Identity and access management

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Identity and access management

Learn about NetApp Console identity and access management

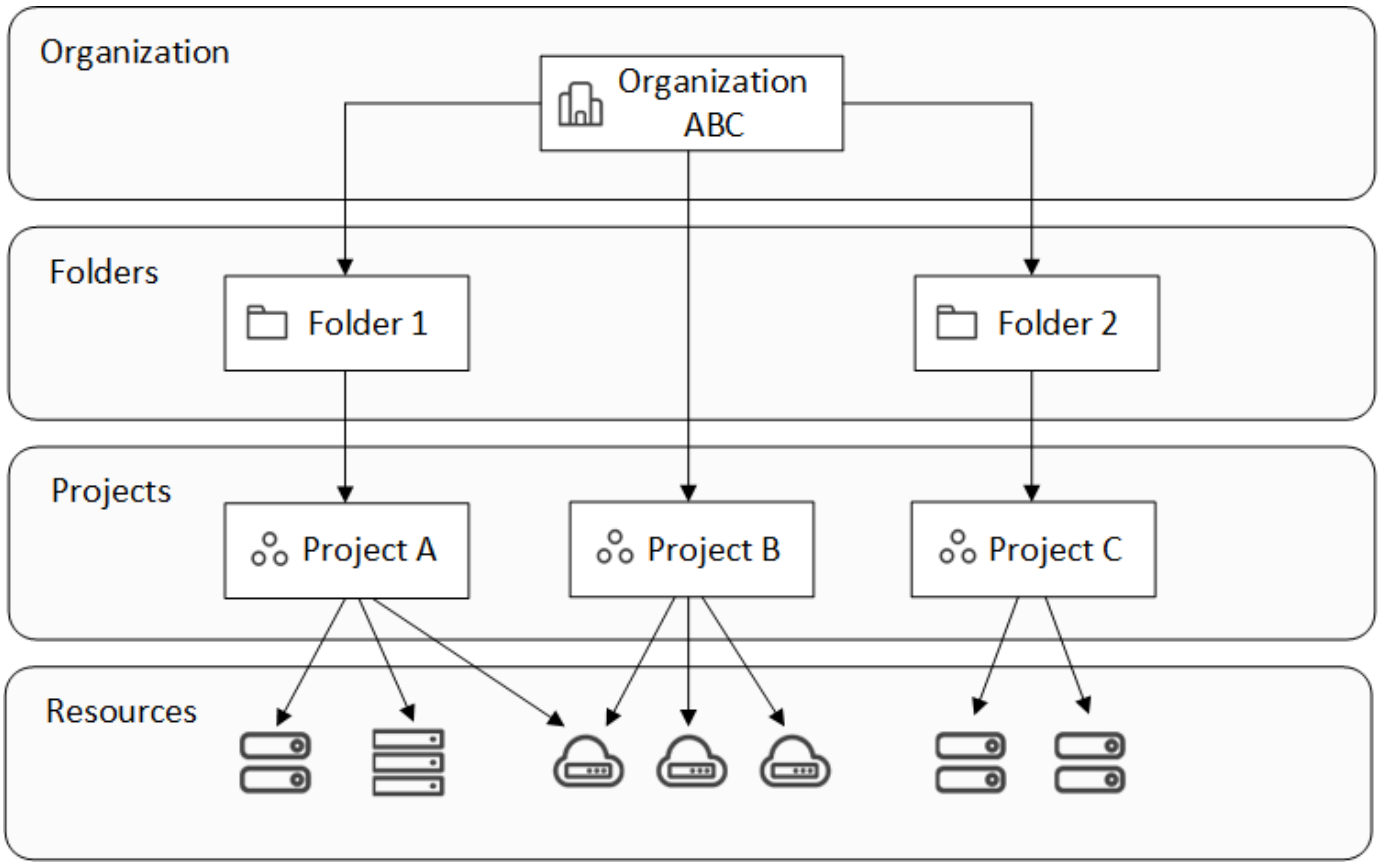
Use NetApp Console's Identity and Access Management (IAM) to organize your NetApp resources and control access according to your business structure—by location, department, or project.

Resources are arranged hierarchically: the organization is at the top, followed by folders (which can contain other folders or projects), and then projects, which contain storage systems, workloads, and agents.

Assign role-based access control (RBAC) permissions to members at the organization, folder, or project level to ensure users have the appropriate access to resources.

You must have the *Super admin*, *Organization admin* , or *Folder or project admin* roles to manage IAM in NetApp Console.

The following image illustrates this hierarchy at a basic level.



]

Identity and access management components

Within NetApp Console, you organize your storage resources using three main components: organizational components, resource components, and user access components.

Projects and folders within your organization

Within your IAM structure, you work with three organizational components are organizations, projects, and folders. You can grant users access by assigning them roles at any of these levels.

Organization

An *organization* is the top level of the Console IAM system and typically represents your company. Your organization consists of folders, projects, members, roles, and resources. Agents are associated with specific projects in the organization.

Projects

A *project* is used to provide access to a storage resource. You must assign a resources to project before anyone can access them. You can assign multiple resources to a single project and you can also have multiple projects. You then assign users permissions to the project to give them access to the resources within it.

For example, you can associate an on-premises ONTAP system with a single project or with all projects in your organization, depending on your needs.

Learn how to add projects to your organization.

Folders

Group related projects in *folders* to organize them by location, site, or business unit. You can't associate resources directly with folders, but assigning a user a role at the folder level gives them access to all projects in that folder.

Learn how to add folders to your organization.

Resources

Resources include storage systems, Keystone subscriptions, as well as Console agents.

+
You must associate a resource with a project before anyone can access it.

+

For example, you might associate a Cloud Volumes ONTAP system with one project or with all projects in your organization. How you associate a resource depends on your organization's needs.

+

Learn how to associate resources to projects.

Storage systems and Keystone subscriptions

Storage systems are the primary resources that you manage in NetApp Console. NetApp Console supports management of both on-premises and cloud storage systems. You must add a storage system to a project before anyone can access it.

Storage systems are automatically associated with the project where they are added, but you can also associate them with other projects or folders from the **Resources** page.

Keystone subscriptions are also resources that you can associate with projects in order to grant users access to the subscription in NetApp Console.

Console agents

Organization admins create Console agents to manage storage systems and enable NetApp data services. Agents are initially tied to the project where they are created, but admins can add them to other projects or folders from the Agents page.

Associating an agent with a project enables management of resources in that project, while associating an agent with a folder lets folder or project admins decide which projects should use the agent. Agents must be linked to specific projects to provide management capabilities.

Learn how to associate agents with projects.

Members and roles

Members

Members of your organization are user accounts or service accounts. A service account is typically used by an application to complete specified tasks without human intervention.

You need to add members to your organization after they sign up for NetApp Console. Once added, you can assign them roles to provide access to resources. You can manually add service accounts from within the Console or automate their creation and management through the NetApp Console IAM API.

Learn how to add members to your organization.

Access roles

The Console provides access roles that you can assign to the members of your organization.

When you associate a member with a role, you can grant that role for the entire organization, a specific folder, or a specific project. The role that you select gives a member permissions to the resources in the selected part of the hierarchy.

NetApp Console provides granular roles that adhere to the principles of "least privilege" which means access roles are designed to give users access to only that that they need

This means users may have multiple roles assigned to them as their duties expand.

Learn about access roles.

IAM strategy examples

Small organization strategy

For organizations with fewer than 50 users and centralized storage management, consider a simplified approach using Super admin and Super viewer roles.

Example: ABC Corporation (5-person team)

- **Structure:** Single organization with 3 projects (Production, Development, Backup)
- **Roles:**
  - 2 senior members: **Super admin** role for full administrative access
  - 3 team members: **Super viewer** role for monitoring without modification rights
- **Agent strategy:** Single agent associated with all projects for shared resource access

- **Benefits:** Simplified administration, reduced role complexity, suitable for teams requiring broad access

Multi-regional enterprise strategy

For large organizations with regional operations and specialized teams, implement a hierarchical approach with folders representing geographical or business unit boundaries.

