Security and compliance

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Security and compliance

Identity federation

Enable single sign-on by using identity federation with NetApp Console

Single-sign on (federation) simplifies the login process and enhances security by allowing users to log in to the NetApp Console using their corporate credentials. You can enable single sign-on (SSO) with your identity provider (IdP) or with the NetApp Support site.

Required role

Organization admin, Federation admin, Federation viewer. Learn more about access roles.

Identity federation with NetApp Support Site

Federating with the NetApp Support Site allows users to log in to the Console, Active IQ Digital Advisor, and other associated apps using the same credentials.

If you federate with the NetApp Support Site, you can't also federate with your corporate identity management provider. Choose which one works best for your organization.

Steps

1. Download and complete the NetApp Federation Request Form.
2. Submit the form to the email address specified in the form.

   The NetApp support team reviews and processes your request.

Set up a federated connection with your identity provider

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

If you previously configured federation using NetApp Cloud Central (an external application to the Console), you need to import your federation using the Federation page to manage it within the Console. Learn how to import your federation.

Supported identity providers

NetApp supports the following protocols and identity providers for federation:

Protocols

- Security Assertion Markup Language (SAML) identity providers
- Active Directory Federation Services (AD FS)

Identity providers

- Microsoft Entra ID
- PingFederate

Federation with NetApp Console workflow

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 federate with your email domain or with a different domain that you own. To federate with a domain different from your email domain, first verify you own the domain.

Verify your domain (if not using your email domain)

To federate with a domain different from your email domain, verify that you own it. You can federate your email domain without any extra steps.

Configure your IdP to trust NetApp as a service provider

Configure your identity provider to trust NetApp by creating a new application and providing details like the ACS URL, Entity ID or other credential information. Service provider information varies by identity provider, so refer to the documentation for your specific identity provider for details. You'll need to work with your IdP administrator to complete this step.

Create the federated connection in the Console

Provide the SAML metadata URL or file from your identity provider to create the connection. This information is used to establish the trust relationship between the Console and your identity provider. The information you provide depends on the IdP that you are using. For example, if you're using Microsoft Entra ID, you need to provide the client ID, secret, and domain.

Test your federation in the Console

Test your federated connection before enabling it. Use the test option on the Federation page in the Console to verify that your test user can authenticate successfully. If the test is successful, you can enable the connection.

Enable your connection in the Console

After you enable the connection, users can log in to the Console using their corporate credentials.

Review the topic for your respective protocol or IdP to get started:

- Set up a federated connection with AD FS
- Set up a federated connection with Microsoft Entra ID
- Set up a federated connection with PingFederate
- Set up a federated connection with a SAML identity provider

Domain verification

Verify the email domain for your federated connection

If you want to federate with a domain that is different than your email domain, you must first verify that you own the domain. You can only use verified domains for federation.

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.

Verifying your domain involves adding a TXT record to your domain's DNS settings. This record is used to prove that you own the domain and allows the NetApp Console to trust the domain for federation. You may need to coordinate with your IT or network administrator to complete this step.

Steps

1. Select **Administration > Identity and access**.
2. Select **Federation** to view the **Federations** page.
3. Select **Configure new federation**.
4. Select **Verify domain ownership**.
5. Enter the domain that you want to verify and select **Continue**.
6. Copy the TXT record that is provided.
7. Go to your domain's DNS settings and configure the TXT value that was provided as a TXT record for your domain. Work with your IT or network administrator if needed.
8. After the TXT record is added, return to the Console and select **Verify**.

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.

Manage federations

Manage federations in NetApp Console

You can manage your federation in the NetApp Console. You can disable it, update expired credentials, as well as disable it if you no longer need it.

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 also add an additional verified domain to an existing federation, which allows you to use multiple domains for your federated connection.

- If you configured federation using NetApp Cloud Central, import it via the **Federation** page to manage it in the Console. Learn how to import your federation
- You can view Federation management events such as enabling, disabling, and updating federations on the Audit page. Learn more about monitoring operations in the NetApp Console.

Enable a federation

If you have created a federation but it is not enabled, you can enable it through the **Federation** page. Enabling a federation allows users associated with the federation to log in to the Console using their corporate credentials. Create and test the federation successfully before enabling it.

