Learn the basics

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Learn the basics

Learn about NetApp Console

The Console unifies storage management and protection across hybrid multi-cloud with integrated data services to protect and optimize data.

It is available as a service (SaaS) platform or a self-hosted option that you can install in your sovereign cloud. It provides storage management, data mobility, data protection, and data analysis and control. Management capabilities are provided through a web-based console and APIs.

Centralized storage management

Discover, deploy, and manage cloud and on-premises storage with the Console.

Supported cloud and on-premises storage

You can manage the following types of storage from the Console:

Cloud storage solutions

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

On-premises flash and object storage

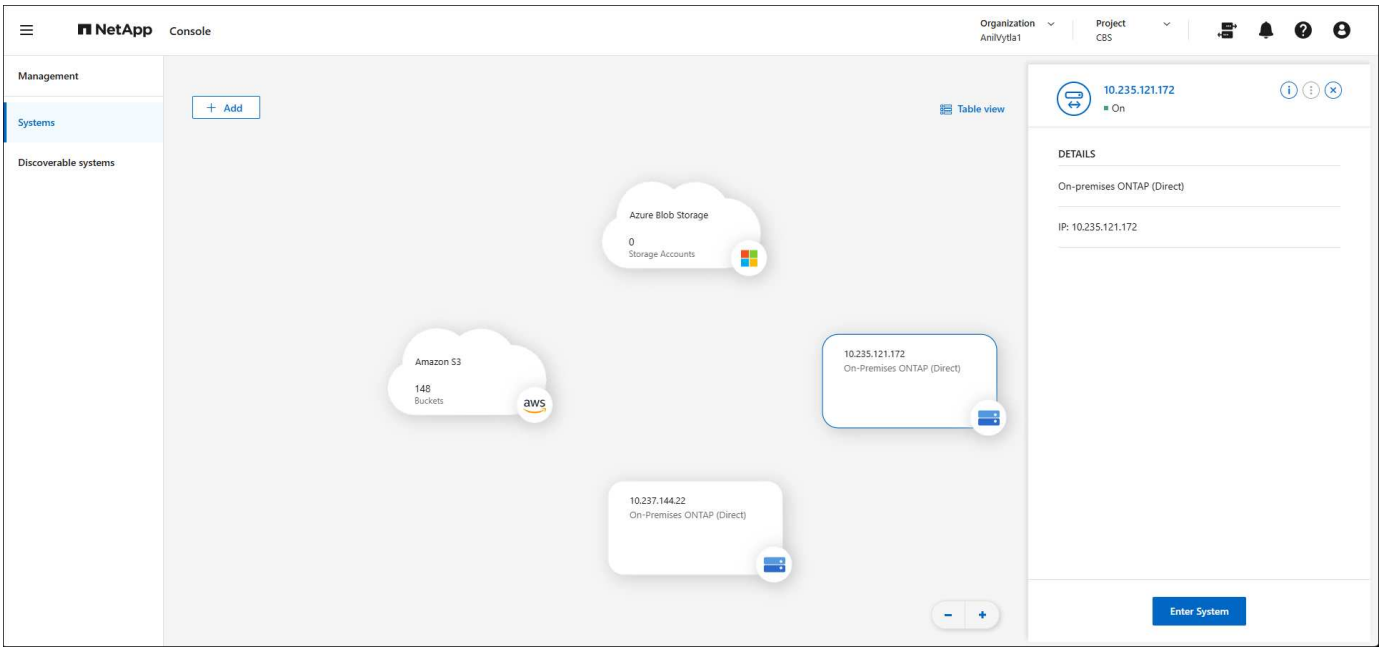
- E-Series systems
- ONTAP clusters
- StorageGRID systems

Cloud object storage

- Amazon S3 storage
- Azure Blob storage
- Google Cloud Storage

Storage management

Within the Console, *systems* represent discovered or deployed storage. You can select a *system* to integrate it with NetApp data services or manage storage, such as adding volumes.



