Add users to your Console organization

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Add users to your Console organization

Add users to a NetApp Console organization

Within the Console, you grant users access to projects or folders to according to an access role. A *access role* contains a set of permissions that enables a member (user or service account) to perform specific actions at the assigned level of the resource hierarchy.

Required access roles

Super admin, Org admin, or Folder or project admin (for folders and projects that they are administering). Learn about access roles.

Understand how access is granted in NetApp Console

NetApp Console uses role-based access control (RBAC) to manage permissions. Assign roles to users individually or through federated groups. Each role defines allowed actions for specific resources.

Note the following about granting access in NetApp Console:

- All users must first sign up for the NetApp Console before they can be granted access to resources
- You must explicitly assign a role to each user in the Console before they can access resources, even if they are members of a federated group that has been assigned a role.
- You can add service accounts directly from the Console and assign them roles.

Add members to your organization

NetApp Console supports three types of members: user accounts, service accounts, and federated groups.

Users must sign up for NetApp Console before you can add them and assign a role, even if they are in a federated group. Create service accounts directly in the Console.

All members must have at least one role explicitly assigned to them in order to access resources.

When adding a member, choose the resource level (organization, folder, or project) and assign a role or roles with the needed permissions.

Add a user

Users sign up for the NetApp Console, but an Org admin or Folder or project admin must add them to an organization, folder, or project so they can access resources.

Before you begin:

The user must have already signed up for the NetApp Console. If they haven't signed up yet, direct them to sign up for the NetApp Console.

> ⓘ If you are adding a user that is part of a federated group, ensure that the user has already signed up for the NetApp Console and been explicitly assigned a role in the Console. NetApp recommends assigning minimum access role such as Organization viewer.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, keep **User** selected.
5. For **User's email**, enter the user's email address that is associated with the login that they created.
6. Use the **Select an organization, folder, or project** section to choose the level of your resource hierarchy that the member should have permissions for.

   Note the following:

   - You can select only the folders and projects for which you have permissions.
   - When you select an organization or folder, you grant the member permissions to all its contents.
   - You can only assign the **Organization admin** role at the organization level.
7. **Select a category** then select a **Role** that provides the member with permissions for the resources that are associated with the organization, folder, or project that you selected.

   Learn about access roles.
8. To give access to more folders, projects, or roles, select **Add role**, choose the folder, project, or role category, and select a role.
9. Select **Add**.

   The Console emails instructions to the user.

Add a service account

Service accounts allow you to automate tasks and securely connect with Console APIs. Choose a client ID and secret for simple setups, or JWT (JSON Web Token) for stronger security in automated or cloud-native environments. Select the method that meets your security requirements.

Before you begin:
For JWT authentication, prepare your public key or certificate.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, select **Service account**.
5. Enter a name for the service account.
6. To use JWT authentication, select **Use private key JWT authentication** and upload your public RSA key or certificate. Skip if using client ID and secret.

   Your X.509 certificate. It must be in PEM, CRT, or CER format.

   a. Set up expiry notifications for your certificate. Choose between seven days or 30 days. Expiry notifications are emailed and shown in the Console to users with the Super admin or Org admin role.

7. Use the **Select an organization, folder, or project** section to choose the level of your resource hierarchy that the member should have permissions for.

   Note the following:

   - You can only select from the folders and projects for which you have permissions.
   - Selecting an organization or folder grants the member permissions to all its contents.
   - You can only assign the **Organization admin** role at the organization level.
8. Select a **Category** then select a **Role** that gives the member permissions for the resources in the organization, folder, or project you selected.

   Learn about access roles.

9. To give access to more folders, projects, or roles, select **Add role**, choose the folder, project, or role category, and select a role.
10. If you didn’t choose to use JWT authentication, download or copy the client ID and client secret.

    The Console shows the client secret only once. Copy it securely; you can recreate it later if you lose it.

11. If you chose JWT authentication, download or copy the client ID and JWT audience. The Console displays this information only once and does not allow you to retrieve it later.
12. Select **Close**.

Add a federated group to your organization

You can add a federated group from your identity provider (IdP) to your organization and assign it a role or roles. Members of the federated group inherit the roles that you assign to the group in the Console.

Before you can assign a role to a federated group, ensure the following:

- Set up federation between your IdP and the Console. Learn how to set up federation.
- The group must already exist in your IdP and been assigned app access to the Console.
- Users belonging to the group must have already signed up for the NetApp Console and been explicitly assigned a role in the Console. NetApp recommends assigning minimum access role such as Organization viewer.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, select **Federated Group**.
5. Select the federation of which the group is a member
6. For **Group name**, enter the exact name of the group in your IdP.
7. Use the **Select an organization, folder, or project** section to choose the level of your resource hierarchy that the member should have permissions for.

   Note the following:

    - You can only select from the folders and projects for which you have permissions.
    - Selecting an organization or folder grants the member permissions to all its contents.
    - You can only assign the **Organization admin** role at the organization level.

8. Select a **Category** then select a **Role** that gives the member permissions for the resources in the organization, folder, or project you selected.

   Learn about access roles.

9. To give access to more folders, projects, or roles, select **Add role**, choose the folder, project, or role category, and select a role.

Related information

- Learn about identity and access management in NetApp Console
- Get started with identity and access
- NetApp Console access roles
- Learn about the API for identity and access

Copyright information

Trademark information