Example: XYZ Corporation (multinational company)

- **Structure:** Organization > Regional folders (North America, Europe, Asia-Pacific) > Project folders per region
- **Platform roles:**
  - 1 **Organization admin**: Global oversight and policy management
  - 3 **Folder or project admins**: Regional control (one per region)
  - 1 **Federation admin**: Corporate identity provider integration
- **Storage roles by region:**
  - 9 **Storage admin**: Discover and manage storage systems in assigned regions
  - 2 **Storage viewer**: Monitor storage resources across regions
  - 1 **System health specialist**: Manage storage health without system modifications
- **Data service roles:**
  - **Backup and Recovery admin**: Per-project based on backup responsibilities
  - **Ransomware Resilience admin**: Security team monitoring across projects
- **Agent strategy:** Regional agents associated with appropriate geographical projects
- **Benefits:** Enhanced security through role segregation, regional autonomy, and compliance with local regulations

Departmental specialization strategy

For organizations with specialized teams requiring specific data service access, use targeted role assignments based on functional responsibilities.

Example: TechCorp (mid-size technology company)

- **Structure:** Organization > Department folders (IT, Security, Development) > Project-specific resources
- **Specialized roles:**
  - Security team: **Ransomware Resilience admin** and **Classification viewer** roles
  - Backup team: **Backup and Recovery super admin** for comprehensive backup operations
  - Development team: **Storage admin** for test environment management
  - Compliance team: **Operation support analyst** for monitoring and support case management
- **Agent strategy:** Agents linked to departmental projects based on resource ownership
- **Benefits:** Tailored access control, improved operational efficiency, and clear accountability for specialized tasks

Next steps with IAM in NetApp Console

- Get started with IAM in NetApp Console
- Monitor or audit IAM activity
- Learn about the API for NetApp Console IAM

Get started with identity and access in NetApp Console

When you sign up for the NetApp Console, you're prompted to create a new organization. The organization includes one member (an Organization admin) and one default project. To set up identity and access management (IAM) to meet your business needs, you'll need to customize your organization's hierarchy, add additional members, add or discover resources, and associate those resources across your hierarchy.

You need the **Org admin** or **Super admin** permissions to manage identity and access for your organization. With **Folder or project admin** permissions, you can manage only the folders and projects you have access to.

Follow these steps to set up a new organization. The order may vary based on your organization's needs.

Edit the default project or add to your organization's hierarchy

Use the default project or create additional projects and folders matching your business hierarchy.

Learn how to organize your resources with folders and projects.

Associate members with your organization

After users sign up for NetApp Console, you must explicitly add them to your Console organization. You also have the option to add service accounts to your organization.

Learn how to manage members and their permissions.

Add or discover resources

Add or discover resources (systems) to the Console. Organization members manage systems from within a project.

Learn how to create or discover resources:

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- E-Series systems
- On-premises ONTAP clusters
- StorageGRID

4 Associate resources with additional projects

Adding or discovering a system in the Console automatically associates the resource with the currently selected project. To make that resource available to another project in your organization, associate it with the respective project. If a Console agent is used to manage the resource, associate the Console agent with the respective project.

- Learn how to manage your organization's resource hierarchy.
- Learn how to associate a Console agent with a folder or project.

Related information

- Learn about identity and access management in NetApp Console
- Learn about the API for identity and access

Set up your Console organization

Add folders and projects to your NetApp Console organization

Add folders and projects to match your business structure. After you create folders and projects, you can associate resources with them and manage member access to those projects.

The Console automatically creates one project for you when you create a new organization. Most organizations have the need for more than one project, as well as folders to keep things organized. Learn about the resource hierarchy in NetApp Console.

Using folders and projects to organize resources

In NetApp Console, an organization contains folders and projects that help you organize your resources. Folders help you group related projects, and projects help you manage resources and member access.

Folders

Folders help you organize related projects. You can create nested folders to represent different levels of your organization's structure. For example, you might create a top-level folder for each business unit and then create subfolders for different teams within that business unit. You then create projects within folders.

Folders also enable you to manage member access more efficiently using role inheritance. When you assign roles to members at the folder level, they inherit permissions for all child projects and folders.

> Folders are an organizational tool and not visible to members who do not have IAM permissions such as the Org admin, Folder or project admin, or Super admin roles. Members access projects, not folders.

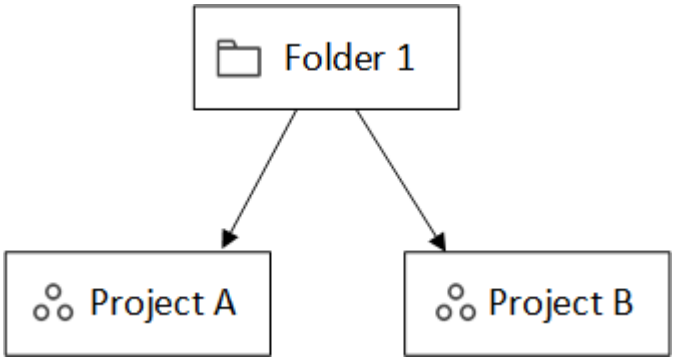
Org admins can delegate administrative responsibilities by creating folders. After creating a folder, an Org admin can assign a member the Folder or project admin roles for particular folders. These members can then manage all projects within that folder without having access to the entire organization.

Folders can have other folders or projects as children, but they cannot have resources directly associated with them. Resources must be associated with a project.

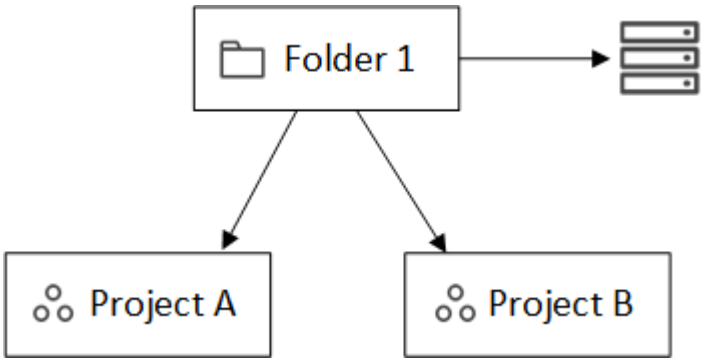
When to associate a resource with a folder

An *Organization administrator* can associate a resource with a folder so a *Folder or project administrator* can link it to the appropriate projects in the folder.

For example, let's say you have a folder that contains two projects:

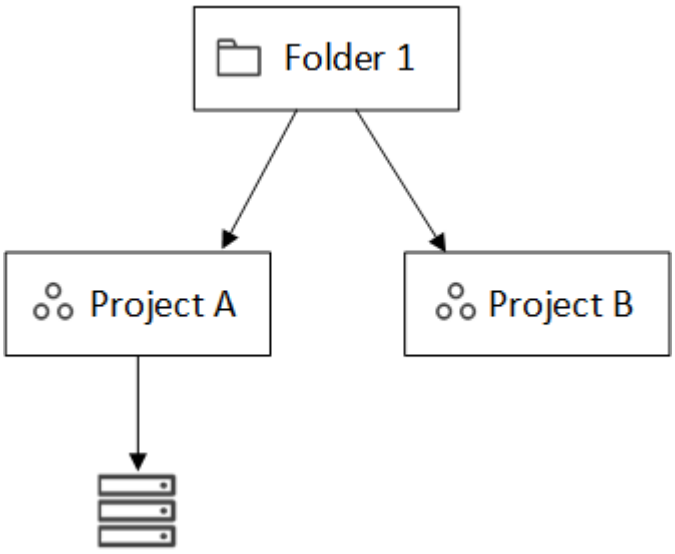


The *Organization admin* can associate a resource with the folder:



Associating a resource with a folder does not make it accessible to all projects; only the *folder or project admin* can see it. The *Folder or project admin* decides which projects can access it and associates the resource with the appropriate projects.

In this example, the admin associates the resource with Project A:



Members who have permissions for project A can now access the resource.

Projects

Associate resources with projects to allow members to manage them. Resources must be associated with a project for management and user access.

An organization can have one or many projects. A project can be directly under the organization or inside a folder. If an agent is used to discover resources within a project, you must also associate the agent with that project.

Users navigate between assigned projects on the **Systems** page to manage the resources associated with each project.

Add a folder or project

Add projects to manage resources and folders to group related projects.
When you create a new organization, the Console includes one project.

You can create up to seven levels of folders and projects in your organization's resource structure. Create nested folders to organize your resources as needed.