Integrated data services and storage management to protect, secure, and optimize data

The Console provides data services to secure and maintain storage availability.

Storage alerts

View issues related to capacity, availability, performance, protection, and security in your ONTAP environment.

Automation hub

Use scripted solutions to automate the deployment and integration of NetApp products and services.

NetApp Backup and Recovery

Back up and restore cloud and on-premises data.

NetApp Data Classification

Get your application data and cloud environments privacy ready.

NetApp Copy and Sync

Sync data between on-premisesand cloud data stores.

NetApp digital advisor (Active IQ)

Use predictive analytics and proactive support to optimize your data infrastructure.

Licenses and subscriptions

Manage and monitor your licenses and subscriptions.

NetApp Disaster Recovery

Protect on-premises VMware workloads using VMware Cloud on Amazon FSx for ONTAP as a disaster recovery site.

Lifecycle planning

Identify clusters with current or forecasted low capacity and implement data tiering or additional capacity recommendations.

NetApp Ransomware Resilience

Detect anomalies that might result in ransomware attacks. Protect and recover workloads.

NetApp Replication

Replicate data between storage systems to support backup and disaster recovery.

Software updates

Automate the assessment, planning, and execution of ONTAP upgrades.

Sustainability dashboard

Analyze the sustainability of your storage systems.

NetApp Cloud Tiering

Extend your on-premises ONTAP storage to the cloud.

NetApp Volume Caching

Create a writable cache volume to speed up access to data or offload traffic from heavily accessed volumes.

NetApp Workloads

Design, set up, and operate key workloads using Amazon FSx for NetApp ONTAP.

Learn more about the NetApp Console and the available data services

Supported cloud providers

The Console enables you to manage cloud storage and use cloud services in Amazon Web Services, Microsoft Azure, and Google Cloud.

Cost

There is no charge for the NetApp Console. You incur costs if you deploy Console agents in the cloud or use Restricted mode deployed in the cloud. There are costs associated with some NetApp data services.
Learn about NetApp data services pricing

How NetApp Console works

The NetApp Console is web-based console that's provided through the SaaS layer, a resource and access management system, Console agents that manage storage systems and enable NetApp data services, and different deployment modes to meet your business requirements.

Software-as-a-service

You access the Console through a web-based interface and APIs. This SaaS experience enables you to automatically access the latest features as they're released.

Identity and access management (IAM)

The Console provides identity and access management (IAM) for resource and access management. This IAM model provides granular management of resources and permissions:

- A top-level *organization* enables you to manage access across your various *projects*
- *Folders* enable you to group related projects together
- Resource management enables you to associate a resource with one or more folders or projects
- Access management enables you to assign a role to members at different levels of the organization hierarchy
- Learn more about IAM in NetApp Console

Console agents

A Console agent is needed for some additional features and data services. It enables you to manage resources and processes across your on-premises and cloud environments. You need it to manage some systems (for example, Cloud Volumes ONTAP) and to use some NetApp data services.

Learn more about Console agents.

SaaS versus sovereign cloud deployment

You can start using NetApp Console by signing up for the SaaS offering or deploying it in your sovereign cloud. When you deploy NetApp Console in a sovereign cloud, NetApp limits outbound connectivity to meet your organization's security and compliance requirements. Not all features and services are available when the Console is deployed in a sovereign cloud.

NetApp continues to offer BlueXP for sites that want no outbound connectivity. BlueXP can be installed on your network with no outbound connectivity. Learn about BlueXP (private mode) for sites with no internet connectivity.

Learn more about deployment modes.

SOC 2 Type 2 certification

An independent certified public accountant firm and services auditor examined the Console and affirmed that it achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

View NetApp's SOC 2 reports

Learn about NetApp Console deployment modes

The NetApp Console offers multiple *deployment modes* that enable you to meet your business and security requirements.

- *Standard mode* leverages a software as a service (SaaS) layer to provide full functionality. Users access the Console through a web-based hosted interface
- *Restricted mode* is available for organizations that have connectivity restrictions who want to install the NetApp Console in their own public cloud. Users access the Console through a web-based interface that's hosted on a Console agent in their cloud environment.

