Unified Manager administration

SANtricity 11.6

NetApp
February 12, 2024

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity-116/um-admin/administrator-password-protection-unified.html on February 12, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Unified Manager administration 1
Concepts 1
How tos 1

Unified Manager administration

Concepts

Administrator password protection

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

Setting an administrator password

Setting an administrator password protects the software from users who unknowingly or maliciously run destructive commands. You are required to set an administrator password when you start Unified Manager for the first time.

There is one administrator password that is shared among all users. Any user who has this password can make configuration changes to storage systems.

Entering your password

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 desired, you can adjust the session timeout.

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.

How tos

Change the admin password

You can change the admin password used for accessing SANtricity 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**.

Change storage array passwords

You can update the passwords used for viewing and accessing storage arrays in SANtricity 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 SANtricity 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**.

Manage session timeouts

You can configure timeouts for SANtricity 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.

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

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

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

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

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

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

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

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

Trademark information

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