Configure federations

NetApp Console setup and administration

NetApp
January 27, 2026

This PDF was generated from https://docs.netapp.com/us-en/console-setup-admin/task-federation-adfs.html on January 27, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Configure federations

Federate NetApp Console with Active Directory Federation Services (AD FS)

Federate your Active Directory Federation Services (AD FS) with the NetApp Console to enable single sign-on (SSO) for the NetApp Console. This allows users to log in to the Console using their corporate credentials.

Required roles

The Federation admin role is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

> ⓘ You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.

NetApp supports service provider-initiated (SP-initiated) SSO only. First, configure the identity provider to trust the NetApp Console as a service provider. Then, create a connection in the Console using your identity provider's configuration.

You can set up federation with your AD FS server to enable single sign-on (SSO) for NetApp Console. The process involves configuring your AD FS to trust the Console as a service provider and then creating the connection in the NetApp Console.

Steps

1. Select **Administration > Identity and access**.
2. Select **Federation** to view the **Federations** page.
3. Select **Configure new federation**.
4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
   b. Enter the name of the federation you are configuring.
   c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Protocol** and then select **Active Directory Federation Services (AD FS)**.
7. Select **Next**.
8. Create a Relying Party Trust in your AD FS server. You can use PowerShell or manually configure it on your AD FS server. Consult the AD FS documentation for details on how to create a relying party trust.

   a. Create the trust using PowerShell by using following script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

   b. Alternatively, you can create the trust manually in the AD FS management console. Use the following NetApp Console values when creating the trust:

      - When creating the Relying Trust Identifier, use the **YOUR_TENANT** value: `netapp-cloud-account`

      - When you select **Enable support for the WS-Federation**, use the **YOUR_AUTH0_DOMAIN** value: `netapp-cloud-account.auth0.com`

   c. After creating the trust, copy the metadata URL from your AD FS server or download the federation metadata file. You'll need this URL or file to complete the connection in the Console.

   NetApp recommends using the metadata URL to let the NetApp Console automatically retrieve the latest AD FS configuration. If you download the federation metadata file, you will need to update it manually in the NetApp Console whenever there are changes to your AD FS configuration.

9. Return to the Console, and select **Next** to create the connection.
10. Create the connection with AD FS.
    a. Enter the **AD FS URL** that you copied from your AD FS server in the previous step or upload the federation metadata file that you downloaded from your AD FS server.
11. Select **Create connection**. Creating the connection might take a few seconds.
12. Select **Next**.
13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials. After you log in, go back to the Console to enable the connection.

    > When using the Console in restricted mode, copy the URL to either an incognito browser window or a separate browser to log in to your IdP.

14. In the Console, select **Next** to review the summary page.
15. Set up notifications.

    Choose between seven days or 30 days. The system emails expiry notifications and shows them in the Console to any user with the following roles: Super admin, Org admin, Federation admin, and Federation viewer.

16. Review the federation details and then select **Enable federation**.
17. Select **Finish** to complete the process.

After you enable the federation, users log in to the NetApp Console using their corporate credentials.

Federate NetApp Console with Microsoft Entra ID

Federate with your Microsoft Entra ID IdP provider to enable single sign-on (SSO) for the

NetApp Console. This allows users to log in using their corporate credentials.

Required roles

The Federation admin role is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

> ⓘ You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in the Console that uses the identity provider's configuration.

You can set up a federated connection with Microsoft Entra ID to enable single sign-on (SSO) for the Console . The process involves configuring your Microsoft Entra ID to trust the Console as a service provider and then creating the connection in the Console.

Steps

1. Select **Administration > Identity and access**.
2. Select **Federation** to view the **Federations** page.
3. Select **Configure new federation**.

Domain details

4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
   b. Enter the name of the federation you are configuring.
   c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.

Connection method

6. For your connection method, choose **Provider** and then select **Microsoft Entra ID**.
7. Select **Next**.

Configuration instructions

1. Configure your Microsoft Entra ID to trust NetApp as a service provider. You need to do this step on your Microsoft Entra ID server.
   a. Use the following values when registering your Microsoft Entra ID app to trust the Console:
      - For the **Redirect URL** , use `https://services.cloud.netapp.com`
      - For the **Reply URL**, use `https://netapp-cloud-account.auth0.com/login/callback`
   b. Create a client secret for your Microsoft Entra ID app. You'll need to provide the client ID, the client secret, and the Entra ID domain name to complete the federation.
2. Return to the Console, and select **Next** to create the connection.

Create connection

1. Create the connection with Microsoft Entra ID
    a. Enter the client ID and Client secret that you created in the previous step.
    b. Enter the Microsoft Entra ID domain name.
2. Select **Create connection**. The system creates the connection in a few seconds.

Test and enable the connection

1. Select **Next**.
2. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials. After you log in, go back to the Console to enable the connection.

    ⓘ When using the Console in restricted mode, copy the URL to either an incognito browser window or a separate browser to log in to your IdP.

3. In the Console, select **Next** to review the summary page.
4. Set up notifications.

    Choose between seven days or 30 days. The system emails expiry notifications and shows them in the Console to any user with the following roles: Super admin, Org admin, Federation admin, and Federation viewer.

5. Review the federation details and then select **Enable federation**.
6. Select **Finish** to complete the process.

After you enable the federation, users log in to the NetApp Console using their corporate credentials.