Steps

1. Select **Administration > Identity and access**.
2. Select the **Federation** tab.
3. Select the actions menu ••• next to the federation that you want to enable and select **Enable**.

Add a verified domain to an existing federation

You can add a verified domain to an existing federation in the Console to use multiple domains with the same identity provider (IdP).

You must have already verified the domain in the Console before you can add it to a federation. If you haven't verified the domain yet, you can do so by following the steps in Verify your domain in the Console.

Steps

1. Select **Administration > Identity and access**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Update domains**. The **Update domains** dialog box displays the domain already associated with this federation.
4. Select a verified domain from the list of available domains.
5. Select **Update**. New domain users may gain federated Console access within 30 seconds.

Updating an expiring federated connection

You can update the details of a federation in the Console. For example, you'll need to update the federation if the credentials such as a certificate or client secret expire. When needed, update the notification date to remind you to update the connection before it expires.

ⓘ Update the Console first before updating your IdP to avoid login issues. Stay logged into the Console during the process.

Steps

1. Select **Administration > Identity and access**.
2. Select the **Federation** tab.
3. Select the actions menu (three vertical dots) next to the federation that you want to update and select **Update federation**.
4. Update the details of the federation as needed.
5. Select **Update**.

Test an existing federation

Test the connection of an existing federation to verify that it works. This can help you identify any issues with the federation and troubleshoot them.

Steps

1. Select **Administration > Identity and access**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Test connection**.
4. Select **Test**. The system prompts you to log in with your corporate credentials. If the connection is successful, you are redirected to the NetApp Console. If the connection fails, you see an error message indicating the issue with the federation.
5. Select **Done** to return to the **Federation** tab.

Disable a federation

If you no longer need a federation, you can disable it. This prevents users associated with the federation from logging in to the Console using their corporate credentials. You can re-enable the federation later if needed.

Disable a federation before deleting it, such as when decommissioning the IdP or discontinuing federation. This allows you to re-enable it later if needed.

Steps

1. Select **Administration > Identity and access**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Disable**.

Delete a federation

If you no longer need a federation, you can delete it. This removes the federation and prevents any users associated with the federation from logging in to the Console using their corporate credentials. For example, if the IdP is being decommissioned or if the federation is no longer needed.

You cannot recover a federation after you delete it. You must create a new federation.

ⓘ You must disable a federation before you can delete it. You cannot undelete a federation after you delete it.

Steps

1. Select **Administration > Identity and access** .
2. Select **Federations** to view the **Federations** page.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Delete**.

Import your federation to NetApp Console

If you have previously set up federation through NetApp Cloud Central (an external application to the NetApp Console) the Federation page prompts you to import your existing federated connection to the Console so you can manage it in the new interface. You can then take advantage of the latest enhancements without having to recreate your federated connection.

ⓘ After you import your existing federation, you can manage the federation from the **Federations** page. Learn more about managing federations.

Required role

Organization admin or Federation admin. Learn more about access roles.

Steps

1. Select **Administration > Identity and access**.
2. Select the **Federation** tab.
3. Select **Import Federation**.

Enforce ONTAP permissions for ONTAP Advanced View (ONTAP System Manager)

By default, the Console agent credentials allow users to access the Advanced View (ONTAP System Manager). You can prompt users for their ONTAP credentials instead. This ensures that a user's ONTAP permissions are applied when they work with ONTAP clusters in both Cloud Volumes ONTAP and ONTAP on-premises clusters.

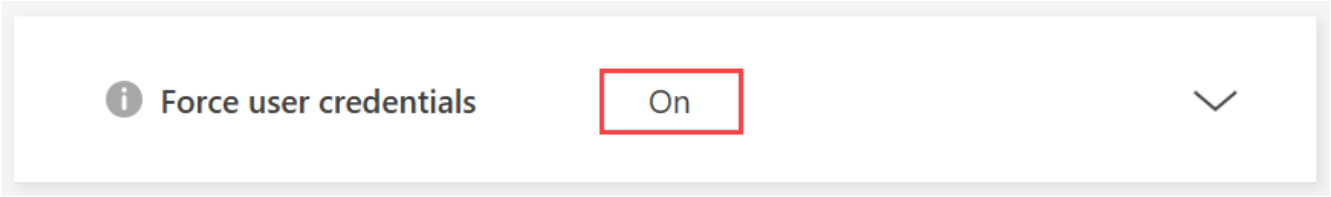
You must have the Organization admin role to edit Console agent settings.

Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select the action menu for a Console agent and select **Edit agent**.

   The Console agent must be active to edit it.

3. Expand the **Force Credentials** option.
4. Select the checkbox to enable the **Force Credentials** option and then select **Save**.
5. Verify that the **Force Credentials** option is enabled.



Enable read-only mode for a NetApp Console organization

As a security precaution, you can enable read-only mode for your NetApp Console organization. In read-only mode, users can view resources and settings but cannot make any changes.

In read-only mode, users with admin roles must manually elevate their permissions to make changes, which ensures that changes are intentional.

Required access roles

Super admin or Org admin.

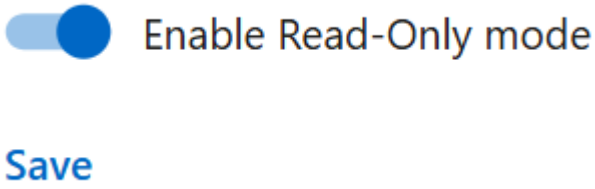
Enable read-only mode for your Console organization

Enable read-only mode to restrict changes to your Console organization. All users can still view resources. Users with admin roles cannot perform any actions in the Console without manually elevating their permissions.

When read-only mode is enabled, users see a banner that notifies them that the organization is in read-only mode. Users must go to User settings to elevate their role.

Steps

1. Select **Administration > Identity and access**.
2. From the **Organizations** tab, select **Edit organization settings** for the organization that you want to set to read-only mode.
3. In the **Read-only mode** section, enable read-only mode by moving the toggle to the **On** position and then select **Save**.



Sign up for NetApp Console as the initial organization administrator

If your company doesn't have a NetApp Console organization, sign up to create one. The first user is the administrator and manages accounts and permissions. You can update roles and add administrators later.

Steps

1. Open a web browser and go to the NetApp Console
2. If you have a NetApp Support Site account, enter the email address associated with your account directly on the **Log in** page.

   The Console signs you up as part of this initial login with your NetApp Support Site credentials.

3. If you want to sign up by creating a Console login, select **Sign up**.
   a. On the **Sign up** page, enter the required information and select **Next**.

      Only English characters are allowed in the sign up form.

   b. Check your inbox for an email from NetApp that includes instructions to verify your email address.

      Verify your email address to complete sign up.

4. After you log in, review and accept the End User License Agreement.
5. On the **Welcome** page, create an organization.
6. Select **Let's Start**.

+ As a first-time administrator, follow the guided process to add storage, create a Console agent, and more. Learn about using the Console Assistant.

Next steps

As an administrator, after you complete the steps included in the Console Assistant, you should plan your identity and access strategy, add users to your organization, and assign roles. Learn about identity and access management for NetApp Console

Sign up or login to NetApp Console when an organization already exists

If your company already has a NetApp Console organization, sign up or log in to access it. Your sign-up or log-in method depends on whether your company uses identity federation or has NetApp Support Site credentials. If not, create a NetApp Console log-in.

Steps

1. Open a web browser and go to the NetApp Console
2. If you have a NetApp Support Site account or if your company has set up single sign-on (SSO), enter your associated email address or SSO credentials on the **Log in** page. Follow the prompts to complete login.

   In both of these cases, you are signed up for the Console as part of this initial login.

3. If you want to sign up by creating a Console login, select **Sign up**.
   a. On the **Sign up** page, enter the required information and select **Next**.

      Only English characters are allowed in the sign up form.

   b. Check your inbox for an email from NetApp that includes instructions to verify your email address.

      Verify your email address to complete sign up.

4. After you log in, review and accept the End User License Agreement.
5. If the system prompts you to create an organization, close the dialog box and tell a Console admin so they can add you to your Console organization and give you access. Learn how to contact an organization administrator.

Next steps

After you are given access to your organization, you can start managing storage and using the data services that you are assigned.

Copyright information

Trademark information