NetApp Console restricts traffic, communication, and data in restricted mode, and you must ensure your environment (on-premises and in the cloud) complies with required regulations.

Overview

Each deployment mode differs in outbound connectivity, location, installation, authentication, data services, and charging methods.

Standard mode

You use a SaaS service from the web-based console. Depending on the data services and features that you plan to use, a Console organization admin creates one or more Console agents to manage data within your hybrid cloud environment.

This mode uses encrypted data transmission over the public internet.

Restricted mode

You install a Console agent in the cloud (in a government, sovereign, or commercial region), and it has limited outbound connectivity to the NetApp Console SaaS layer.

This mode is typically used by state and local governments and regulated companies.

Learn more about outbound connectivity to the SaaS layer.

BlueXP private mode (legacy BlueXP interface only)

BlueXP private mode (legacy BlueXP interface) is typically used with on-premises environments that have no internet connection and with secure cloud regions, which includes AWS Secret Cloud, AWS Top Secret Cloud, and Azure IL6. NetApp continues to support these environments with the legacy BlueXP interface.
PDF documentation for BlueXP private mode

The following table provides a comparison of the NetApp console.

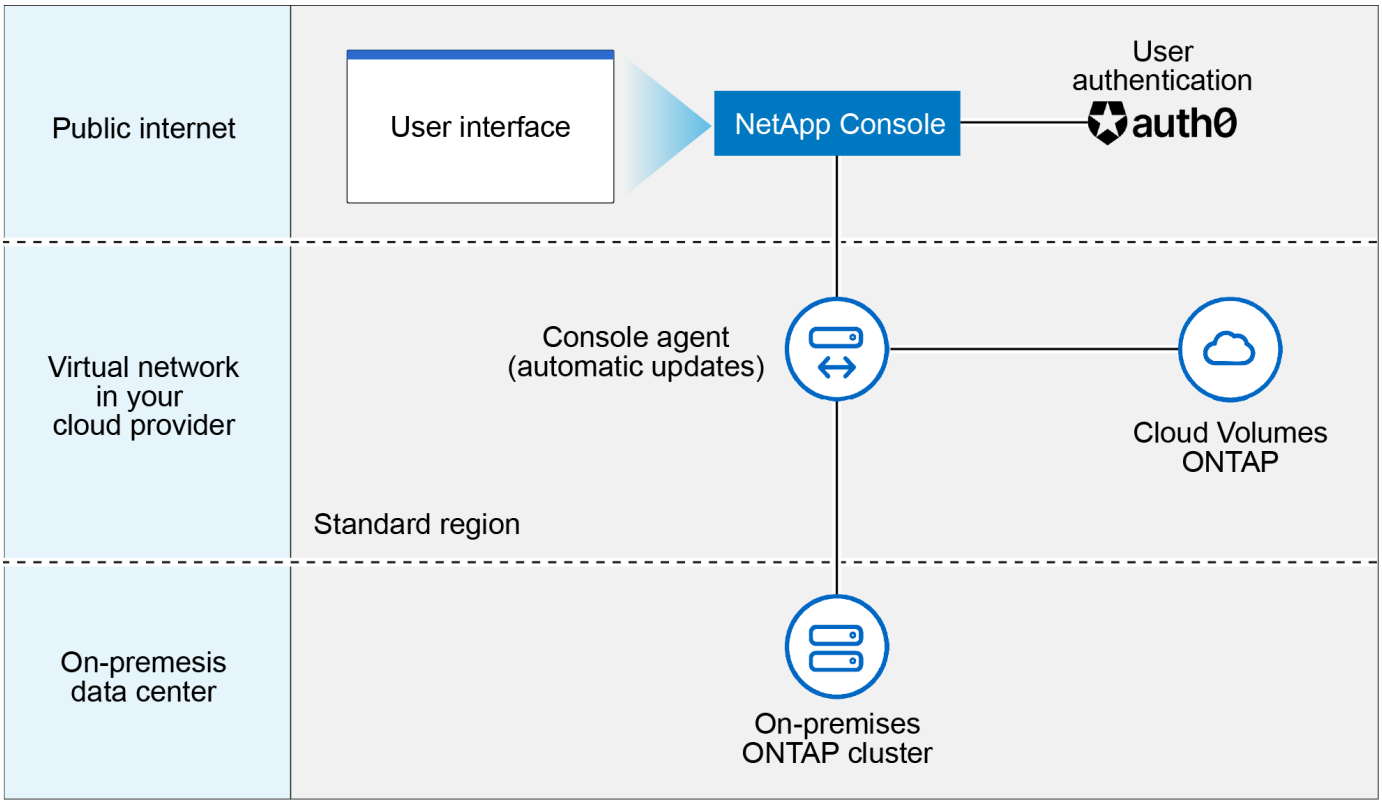
	Standard mode	Restricted mode
Connection required to NetApp Console SaaS layer?	Yes	Outbound only
Connection required to your cloud provider?	Yes	Yes, within the region
Console agent installation	From the Console, cloud marketplace, or manual install	Cloud marketplace or manual install
Console agent upgrades	Automatic upgrades	Automatic upgrades
UI access	From the Console SaaS layer	Locally from an agent VM
API endpoint	The Console SaaS layer	A Console agent
Authentication	Through SaaS using auth0, NSS login, or identity federation	Through SaaS using auth0 or identity federation
Multi-factor authentication	Available for local users	Not available

