Main interface

SANtricity 11.8

NetApp
May 08, 2024

Table of Contents

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**.

Copyright information

Trademark information