network and the channel extension technology.	Restricted to shorter distances between arrays. Typically, the distance must be within about 10 km (6.2 miles) of the local storage array to meet the latency and application performance requirements.

Attribute	Asynchronous	Synchronous
Communication method	A standard IP or Fibre Channel network.	Fibre Channel network only.
Volume types	Standard or thin.	Standard only.

Mirroring configuration workflow

You configure asynchronous or synchronous mirroring in Unified Manager, and then use System Manager to manage synchronizations.

Asynchronous mirroring workflow

Asynchronous mirroring involves the following workflow:

1. Perform the initial configuration in Unified Manager:
   a. Select the local storage array as the source for the data transfer.
   b. Create or select an existing mirror consistency group, which is a container for the primary volume on the local array and the secondary volume on the remote array. The primary and secondary volumes are referred to as the "mirrored pair." If you are creating the mirror consistency group for the first time, you specify whether you want to perform manual or scheduled synchronizations.
   c. Select a primary volume from the local storage array, and then determine its reserved capacity. Reserved capacity is the physical allocated capacity to be used for the copy operation.
   d. Select a remote storage array as the destination of the transfer, a secondary volume, and then determine its reserved capacity.
   e. Begin the initial data transfer from the primary volume to the secondary volume. Depending on the volume size, this initial transfer could take several hours.
2. Check the progress of the initial synchronization:
   a. In Unified Manager, launch System Manager for the local array.
   b. In System Manager, view the status of the mirroring operation. When mirroring is complete, the status of the mirrored pair is "Optimal."
3. Optionally, you can reschedule or manually perform subsequent data transfers in System Manager. Only new and changed blocks are transferred from the primary volume to the secondary volume.

> ⓘ Because asynchronous replication is periodic, the system can consolidate the changed blocks and conserve network bandwidth. There is minimal impact on write throughput and write latency.

Synchronous mirroring workflow

Synchronous mirroring involves the following workflow:

1. Perform the initial configuration in Unified Manager:
   a. Select a local storage array as the source for the data transfer.
   b. Select a primary volume from the local storage array.

   c. Select a remote storage array as the destination for the data transfer, and then select a secondary volume.
   d. Select synchronization and resynchronization priorities.
   e. Begin the initial data transfer from the primary volume to the secondary volume. Depending on the volume size, this initial transfer could take several hours.
2. Check the progress of the initial synchronization:
   a. In Unified Manager, launch System Manager for the local array.
   b. In System Manager, view the status of the mirroring operation. When mirroring is complete, the status of the mirrored pair is "Optimal." The two arrays attempt to stay synchronized through normal operations. Only new and changed blocks are transferred from the primary volume to the secondary volume.
3. Optionally, you can change synchronization settings in System Manager.

> ⓘ Because synchronous replication is continuous, the replication link between the two sites must provide sufficient bandwidth capabilities.

Mirroring terminology

Learn how the mirroring terms apply to your storage array.

Term	Description
Local storage array	The local storage array is the storage array that you are acting upon.
Mirror consistency group	A mirror consistency group is a container for one or more mirrored pairs. For asynchronous mirroring operations, you must create a mirror consistency group. All mirrored pairs in a group are resynchronized simultaneously, thus preserving a consistent recovery point. Synchronous mirroring does not use mirror consistency groups.
Mirrored pair	A mirrored pair is comprised of two volumes, a primary volume and a secondary volume. In asynchronous mirroring, a mirrored pair always belongs to a mirror consistency group. Write operations are performed first to the primary volume and then replicated to the secondary volume. Each mirrored pair in a mirror consistency group share the same synchronization settings.
Primary volume	The primary volume of a mirrored pair is the source volume to be mirrored.
Remote storage array	The remote storage array is usually designated as the secondary site, which usually holds a replica of the data in a mirroring configuration.

Term	Description
Reserved capacity	Reserved capacity is the physical allocated capacity that is used for any copy service operation and storage object. It is not directly readable by the host. These volumes are required so that the controller can persistently save information needed to maintain mirroring in an operational state. They contain information such as delta logs and copy-on-write data.
Secondary volume	The secondary volume of a mirrored pair is usually located at a secondary site and holds a replica of the data.
Synchronization	Synchronization occurs at initial synchronization between the local storage array and the remote storage array. Synchronization also occurs when the primary and secondary volumes become unsynchronized after a communication interruption. When the communication link is working again, any unreplicated data is synchronized to the secondary volume’s storage array.

Requirements for using mirroring

If you plan to configure mirroring, keep the following requirements in mind.

Unified Manager

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Storage arrays

ⓘ Synchronous mirroring is not available on the EF600 or EF300 storage array.

- You must have two storage arrays.
- Each storage array must have two controllers.
- The two storage arrays must be discovered in Unified Manager.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- You must have enough free capacity on the remote storage array to create a secondary volume equal to or greater than the primary volume that you want to mirror.
- Asynchronous mirroring is supported on controllers with Fibre Channel (FC) or iSCSI host ports, while synchronous mirroring is supported only on controllers with FC host ports.

