Use local user roles

SANtricity 11.7

NetApp
February 12, 2024

Table of Contents

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**.

Copyright information

Trademark information