# Use local user roles

## SANtricity software

NetApp
March 12, 2026

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity/um-certificates/view-local-user-roles-unified.html on March 12, 2026. Always check docs.netapp.com for the latest.

# Table of Contents

Use local user roles . . . . . 1
View local user roles . . . . . 1
Change passwords for local user profiles in SANtricity Unified Manager . . . . . 1
Change local user password settings in SANtricity Unified Manager . . . . . 2

# 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 SANtricity Unified Manager.

**Before you begin**

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

**About this task**

The users and mappings cannot be changed. Only passwords can be modified.

**Steps**

1. Select **Access Management**.
2. Select the **Local User Roles** tab.

   The users are shown in the table:

   - **admin** — Super administrator who has access to all functions in the system. This user includes all roles.
   - **storage** — The administrator responsible for all storage provisioning. This user includes the following roles: Storage Admin, Support Admin, and Monitor.
   - **security** — The user responsible for security configuration, including Access Management and Certificate Management. This user includes the following roles: Security Admin and Monitor.
   - **support** — The user responsible for hardware resources, failure data, and firmware upgrades. This user includes the following roles: Support Admin and Monitor.
   - **monitor** — A user with read-only access to the system. This user includes only the Monitor role.
   - **rw** (read/write) — This user includes the following roles: Storage Admin, Support Admin, and Monitor.
   - **ro** (read only) — This user includes only the Monitor role.

# Change passwords for local user profiles in SANtricity Unified Manager

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 in SANtricity Unified Manager

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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

## Trademark information

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