Connectivity requirements

Mirroring through an FC interface (asynchronous or synchronous) requires the following:

- Each controller of the storage array dedicates its highest numbered FC host port to mirroring operations.
- If the controller has both base FC ports and host interface card (HIC) FC ports, the highest numbered port is on a HIC. Any host logged on to the dedicated port is logged out, and no host login requests are accepted. I/O requests on this port are accepted only from controllers that are participating in mirroring operations.
- The dedicated mirroring ports must be attached to an FC fabric environment that supports the directory service and name service interfaces. In particular, FC-AL and point-to-point are not supported as connectivity options between the controllers that are participating in mirror relationships.

Mirroring through an iSCSI interface (asynchronous only) requires the following:

- Unlike FC, iSCSI does not require a dedicated port. When asynchronous mirroring is used in iSCSI environments, it is not necessary to dedicate any of the storage array’s front-end iSCSI ports for use with asynchronous mirroring; those ports are shared for both asynchronous mirror traffic and host-to-array I/O connections.
- The controller maintains a list of remote storage systems with which the iSCSI initiator attempts to establish a session. The first port that successfully establishes an iSCSI connection is used for all subsequent communication with that remote storage array. If communication fails, a new session is attempted using all available ports.
- iSCSI ports are configured at the array level on a port-by-port basis. Intercontroller communication for configuration messaging and data transfer uses the global settings, including settings for:
  - VLAN: Both local and remote systems must have the same VLAN setting to communicate
  - iSCSI listening port
  - Jumbo frames
  - Ethernet priority

ⓘ The iSCSI intercontroller communication must use a host connect port and not the management Ethernet port.

Mirrored volume candidates

- RAID level, caching parameters, and segment size can be different on the primary and secondary volumes of a mirrored pair.

  ⓘ For EF600 and EF300 controllers, the primary and secondary volumes of an asynchronous mirrored pair must match the same protocol, tray level, segment size, security type, and RAID level. Non-eligible asynchronous mirrored pairs will not appear in the list of available volumes.

- The secondary volume must be at least as large as the primary volume.
- A volume can participate in only one mirror relationship.
- For a synchronous mirrored pair, the primary and secondary volumes must be standard volumes. They cannot be thin volumes or snapshot volumes.
- For synchronous mirroring, there are limits to the number of volumes that are supported on a given storage array. Make sure that the number of configured volumes on your storage array is less than the supported

limit. When synchronous mirroring is active, the two reserved capacity volumes that are created count against the volume limit.

- For asynchronous mirroring, the primary volume and the secondary volume must have the same Drive Security capabilities.
  - If the primary volume is FIPS capable, the secondary volume must be FIPS capable.
  - If the primary volume is FDE capable, the secondary volume must be FDE capable.
  - If the primary volume is not using Drive Security, the secondary volume must not be using Drive Security.

Reserved capacity

Asynchronous mirroring:

- A reserved capacity volume is required for a primary volume and for a secondary volume in a mirrored pair for logging write information to recover from controller resets and other temporary interruptions.
- Because both the primary volume and the secondary volume in a mirrored pair require additional reserved capacity, you must ensure that you have free capacity available on both storage arrays in the mirror relationship.

Synchronous mirroring:

- Reserved capacity is required for a primary volume and for a secondary volume for logging write information to recover from controller resets and other temporary interruptions.
- The reserved capacity volumes are created automatically when synchronous mirroring is activated. Because both the primary volume and the secondary volume in a mirrored pair require reserved capacity, you must ensure that you have enough free capacity available on both storage arrays that are participating in the synchronous mirror relationship.

Drive Security feature

- If you are using secure-capable drives, the primary volume and the secondary volume must have compatible security settings. This restriction is not enforced; therefore, you must verify it yourself.
- If you are using secure-capable drives, the primary volume and the secondary volume should use the same drive type. This restriction is not enforced; therefore, you must verify it yourself.
- If you are using Data Assurance (DA), the primary volume and the secondary volume must have the same DA settings.

Configure mirroring

Create asynchronous mirrored pair

To configure asynchronous mirroring, you create a mirrored pair that includes a primary volume on the local array and a secondary volume on the remote array.

Before you begin

Before you create a mirrored pair, meet the following requirements for Unified Manager:

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.

- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Also be sure to meet the following requirements for storage arrays and volumes:

- Each storage array must have two controllers.
- The two storage arrays must be discovered in Unified Manager.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- You must have enough free capacity on the remote storage array to create a secondary volume equal to or greater than the primary volume that you want to mirror.
- Your local and remote storage arrays are connected through a Fibre Channel fabric or iSCSI interface.
- You have created both the primary and secondary volumes that you want to use in the asynchronous mirror relationship.
- The secondary volume must be at least as large as the primary volume.

