Manage interface settings

SANtricity software

NetApp
March 27, 2025

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity-117/sm-interface/administrator-password-protection.html on March 27, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Manage interface settings . . . 1
- Manage password protection . . . 1
  - Set and change passwords . . . 1
  - Re-enter passwords after session timeouts . . . 1
  - Remove drives or password protection . . . 1
- Set default units for capacity values . . . 2
- Set default time frame for performance graphs . . . 2
- Configure login banner . . . 2
- Manage session timeouts . . . 3

Manage interface settings

Manage password protection

You must configure the storage array with passwords to protect it from unauthorized access.

Set and change passwords

When you start System 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 array, such as adding, changing, or removing objects or settings. To set the admin password during initial startup, see Access System Manager.

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

In addition to the admin password, the storage array includes pre-defined user profiles with one or more roles mapped to them. For more information, see Permissions for mapped roles. The user profiles and mappings cannot be changed. Only passwords can be modified. If you want to change the admin password or other user passwords, see Change passwords.

Re-enter passwords after session timeouts

The system prompts you for the password only once during a single management session. However, a session times out after 30 minutes of inactivity, at which time, you must enter the password again. If another user managing the same storage array from another management client 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.

You can adjust the session timeout or you can disable session timeouts altogether. See Manage session timeouts.

Remove drives or password protection

If you remove password-protected drives or you want to disable password protection, be aware of the following:

- **If you remove drives with password protection** — The password is stored on a reserved area of each drive on the storage array. If you remove all drives from a storage array, its password will no longer work. To correct this condition, re-install one of the original drives to the storage array.
- **If you want to remove password protection** — If you no longer want to have commands password-protected, enter the current administrator password, and leave the new password text boxes blank.

Running configuration commands on a storage array can cause serious damage, including data loss. For this reason, you should always set an administrator password for your storage array. Use a long administrator password with at least 15 alphanumeric characters to increase security.

Set default units for capacity values

SANtricity System Manager can display capacity values in either gibibytes (GiB) or tebibytes (TiB).

Preferences are stored in the browser's local storage so all users can have their own settings.

Steps

1. Select **Preferences › Set preferences**.
2. Click the radio button for either **Gibibytes** or **Tebibytes**, and confirm that you want to perform the operation.

   See the following table for abbreviations and values.

Abbreviation	Value
GiB	$1{,}024^3$ bytes
TiB	$1{,}024^4$ bytes

Set default time frame for performance graphs

You can change the default time frame shown by the performance graphs.

About this task

Performance graphs shown on the Home page and on the Performance page initially show a time frame of 1 hour. Preferences are stored in the browser's local storage so all users can have their own settings.

Steps

1. Select **Preferences › Set preferences**.
2. In the drop-down list, select either **5 minutes**, **1 hour**, **8 hours**, **1 day**, or **7 days**, and confirm that you want to perform the operation.

Configure login banner

You can create a login banner that is presented to users before they establish sessions in SANtricity System Manager. The banner can include an advisory notice and a consent message.

About this task

When you create a banner, it appears before the login screen in a dialog box.

Steps

1. Select **Settings › System**.
2. Under the General section, select **Configure Login Banner**.

   The Configure Login Banner dialog box opens.

3. Enter the text you want to appear in the login banner.

   Do not use HTML or other markup tags for formatting.

4. Click **Save**.

Results

The next time users log in to System Manager, the text opens in a dialog box. Users must click **OK** to continue to the login screen.

Manage session timeouts

You can configure timeouts in SANtricity System Manager, so that users' inactive sessions are disconnected after a specified time.

About this task

By default, the session timeout for System 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. Select **Settings › System**.
2. Under the General section, 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 for System Manager is 15 minutes.

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

4. Click **Save**.

Copyright information

Copyright © 2025 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.