Use SAML

SANtricity 11.8

NetApp
October 10, 2023

This PDF was generated from https://docs.netapp.com/us-en/e-series-santricity/um-certificates/configure-saml.html on October 10, 2023. Always check docs.netapp.com for the latest.

Table of Contents

Use SAML

Configure SAML

To configure authentication for Access Management, you can use the Security Assertion Markup Language (SAML) capabilities embedded in the storage array. This configuration establishes a connection between an Identity Provider and the Storage Provider.

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.
- You must know the IP address or domain name the controller in the storage array.
- An IdP administrator has configured an 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 is available on the local system used for accessing Unified Manager.

About this task

An Identity Provider (IdP) is an external system used to request credentials from a user and to determine if that user is successfully authenticated. The IdP can be configured to provide multi-factor authentication and to use any user database, such as Active Directory. Your security team is responsible for maintaining the IdP. A Service Provider (SP) is a system that controls user authentication and access. When Access Management is configured with SAML, the storage array acts as the Service Provider for requesting authentication from the Identity Provider. To establish a connection between the IdP and storage array, you share metadata files between these two entities. Next, you map the IdP user entities to the storage array roles. And finally, you test the connection and SSO logins before enabling SAML.

SAML and Directory Services. If you enable SAML when Directory Services is configured as the authentication method, SAML supersedes Directory Services in Unified Manager. If you disable SAML later, the Directory Services configuration returns to its previous configuration.

Editing and Disabling. 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.

Configuring SAML authentication is a multi-step procedure.

Step 1: Upload the IdP metadata file

To provide the storage array with IdP connection information, you import IdP metadata into Unified Manager. The IdP system needs this metadata to redirect authentication requests to the correct URL and to validate responses received.

Steps

1. Select **Settings › Access Management**.

2. Select the **SAML** tab.

   The page displays an overview of configuration steps.

3. Click the **Import Identity Provider (IdP) file** link.

   The Import Identity Provider File dialog box opens.

4. Click **Browse** to select and upload the IdP metadata file you copied to your local system.

   After you select the file, the IdP Entity ID is displayed.

5. Click **Import**.

Step 2: Export Service Provider files

To establish a trust relationship between the IdP and the storage array, you import the Service Provider metadata into the IdP. The IdP needs this metadata to establish a trust relationship with the controller and to process authorization requests. The file includes information such as the controller domain name or IP address, so that the IdP can communicate with the Service Providers.

Steps

1. Click the **Export Service Provider files** link.

   The Export Service Provider Files dialog box opens.

2. Enter the controller IP address or DNS name in the **Controller A** field, and then click **Export** to save the metadata file to your local system.

   After you click **Export**, the Service Provider metadata is downloaded to your local system. Make a note of where the file is stored.

3. From the local system, locate the XML-formatted Service Provider metadata file you exported.
4. From the IdP server, import the Service Provider metadata file to establish the trust relationship. You can either import the file directly or you can manually enter the controller information from the file.

Step 3: Map roles

To provide users with authorization and access to Unified Manager, you must map the IdP user attributes and group memberships to the storage array's predefined roles.

Before you begin

- An IdP administrator has configured user attributes and group membership in the IdP system.
- The IdP metadata file is imported into Unified Manager.
- A Service Provider metadata file for the controller is imported into the IdP system for the trust relationship.

Steps

1. Click the link for **mapping Unified Manager** roles.

   The Role Mapping dialog box opens.

2. Assign IdP user attributes and groups to the predefined roles. A group can have multiple assigned roles.

Field details

Setting	Description
Mappings	
User Attribute	Specify the attribute (for example, "member of") for the SAML group to be mapped.
Attribute Value	Specify 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: \.[]{}()<>*+-=!?^$|
Roles	Click in the field and select one of the storage array's roles to be mapped to the Attribute. You must individually select each role you want to include. The Monitor role is required in combination with the other roles to log in to Unified Manager. The Security Admin role is also required for at least one group. The mapped roles include the following permissions: • **Storage admin** — Full read/write access to the storage objects (for example, volumes and disk pools), but no access to the security configuration. • **Security admin** — Access to the security configuration in Access Management, certificate management, audit log management, and the ability to turn the legacy management interface (SYMbol) on or off. • **Support admin** — Access to all hardware resources on the storage array, failure data, MEL events, and controller firmware upgrades. 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. Unified Manager will not operate correctly for any user without the Monitor role present.