About this task

The process to create an asynchronous mirrored pair is a multi-step procedure.

Step 1: Create or select a mirror consistency group

In this step, you create a new mirror consistency group or select an existing one. A mirror consistency group is a container for the primary and secondary volumes (the mirrored pair), and specifies the desired resynchronization method (manual or automatic) for all pairs in the group.

Steps

1. From the **Manage** page, select the local storage array that you want to use for the source.
2. Select **Actions › Create Asynchronous Mirrored Pair**.

   The Create Asynchronous Mirrored Pair wizard opens.

3. Select either an existing mirror consistency group or create a new one.

   To select an existing group, make sure **An existing mirror consistency group** is selected, and then select the group from the table. A consistency group can include multiple mirrored pairs.

   To create a new group, do the following:

   a. Select **A new mirror consistency group**, and then click **Next**.

   b. Enter a unique name that best describes the data on the volumes that will be mirrored between the two storage arrays. A name can only consist of letters, numbers, and the special characters underscore (_), dash (-), and the hash sign (#). A name may not exceed 30 characters and may not contain spaces.

   c. Select the remote storage array on which you want to establish a mirror relationship with the local storage array.

      ⓘ If your remote storage array is password protected, the system prompts for a password.

d. Choose whether you want to synchronize the mirrored pairs manually or automatically:

   - **Manual** — Select this option to manually start synchronization for all mirrored pairs within this group. Note that when you want to perform a resynchronization later, you must launch System Manager for the primary storage array, and then go to **Storage › Asynchronous Mirroring**, select the group from the **Mirror Consistency Groups** tab, and then select **More › Manually resynchronize**.
   - **Automatic** — Select the desired interval in **Minutes**, **Hours**, or **Days**, from the beginning of the previous update to the beginning of the next update. For example, if the synchronization interval is set at 30 minutes, and the synchronization process starts at 4:00 p.m., the next process starts at 4:30 p.m.

e. Select the desired alert settings:

   - For manual synchronizations, specify the threshold (defined by the percentage of the capacity remaining) for when you receive alerts.
   - For automatic synchronizations, you can set three methods of alerting: when the synchronization has not completed in a specific length of time, when the recovery point data on the remote array is older than a specific time limit, and when the reserved capacity is nearing a specific threshold (defined by the percentage of the capacity remaining).

4. Select **Next** and go to Step 2: Select the primary volume.

   If you defined a new mirror consistency group, Unified Manager creates the mirror consistency group on the local storage array first and then creates the mirror consistency group on the remote storage array. You can view and manage the mirror consistency group by launching System Manager for each array.

   > If Unified Manager successfully creates the mirror consistency group on the local storage array, but fails to create it on the remote storage array, it automatically deletes the mirror consistency group from the local storage array. If an error occurs while Unified Manager is attempting to delete the mirror consistency group, you must manually delete it.

Step 2: Select the primary volume

In this step, you select the primary volume to use in the mirror relationship and allocate its reserved capacity. When you select a primary volume on the local storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list.

Any volumes you add to the mirror consistency group on the local storage array will hold the primary role in the mirror relationship.

Steps

1. From the list of eligible volumes, select a volume that you want to use as the primary volume, and then click **Next** to allocate the reserved capacity.
2. From the list of eligible candidates, select reserved capacity for the primary volume.

   Keep the following guidelines in mind:

   - The default setting for reserved capacity is 20% of the capacity of the base volume, and usually this capacity is sufficient. If you change the percentage, click **Refresh Candidates**.
   - The capacity needed varies, depending on the frequency and size of I/O writes to the primary volume and how long you need to keep the capacity.
   - In general, choose a larger capacity for reserved capacity if one or both of these conditions exist:

        - You intend to keep the mirrored pair for a long period of time.
        - A large percentage of data blocks will change on the primary volume due to heavy I/O activity. Use historical performance data or other operating system utilities to help you determine typical I/O activity to the primary volume.

3. Select **Next** and go to Step 3: Select the secondary volume.

Step 3: Select the secondary volume

In this step, you select the secondary volume to use in the mirror relationship and allocate its reserved capacity. When you select a secondary volume on the remote storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list.

Any volumes you add to the mirror consistency group on the remote storage array will hold the secondary role in the mirror relationship.

Steps

1. From the list of eligible volumes, select a volume that you want to use as the secondary volume in the mirrored pair, and then click **Next** to allocate the reserved capacity.
2. From the list of eligible candidates, select reserved capacity for the secondary volume.

   Keep the following guidelines in mind:

    - The default setting for reserved capacity is 20% of the capacity of the base volume, and usually this capacity is sufficient. If you change the percentage, click **Refresh Candidates**.
    - The capacity needed varies, depending on the frequency and size of I/O writes to the primary volume and how long you need to keep the capacity.
    - In general, choose a larger capacity for reserved capacity if one or both of these conditions exist:
        - You intend to keep the mirrored pair for a long period of time.
        - A large percentage of data blocks will change on the primary volume due to heavy I/O activity. Use historical performance data or other operating system utilities to help you determine typical I/O activity to the primary volume.
3. Select **Finish** to complete the asynchronous mirroring sequence.