	Standard mode	Restricted mode
Storage and data services	All are supported	Many are supported
Data service licensing options	Marketplace subscriptions and BYOL	Marketplace subscriptions and BYOL

Read through the following sections to learn more about these modes, including which NetApp Console features and services are supported.

Standard mode

The following image is an example of a standard mode deployment.



The Console works as follows in standard mode:

Outbound communication

Connectivity is required from a Console agent to the Console SaaS layer, to your cloud provider's publicly available resources, and to other essential components for day-to-day operations.

- Endpoints that an agent contacts in AWS
- Endpoints that an agent contacts in Azure
- Endpoints that an agent contacts in Google Cloud

Supported location for an agent

In standard mode, an agent is supported in the cloud or on your premises.

Console agent installation

You can install an agent using one of the following methods:

- From the Console
- From the AWS or Azure Marketplace
- From the Google Cloud SDK
- Manually using an installer on a Linux host in your data center or cloud
- Use the provided OVA in your VCenter environment.

Console agent upgrades

NetApp automatically upgrades your agent monthly.p.

User interface access

The user interface is accessible from the web-based console that's provided through the SaaS layer.

API endpoint

API calls are made to the following endpoint:
https://api.bluexp.netapp.com

Authentication

Authentication with auth0 or NetApp Support Site (NSS) logins. Identity federation is available.

Supported data services

All NetApp data services are supported. Learn more about NetApp data services.

Supported licensing options

Marketplace subscriptions and BYOL are supported with standard mode; however, the supported licensing options depends on which NetApp data service you are using. Review the documentation for each service to learn more about the available licensing options.

