FAQs

SANtricity 11.8

NetApp
April 05, 2024

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity/um-certificates/why-cant-i-log-in-unified.html on April 05, 2024. Always check docs.netapp.com for the latest.

Table of Contents

FAQs

Why can’t I log in?

If you receive an error when attempting to log in, review these possible causes.

Login errors might occur for one of these reasons:

- You entered an incorrect user name or password.
- You have insufficient privileges.
- You attempted to log in unsuccessfully multiple times, which triggered the lockout mode. Wait 10 minutes to re-login.
- SAML authentication is enabled. Refresh your browser to log in.

What do I need to know before adding a directory server?

Before adding a directory server in Access Management, you must meet certain requirements.

- User groups must be defined in your directory service.
- LDAP server credentials must be available, including the domain name, server URL, and optionally the bind account user name and password.
- For LDAPS servers using a secure protocol, the LDAP server’s certificate chain must be installed on your local machine.

What do I need to know about mapping to storage array roles?

Before mapping groups to roles, review the guidelines.

The RBAC (role-based access control) capabilities include the following roles:

- **Storage admin** — Full read/write access to storage objects on the arrays, but no access to the security configuration.
- **Security admin** — Access to the security configuration in Access Management and Certificate Management.
- **Support admin** — Access to all hardware resources on storage arrays, failure data, and MEL events. No access to storage objects or the security configuration.
- **Monitor** — Read-only access to all storage objects, but no access to the security configuration.

The Monitor role is required for all users, including the administrator.

If you are using an LDAP (Lightweight Directory Access Protocol) server and Directory Services, make sure that:

- An administrator has defined user groups in the directory service.

- You know the group domain names for the LDAP user groups.

SAML

If you are using the Security Assertion Markup Language (SAML) capabilities embedded in the storage array, make sure that:

- An Identity Provider (IdP) administrator has configured user attributes and group membership in the IdP system.
- You know the group membership names.
- You know the attribute value for the group to be mapped. Regular expressions are supported. These special regular expression characters must be escaped with a backslash (\) if they are not part of a regular expression pattern:

```
\.[]{}()<>*+-=!?^$|
```

- The Monitor role is required for all users, including the administrator. Unified Manager will not operate correctly for any user without the Monitor role present.

What do I need to know before configuring and enabling SAML?

Before configuring and enabling the Security Assertion Markup Language (SAML) capabilities for authentication, make sure you meet the following requirements and understand SAML restrictions.

Requirements

Before you begin, make sure that:

- An Identity Provider (IdP) is configured in your network. An IdP is an external system used to request credentials from a user and determine if the user is successfully authenticated. Your security team is responsible for maintaining the IdP.
- An IdP administrator has configured user attributes and groups in the IdP system.
- An IdP administrator has ensured that the IdP supports the ability to return a Name ID on authentication.
- An administrator has ensured that the IdP server and controller clock is synchronized (either through an NTP server or by adjusting the controller clock settings).
- An IdP metadata file is downloaded from the IdP system and available on the local system used for accessing Unified Manager.
- You know the IP address or domain name the controller in the storage array.

Restrictions

In addition to the requirements above, make sure you understand the following restrictions:

- Once SAML is enabled, you *cannot* disable it through the user interface, nor can you edit the IdP settings. If you need to disable or edit the SAML configuration, contact Technical Support for assistance. We

recommend that you test the SSO logins before you enable SAML in the final configuration step. (The system also performs an SSO login test before enabling SAML.)

- If you disable SAML in the future, the system automatically restores the previous configuration (Local User Roles and/or Directory Services).
- If Directory Services are currently configured for user authentication, SAML overrides that configuration.
- When SAML is configured, the following clients cannot access storage array resources:
  - Enterprise Management Window (EMW)
  - Command-line interface (CLI)
  - Software Developer Kits (SDK) clients
  - In-band clients
  - HTTP Basic Authentication REST API clients
  - Login using standard REST API endpoint

What are the local users?

Local users are predefined in the system and include specific permissions.

Local users include:

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

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.