Results

Unified Manager performs the following actions:

- Begins initial synchronization between the local storage array and the remote storage array.
- Creates the reserved capacity for the mirrored pair on the local storage array and on the remote storage array.

> ⓘ If the volume being mirrored is a thin volume, only the provisioned blocks (allocated capacity rather than reported capacity) are transferred to the secondary volume during the initial synchronization. This reduces the amount of data that must be transferred to complete the initial synchronization.

Create synchronous mirrored pair

To configure synchronous mirroring, you create a mirrored pair that includes a primary volume on the local array and a secondary volume on the remote array.

This feature is not available on the EF600 or EF300 storage system.

Before you begin

Before you create a mirrored pair, meet the following requirements for Unified Manager:

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Also be sure to meet the following requirements for storage arrays and volumes:

- The two storage arrays you plan to use for mirroring are discovered in Unified Manager.
- Each storage array must have two controllers.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- Your local and remote storage arrays are connected through a Fibre Channel fabric.
- You have created both the primary and secondary volumes that you want to use in the synchronous mirror relationship.
- The primary volume must be a standard volume. It cannot be a thin volume or a snapshot volume.
- The secondary volume must be a standard volume. It cannot be a thin volume or a snapshot volume.
- The secondary volume should be at least as large as the primary volume.

About this task

The process to create synchronous mirrored pairs is a multi-step procedure.

Step 1: Select the primary volume

In this step, you select the primary volume to use in the synchronous mirror relationship. When you select a primary volume on the local storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list. The volume you select holds the primary role in the mirror relationship.

Steps

1. From the **Manage** page, select the local storage array that you want to use for the source.
2. Select **Actions › Create Synchronous Mirrored Pair**.

   The Create Synchronous Mirrored Pair wizard opens.

3. From the list of eligible volumes, select a volume that you want to use as the primary volume in the mirror.
4. Select **Next** and go to Step 2: Select the secondary volume.

Step 2: Select the secondary volume

In this step, you select the secondary volume to use in the mirror relationship. When you select a secondary volume on the remote storage array, the system displays a list of all the eligible volumes for that mirrored pair. Any volumes that are not eligible to be used do not display in that list. The volume you select will hold the secondary role in the mirror relationship.

Steps

1. Select the remote storage array on which you want to establish a mirror relationship with the local storage array.

   ⓘ If your remote storage array is password protected, the system prompts for a password.

   - Storage arrays are listed by their storage array name. If you have not named a storage array, it will be listed as "unnamed."
   - If the storage array you want to use is not in the list, make sure it has been discovered in Unified Manager.

2. From the list of eligible volumes, select a volume that you want to use as the secondary volume in the mirror.

   ⓘ If a secondary volume is chosen with a capacity that is larger than the primary volume, the usable capacity is restricted to the size of the primary volume.

3. Click **Next** and go to Step 3: Select synchronization settings.

Step 3: Select synchronization settings

In this step, you select the settings that determine how data is synchronized after a communication interruption. You can set the priority at which the controller owner of the primary volume resynchronizes data with the secondary volume after a communication interruption. You must also select the resynchronization policy, either manual or automatic.

Steps

1. Use the slider bar to set the synchronization priority.

   The synchronization priority determines how much of the system resources are used to complete initial synchronization and the resynchronization operation after a communication interruption as compared to service I/O requests.

   The priority set on this dialog applies to both the primary volume and the secondary volume. You can modify the rate on the primary volume at a later time by going to System Manager and selecting **Storage › Synchronous Mirroring › More › Edit Settings**.

   There are five synchronization priority rates:

   - Lowest
   - Low
   - Medium
   - High
   - Highest

If the synchronization priority is set to the lowest rate, I/O activity is prioritized, and the resynchronization operation takes longer. If the synchronization priority is set to the highest rate, the resynchronization operation is prioritized, but I/O activity for the storage array might be affected.

2. Choose whether you want to resynchronize the mirrored pairs on the remote storage array either manually or automatically.
   - **Manual** (the recommended option) — Select this option to require synchronization to be manually resumed after communication is restored to a mirrored pair. This option provides the best opportunity for recovering data.
   - **Automatic** — Select this option to start resynchronization automatically after communication is restored to a mirrored pair.

     To manually resume synchronization, go to System Manager and select **Storage › Synchronous Mirroring**, highlight the mirrored pair in the table, and select **Resume** under **More**.
3. Click **Finish** to complete the synchronous mirroring sequence.

Results

Once mirroring is activated, the system performs the following actions:

- Begins initial synchronization between the local storage array and the remote storage array.
- Sets the synchronization priority and resynchronization policy.
- Reserves the highest-numbered port of the controller’s HIC for mirror data transmission.