Steps

1. Select **Administration > Identity and access**.
2. Select **Organization**.
3. From the **Organization** page, select **Add folder or project**.
4. Select **Folder** or **Project**.
5. Enter folder or project details:

    - **Name and location**: Enter a name and choose a location for the folder or project. You can place folders or projects under the organization or inside another folder.
    - **Resources**: Select the resources that you want to associate with this folder or project. If you haven't added storage systems to the Console yet, you can do this step later.

    > Members can't access resources in a folder until those resources are assigned to a project. Use folders to hold resources temporarily until you create the necessary projects. This can help the Organization admin delegate resource allocation to a Folder or project admin, who then assigns resources to projects within the folder.

    - **Access**: Select **Add a member** to assign access and a role. You can add or remove members from the project or folder at any time.

      Learn about access roles.

6. Select **Add**.

Rename a folder or project

Rename a folder or project as needed. Renaming does not affect associated resources or member access.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, enter a new name and select **Apply**.

Delete a folder or project

Delete folders and projects you no longer need, such as after team restructuring or project completion.

Before you delete a folder or project, make sure it does not contain any resources. Learn how to remove resources.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Delete**.
2. Confirm that you want to delete the folder or project.

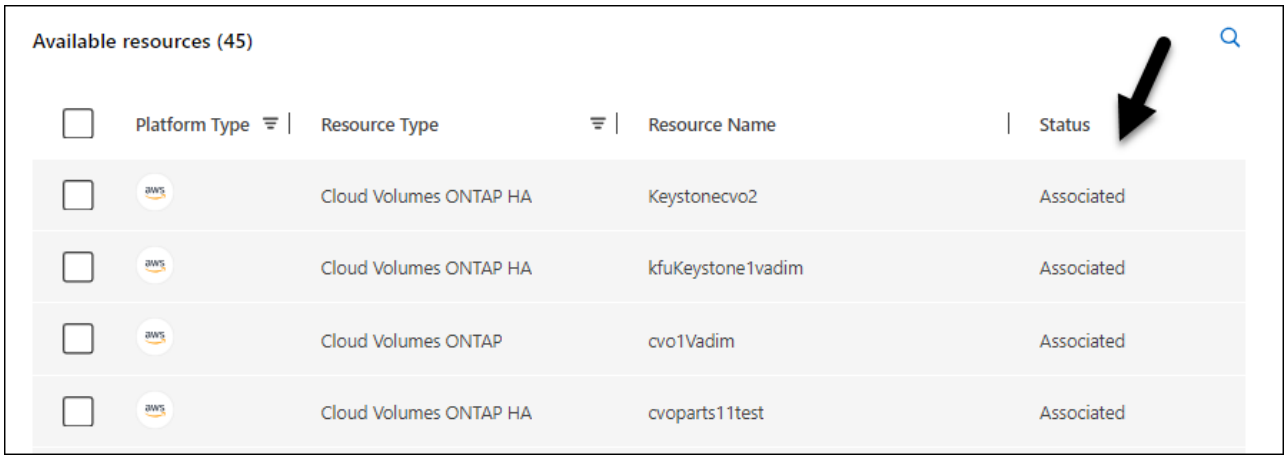
View the resources associated with a folder or project

View which resources and members are associated with a folder or project.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Edit folder** or **Edit project**.

2. On the **Edit** page, you can view details about the selected folder or project by expanding the **Resources** or **Access** sections.
   - Select **Resources** to view the associated resources. In the table, the **Status** column identifies the resources that are associated with the folder or project.



Change the resources associated with a folder or project

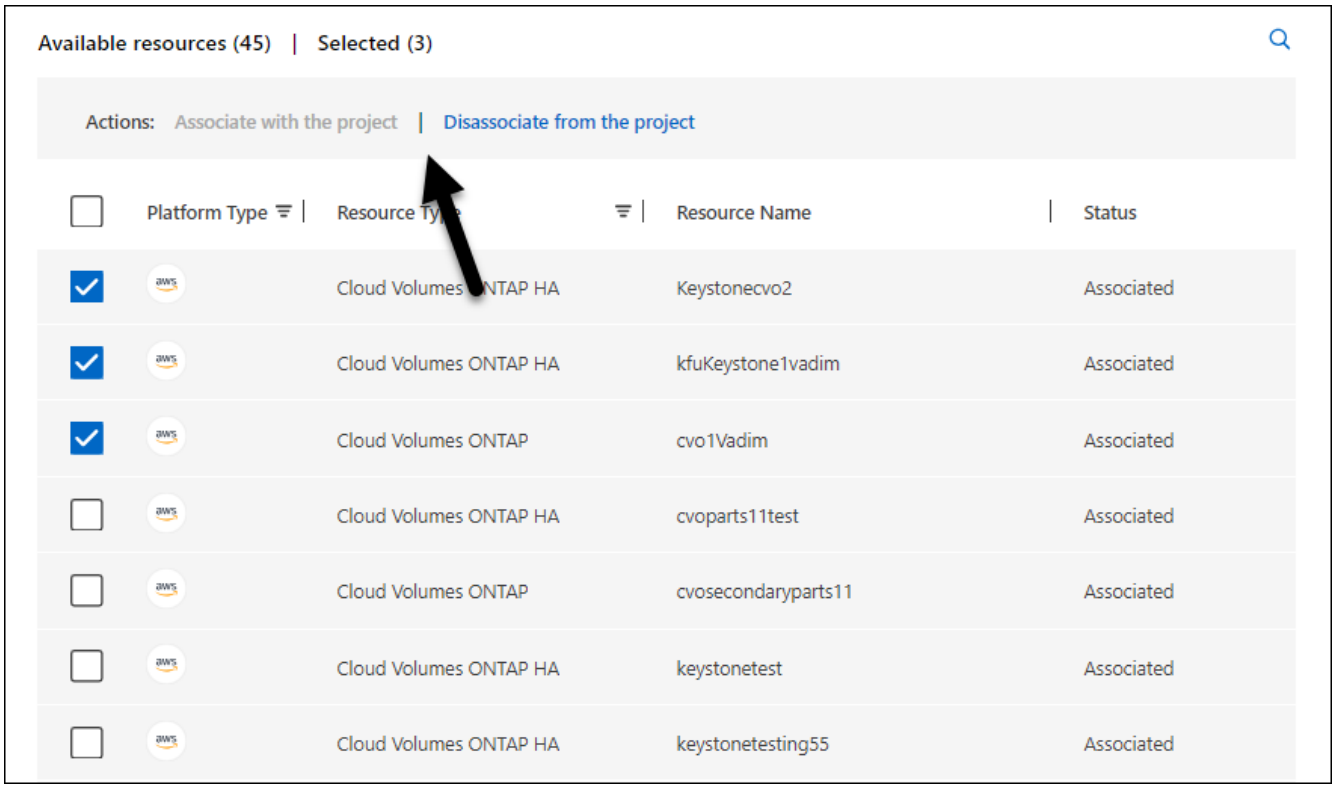
You can change the resources associated with a folder or project as your organization's needs change.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, select **Resources**.

   In the table, the **Status** column identifies the resources that are associated with the folder or project.

3. Select the resources that you'd like to associate or disassociate.
4. Based on the resources that you selected, select either **Associate with the project** or **Disassociate from the project**.