Federate NetApp Console with PingFederate

Federate with your PingFederate IdP provider to enable single sign-on (SSO) for the NetApp Console. This allows users to log in using their corporate credentials.

Required roles

The Federation admin role is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

ⓘ You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in the Console that uses the identity provider's configuration.

You can set up a federated connection with PingFederate to enable single sign-on (SSO) for the Console . The process involves configuring your PingFederate server to trust the Console as a service provider and then creating the connection in the Console .

Steps

1. Select **Administration > Identity and access**.
2. Select **Federation** to view the **Federations** page.
3. Select **Configure new federation**.
4. Enter your domain details:
    a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
    b. Enter the name of the federation you are configuring.
    c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Provider** and then select **PingFederate**.
7. Select **Next**.
8. Configure your PingFederate server to trust NetApp as a service provider. You need to do this step on your PingFederate server.
    a. Use the following values when configuring PingFederate to trust the NetApp Console:
        - For the **Reply URL** or **Assertion Consumer Service (ACS) URL**, use `https://netapp-cloud-account.auth0.com/login/callback`
        - For the **Logout URL**, use `https://netapp-cloud-account.auth0.com/logout`
        - For **Audience/Entity ID**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` where <fed-domain-name-pingfederate> is the domain name for the federation. For example, if your domain is `example.com`, the Audience/Entity ID would be `urn:auth0:netappcloud-account:fed-example-com-pingfederate`.
    b. Copy the PingFederate server URL. You will need this URL when creating the connection in the Console.
    c. Download the X.509 certificate from your PingFederate server. It needs to be in Base64-encoded PEM format (.pem, .crt, .cer).
9. Return to the Console, and select **Next** to create the connection.
10. Create the connection with PingFederate
    a. Enter the PingFederate server URL that you copied in the previous step.
    b. Upload the X.509 signing certificate. The certificate must be in PEM, CER, or CRT format.
11. Select **Create connection**. The system creates the connection in a few seconds.
12. Select **Next**.
13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials. After you log in, go back to the Console to enable the connection.

    ⓘ When using the Console in restricted mode, copy the URL to either an incognito browser window or a separate browser to log in to your IdP.

14. In the Console, select **Next** to review the summary page.
15. Set up notifications.

    Choose between seven days or 30 days. The system emails expiry notifications and shows them in the Console to any user with the following roles: Super admin, Org admin, Federation admin, and Federation viewer.

16. Review the federation details and then select **Enable federation**.
17. Select **Finish** to complete the process.

After you enable the federation, users log in to the NetApp Console using their corporate credentials.

Federate with a SAML identity provider

Federate with your SAML 2.0 IdP provider to enable single sign-on (SSO) for the NEtApp Console. This allows users to log in using their corporate credentials.

Required role

The Federation admin role is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

> ⓘ You can federate with your corporate IdP or with the NetApp Support Site. You can’t federate with both.

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in the Console that uses the identity provider’s configuration.

You can set up a federated connection with your SAML 2.0 provider to enable single sign-on (SSO) for the Console. The process involves configuring your provider to trust NetApp as a service provider and then creating the connection in the Console.

Steps

1. Select **Administration > Identity and access**.
2. Select **Federation** to view the **Federations** page.
3. Select **Configure new federation**.
4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
   b. Enter the name of the federation you are configuring.
   c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Protocol** and then select **SAML Identity Provider**.
7. Select **Next**.
8. Configure your SAML identity provider to trust NetApp as a service provider. You need to do this step on your SAML provider server.
   a. Ensure that your IdP has the attribute `email` set to the user’s email address. This is required for the Console to identify users correctly:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

a. Use the following values when registering your SAML application with the Console:

   - For the **Reply URL** or **Assertion Consumer Service (ACS) URL**, use `https://netapp-cloud-account.auth0.com/login/callback`
   - For the **Logout URL**, use `https://netapp-cloud-account.auth0.com/logout`
   - For **Audience/Entity ID**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` where <fed-domain-name-saml> is the domain name you want to use for federation. For example, if your domain is `example.com`, the Audience/Entity ID would be `urn:auth0:netapp-cloud-account:fed-example-com-samlp`.

b. After creating the trust, copy the following values from your SAML provider server:

   - Sign In URL
   - Sign Out URL (optional)

c. Download the X.509 certificate from your SAML provider server. It needs to be in PEM, CER, or CRT format.

   1. Return to the Console, and select **Next** to create the connection.
   2. Create the connection with SAML.

d. Enter the **Sign In URL** of your SAML server.

e. Upload the X.509 certificate that you downloaded from your SAML provider server.

f. Optionally, enter the **Sign Out URL** of your SAML server.

   1. Select **Create connection**. The system creates the connection in a few seconds.
   2. Select **Next**.
   3. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials. After you log in, go back to the Console to enable the connection.

   > ⓘ When using the Console in restricted mode, copy the URL to either an incognito browser window or a separate browser to log in to your IdP.

   1. In the Console, select **Next** to review the summary page.
   2. Set up notifications.

      Choose between seven days or 30 days. The system emails expiry notifications and shows them in the Console to any user with the following roles: Super admin, Org admin, Federation admin, and Federation viewer.

3. Review the federation details and then select **Enable federation**.
4. Select **Finish** to complete the process.

After you enable the federation, users log in to the NetApp Console using their corporate credentials.

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.