  I/O requests received on this port are accepted only from the remote preferred controller owner of the secondary volume in the mirrored pair. (Reservations on the primary volume are allowed.)
- Creates two reserved capacity volumes, one for each controller, which are used for logging write information to recover from controller resets and other temporary interruptions.

  The capacity of each volume is 128 MiB. However, if the volumes are placed in a pool, 4 GiB will be reserved for each volume.

After you finish

Go to System Manager and select **Home › View Operations in Progress** to view the progress of the synchronous mirroring operation. This operation can be lengthy and could affect system performance.

FAQs

What do I need to know before creating a mirror consistency group?

Follow these guidelines before you create a mirror consistency group.

Meet the following requirements for Unified Manager:

- The Web Services Proxy service must be running.
- Unified Manager must be running on your local host through an HTTPS connection.
- Unified Manager must be showing valid SSL certificates for the storage array. You can accept a self-signed certificate or install your own security certificate using Unified Manager and navigating to **Certificate › Certificate Management**.

Also be sure to meet the following requirements for storage arrays:

- The two storage arrays must be discovered in Unified Manager.
- Each storage array must have two controllers.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- Your local and remote storage arrays are connected through a Fibre Channel fabric or iSCSI interface.

> ⓘ Synchronous mirroring is not available on the EF600 or EF300 storage system.

What do I need to know before creating a mirrored pair?

Before creating a mirrored pair, follow these guidelines.

- You must have two storage arrays.
- Each storage array must have two controllers.
- The two storage arrays must be discovered in Unified Manager.
- Each controller in both the primary array and secondary array must have an Ethernet management port configured and must be connected to your network.
- The storage arrays have a minimum firmware version of 7.84. (They can each run different OS versions.)
- You must know the password for the local and remote storage arrays.
- You must have enough free capacity on the remote storage array to create a secondary volume equal to or greater than the primary volume that you want to mirror.
- Asynchronous mirroring is supported on controllers with Fibre Channel (FC) or iSCSI host ports, while synchronous mirroring is supported only on controllers with FC host ports.

> ⓘ Synchronous mirroring is not available on the EF600 or EF300 storage system.

Why would I change this percentage?

Reserved capacity is typically 20 percent of the base volume for asynchronous mirroring operations. Usually this capacity is sufficient.

The capacity needed varies, depending on the frequency and size of I/O writes to the base volume and how long you intend to use the storage object’s copy service operation. In general, choose a larger percentage for reserved capacity if one or both of these conditions exist:

- If the lifespan of a particular storage object’s copy service operation will be very long.
- If a large percentage of data blocks will change on the base volume due to heavy I/O activity. Use historical performance data or other operating system utilities to help you determine typical I/O activity to the base volume.

Why do I see more than one reserved capacity candidate?

If there is more than one volume in a pool or volume group that meets the capacity percentage amount you selected for the storage object, then you will see multiple candidates.

You can refresh the list of recommended candidates by changing the percentage of physical drive space that you want to reserve on the base volume for copy service operations. The best candidates are displayed based on your selection.

Why don’t I see all my volumes?

When you are selecting a primary volume for a mirrored pair, a list shows all the eligible volumes.

Any volumes that are not eligible to be used do not display in that list. Volumes might not be eligible for any of the following reasons:

- The volume is not optimal.
- The volume is already participating in a mirroring relationship.
- For synchronous mirroring, the primary and secondary volumes in a mirrored pair must be standard volumes. They cannot be thin volumes or snapshot volumes.
- For asynchronous mirroring, thin volumes must have auto-expansion enabled.

> For EF600 and EF300 controllers, the primary and secondary volumes of an asynchronous mirrored pair must match the same protocol, tray level, segment size, security type, and RAID level. Non-eligible asynchronous mirrored pairs will not appear in the list of available volumes.

Why don’t I see all the volumes on the remote storage array?

When you are selecting a secondary volume on the remote storage array, a list shows all the eligible volumes for that mirrored pair.

Any volumes that are not eligible to be used, do not display in that list. Volumes may not be eligible for any of the following reasons:

- The volume is a non-standard volume, such as a snapshot volume.
- The volume is not optimal.
- The volume is already participating in a mirroring relationship.
- For asynchronous mirroring, the thin volume attributes between the primary volume and the secondary volume do not match.
- If you are using Data Assurance (DA), the primary volume and the secondary volume must have the same DA settings.
  - If the primary volume is DA enabled, the secondary volume must be DA enabled.
  - If the primary volume is not DA enabled, the secondary volume must not be DA enabled.
- For asynchronous mirroring, the primary volume and the secondary volume must have the same Drive Security capabilities.

- ◦ If the primary volume is FIPS capable, the secondary volume must be FIPS capable.
- ◦ If the primary volume is FDE capable, the secondary volume must be FDE capable.
- ◦ If the primary volume is not using Drive Security, the secondary volume must not be using Drive Security.