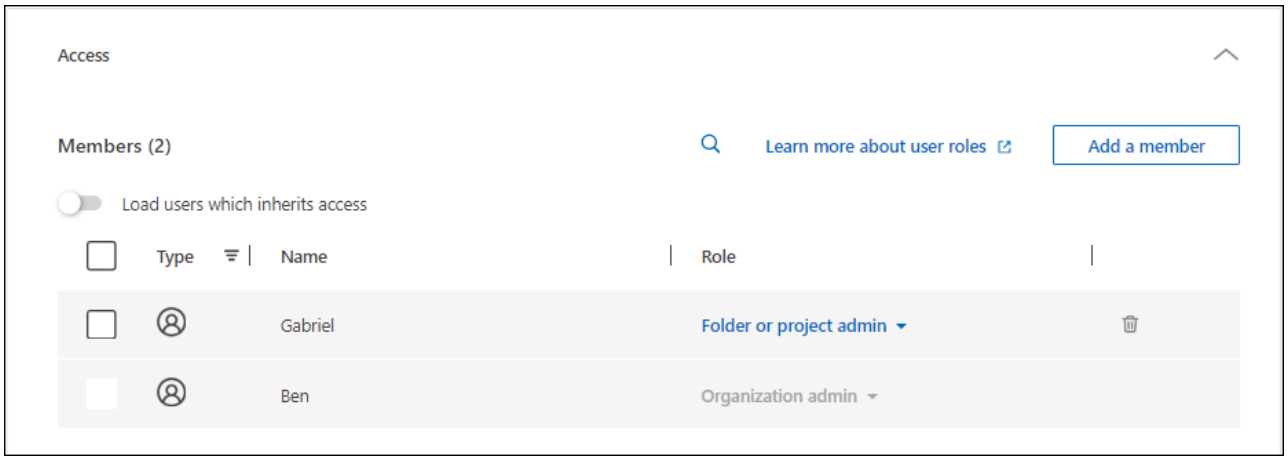
5. Select **Apply**.

View members associated with a folder or project

You can view the members associated with a folder or project from the **Organization** page.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, select **Access** to view the list of members who have access to the selected folder or project.
   - Select **Access** to view the members who have access to the folder or project.



Modify member access to a folder or project

Modify member access to control resource access. Remember that roles assigned at the folder level are inherited by all child projects and folders.

You cannot change member access at lower levels if it is inherited from the folder or organization level. Change the member's permission at the higher hierarchy level to change access Alternatively, you can manage permissions from the Members page.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, select **Access** to view the list of members who have access to the selected folder or project.
3. Modify member access:
   - **Add a member**: Select the member that you'd like to add to the folder or project and assign them a role.
   - **Change a member's role**: For any members with a role other than Organization Admin, select their existing role and then choose a new role.
   - **Remove member access**: For members who have a role defined at the folder or project for which you're viewing, you can remove their access.
4. Select **Apply**.

Related information

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

Add resources to folders and projects in NetApp Console

Control user access to resources by adding them to projects and folders in your NetApp Console organization. Grant access to users at the project level.

A *resource* is an entity that the Console is aware of, such as a storage resource, a Console agent, or a Backup

and Recovery workload.

You can view and manage resources from the **Resources** page in the Console.

Console resource types

You can associate several types of resources to projects in your NetApp Console organization:

Storage resources

Storage resources are the most common type of resource in your organization and represent both on-premises and cloud storage systems. When you add a storage system to the Console, you can add it to a folder or project. Until then, the Console marks it as undiscovered and does not display it on the **Resources** page.

Console agents

If you used a Console agent to discover storage systems, add the agent to the same folder or project. This allows users to perform agent-enabled functions, such as data services or Console-native storage management. You can add agents to folders or projects from the **Agents** page in the Console. Learn how to associate a Console agent with a folder or project.

Keystone subscriptions

If you have Keystone subscriptions in your organization, you can view them on the **Resources** page. You can associate Keystone subscriptions with folders or projects to provide access to members who have permissions for those folders or projects.

View the resources in your organization

You can view both discovered and undiscovered resources associated with your organization. The system finds storage resources and marks them as undiscovered until you add them to the Console.

The Console excludes Amazon FSx for NetApp ONTAP resources from the Resources page because users cannot associate them with a role. You can view these resources on the **Systems** page or from Workloads.

Steps

1. Select **Administration > Identity and access**.
2. Select **Resources**.
3. Select **Advanced Search & Filtering**.
4. Use the available options to find a resource:
   - **Search by resource name**: Enter a text string and select **Add**.
   - **Platform**: Select one or more platforms, such as Amazon Web Services.
   - **Resources**: Select one or more resources, such as Cloud Volumes ONTAP.
   - **Organization, folder, or project**: Select the entire organization, a specific folder, or a specific project.
5. Select **Search**.

Associate a resource with folders and projects

Associate a resource to a folder or project to make it available to members who have permissions for that folder or project.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **Associate to folders or projects**.
2. Select a folder or project and then select **Accept**.
3. To associate an additional folder or project, select **Add folder or project** and then select the folder or project.

   Note that you can only select from the folders and projects for which you have admin permissions.

4. Select **Associate resources**.
   - If you associated the resource with projects, members who have permissions for those projects now have the ability to access the resource from the Console.
   - If you associated the resource with a folder, a *Folder or project admin* can now access the resource and associate it with a project within the folder. Learn about associating a resource with a folder.

After you finish

If you discover a resource using a Console agent, associate the Console agent with the project to grant access. Otherwise, the Console agent and its associated resource are not accessible by members without the *Organization admin* role.

Learn how to associate a Console agent with a folder or project.

View the folders and projects associated with a resource

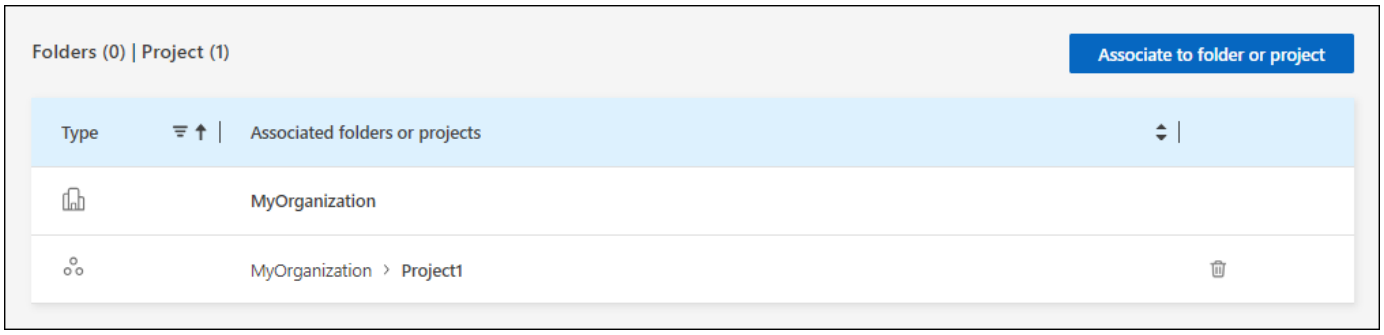
You can view the folders and projects that are associated with a particular resource.

If you need to find out which organization members have access to the resource, you can view the members who have access to the folders and projects that are associated with the resource.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **View details**.

The following example shows a resource that is associated with one project.



To see which organization members have access to the resource, view members with access to associated folders and projects.

Remove a resource from a folder or project

To remove a resource from a folder or project, remove its association. This prevents members from managing the resource in that folder or project.

To remove a discovered resource from the entire organization, go to the **Systems** page and remove the system.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **View details**.
2. To remove a resource from a folder or project, select 🗑 next to the folder or project.
3. Select **Delete** to remove the association.

Related information

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

Associate a Console agent with other folders and projects

Associate Console agents with specific projects to enable resource management and data service access. Resources discovered through a Console agent require both the resource and agent to be associated with the same respective projects for team access.

Super admins and Org admins can create agents and associate any agent with any project or folder. Folder or project admins can only associate existing agents with folders and projects that they have permissions for. Learn more about the actions that a *Folder or project admin* can complete.

Steps

1. Select **Administration > Identity and access** > **Agents**.
2. From the table, find the Console agent that you want to associate.

   Use the search above the table to find a specific Console agent or filter the table by resource hierarchy.
3. To view the folders and projects linked to the Console agent, select ••• and then select **View details**.

   The page displays details about the folders and projects that are associated with the Console agent.
4. Select **Associate to folder or project**.
5. Select a folder or project and then select **Accept**.
6. To associate the Console agent with an additional folder or project, select **Add a folder or project** and then select the folder or project.
7. Select **Associate Agent**.

After you finish

Associate the Console agent's resources with the same folders and projects from the **Resources** page.

Learn how to associate a resource with folders and projects.

Related information

- Learn about NetApp Console agents
- Learn about NetApp Console identity and access management

- Get started with identity and access
- Learn about the API for identity and access management

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

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.

