Use NetApp Console

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Use NetApp Console . . . 1
- Log in to the NetApp Console . . . 1
- Work with multiple Console agents . . . 3
  - Switch between Console agents . . . 3
- View metrics on the NetApp Console Home page . . . 4
  - Required NetApp Console roles . . . 4
  - Enable metrics to appear on the Home page . . . 6
  - View the overall storage capacity . . . 6
  - View ONTAP alerts . . . 6
  - View storage performance capacity . . . 7
  - View the licenses and subscriptions that you have . . . 8
  - View Ransomware Resilience status . . . 8
  - View Backup and Recovery status . . . 8
- Manage your NetApp Console user settings . . . 9
  - Change your display name . . . 9
  - Elevate your role in read-only mode . . . 9
  - Configure multi-factor authentication . . . 9
  - Regenerate your MFA recovery code . . . 10
  - Delete your MFA configuration . . . 10
  - Contact your Organization administrator . . . 11
  - Configure dark mode (dark theme) . . . 11

Use NetApp Console

Log in to the NetApp Console

How you log in to the NetApp Console depends on which deployment mode that you're using.

You are automatically logged out after 24 hours or if you close your browser.

Learn about Console deployment modes.

Standard mode

After you sign up to the NetApp Console, you can log in from the web-based console to start managing your data and storage infrastructure.

About this task

You can log in to the NetApp Console using one of the following options:

- Your existing NetApp Support Site (NSS) credentials
- A NetApp Console account using your email address and a password
- A federated connection

  You can use single sign-on to log in using credentials from your corporate directory (federated identity). Learn how to set up identity federation.

Steps

1. Open a web browser and go to the NetApp Console
2. On the **Log in** page, enter the email address that's associated with your login.
3. Depending on the authentication method associated with your login, you'll be prompted to enter your credentials:
   - NetApp cloud credentials: Enter your password
   - Federated user: Enter your federated identity credentials
   - NetApp Support Site account: Enter your NetApp Support Site credentials

Result

You're now logged in and can start using to manage your hybrid multi-cloud infrastructure.

Restricted mode

When you use the Console in restricted mode, you need to log in to the the Console from the user interface that runs locally on the agent.

About this task

The Console supports logging in with one of the following options when in restricted mode:

- A NetApp Console login using your email address and a password
- A federated connection

  You can use single sign-on to log in using credentials from your corporate directory (federated identity). Learn how to use identity federation.

Steps

1. Open a web browser and enter the IP address where the agent is installed.
2. Enter your user name and password to log in.

Work with multiple Console agents

If you use multiple Console agents, you can switch between those Console agents directly from the Console to view the associated systems.