What impact does synchronization priority have on synchronization rates?

The synchronization priority defines how much processing time is allocated for synchronization activities relative to system performance.

The controller owner of the primary volume performs this operation in the background. At the same time, the controller owner processes local I/O writes to the primary volume and associated remote writes to the secondary volume. Because the resynchronization diverts controller processing resources from I/O activity, resynchronization can have a performance impact to the host application.

Keep these guidelines in mind to help you determine how long a synchronization priority might take and how the synchronization priorities can affect system performance.

These priority rates are available:

- Lowest
- Low
- Medium
- High
- Highest

The lowest priority rate supports system performance, but the resynchronization takes longer. The highest priority rate supports resynchronization, but system performance might be compromised.

These guidelines roughly approximate the differences between the priorities.

Priority rate for full synchronization	Time elapsed compared to highest synchronization rate
Lowest	Approximately eight times as long as at the highest priority rate.
Low	Approximately six times as long as at the highest priority rate.
Medium	Approximately three-and-a-half times as long as at the highest priority rate.
High	Approximately twice as long as at the highest priority rate.

Volume size and host I/O rate loads affect the synchronization time comparisons.

Why is it recommended to use a manual synchronization policy?

Manual resynchronization is recommended because it lets you manage the resynchronization process in a way that provides the best opportunity for recovering data.

If you use an Automatic resynchronization policy and intermittent communication problems occur during resynchronization, data on the secondary volume could be temporarily corrupted. When resynchronization is complete, the data is corrected.

Certificates

Certificates overview

Certificate Management allows you to create certificate signing requests (CSRs), import certificates, and manage existing certificates.

What are certificates?

Certificates are digital files that identify online entities, such as websites and servers, for secure communications on the internet. There are two types of certificates: a *signed certificate* is validated by a certificate authority (CA) and a *self-signed certificate* is validated by the owner of the entity instead of a third party.

Learn more:

- How certificates work
- Certificate terminology

How do I configure certificates?

From Certificate Management, you can configure certificates for the management station hosting Unified Manager and also import certificates for the controllers in the arrays.

Learn more:

- Use CA-signed certificates for the management system
- Import certificates for arrays

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.
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."

Term	Description
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.

Use CA-signed certificates for the management system

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 three-step procedure.

Step 1: Complete a CSR file

You must first generate a certificate signing request (CSR) file, which identifies your organization and the host system where the Web Services Proxy and Unified Manager are installed.

> Alternatively, you can generate a CSR file using a tool such as OpenSSL and skip to Step 2: Submit CSR file.

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 where the Web Services Proxy is installed:
   - **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://. The DNS name cannot begin with a wildcard.
   - **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. The DNS name cannot begin with a wildcard.
5. Make sure that the host information is correct. If it is not, the certificates returned from the CA will fail when you try to import them.
6. Click **Finish**.
7. Go to Step 2: Submit CSR file.

Step 2: Submit CSR file

After you create a certificate signing request (CSR) file, you send it to a Certificate Authority (CA) to receive signed, management certificates for the system hosting Unified Manager and the Web Services Proxy.

> E-Series systems require PEM format (Base64 ASCII encoding) for signed certificates, which includes the following file types: .pem, .crt, .cer, or .key.

Steps

1. Locate the downloaded CSR file.

   The folder location of the download depends on your browser.

2. Submit the CSR file to a CA (for example, Verisign or DigiCert), and request signed certificates in PEM format.

   > **After you submit a CSR file to the CA, do NOT regenerate another CSR file.** Whenever 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 system's keystore. When you receive the signed certificates and import them, the system ensures that both the private and public keys are the original pair. If the keys do not match, the signed certificates will not work and you must request new certificates from the CA.

3. When the CA returns the signed certificates, go to Step 3: Import management certificates.

Step 3: Import management certificates

After you receive signed certificates from the Certificate Authority (CA), import the certificates into the host system where the Web Services Proxy and Unified Manager interface are installed.

Before you begin

- You have received signed certificates from the CA. These files include the root certificate, one or more intermediate certificates, and the server certificate.
- If the CA provided a chained certificate file (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**). Base-64 encoding is recommended. When the exports are complete, a CER file is shown for each certificate file in the chain.

- You have copied the certificate files to the host system where the Web Services Proxy is running.

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 certificate files, and then select the server certificate. If you generated the CSR from an external tool, you must also import the private key file that was created along with the CSR.

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

Steps

1. Select **Settings > Certificates**.
2. Select the **Array Management** tab, then 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.

Use array certificates

Import certificates for arrays

If necessary, you can import certificates for the storage arrays so they can authenticate with the system hosting 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 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.

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**.

   > i 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 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.

Manage certificates

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.

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.
- **SAML** — Authentication is managed through an Identity Provider (IdP) using SAML 2.0.

Learn more:

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

How do I configure Access Management?