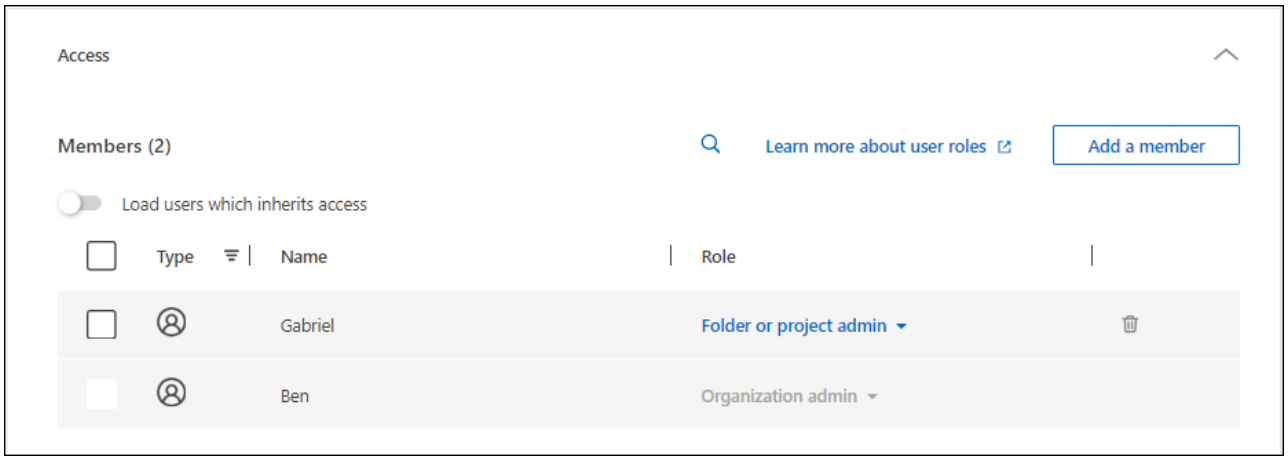
1. From the **Members** page, navigate to a member in the table, select ••• and then select **View details**.
2. In the table, expand the respective row for organization, folder, or project where you want to view the member's assigned role and select **View** in the **Role** column.

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.

NetApp Console access roles

Learn about NetApp Console access roles

Identity and access management (IAM) in the NetApp Console provides predefined roles that you can assign to the members of your organization across different levels of your resource hierarchy. Before you assign these roles, you should understand the permissions that each role includes. Roles fall into the following categories: platform, application, and data service.

Platform roles

Platform roles grant NetApp Console administration permissions, including role assignment and user management. The Console has several platform roles.

Platform role	Responsibilities
Organization admin	Allows a user unrestricted access to all projects and folders within an organization, add members to any project or folder, as well as perform any task and use any data service that does not have an explicit role associated with it. Users with this role manage your organization by creating folders and projects, assigning roles, adding users, and managing systems if they have the proper credentials. This is the only access role that can create Console agents.
Folder or project admin	Allows a user unrestricted access to assigned projects and folders. Can add members to folders or projects they manage, as well as perform any task and use any data service or application on resources within the folder or project they are assigned. Folder or project admins cannot create Console agents.
Federation admin	Allows a user to create and manage federations with the Console, which enables single-sign on (SSO).
Federation viewer	Allows a user to view existing federations with the Console. Cannot create or manage federations.

Platform role	Responsibilities
Partnership admin	Allows a user to create and manage partnerships.
Partnership viewer	Allows a user to view existing partnerships. Cannot create or manage partnerships.
Super admin	Gives the user a subset of admin roles. This role is designed for smaller organizations that may not need to distribute Console responsibilities across multiple users.
Super viewer	Gives the user a subset viewer roles. This role is designed for smaller organizations that may not need to distribute Console responsibilities across multiple users.

Application roles

The following is a list of roles in the application category. Each role grants specific permissions within its designated scope. Users without the required application or platform role cannot access the respective application.

Application role	Responsibilities
Google Cloud NetApp Volumes admin	Users with the Google Cloud NetApp Volumes role can discover and manage Google Cloud NetApp Volumes.
Google Cloud NetApp Volumes viewer	Users with the Google Cloud NetApp Volumes user role can view Google Cloud NetApp Volumes.
Keystone admin	Users with the Keystone admin role can create service requests. Allows users to monitor and view usage, resources, and admin details within the Keystone tenant they are accessing.
Keystone viewer	Users with the Keystone viewer role CANNOT create service requests. Allows users to monitor and view consumption, assets, and administrative information within the Keystone tenant they are accessing.
ONTAP Mediator setup role	Service accounts with the ONTAP Mediator setup role can create service requests. This role is required in a service account to configure an instance of the ONTAP Cloud Mediator.
Operation support analyst	Provides access to alerts and monitoring tools and ability to enter and manage support cases.
Storage admin	Administer storage health and governance functions, discover storage resources, as well as modify and delete existing systems.
Storage viewer	View storage health and governance functions, as well as view previously discovered storage resources. Cannot discover, modify, or delete existing storage systems.
System health specialist	Administer storage and health and governance functions, all permissions of the Storage admin except cannot modify or delete existing systems.

Data service roles

The following is a list of roles in the data service category. Each role grants specific permissions within its designated scope. Users who do not have the required data service role or a platform role will be unable to

access the data service.

Data service role	Responsibilities
Backup and Recovery super admin	Perform any actions in NetApp Backup and Recovery.
Backup and Recovery admin	Perform backups to local snapshots, replicate to secondary storage, and back up to object storage.
Backup and Recovery restore admin	Restore workloads in the Backup and Recovery.
Backup and Recovery clone admin	Clone applications and data in the Backup and Recovery.
Backup and Recovery viewer	View Backup and Recovery information.
Disaster Recovery admin	Perform any actions in NetApp Disaster Recovery service.
Disaster Recovery failover admin	Perform failover and migrations.
Disaster Recovery application admin	Create replication plans, change replication plans, and start test failovers.
Disaster Recovery viewer	View information only.
Classification viewer	Allows users to view NetApp Data Classification scan results. Users with this role can view compliance information and generate reports for resources that they have permission to access. These users can't enable or disable scanning of volumes, buckets, or database schemas. Classification does not have an admin role.
Ransomware Resilience admin	Manage actions on the Protect, Alerts, Recover, Settings, and Reports tabs of NetApp Ransomware Resilience.
Ransomware Resilience viewer	View workload data, view alert data, download recovery data, and download reports in Ransomware Resilience.
Ransomware Resilience user behavior admin	Configure, manage, and view suspicious user behavior detection, alerts, and monitoring in Ransomware Resilience.
Ransomware Resilience user behavior viewer	View suspicious user behavior alerts and insights in Ransomware Resilience.
SnapCenter admin	Provides the ability to back up snapshots from on-premises ONTAP clusters using NetApp Backup and Recovery for applications. A member who has this role can complete the following actions: * Complete any action from Backup and Recovery > Applications * Manage all systems in the projects and folders for which they have permissions * Use all NetApp Console services SnapCenter does not have a viewer role.

Related links

- Learn about NetApp Console identity and access management
- Get started with NetApp Console IAM
- Manage NetApp Console members and their permissions
- Learn about the API for NetApp Console IAM

NetApp Console platform access roles

Assign platform roles to users to grant permissions to manage the NetApp Console, assign roles, add users, create Console agents, and manage federations.

Example for organization roles for a large multi-national organization

XYZ Corporation organizes data storage access by region—North America, Europe, and Asia-Pacific—providing regional control with centralized oversight.

The **Organization admin** in XYZ Corporation's Console creates an initial organization and separate folders for each region. The **Folder or project admin** for each region organizes projects (with associated resources) within the region's folder.

Regional admins with the **Folder or project admin** role actively manage their folders by adding resources and users. These regional admins can also add, remove, or rename folders and projects they manage. The **Organization admin** inherits permissions for any new resources, maintaining visibility of storage usage across the entire organization.

Within the same organization, one user is assigned the **Federation admin** role to manage the federation of the organization with their corporate IdP. This user can add or remove federated organizations, but cannot manage users or resources within the organization. The **Organization admin** assigns a user the **Federation viewer** role to check federation status and view federated organizations.

The following tables indicate the actions that each Console platform role can perform.