3. If desired, click **Add another mapping** to enter more group-to-role mappings.

Role mappings can be modified after SAML is enabled.

4. When you are finished with the mappings, click **Save**.

Step 4: Test SSO login

To ensure that the IdP system and storage array can communicate, you can optionally test an SSO login. This test is also performed during the final step for enabling SAML.

Before you begin

- The IdP metadata file is imported into Unified Manager.
- A Service Provider metadata file for the controller is imported into the IdP system for the trust relationship.

Steps

1. Select the **Test SSO Login** link.

   A dialog box opens for entering SSO credentials.

2. Enter login credentials for a user with both Security Admin permissions and Monitor permissions.

   A dialog box opens while the system tests the login.

3. Look for a Test Successful message. If the test completes successfully, go to the next step for enabling SAML.

   If the test does not complete successfully, an error message appears with further information. Make sure that:

   - The user belongs to a group with permissions for Security Admin and Monitor.
   - The metadata you uploaded for the IdP server is correct.
   - The controller address in the SP metadata files is correct.

Step 5: Enable SAML

Your final step is to finish the SAML configuration for user authentication. During this process, the system also prompts you to test an SSO login. The SSO Login test process is described in the previous step.

Before you begin

- The IdP metadata file is imported into Unified Manager.
- A Service Provider metadata file for the controller is imported into the IdP system for the trust relationship.
- At least one Monitor and one Security Admin role mapping is configured.

Editing and Disabling. 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.

Steps

1. From the **SAML** tab, select the **Enable SAML** link.

   The Confirm Enable SAML dialog box opens.

2. Type `enable`, and then click **Enable**.
3. Enter user credentials for an SSO login test.

Results

After the system enables SAML, it terminates all active sessions and begins authenticating users through SAML.

Change SAML role mappings

If you previously configured SAML for Access Management, you can change the role mappings between the IdP groups and the storage array's predefined roles.

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.
- An IdP administrator has configured user attributes and group membership in the IdP system.
- SAML is configured and enabled.

Steps

1. Select **Settings › Access Management**.
2. Select the **SAML** tab.
3. Select **Role Mapping**.

   The Role Mapping dialog box opens.

4. Assign IdP user attributes and groups to the predefined roles. A group can have multiple assigned roles.

   Be careful that you do not remove your permissions while SAML is enabled, or you will lose access to Unified Manager.

Field details

Setting	Description
Mappings	
User Attribute	Specify the attribute (for example, "member of") for the SAML group to be mapped.
Attribute Value	Specify the attribute value for the group to be mapped.
Roles	Click in the field and select one of the storage array's roles to be mapped to the attribute. You must individually select each role you want to include for this group. The Monitor role is required in combination with the other roles to log in to Unified Manager. A Security Admin role must be assigned to at least one group. The mapped roles include the following permissions: • **Storage admin** — Full read/write access to the storage objects (for example, volumes and disk pools), but no access to the security configuration. • **Security admin** — Access to the security configuration in Access Management, certificate management, audit log management, and the ability to turn the legacy management interface (SYMbol) on or off. • **Support admin** — Access to all hardware resources on the storage array, failure data, MEL events, and controller firmware upgrades. 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. Unified Manager will not operate correctly for any user without the Monitor role present.

5. Optionally, click **Add another mapping** to enter more group-to-role mappings.
6. Click **Save**.

Results

After you complete this task, any active user sessions are terminated. Only your current user session is retained.

Export SAML Service Provider files

If necessary, you can export Service Provider metadata for the storage array and re-import the file into the Identity Provider (IdP) system.

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.

- SAML is configured and enabled.

About this task

In this task, you export metadata from the controller. The IdP needs this metadata to establish a trust relationship with the controller and to process authentication requests. The file includes information such as the controller domain name or IP address that the IdP can use for sending requests.

Steps

1. Select **Settings › Access Management**.
2. Select the **SAML** tab.
3. Select **Export**.

   The Export Service Provider Files dialog box opens.

4. Click **Export** to save the metadata file to your local system.

   The domain name field is read-only.

   Make a note of where the file is stored.

5. From the local system, locate the XML-formatted Service Provider metadata file you exported.
6. From the IdP server, import the Service Provider metadata file. You can either import the file directly or you can manually enter the controller information.
7. Click **Close**.

Copyright information

Copyright © 2023 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.