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

Learn more:

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

Concepts

How Access Management works

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

4. The administrator provides users with login credentials for Unified Manager.
5. Users log in to the system by entering their credentials. During login, the system performs the following background tasks:
   - Authenticates the user name and password against the user account.
   - Determines the user's permissions based on the assigned roles.
   - Provides the user with access to functions in the user interface.
   - Displays the user name in the top banner.

Functions available in Unified Manager

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

- **Storage admin** — Full read/write access to storage objects on the arrays, but no access to the security configuration.
- **Security admin** — Access to the security configuration in Access Management and Certificate Management.
- **Support admin** — Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration.
- **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

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

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.
SAML	Security Assertion Markup Language (SAML) is an XML-based standard for authentication and authorization between two entities. SAML allows for multi-factor authentication, in which users must provide two or more items for proving their identity (for example, a password and fingerprint). The storage array's embedded SAML feature is SAML2.0 compliant for identity assertion, authentication, and authorization.
SSO	Single sign-on (SSO) is an authentication service that allows for one set of login credentials to access multiple applications.
Web Services Proxy	The Web Services Proxy, which provides access through standard HTTPS mechanisms, allows administrators to configure management services for storage arrays. The proxy can be installed on Windows or Linux hosts. The Unified Manager interface is available with the Web Services Proxy.

Permissions for mapped roles

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

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 Unified Manager with a user profile that includes Security Admin permissions.

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

2. The administrator goes to the **SAML** tab under Access Management.
3. An administrator configures communications with the Identity Provider (IdP). An IdP is an external system used to request credentials from a user and determine if the user is successfully authenticated. To configure communications with the storage array, the administrator downloads the IdP metadata file from the IdP system, and then uses Unified Manager to upload the file to the storage array.
4. An administrator establishes a trust relationship between the Service Provider and the IdP. A Service Provider controls user authorization; in this case, the controller in the storage array acts as the Service Provider. To configure communications, the administrator uses Unified Manager to export a Service Provider metadata file for the controller. From the IdP system, the administrator then imports the metadata file to the IdP.

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

5. The administrator maps the storage array’s roles to user attributes defined in the IdP. To do this, the administrator uses Unified Manager to create the mappings.
6. The administrator tests the SSO login to the IdP URL. This test ensures the storage array and IdP can communicate.

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

7. From Unified Manager, the administrator enables SAML for the storage array.
8. Users log in to the system with their SSO credentials.

Management

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

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

Access restrictions

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

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

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

Use local user roles

View local user roles

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

Use SAML

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.

Before you begin

- You must be logged in with a user profile that includes Security admin permissions. Otherwise, the Access Management functions do not appear.
- You must know the IP address or domain name the controller in the storage array.
- An IdP administrator has configured an IdP system.
- An IdP administrator has ensured that the IdP supports the ability to return a Name ID on authentication.
- An administrator has ensured that the IdP server and controller clock is synchronized (either through an NTP server or by adjusting the controller clock settings).
- An IdP metadata file is downloaded from the IdP system and is available on the local system used for accessing Unified Manager.

About this task

An Identity Provider (IdP) is an external system used to request credentials from a user and to determine if that user is successfully authenticated. The IdP can be configured to provide multi-factor authentication and to use any user database, such as Active Directory. Your security team is responsible for maintaining the IdP. A Service Provider (SP) is a system that controls user authentication and access. When Access Management is configured with SAML, the storage array acts as the Service Provider for requesting authentication from the Identity Provider. To establish a connection between the IdP and storage array, you share metadata files between these two entities. Next, you map the IdP user entities to the storage array roles. And finally, you test the connection and SSO logins before enabling SAML.

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

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

Configuring SAML authentication is a multi-step procedure.

Step 1: Upload the IdP metadata file

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

Steps

1. Select **Settings › Access Management**.
2. Select the **SAML** tab.

   The page displays an overview of configuration steps.

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

   The Import Identity Provider File dialog box opens.

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

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

5. Click **Import**.

Step 2: Export Service Provider files

To establish a trust relationship between the IdP and the storage array, you import the Service Provider metadata into the IdP. The IdP needs this metadata to establish a trust relationship with the controller and to process authorization requests. The file includes information such as the controller domain name or IP address, so that the IdP can communicate with the Service Providers.

Steps

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

   The Export Service Provider Files dialog box opens.

2. Enter the controller IP address or DNS name in the **Controller A** field, and then click **Export** to save the metadata file to your local system.

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

3. From the local system, locate the XML-formatted Service Provider metadata file you exported.
4. From the IdP server, import the Service Provider metadata file to establish the trust relationship. You can either import the file directly or you can manually enter the controller information from the file.

Step 3: Map roles

To provide users with authorization and access to Unified Manager, you must map the IdP user attributes and group memberships to the storage array's predefined roles.

Before you begin

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

Steps

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

   The Role Mapping dialog box opens.