Switch between Console agents

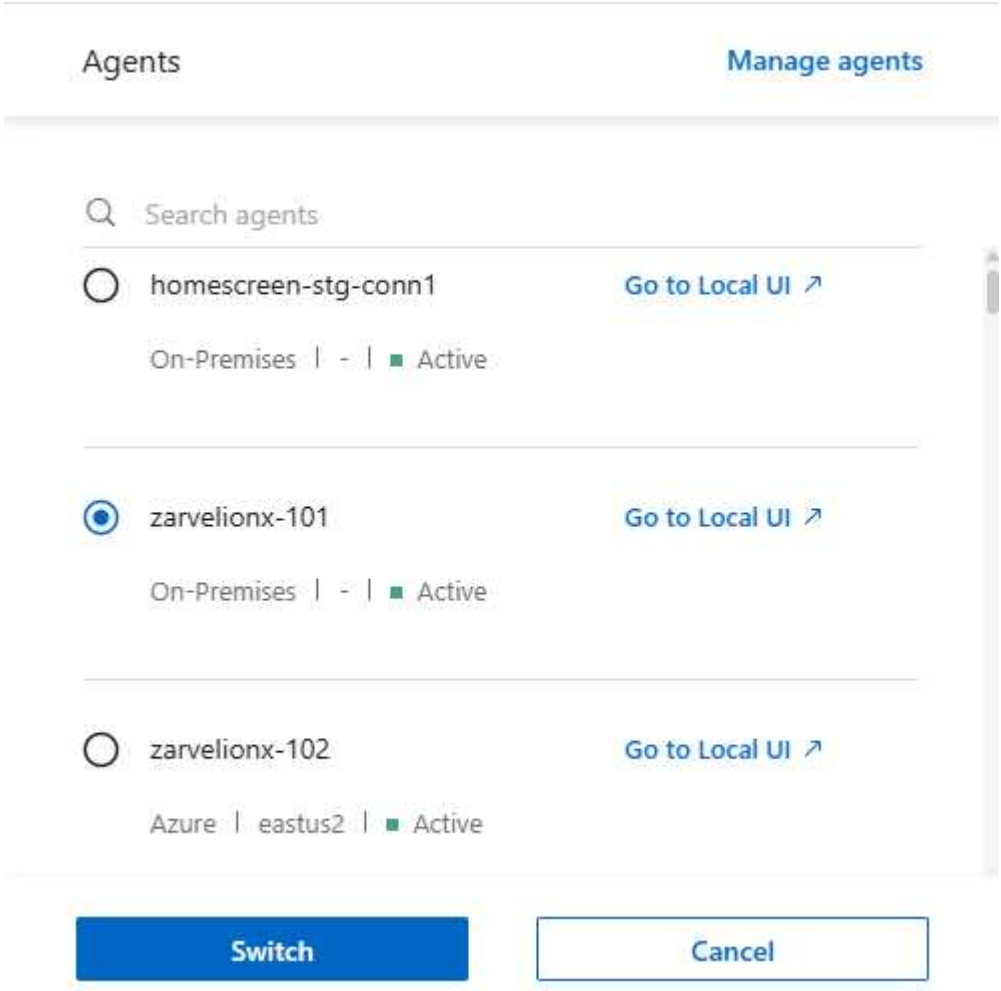
If you have multiple Console agents, you can switch between them to see the systems that are associated with a specific agent.

For example, in a multi-cloud environment, you might have one agent in AWS and another in Google Cloud. Switch between these agents to manage the Cloud Volumes ONTAP systems in the respective cloud environments.

This option is not available when viewing the NetApp Console from the agent's local UI

Step

1. Select the Console agents icon ( ) in the top right to view the list of available agents.



Result

The Console refreshes and shows the systems associated with the selected agent.

View metrics on the NetApp Console Home page

Monitoring the health of your storage estate ensures that you are aware of issues with storage protection and can take steps to resolve them. Using the NetApp Console Home page, view a status of your backups and restores from NetApp Backup and Recovery and the number of workloads that are at risk for a ransomware attack or protected as indicated by NetApp Ransomware Resilience. You can review the storage capacity for individual clusters and Cloud Volumes ONTAP, ONTAP alerts, storage performance capacity per cluster or Cloud Volumes ONTAP system, the different types of licenses you have, and more.

All panes on the Home page show data at the organization level. The Storage capacity and Storage performance panes show systems associated with projects that the user can access based on IAM permissions.

The system refreshes the data on the Home page every five minutes. Caching may cause the data on this page to differ from real values for up to 15 minutes.

Accurate metrics on the Home page require appropriately sized and configured Console agents.

Required NetApp Console roles

Each pane in the Home page requires different user roles:

- **Storage capacity pane**: Ability to see the NetApp Console Systems page
- **ONTAP alerts pane**: Folder or project admin, Operations Support Analyst, Organization admin, Organization viewer, Super admin, Super viewer
- **Storage performance capacity pane**: Ability to see the NetApp Console Systems page
- **Licenses and subscriptions pane**: Folder or project admin, Organization admin, Organization viewer, Super admin, Super viewer
- **Ransomware Resilience pane**: Folder or project admin, Organization admin, Ransomware Resilience admin, Ransomware Resilience viewer, Super admin, Super viewer
- **Backup and Recovery pane**: Backup and recovery backup admin, Backup and recovery super admin, Backup and recovery backup viewer, Backup and recovery clone admin, Folder or project admin, Organization admin, Backup and recovery restore admin, Super admin, Super viewer

