Manage users and access

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

Manage users and access

Manage member access in NetApp Console local deployment

In NetApp Console local deployment, review or change a user's roles across multiple folders or fleets, such as checking everything a storage engineer can access, adding a new role in another region, or removing that user's access when responsibilities change.

Required access roles

Super admin, Organization admin, or Folder or fleet admin (for folders and fleets that they are administering). Learn about access roles.

You can view and manage access in two ways depending on your needs. If you want to view the roles that a particular user has across all the fleet in your organization, use the **Members** page.

If you want to confirm who can access a specific fleet, review the members assigned to that fleet instead. Manage fleet access assignments.

To add a new member, service account, or directory user and assign their first role, use the onboarding task instead. Add members and assign roles.

Understand how access is granted in NetApp Console

NetApp Console uses role-based access control (RBAC) to manage member permissions. You can assign predefined roles at the organization, folder, or fleet level, depending on the scope of access that a member needs.

Using role inheritance

A role that you assign at the organization or folder level is inherited by the child scopes beneath it, so change an inherited assignment at the higher scope where you originally granted it.

Learn about role inheritance in NetApp Console local deployment.

View roles assigned to a member

Confirm exactly which roles a member holds and at which scope before you make a change. For example, check whether a teammate already has the Storage admin role on the `Production-EU-West` fleet.

If you have the *Folder or fleet admin* role, the page displays all members in the organization. However, you can view and manage permissions only for the folders and fleets that you administer. Learn about Folder or fleet admin actions in NetApp Console local deployment.

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 fleet where you want to view the member's assigned role and select **View** in the **Role** column.

Assign or modify member access

You can adjust a member's access whenever responsibilities change. For example, when a teammate takes on backup duties for a second region, add the Backup and Recovery admin role on that region's fleet without touching their existing storage roles.

If you need to add a new member and assign their first role, see Add members and assign roles.

Add an access role to an existing member

Grant a member an additional role at the organization, folder, or fleet level when their responsibilities expand. For example, give a Storage admin the Backup and recovery admin role at the organization level so they can manage backup and recovery tasks across every fleet without losing their existing storage permissions.

You can assign a member an access role for your organization, folder, or fleet.

Members can have multiple roles within the same fleet and in different fleets. 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 fleets 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**, **Directory users**, or **Service accounts**.
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 fleet**: 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 fleet that you selected.
   - **Add role**: If you want to provide access to additional folders or fleets within your organization, select **Add role**, specify another folder or fleet or role category, and then select a role category and a corresponding role.
6. Select **Add new roles**.

Change a member's assigned role

Replace a member's existing role with a different one when their responsibilities shift. For example, when a Storage viewer on the `Production-US-East` fleet needs the Storage admin role instead.

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

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select one of the member tabs: **Users**, **Directory users**, or **Service accounts**.
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 fleet 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 unassign the member the respective role. You'll be asked to confirm the removal.

Remove a member from your organization

Remove a member when they leave the organization or change roles in a way that ends their need for Console access. For example, when a contractor's engagement ends or an employee transfers to a team outside your Console organization.

Directory users

Removing a user from your directory prevents that user from authenticating. You should also remove the user from your Console organization to keep the member list accurate and to remove any roles that were assigned in Console local deployment.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select one of the member tabs: **Users**, **Directory users**, or **Service accounts**.
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.

View or change fleet access assignments in NetApp Console local deployment

Audit or change member access assignments for folders and storage fleets in NetApp Console local deployment. Folder and fleet admins typically work from this view because it shows only the scopes that they administer.

Required access roles

Super admin, Organization admin, or Folder or fleet admin. Learn about access roles.

Alternatively, you can manage all roles for a particular member across multiple folders or fleets. Manage member access.

How folder and fleet access works

Console local deployment uses role-based access control (RBAC). A role that you assign at the folder level applies to all fleets and subfolders within that folder; a role that you assign at the fleet level applies only to that fleet's resources. Learn about role inheritance in NetApp Console local deployment.

> ⓘ You can't change a role at the fleet level if a member inherits it from a folder or from the organization. To change inherited access, change the role at the higher scope.

View members assigned to a folder or fleet

Review exactly who can manage specific folder or fleet. For example, before associating a new production ONTAP cluster with the `Production-US-East` fleet, open the fleet's Access tab to confirm who has access.

Steps

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

Modify member access from a folder or fleet

Adjust the roles of members who already belong to your organization, scoped to a single folder or fleet. For example, when a teammate moves from a development fleet to a production fleet, promote them from Storage viewer to Storage admin on the production fleet without affecting their access elsewhere.

To add a new member and assign their first role, use the onboarding task instead. Add members and assign roles.

Steps

1. From the Organization page, navigate to a folder or fleet in the table, select ••• and then select **Edit folder** or **Edit fleet**.
2. Select **Access** to view the list of members who have access.
3. Modify member access:
   - **Change a member's role**: For any member with a role other than Organization admin, select their existing role and choose a new role. The change applies only at this scope; roles inherited from a higher scope don't appear here.
   - **Remove member access at this scope**: For a member who has a role defined directly at this folder or fleet, remove the role to revoke their access at this scope. This doesn't remove the member from your organization or affect roles they have at other scopes.

     Remove a member from your organization.
4. Select **Apply**.

Manage member security in NetApp Console local deployment

Secure user access to your NetApp Console local deployment organization by managing member security settings. You can direct local users to change their own passwords, manage local users' multi-factor authentication (MFA), and recreate service account credentials.

Required access roles

Super admin, Organization admin, or Folder or fleet admin. Learn about access roles.

Reset user passwords (local users only)

Administrators cannot reset local user passwords directly.

Direct local users to reset their passwords from the Console local deployment login page by selecting **Forgot password?**.

This option is not available for directory users.

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

If a local 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. Directory users cannot enable MFA through Console local deployment.

Use these guidelines to choose the right action:

- Select **Disable** when the user temporarily loses access to their MFA device. Disabling MFA allows one sign-in without MFA for eight hours and then automatically re-enables MFA.
- Select **Remove** when the user must fully reset MFA. After you remove MFA, the user signs in without MFA until they configure MFA again.

If a user has a saved recovery code, they can sign in with it. If a user does not have a recovery code, disable MFA so the user can sign in and regain access.

To manage a local 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**.
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.

After you finish

Review the audit log to confirm who changed MFA access, when they changed it, and whether the action succeeded. Learn how to audit NetApp Console local deployment activity.

Recreate the credentials for a service account

You can create new credentials for a service account 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 local deployment shows the client secret only once. Make sure you copy or download it and store it securely.

Copyright information

Trademark information