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

   Field details

Setting	Description
Mappings	
User Attribute	Specify the attribute (for example, "member of") for the SAML group to be mapped.
Attribute Value	Specify the attribute value for the group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern: \.[]{}()<>*+-=!?^$|
Roles	Click in the field and select one of the storage array's roles to be mapped to the Attribute. You must individually select each role you want to include. The Monitor role is required in combination with the other roles to log in to Unified Manager. The Security Admin role is also required for at least one group. The mapped roles include the following permissions: • **Storage admin** — Full read/write access to the storage objects (for example, volumes and disk pools), but no access to the security configuration. • **Security admin** — Access to the security configuration in Access Management, certificate management, audit log management, and the ability to turn the legacy management interface (SYMbol) on or off. • **Support admin** — Access to all hardware resources on the storage array, failure data, MEL events, and controller firmware upgrades. No access to storage objects or the security configuration. • **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

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

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

   ⓘ Role mappings can be modified after SAML is enabled.

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

Step 4: Test SSO login

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

Before you begin

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

Steps

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

   A dialog box opens for entering SSO credentials.

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

   A dialog box opens while the system tests the login.

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

   If the test does not complete successfully, an error message appears with further information. Make sure that:

   - The user belongs to a group with permissions for Security Admin and Monitor.
   - The metadata you uploaded for the IdP server is correct.
   - The controller address in the SP metadata files is correct.

Step 5: Enable SAML

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

Before you begin

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

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

Steps

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

   The Confirm Enable SAML dialog box opens.

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

Results

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

Change SAML role mappings

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

Before you begin

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

Steps

1. Select **Settings › Access Management**.
2. Select the **SAML** tab.
3. Select **Role Mapping**.

   The Role Mapping dialog box opens.

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

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

Field details

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

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

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

Results

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

Export SAML Service Provider files

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

Before you begin

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

- SAML is configured and enabled.

About this task

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

Steps

1. Select **Settings › Access Management**.
2. Select the **SAML** tab.
3. Select **Export**.

   The Export Service Provider Files dialog box opens.

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

   > ⓘ The domain name field is read-only.

   Make a note of where the file is stored.

5. From the local system, locate the XML-formatted Service Provider metadata file you exported.
6. From the IdP server, import the Service Provider metadata file. You can either import the file directly or you can manually enter the controller information.
7. Click **Close**.

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.
- SAML authentication is enabled. Refresh your browser to log in.

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

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

- User groups must be defined in your directory service.
- LDAP server credentials must be available, including the domain name, server URL, and optionally the bind account user name and password.
- For LDAPS servers using a secure protocol, the LDAP server’s certificate chain must be installed on your local machine.

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

Before mapping groups to roles, review the guidelines.

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

- **Storage admin** — Full read/write access to storage objects on the arrays, but no access to the security configuration.
- **Security admin** — Access to the security configuration in Access Management and Certificate Management.
- **Support admin** — Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration.
- **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

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

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

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

SAML

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

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

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

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

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

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

Requirements

Before you begin, make sure that:

- An Identity Provider (IdP) is configured in your network. An IdP is an external system used to request credentials from a user and determine if the user is successfully authenticated. Your security team is responsible for maintaining the IdP.
- An IdP administrator has configured user attributes and groups in the IdP system.
- An IdP administrator has ensured that the IdP supports the ability to return a Name ID on authentication.
- An administrator has ensured that the IdP server and controller clock is synchronized (either through an NTP server or by adjusting the controller clock settings).
- An IdP metadata file is downloaded from the IdP system and available on the local system used for accessing Unified Manager.
- You know the IP address or domain name the controller in the storage array.

Restrictions

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

- Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance. We recommend that you test the SSO logins before you enable SAML in the final configuration step. (The system also performs an SSO login test before enabling SAML.)
- If you disable SAML in the future, the system automatically restores the previous configuration (Local User Roles and/or Directory Services).
- If Directory Services are currently configured for user authentication, SAML overrides that configuration.
- When SAML is configured, the following clients cannot access storage array resources:
  - Enterprise Management Window (EMW)
  - Command-line interface (CLI)
  - Software Developer Kits (SDK) clients
  - In-band clients
  - HTTP Basic Authentication REST API clients
  - Login using standard REST API endpoint

What are the local users?

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

Local users include:

- **admin** — Super administrator who has access to all functions in the system. This user includes all roles. The password must be set on first-time login.
- **storage** — The administrator responsible for all storage provisioning. This user includes the following roles: Storage Admin, Support Admin, and Monitor. This account is disabled until a password is set.
- **security** — The user responsible for security configuration, including Access Management and Certificate Management. This user includes the following roles: Security Admin and Monitor. This account is disabled until a password is set.
- **support** — The user responsible for hardware resources, failure data, and firmware upgrades. This user includes the following roles: Support Admin and Monitor. This account is disabled until a password is set.
- **monitor** — A user with read-only access to the system. This user includes only the Monitor role. This

account is disabled until a password is set.

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

Copyright information

Trademark information