Organization administration roles

Task	Organization admin	Folder or project admin
Create agents	Yes	No
Create, modify or delete systems from the Console (add or discover systems)	Yes	Yes
Create folders and projects, including deleting	Yes	No
Rename existing folders and projects	Yes	Yes
Assign roles and add users	Yes	Yes
Associate resources with folders and projects	Yes	Yes
Associate agents with folders and projects	Yes	No
Remove agents from folders and projects	Yes	No
Manage agents (edit certificates, settings, and so on)	Yes	No
Manage credentials from Administration > Credentials	Yes	Yes

Task	Organization admin	Folder or project admin
Create, manage, and view federations	Yes	No
Register for support and submit cases through the Console	Yes	Yes
Use data services that are not associated with an explicit access role	Yes	Yes
View the Audit page and notifications	Yes	Yes

Federation roles

Task	Federation admin	Federation viewer
Create a federation	Yes	No
Verify a domain	Yes	No
Add a domain to a federation	Yes	No
Disable and delete federations	Yes	No
Test federations	Yes	No
View federations and their details	Yes	Yes

Partnership roles

Task	Partnership admin	Partnership viewer
Can create a partnership	Yes	No
Assign roles to partner members	Yes	No
Can add members to a partnership	Yes	No
Can view organization partnership details	Yes	Yes

Super admin and viewer roles

The **Super admin** role provides full access to manage Console features, storage, and data services. This role suits those overseeing administration and governance. In contrast, the **Super viewer** role offers read-only access, ideal for auditors or stakeholders who need visibility without making changes.

Organizations should use **Super admin** access sparingly to minimize security risks and align with the principle of least privilege. Most organizations should assign fine-grained roles with only the necessary permissions to reduce risk and improve auditability.

Example for super roles

ABC Corporation has a small team of five that leverages the NetApp Console for data services and storage management. Instead of distributing multiple roles, they assign the **Super admin** role to two senior team members who handle all administrative tasks, including user management and resource configuration. The remaining three team members are assigned the **Super viewer** role, allowing them to monitor storage health and data service status without the ability to modify settings.

Role	Inherited roles
Super admin	• Organization admin • Folder or project admin • Federation admin • Partnership admin • Ransomware Resilience admin • Disaster recovery admin • Backup super admin • Storage admin • Keystone admin • Google Cloud NetApp Volumes admin
Super viewer	• Organization viewer • Federation viewer • Partnership viewer • Ransomware Resilience viewer • Disaster recovery viewer • Backup viewer • Storage viewer • Keystone viewer • Google Cloud NetApp Volumes viewer

Application roles

Google Cloud NetApp Volumes roles in NetApp Console

You can assign the following role to users to provide them access to the Google Cloud NetApp Volumes in the NetApp Console.

Google Cloud NetApp Volumes uses the following role:

- **Google Cloud NetApp Volumes admin**: Discover and manage Google Cloud NetApp Volumes in the Console.
- **Google Cloud NetApp Volumes viewer**: View Google Cloud NetApp Volumes in the Console.

Keystone access roles in NetApp Console

Keystone roles provide access to the Keystone dashboards and allow users to view and manage their Keystone subscription. There are two Keystone roles: Keystone admin and Keystone viewer. The main difference between the two roles is the actions they can take

in Keystone. The Keystone admin role is the only role that is allowed to create service requests or modify subscriptions.

Example for Keystone roles in NetApp Console

XYZ Corporation has four storage engineers from different departments who view Keystone subscription information. Although all of these users need to monitor the Keystone subscription, only the team lead is allowed to make service requests. Three of the team members are given the **Keystone viewer** role, while the team lead is given the **Keystone admin** role so that there is a point of control over service requests for the company.

The following table indicates the actions that each Keystone role can perform.

Feature and action	Keystone admin	Keystone viewer
View the following tabs: Subscription, Assets, Monitor, and Administration	Yes	Yes
Keystone subscription page:		
View subscriptions	Yes	Yes
Amend or renew subscriptions	Yes	No
Keystone assets page:		
View assets	Yes	Yes
Manage assets	Yes	No
Keystone alerts page:		
View alerts	Yes	Yes
Manage alerts	Yes	No
Create alerts for self	Yes	Yes
Licenses and subscriptions:		
Can view licenses and subscriptions	Yes	Yes
Keystone reports page:		
Download reports	Yes	Yes
Manage reports	Yes	Yes
Create reports for self	Yes	Yes
Service requests:		
Create service requests	Yes	No

Feature and action	Keystone admin	Keystone viewer
View service requests created by any user within the Organization	Yes	Yes

Operational support analyst access role for NetApp Console

You can assign the Operational support analyst role to users to provide them access to alerts and monitoring. Users with this role can also open support cases.

Operational support analyst

Task	Can perform
Manage own user credentials from Settings > Credentials	Yes
View discovered resources	Yes
Register for support and submit cases through the Console	Yes
View the Audit page and notifications	Yes
View, download, and configure alerts	Yes

Storage access roles for NetApp Console

You can assign the following roles to users to provide them access to the storage management features in the NetApp Console. You can assign users an administrative role to manage storage or a viewer role for monitoring.

These roles are not available from the NetApp Console partnership API.

Administrators can assign storage roles to users for the following storage resources and features:

Storage resources:

- On-premises ONTAP clusters
- StorageGRID
- E-Series

Console services and features:

- Digital advisor
- Software updates
- Lifecycle planning
- Sustainability

Example for storage roles in NetApp Console

XYZ Corporation, a multinational company, has a large team of storage engineers and storage administrators. They allow this team to manage storage assets for their regions while limiting access to core Console tasks like user management, agent creation, and license management.

Within a team of 12, two users are given the **Storage viewer** role which allows them to monitor the storage resources associated with the Console projects they are assigned to. The remaining nine are given the **Storage admin** role which includes the ability to manage software updates, access ONTAP System Manager through the Console, as well as discover storage resources (add systems). One person on the team is given the **System health specialist** role so they can manage the health of the storage resources in their region, but not modify or delete any systems. This person can also perform software updates on the storage resources for projects they are assigned.

The organization has two additional users with the **Organization admin** role who can manage all aspects of the Console, including user management, agent creation, and license management, as well as several users with the **Folder or project admin** role who can perform Console administration tasks for the folders and projects they are assigned to.

The following table shows the actions each storage role performs.

Feature and action	Storage admin	System health specialist	Storage viewer
Storage Management:			
Discover new resources (create systems)	Yes	Yes	No
View discovered systems	Yes	Yes	No
Delete systems from the Console	Yes	No	No
Modify systems	Yes	No	No
Create agents	No	No	No
Digital advisor			
View all pages and functions	Yes	Yes	Yes
Licenses and subscriptions			
View all pages and functions	No	No	No
Software updates			
View landing page and recommendations	Yes	Yes	Yes
Review potential version recommendations and key benefits	Yes	Yes	Yes
View update details for a cluster	Yes	Yes	Yes
Run pre-update checks and download upgrade plan	Yes	Yes	Yes

Feature and action	Storage admin	System health specialist	Storage viewer
Install software updates	Yes	Yes	No
Lifecycle planning			
Review capacity planning status	Yes	Yes	Yes
Choose next action (best practice, tier)	Yes	No	No
Tier cold data to cloud storage and free up storage	Yes	Yes	No
Set up reminders	Yes	Yes	Yes
Sustainability			
View dashboard and recommendations	Yes	Yes	Yes
Download report data	Yes	Yes	Yes
Edit carbon mitigation percentage	Yes	Yes	No
Fix recommendations	Yes	Yes	No
Defer recommendations	Yes	Yes	No
System manager access			
May enter credentials	Yes	Yes	No
Credentials			
User credentials	Yes	Yes	No

Data services roles

NetApp Backup and Recovery roles in NetApp Console

You can assign the following roles to users to provide them access to NetApp Backup and Recovery within the Console. Backup and Recovery roles give you the flexibility to assign users a role specific to the tasks they need to accomplish within your organization. How you assign roles depends on your own business and storage management practices.

The service uses the following roles that are specific to NetApp Backup and Recovery.

- **Backup and Recovery super admin**: Perform any actions in NetApp Backup and Recovery.

- **Backup and Recovery Backup admin**: Perform backups to local snapshots, replicate to secondary storage, and back up to object storage actions in NetApp Backup and Recovery.
- **Backup and Recovery Restore admin**: Restore workloads using NetApp Backup and Recovery.
- **Backup and Recovery Clone admin**: Clone applications and data using NetApp Backup and Recovery.
- **Backup and Recovery viewer**: View information in NetApp Backup and Recovery, but not perform any actions.