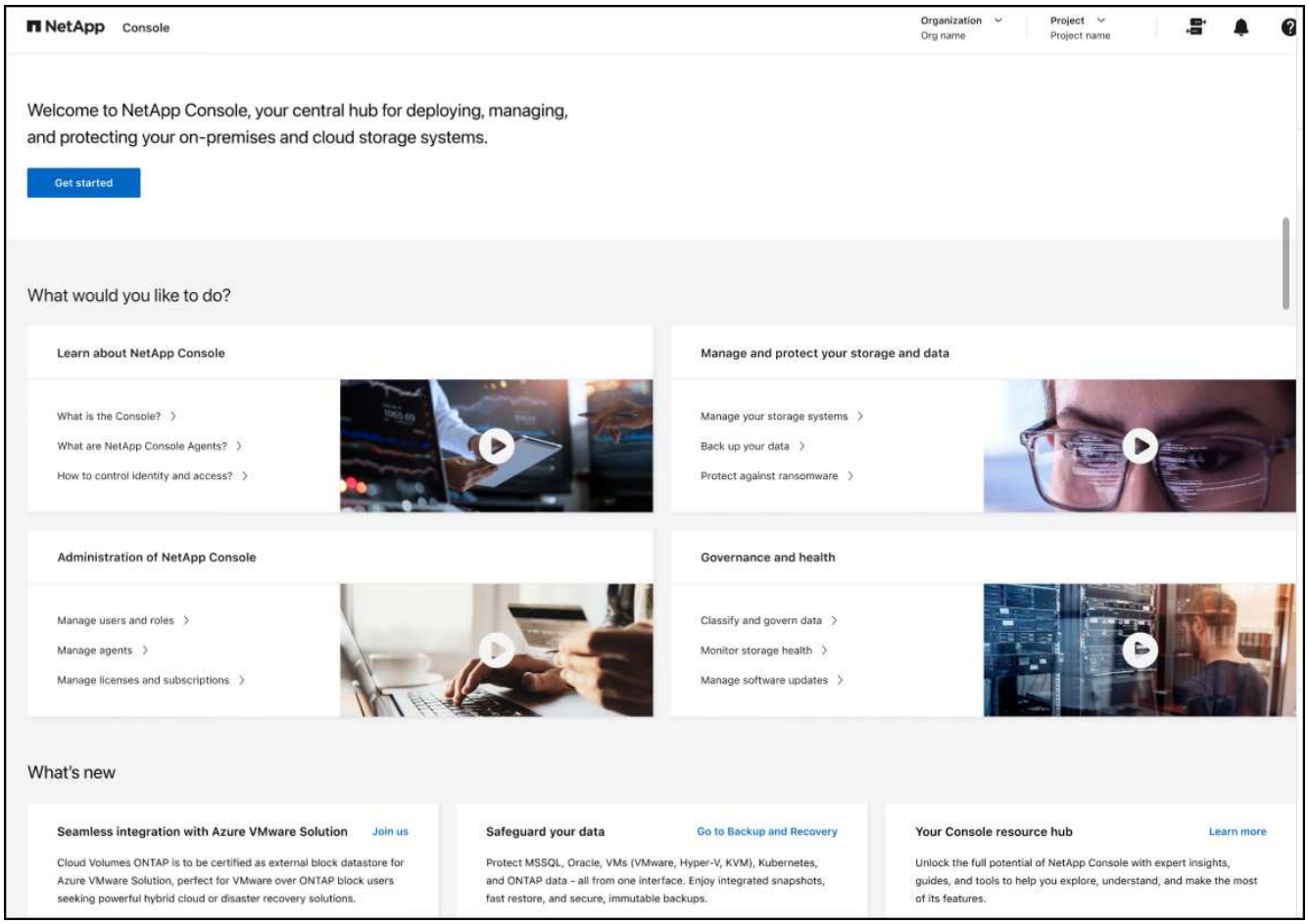
If you do not have permissions to access a pane, the pane displays a message indicating you lack permissions to use it.

