Manage user access and security

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Manage user access and security

Learn about NetApp Console role-based access control (RBAC)

Manage user access to NetApp Console with role-based access control (RBAC), assigning predefined roles at the organization, folder, or project level. Each role grants specific permissions that define what actions users can perform within their assigned scope.

NetApp designs Console roles with least-privilege, so each role includes only the permissions needed for its tasks. This approach enhances security by limiting access to what each member requires.

After you organize resources into folders and projects, assign organization members a role or roles for specific folders or projects, that allow them to perform only the ir responsibilities.

For example, you can assign a member the Ransomware Resilience admin role for a specific project level, allowing them to perform Ransomware Resilience operations for resources within that project, without granting them broader access to the entire organization. This same user can be granted the role for several projects within your organization.

You can assign users multiple roles for the same scope or different scopes, depending on their responsibilities. For example, a smaller organization might have the same user manage both Ransomware Resilience and Backup and Recovery tasks at the organization level, while a larger organization might have different users assigned to each role at the project level.

Types of Console organization members

There are three types of members in a NetApp Console organization:
* *User accounts*: Individual users who log in to the NetApp Console to manage resources. Users must sign up for the NetApp Console before they can be added to an organization.
* *Service accounts*: Non-human accounts used by applications or services to interact with the NetApp Console via APIs. You can add service accounts directly to your Console organization.
* *Federated groups*: Groups synchronized from your identity provider (IdP) that allow you to manage access for multiple users collectively. Each user within a federated group must have signed up for the NetApp Console and been added to your organization with an access role before they can access resources granted to the group.

Learn how to add members to your organization.

Predefined roles in NetApp Console

NetApp Console includes predefined roles that you can assign to organization members. Each role includes permissions that specify what actions a member can do within their assigned scope (organization, folder, or project).

NetApp Console roles use least-privilege principles that ensure members have only the permissions needed for their tasks, and categorizes roles by the type of access they provide:

- Platform roles: Provide Console administration permissions
- Data services roles: Provide permissions for managing specific data services, such as Ransomware

Resilience and Backup and Recovery

- Application roles: Provide permissions for managing storage as well as audit Console events and alerts

You can assign multiple roles to a member based on their responsibilities. For example, you might assign a member both the Ransomware Resilience admin role and the Backup and Recovery admin role for a specific project.

Learn about the predefined roles available in NetApp Console.

Manage member access in NetApp Console

Manage member access in your Console organization. Assign roles to set permissions. Remove members when they leave.

Required access roles

Super admin, Org admin, or Folder or project admin (for folders and projects that they are administering). Link:reference-iam-predefined-roles.html[Learn about access roles].

You can assign access roles on a project or folder basis. For example, assign a role to a user for two specific projects or assign the role at the folder level to give a user the Ransomware Resilience admin role for all projects in a folder

Add your folders and projects before assigning users access. Learn how to add folders and projects.

Understand how access is granted in NetApp Console

NetApp Console uses a role-based access control (RBAC) model to manage user permissions. You can assign predefined roles to members individually or through federated groups. You can add and assign roles to service accounts, as well as federated groups. Each role defines what actions a member can perform at the associated 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.

Using role inheritance

When you assign a role at the organization, folder, or project level in NetApp Console, that role is automatically inherited by all resources within the selected scope. For example, folder-level roles apply to all contained projects, while project-level roles apply to all resources within that project.

View organization members

To understand which resources and permissions are available to a member, you can view the roles assigned to the member at different levels of your organization's resource hierarchy. Learn how to use roles to control access to Console resources.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.

   The **Members** table lists the members of your organization.

3. From the **Members** page, navigate to a member in the table, select ••• and then select **View details**.

View roles(s) assigned to a member

You can verify which roles they are currently assigned.

If you have the *Folder or project admin* role, the page displays all members in the organization. However, you can only view and manage member permissions for the folders and projects for which you have permissions. Learn more about the actions that a *Folder or project admin* can complete.

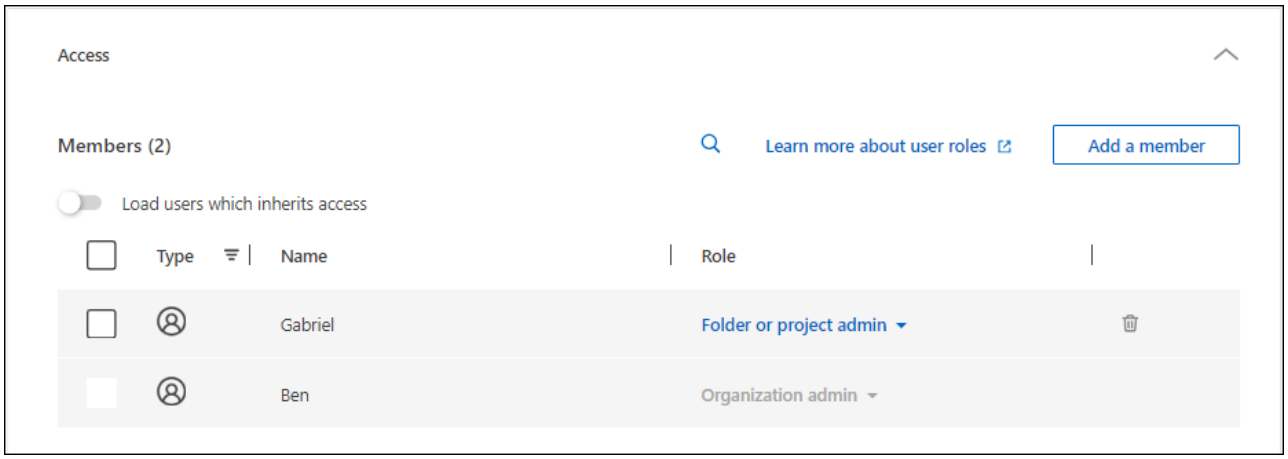
1. From the **Members** page, navigate to a member in the table, select ••• and then select **View details**.
2. In the table, expand the respective row for organization, folder, or project where you want to view the member's assigned role and select **View** in the **Role** column.