For details about all NetApp Console access roles, see the Console setup and administration documentation.

Roles used for common actions

The following table indicates the actions that each NetApp Backup and Recovery role can perform for all workloads.

Feature and action	Backup and Recovery super admin	Backup and Recovery backup admin	Backup and Recovery restore admin	Backup and Recovery clone admin	Backup and Recovery viewer
Add, edit, or delete hosts	Yes	No	No	No	No
Install plugins	Yes	No	No	No	No
Add credentials (host, instance, vCenter)	Yes	No	No	No	No
View dashboard and all tabs	Yes	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No	No
Initiate discovery of workloads	No	Yes	Yes	Yes	No
View license information	Yes	Yes	Yes	Yes	Yes
Activate license	Yes	No	No	No	No
View hosts	Yes	Yes	Yes	Yes	Yes
Schedules:					
Activate schedules	Yes	Yes	Yes	Yes	No
Suspend schedules	Yes	Yes	Yes	Yes	No
Policies and protection:					
View protection plans	Yes	Yes	Yes	Yes	Yes

Feature and action	Backup and Recovery super admin	Backup and Recovery backup admin	Backup and Recovery restore admin	Backup and Recovery clone admin	Backup and Recovery viewer
Create, modify, or delete protection plans	Yes	Yes	No	No	No
Restore workloads	Yes	No	Yes	No	No
Create, split, or delete clones	Yes	No	No	Yes	No
Create, modify, or delete policy	Yes	Yes	No	No	No
Reports:					
View reports	Yes	Yes	Yes	Yes	Yes
Create reports	Yes	Yes	Yes	Yes	No
Delete reports	Yes	No	No	No	No
Import from SnapCenter and manage host:					
View imported SnapCenter data	Yes	Yes	Yes	Yes	Yes
Import data from SnapCenter	Yes	Yes	No	No	No
Manage (migrate) host	Yes	Yes	No	No	No
Configure settings:					
Configure log directory	Yes	Yes	Yes	No	No
Associate or remove instance credentials	Yes	Yes	Yes	No	No
Buckets:					
View buckets	Yes	Yes	Yes	Yes	Yes
Create, edit, or delete bucket	Yes	Yes	No	No	No

Roles used for workload-specific actions

The following table indicates the actions that each NetApp Backup and Recovery role can perform for specific workloads.

Kubernetes workloads

This table indicates the actions that each NetApp Backup and Recovery role can perform for actions specific to Kubernetes workloads.

Feature and action	Backup and Recovery super admin	Backup and Recovery backup admin	Backup and Recovery restore admin	Backup and Recovery viewer
View clusters, namespaces, storage classes, and API resources	Yes	Yes	Yes	Yes
Add new Kubernetes clusters	Yes	Yes	No	No
Update cluster configurations	Yes	No	No	No
Remove clusters from management	Yes	No	No	No
View applications	Yes	Yes	Yes	Yes
Create and define new applications	Yes	Yes	No	No
Update application configurations	Yes	Yes	No	No
Remove applications from management	Yes	Yes	No	No
View protected resources and backup status	Yes	Yes	Yes	Yes
Create backups and protect applications with policies	Yes	Yes	No	No
Unprotect apps and delete backups	Yes	Yes	No	No
View recovery points and resource viewer results	Yes	Yes	Yes	Yes
Restore applications from recovery points	Yes	No	Yes	No
View Kubernetes backup policies	Yes	Yes	Yes	Yes
Create Kubernetes backup policies	Yes	Yes	Yes	No
Update backup policies	Yes	Yes	Yes	No

Feature and action	Backup and Recovery super admin	Backup and Recovery backup admin	Backup and Recovery restore admin	Backup and Recovery viewer
Delete backup policies	Yes	Yes	Yes	No
View execution hooks and hook sources	Yes	Yes	Yes	Yes
Create execution hooks and hook sources	Yes	Yes	Yes	No
Update execution hooks and hook sources	Yes	Yes	Yes	No
Delete execution hooks and hook sources	Yes	Yes	Yes	No
View execution hook templates	Yes	Yes	Yes	Yes
Create execution hook templates	Yes	Yes	Yes	No
Update execution hook templates	Yes	Yes	Yes	No
Delete execution hook templates	Yes	Yes	Yes	No
View workload summary and analytics dashboards	Yes	Yes	Yes	Yes
View StorageGRID buckets and storage targets	Yes	Yes	Yes	Yes

NetApp Disaster Recovery roles in NetApp Console

You can assign the following roles to users to provide them access to NetApp Disaster Recovery within the Console. Disaster Recovery roles give you the flexibility to assign users a role specific to the tasks they need to accomplish within your organization. How you assign roles depends on your own business and storage management practices.

Disaster Recovery uses the following roles:

- **Disaster recovery admin**: Perform any actions.
- **Disaster recovery failover admin**: Perform failover and migrations.
- **Disaster recovery application admin**: Create replication plans. Modify replication plans. Start test failovers.
- **Disaster recovery viewer**: View information only.

The following table indicates the actions that each role can perform.

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View dashboard and all tabs	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No
Initiate discovery of workloads	Yes	No	No	No
View license information	Yes	Yes	Yes	Yes
Activate license	Yes	No	Yes	No
On the Sites tab:				
View sites	Yes	Yes	Yes	Yes
Add, modify, or delete sites	Yes	No	No	No
On the Replication plans tab:				
View replication plans	Yes	Yes	Yes	Yes
View replication plan details	Yes	Yes	Yes	Yes
Create or modify replication plans	Yes	Yes	Yes	No
Create reports	Yes	No	No	No
View snapshots	Yes	Yes	Yes	Yes
Perform failover tests	Yes	Yes	Yes	No
Perform failovers	Yes	Yes	No	No
Perform failbacks	Yes	Yes	No	No
Perform migrations	Yes	Yes	No	No
On the Resource groups tab:				
View resource groups	Yes	Yes	Yes	Yes
Create, modify, or delete resource groups	Yes	No	Yes	No
On the Job Monitoring tab:				

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View jobs	Yes	No	Yes	Yes
Cancel jobs	Yes	Yes	Yes	No

Ransomware Resilience access roles for NetApp Console

Ransomware Resilience roles provide users access to NetApp Ransomware Resilience. Ransomware Resilience supports the following roles:

Baseline roles

- Ransomware Resilience admin - Configure Ransomware Resilience settings; investigate and respond to encryption alerts
- Ransomware Resilience viewer - View encryption incidents, reports, and discovery settings

User behavior activity roles

Suspicious user activity detection alerts provide visibility into data such as file activity events; these alerts include file names and file actions (such as Read, Write, Delete, Rename) performed by the user. To limit the visibility of this data, only users with these roles can manage or view these alerts.

- Ransomware Resilience user behavior admin - Activate suspicious user activity detection, investigate and respond to suspicious user activity alerts
- Ransomware Resilience user behavior viewer - View suspicious user activity alerts

> ⓘ User behavior roles are not standalone roles; they are designed to be added to Ransomware Resilience admin or viewer roles. For more information, see User behavior roles.

Consult the following tables for detailed descriptions of each role.

Baseline roles

The following table describes the actions available to the Ransomware Resilience admin and viewer roles.