Learn about NetApp Console access roles..

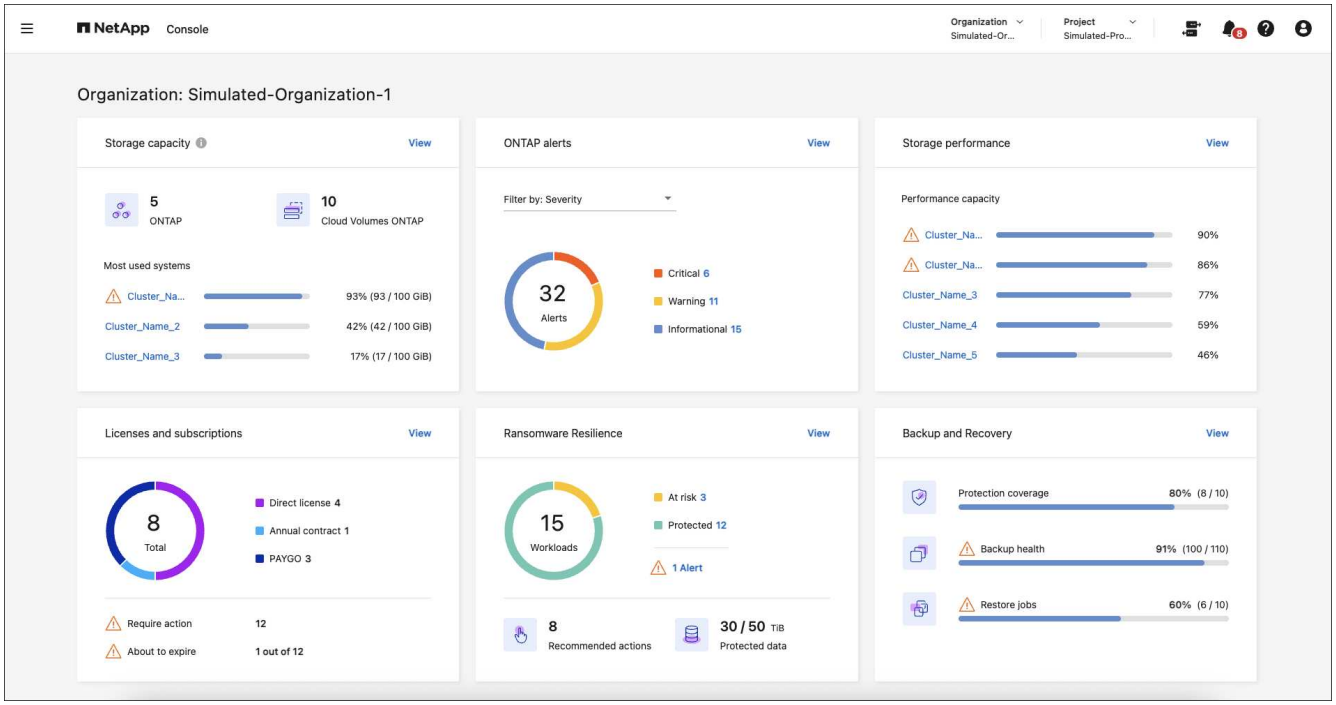
Steps

1. From the NetApp Console menu, select **Home**.

   If you have the Organization admin role and no agent or storage systems are set up, the Home page displays getting started information.



If you already set up the NetApp Console, at least one Console agent is enabled, and at least one cluster or Cloud Volumes ONTAP system has been added on that agent, the Home page shows metrics about your storage environment.



Enable metrics to appear on the Home page

You can see metrics on the Home page when the following conditions are met:

- You are logged into a SaaS instance of the NetApp Console.
- You belong to an organization with existing storage resources (agent and cluster or Cloud Volumes ONTAP system).
- At least one Console agent is enabled.
- At least one cluster or Cloud Volumes ONTAP system has been added on that agent.