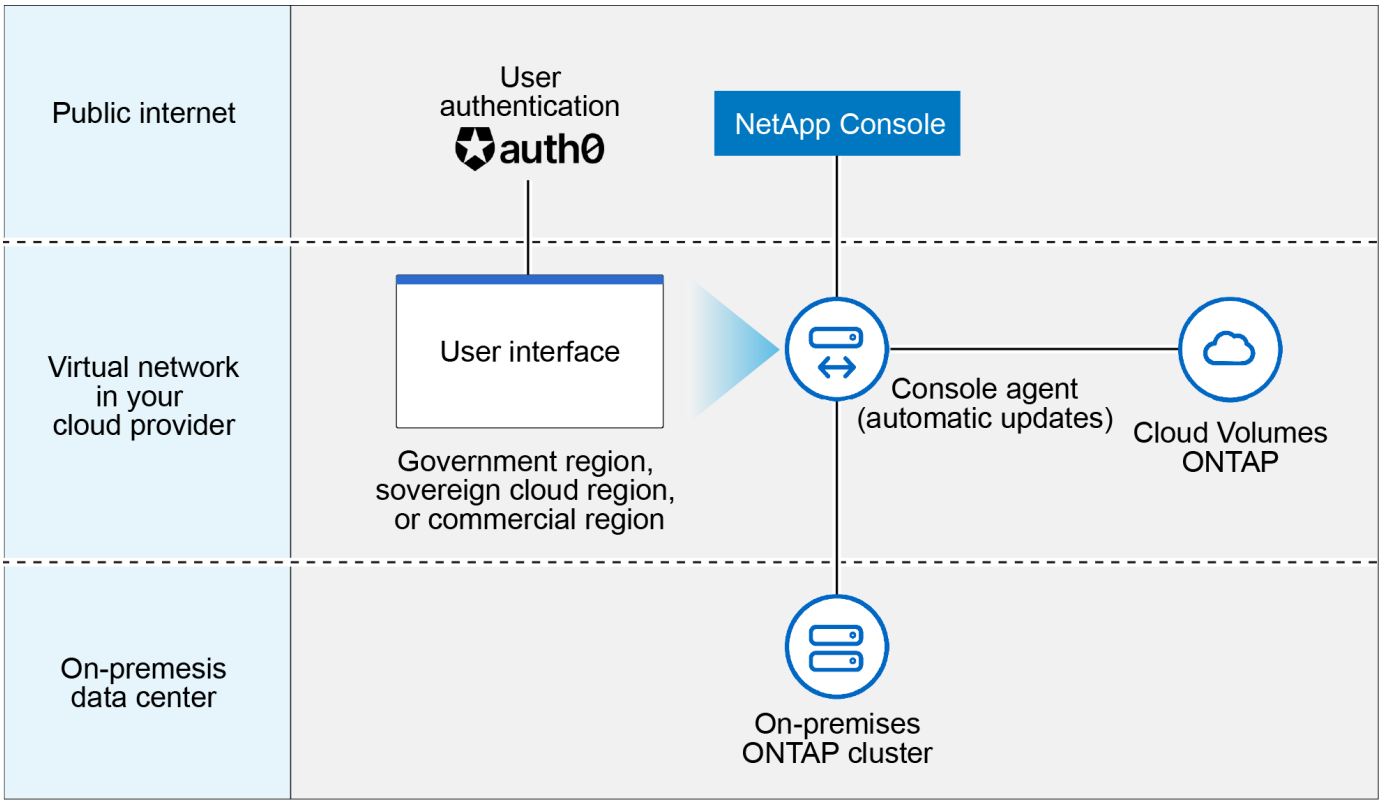
How to get started with standard mode

Go to the NetApp Console and sign up.

Learn how to get started with standard mode.

Restricted mode

The following image is an example of a restricted mode deployment.



The Console works as follows in restricted mode:

Outbound communication

An agent requires outbound connectivity to the Console SaaS layer for data services, software upgrades, authentication, and metadata transmission.

The Console SaaS layer does not initiate communication to an agent. Agents initiate all communication with the Console SaaS layer, pulling or pushing data as needed.

A connection is also required to cloud provider resources from within the region.

Supported location for an agent

In restricted mode, an agent is supported in the cloud: in a government region, sovereign region, or commercial region.

Console agent installation

You can install from the AWS or Azure Marketplace or a manual installation on your own Linux host or us a downloadable OVA in your VCenter environment.

Console agent upgrades

NetApp automatically upgrades your agent software with monthly updates.

User interface access

The user interface is accessible from an agent virtual machine that's deployed in your cloud region.

API endpoint

API calls are made to the agent virtual machine.

Authentication

Authentication is provided through auth0. Identity federation is also available.

