NetApp Console access roles

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

NetApp Console access roles . . . 1
- Learn about NetApp Console access roles . . . 1
  - Platform roles . . . 1
  - Application roles . . . 2
  - Data service roles . . . 2
  - Related links . . . 3
- NetApp Console platform access roles . . . 3
  - Organization administration roles . . . 4
  - Federation roles . . . 5
  - Partnership roles . . . 5
  - Super admin and viewer roles . . . 5
- Application roles . . . 6
  - Google Cloud NetApp Volumes roles in NetApp Console . . . 6
  - Keystone access roles in NetApp Console . . . 6
  - Operational support analyst access role for NetApp Console . . . 8
- Storage access roles for NetApp Console . . . 8
- Data services roles . . . 10
  - NetApp Backup and Recovery roles in NetApp Console . . . 10
  - NetApp Disaster Recovery roles in NetApp Console . . . 14
  - Ransomware Resilience access roles for NetApp Console . . . 16

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.
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.

Data service role	Responsibilities
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
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:		

Feature and action	Keystone admin	Keystone viewer
Create service requests	Yes	No
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

Feature and action	Storage admin	System health specialist	Storage viewer
View update details for a cluster	Yes	Yes	Yes
Run pre-update checks and download upgrade plan	Yes	Yes	Yes
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

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
Policies and protection:					
View protection plans	Yes	Yes	Yes	Yes	Yes
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

Feature and action	Backup and Recovery super admin	Backup and Recovery backup admin	Backup and Recovery restore admin	Backup and Recovery viewer
Update backup policies	Yes	Yes	Yes	No
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

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
On the Job Monitoring tab:				
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

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
Initiate rediscovery of workloads	Yes	No
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

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
Download recovery data from encryption event	Yes	Yes
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

Copyright information

Trademark information