To enable metrics to appear on the Home page, complete the following tasks:

- Enable at least one Console agent.
- Add at least one cluster or one Cloud Volumes ONTAP using that agent.

View the overall storage capacity

The Storage capacity pane provides the following information across ONTAP clusters and Cloud Volumes ONTAP systems:

- Number of ONTAP systems discovered in the Console
- Number of Cloud Volumes ONTAP systems discovered in the Console
- Capacity usage per cluster

The order of the clusters or Cloud Volumes ONTAP systems is based on the amount of capacity used. The cluster or system with the highest capacity appears first for easy identification.

Warning indicators show for clusters at 80% capacity, with data updating every five minutes.

If you have multiple projects, you might see different data in the Storage capacity pane compared to the Systems page. This is because the Systems page shows information based on the project level, whereas the Storage capacity pane shows information at the organization level. Also, the data on this pane might differ from real values for a maximum of 15 minutes because the data is cached for that duration to optimize performance.

Steps

1. From the NetApp Console menu, review the Storage capacity pane.
2. In the Storage capacity pane, select **View** to go to the Console Systems page.
3. On the Systems page, select the project containing the cluster you want to view.
4. On the Systems page, select a cluster to view more details about that cluster.

View ONTAP alerts

View issues or potential risks in your NetApp on-premises ONTAP environments. You can see some non-EMS alerts and some EMS alerts.

The data updates every 5 minutes.

You can see ONTAP alerts with these severities:

- Critical
- Warning
- Informational

You can see ONTAP alerts for these impact areas:

- Capacity
- Performance
- Protection
- Availability
- Security

Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

Systems supported

- An on-premises ONTAP NAS or SAN system is supported.
- Cloud Volumes ONTAP systems are not supported.

Data sources supported

View alerts regarding certain events that occur in ONTAP. They are a combination of EMS and metric-based alerts.

For details about ONTAP alerts, refer to About ONTAP alerts.

For a list of alerts that you might see, refer to View potential risks in ONTAP storage.

Steps

1. From the NetApp Console menu, review the ONTAP alerts pane.
2. Optionally, filter the alerts by selecting the severity level or change the filter to show alerts based on impact area.
3. In the ONTAP alerts pane, select **View** to go to the Console Alerts page.

View storage performance capacity

Review the storage performance capacity used per cluster or Cloud Volumes ONTAP system to determine how performance capacity, latency, and IOPS are impacting your workloads. For example, you might find that you need to shift workloads to minimize latency and maximize IOPS and throughput for your critical workloads.

The system arranges clusters and systems by performance capacity, listing the highest capacity first for easy identification.

Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

Steps

1. From the NetApp Console menu, review the Storage performance pane.

2. In the Storage performance pane, select **View** to go to a Performance page that lists all the clusters and Cloud Volumes ONTAP systems data for performance capacity, IOPS, and latency.
3. Select a cluster to view its details in System Manager.

View the licenses and subscriptions that you have

Review the following information on the Licenses and subscriptions pane:

- The total number of licenses and subscriptions that you have.
- The number of each type of license and subscription that you have (direct license, annual contract, or PAYGO).
- The number of licenses and subscriptions that are active, require action, or nearing expiration.
- The system displays indicators next to the license types that require action or are nearing expiration.

The data refreshes every 5 minutes.

Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

Steps

1. From the NetApp Console menu, review the Licenses and subscriptions pane.
2. In the Licenses and subscriptions pane, select **View** to go to the Console Licenses and subscriptions page.

View Ransomware Resilience status

Find out if workloads are at risk of ransomware attacks or protected with the NetApp Ransomware Resilience data service. You can review the total amount of data that is protected, view the number of recommended actions, and view the number of alerts related to ransomware protection.

The data refreshes every 5 minutes and matches the data shown in the NetApp Ransomware Resilience Dashboard.

Learn about NetApp Ransomware Resilience.