View members associated with a folder or project

You can view members who have access to a specific folder or project.

Steps

1. Select **Administration > Identity and access**.
2. Select **Organization**.
3. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Edit folder** or **Edit project**.
   - Select **Access** to view the members who have access to the folder or project.



Assign or modify member access

After a user signs up for NetApp Console, you can add them to your organization and assign them a role to provide access to resources. Learn how to add members to your organization.

You can adjust a member's access by adding or removing roles as needed.

Add an access role to a member

You typically assign a role when adding a member to your organization, but you can update it at any time by removing or adding roles.

You can assign a user an access role for your organization, folder, or project.

Members can have multiple roles within the same project and in different projects. For example, smaller organizations may assign all available access roles to the same user, while larger organizations may have users do more specialized tasks. Alternatively, you could also assign one user the Ransomware Resilience admin role at the organization level. In that example, the user would be able to perform Ransomware Resilience tasks on all projects within your organization.

Your access role strategy should align with the way you have organized your NetApp resources.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select one of the member tabs: **Users**, **Service accounts**, or **Federated groups**.
4. Select the actions menu ••• next to the member that you want to assign a role and select **Add a role**.
5. To add a role, complete the steps in the dialog box:
   - **Select an organization, folder, or project**: Choose the level of your resource hierarchy that the member should have permissions for.

     If you select the organization or a folder, the member will have permissions to everything that resides within the organization or folder.
   - **Select a category**: Choose a role category. Learn about access roles.
   - Select a **Role**: Choose a role that provides the member with permissions for the resources that are associated with the organization, folder, or project that you selected.
   - **Add role**: If you want to provide access to additional folders or projects within your organization, select **Add role**, specify another folder or project or role category, and then select a role category and a corresponding role.
6. Select **Add new roles**.

Change a member's assigned role

Change a member's roles to update their access.

Users must have at least one role assigned to them. You can't remove all roles from a user. If you need to remove all roles, you must delete the user from your organization.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select one of the member tabs: **Users**, **Service accounts**, or **Federated groups**.
4. From the **Members** page, navigate to a member in the table, select ••• and then select **View details**.
5. In the table, expand the respective row for organization, folder, or project where you want to change the

member's assigned role and select **View** in the **Role** column to view the roles assigned to this member.

6. You can change an existing role for a member or remove a role.
   a. To change a member's role, select **Change** next to the role you want to change. You can only change a role to a role within the same role category. For example, you can change from one data service role to another. Confirm the change.
   b. To unassign a member's role, select next to the role to remove the respective role from the member.. You'll be asked to confirm the removal.

Remove a member from your organization

Remove a member if they leave your organization.

When you remove a member, the system revokes their Console permissions but retains their Console and NetApp Support Site accounts.

Federated members

- Federated users automatically lose access to the NetApp Console when they are removed from your IdP. But you should still remove them from your Console organization to keep your member list up to date.
- If you remove a user from a federated group in your IdP, they lose the Console access associated with that group. However, they still retain any access associated with an explicit role assigned to them in the Console.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select one of the member tabs: **Users**, **Service accounts**, or **Federated groups**.
4. From the **Members** page, navigate to a member in the table, select then select **Delete user**.
5. Confirm that you want to remove the member from your organization.

User security

Secure user access to your NetApp Console organization by managing member security settings. You can reset user passwords, manage multi-factor authentication (MFA), and recreate service account credentials.

Required access roles

Super admin, Org admin, or Folder or project admin (for folders and projects that they are administering). Link:reference-iam-predefined-roles.html[Learn about access roles].

Reset user passwords (local users only)

Org admins cannot reset user passwords for local users. However, they can instruct users to reset their own passwords.

Instruct a user to reset their password from the Console login page by selecting **Forgot password?**.

This option is not available for users in a federated organization.

Manage a user's multi-factor authentication (MFA)

If a user loses access to their MFA device, you can either remove or disable their MFA configuration.

Multi-factor authentication is only available for local users. Federated users cannot enable MFA.

Users must set up MFA again when they log in after removal. If the user temporarily loses access to their MFA device, they can use their saved recovery code to log in.

If they do not have their recovery code, temporarily disable MFA to allow login. When you disable MFA for a user, it is disabled for only eight hours and then re-enabled automatically. The user is allowed one login during that time without MFA. After the eight hours, the user must use MFA to log in.

To manage a user's multi-factor authentication, you must have an email address in the same domain as the affected user.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.

   The **Members** table lists the members of your organization.
3. From the **Members** page, navigate to a member in the table, select ••• and then select **Manage multi-factor authentication**.
4. Choose whether to remove or to disable the user's MFA configuration.

Recreate the credentials for a service account

You can create new credentials for a service if you lose or need to update them.

Creating new credentials deletes the old ones. You cannot use the old credentials.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. In the **Members** table, navigate to a service account, select ••• and then select **Recreate secrets**.
4. Select **Recreate**.
5. Download or copy the client ID and client secret.

   The Console shows the client secret only once. Make sure you copy or download it and store it securely.

Copyright information

Trademark information