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
View dashboard and all tabs	Yes	Yes
On dashboard, update recommendation status	Yes	No
Start free trial	Yes	No
Initiate discovery of workloads	Yes	No
Initiate rediscovery of workloads	Yes	No

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
On the Protect tab:		
Add, modify, or delete protection plans for *encryption* policies	Yes	No
Protect workloads	Yes	No
Identify exposure to sensitive data with Data Classification	Yes	No
List protection plans and details	Yes	Yes
List protection groups	Yes	Yes
View protection group details	Yes	Yes
Create, edit, or delete protection groups	Yes	No
Download data	Yes	Yes
On the Alerts tab:		
View encryption alerts and alert details	Yes	Yes
Edit encryption incident status	Yes	No
Mark encryption alert for recovery	Yes	No
View encryption incident details	Yes	Yes
Dismiss or resolve encryption incidents	Yes	No
Get full list of impacted files in encryption event	Yes	No
Download encryption event alerts data	Yes	Yes
Block user (with Workload Security agent configuration)	Yes	No
On the Recover tab:		
Download impacted files from encryption event	Yes	No
Restore workload from encryption event	Yes	No
Download recovery data from encryption event	Yes	Yes

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
Download reports from encryption event	Yes	Yes
On the Settings tab:		
Add or modify backup destinations	Yes	No
List backup destinations	Yes	Yes
View connected SIEM targets	Yes	Yes
Add or modify SIEM targets	Yes	No
Configure readiness drill	Yes	No
Start, reset, or edit readiness drill	Yes	No
Review readiness drill status	Yes	Yes
Update discovery configuration	Yes	No
View discovery configuration	Yes	Yes
On the Reports tab:		
Download reports	Yes	Yes

User behavior roles

To configure suspicious user behavior settings and respond to alerts, a user must have the Ransomware Resilience user behavior admin role. To only view suspicious user behavior alerts, a user should have the Ransomware Resilience user behavior viewer role.

User behavior roles should be conferred on users with existing Ransomware Resilience admin or viewer priviliges who need access to suspicious user activity settings and alerts. A user with the Ransomware Resilience admin role, for example, should receive the Ransomware Resilience user behavior admin role to configure user activity agents and block or unblock users. The Ransomware Resilience user behavior admin role should not be conferred on a Ransomware Resilience viewer.

To activate suspicious user activity detection, you must have the Console Organization admin role.

The following table describes the actions available to the Ransomware Resilience user behavior admin and viewer roles.

Feature and action	Ransomware Resilience user behavior admin	Ransomware Resilience user behavior viewer
On the Settings tab:		
Create, modify, or delete user activity agent	Yes	No
Create or delete user directory connector	Yes	No
Pause or resume data collector	Yes	No
Run data breach readiness drill	Yes	No
On the Protect tab:		
Add, modify, or delete protection plans for *suspicious user behavior* policies	Yes	No
On the Alerts tab:		
View user activity alerts and alert details	Yes	Yes
Edit user activity incident status	Yes	No
Mark user activity alert for recovery	Yes	No
View user activity incident details	Yes	Yes
Dismiss or resolve user activity incidents	Yes	No
Get full list of impacted files by suspicious user	Yes	Yes
Download user activity event alerts data	Yes	Yes
Block or unblock user	Yes	No
On the Recover tab:		
Download impacted files for user activity event	Yes	No
Restore workload from user activity event	Yes	No
Download recovery data from user activity event	Yes	Yes
Download reports from user activity event	Yes	Yes

Identity and access API

Organization and project IDs

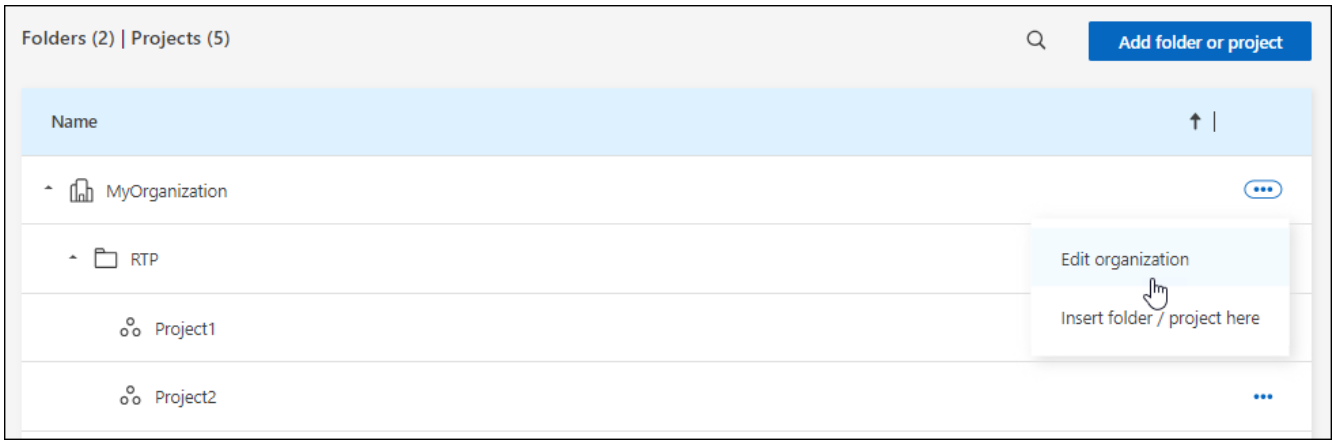
Your NetApp Console organization has a name and an ID. You can choose a name for your organization to help identify it. You may also need to retrieve the organization ID for certain integrations.

Rename your organization

You can rename your organization. This is helpful if you support more than organization.

Steps

1. Select **Administration > Identity and access**.
2. Select **Organization**.
3. From the **Organization** page, navigate to the first row in the table, select ••• and then select **Edit organization**.



4. Enter a new organization name and select **Apply**.

Get the organization ID

The organization ID is used for certain integrations with the Console.

You can view the organization ID from the Organizations page and copy it to the clipboard for your needs.

Steps

1. Select **Administration > Identity and access** > **Organization**.
2. On the **Organization** page, look for your organization ID in the summary bar and copy it to the clipboard. You can save this for use later or copy it directly to where you need to use it.

Obtain the ID for a project

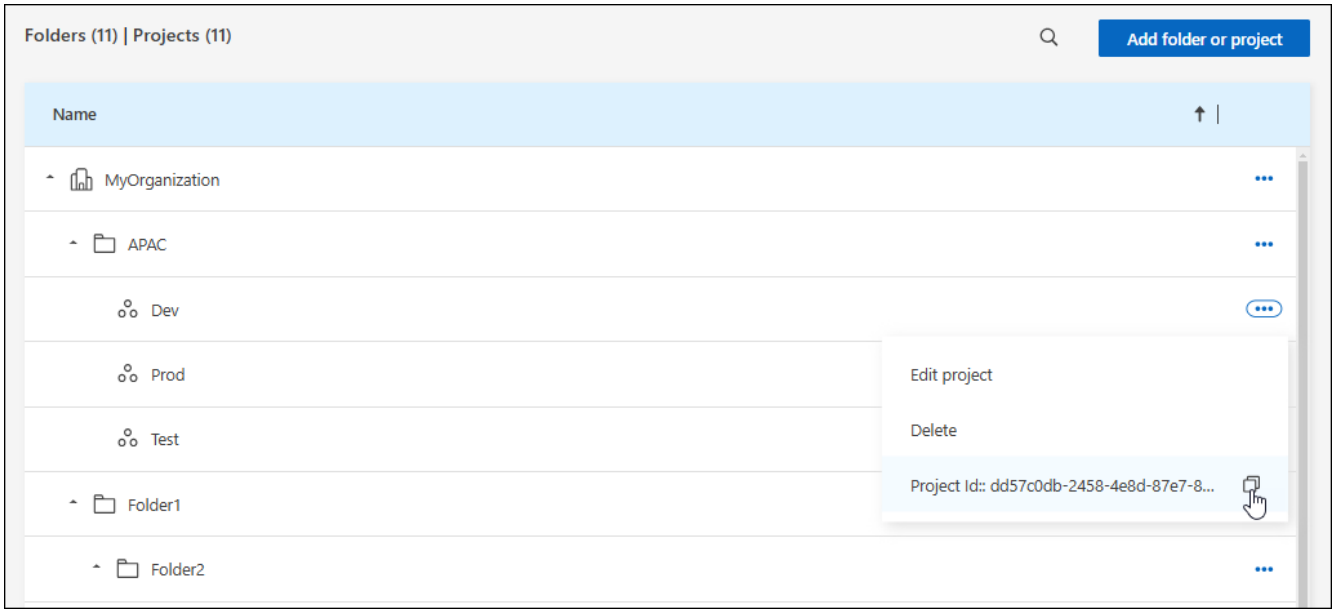
You'll need to obtain the ID for a project if you are using the API. For example, when creating a Cloud Volumes ONTAP system.

Steps

1. From the **Organization** page, navigate to a project in the table and select •••

   The project ID displays.

2. To copy the ID, select the copy button.



Related information

- Learn about identity and access management
- Get started with identity and access
- Learn about the API for identity and access

Copyright information

Trademark information