Steps

1. From the NetApp Console menu, review the Ransomware Resilience pane.
2. Do one of the following in the Ransomware Resilience pane:
    - Select **View** to go to the NetApp Ransomware Resilience Dashboard. For details, refer to Monitor workload health using the NetApp Ransomware Resilience Dashboard.
    - Review "Recommended actions" in the NetApp Ransomware Resilience Dashboard. For details, refer to Review protection recommendations on the NetApp Ransomware Resilience Dashboard.
    - Select the alerts link to review alerts in NetApp Ransomware Resilience Alerts page. For details, refer Handle detected ransomware alerts with NetApp Ransomware Resilience.

View Backup and Recovery status

Review the overall status of your backups and restores from NetApp Backup and Recovery. You can see the number of protected and unprotected resources. You can also see the percentage of backups and restore operations for protection of your workloads. A higher percentage indicates improved data protection.

The data refreshes every 5 minutes.

Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

Steps

1. From the NetApp Console menu, review the Backup and Recovery pane.
2. Select **View** to go to the NetApp Backup and Recovery Dashboard. For details, refer to NetApp Backup and Recovery documentation.

Manage your NetApp Console user settings

You can modify your Console profile including change your password, enable multi-factor authentication (MFA), and see who your Console administrator is.

Within the Console, each user has a profile that contains information about the user and their settings. You can view and edit your profile settings.

Change your display name

You can change your Console display name, which identifies you to other users. You cannot change your username or email address.

Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. Select the **Edit** icon next to your name.
3. Enter your new display name in the **Name** field.

Elevate your role in read-only mode

In some cases, your Organization admin may put your organization into read-only mode. If you have an admin role, you must elevate permissions to make changes. This ensures changes are intentional and authorized.

After elevating your role, you can make changes in the Console until your current session expires.

When you're finished, either log out of the Console or move the slider back to return to read-only mode. The system removes your elevated permissions when your session expires.

Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. For **Read-only mode status**, move the slider to the **Elevated** position and confirm the changes.

Configure multi-factor authentication

Configure multi-factor authentication (MFA) to improve security by requiring a second verification method.

Users who use single sign-on with an external identity provider or the NetApp Support Site cannot enable MFA. If either of these are true for you, you don't see the option to enable MFA in your profile settings.

Do not enable MFA if your user account is used for API access. Multi-factor authentication stops API access when enabled for a user account. Use service accounts for all API access.

Before you begin

- You must have already downloaded an authentication app, such as Google Authenticator or Microsoft Authenticator, to your device.
- You'll need your password to set up MFA.

If you do not have access to your authentication app or lose your recovery code, contact your Console administrator for help.

Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. Select **Configure** next to the **Multi-Factor Authentication** header.
3. Follow the prompts to set up MFA for your account.
4. When you finish, you'll be prompted to save your recovery code. Choose to either copy the code or download a text file containing the code. Keep this code somewhere safe. You need the recovery code if you lose access to your authentication app.

   After you set up MFA, the Console prompts you to enter a one-time code from your authentication app each time you log in.

Regenerate your MFA recovery code

You can only use recovery codes once. If you use or lose yours, create a new one.

Steps

1. Select the profile icon in the upper right corner of the the Console to view the User settings panel.
2. Select ••• next to the **Multi-Factor Authentication** header.
3. Select **Regenerate recovery code**.
4. Copy the generated recovery code and save it in a secure location.

Delete your MFA configuration

When you're finished, either log out of the Console or move the slider back to return to read-only mode. The system removes your elevated permissions when your session expires.

If you are unable to access your authentication app or recovery code, you will need to contact your Organization administrator to reset your MFA configuration.

Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. Select ••• next to the **Multi-Factor Authentication** header.
3. Select **Delete**.

Contact your Organization administrator

If you need to contact your organization administrator, you can send an email to them directly from the Console. The administrator manages user accounts and permissions within your organization.

> You must have a default email application configured for your browser to use the **Contact admins** feature.

Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. Select **Contact admins** to send an email to your organization administrator.
3. Select the email application to use.
4. Finish the email and select **Send**.

Configure dark mode (dark theme)

You can set the Console to display in dark mode.

Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. Move the **Dark theme** slider to enable it.

Copyright information

Trademark information