Supported storage management and data services

The following storage and data services with restricted mode:

Supported services	Notes
Azure NetApp Files	Full support
Backup and recovery	Supported in Government regions and commercial regions with restricted mode. Not supported in sovereign regions with restricted mode. In restricted mode, NetApp Backup and Recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data Back up and restore of application data and virtual machine data is not supported.
NetApp Data Classification	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode.
Cloud Volumes ONTAP	Full support
Licenses and subscriptions	You can access license and subscription information with the supported licensing options listed below for restricted mode.
On-premises ONTAP clusters	Discovery with a Console agent and discovery without a Console agent (direct discovery) are both supported. When you discover an on-premises cluster without a Console agent, the Advanced view (System Manager) is not supported.
Replication	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode.

Supported licensing options

The following licensing options are supported with restricted mode:

- Marketplace subscriptions (hourly and annual contracts)

  Note the following:

  - For Cloud Volumes ONTAP, only capacity-based licensing is supported.
  - In Azure, annual contracts are not supported with government regions.

- BYOL

  For Cloud Volumes ONTAP, both capacity-based licensing and node-based licensing are supported with BYOL.

How to get started with restricted mode

You need to enable restricted mode when you create your NetApp Console organization.

If you don’t have an organization yet, you are prompted to create your organization and enable restricted mode when you log in to the Console for the first time from a Console agent that you manually installed or that you created from your cloud provider’s marketplace.

You cannot change the restricted mode setting after creating the organization.

Learn how to get started with restricted mode.

Service and feature comparison

The following table can help you quickly identify which services and features are supported with restricted mode.

Note that some services might be supported with limitations. For more details about how these services are supported with restricted mode, refer to the sections above.

Product area	NetApp data service or feature	Restricted mode
Storage This portion of the table lists support for storage systems management from the Console. It does not indicate the supported backup destinations for NetApp Backup and Recovery.	Amazon FSx for ONTAP	No
	Amazon S3	No
	Azure Blob	No
	Azure NetApp Files	Yes
	Cloud Volumes ONTAP	Yes
	Google Cloud NetApp Volumes	No
	Google Cloud Storage	No
	On-premises ONTAP clusters	Yes
	E-Series	No
	StorageGRID	No
Data Services	NetApp Backup and recovery	Yes View the list of supported backup destinations for ONTAP volume data
	NetApp Data Classification	Yes
	NetApp Copy and Sync	No
	NetApp Disaster Recovery	No
	NetApp Ransomware Resilience	No
	NetApp Replication	Yes
	NetApp Cloud Tiering	No
	NetApp Volume caching	No
	NetApp Workload factory	No

Product area	NetApp data service or feature	Restricted mode
Features	Alerts	No
	Digital Advisor	No
	License and subscription management	Yes
	Identity and access management	Yes
	Credentials	Yes
	Federation	Yes
	Lifecycle planning	No
	Multi-factor authentication	Yes
	NSS accounts	Yes
	Notifications	Yes
	Search	Yes
	Software updates	No
	Sustainability	No
	Audit	Yes

Manage NSS credentials associated with NetApp Console

Associate a NetApp Support Site account with your Console organization to enable key workflows for storage management. These NSS credentials are associated with the entire organization.

The Console also supports associating one NSS account per user account. Learn how to manage user-level credentials.

Overview

Associating NetApp Support Site credentials with your specific Console account serial number is required to enable the following tasks:

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that the Console can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Registering pay-as-you-go Cloud Volumes ONTAP systems

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Upgrading Cloud Volumes ONTAP software to the latest release

These credentials are associated with your specific Console account serial number. Users can access these credentials from **Support > NSS Management**.

Add an NSS account

You can add and manage your NetApp Support Site accounts for use with the Console from the Support Dashboard within the Console.

When you have added your NSS account, the Console uses this information for things like license downloads, software upgrade verification, and future support registrations.

You can associate multiple NSS accounts with your organization; however, you cannot have customer accounts and partner accounts within the same organization.

NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. Select **Add NSS Account**.
4. Select **Continue** to be redirected to a Microsoft login page.
5. At the login page, provide your NetApp Support Site registered email address and password.

   Upon successful login, NetApp will store the NSS user name.

   This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

   - If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu.

     Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems and when registering existing Cloud Volumes ONTAP systems.

- Launching Cloud Volumes ONTAP in AWS
- Launching Cloud Volumes ONTAP in Azure
- Launching Cloud Volumes ONTAP in Google Cloud
- Registering pay-as-you-go systems

Update NSS credentials

For security reasons, you must update your NSS credentials every 90 days. You'll be notified in the Console notification center if your NSS credential has expired. Learn about the Notification Center.

Expired credentials can disrupt the following, but are not limited to:

- License updates, which mean you won't be able to take advantage of newly purchased capacity.

- Ability to submit and track support cases.

Additionally, you can update the NSS credentials associated with your organization if you want to change the NSS account associated with your organization. For example, if the person associated with your NSS account has left your company.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ••• and then select **Update Credentials**.
4. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID as the identity provider for authentication services related to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password.

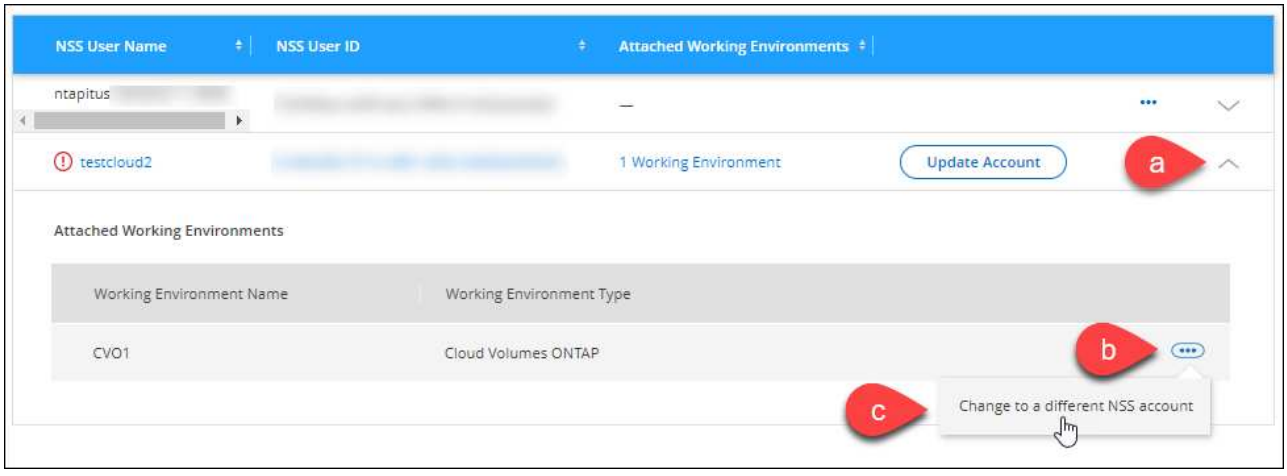
Attach a system to a different NSS account

If your organization has multiple NetApp Support Site accounts, you can change which account is associated with a Cloud Volumes ONTAP system.

You must first have associated the account with the Console.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. Complete the following steps to change the NSS account:
   a. Expand the row for the NetApp Support Site account that the system is currently associated with.
   b. For the system that you want to change the association for, select •••
   c. Select **Change to a different NSS account**.



   d. Select the account and then select **Save**.

Display the email address for an NSS account

For security, the email address associated with an NSS account is not displayed by default. You can view the email address and associated user name for an NSS account.

When you go to the NSS Management page, the Console generates a token for each account in the table. That token includes information about the associated email address. The token is removed when you leave the page. The information is never cached, which helps protect your privacy.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ••• and then select **Display Email Address**. You can use the copy button to copy the email address.

Remove an NSS account

Delete any of the NSS accounts that you no longer want to use with the Console.

You can't delete an account that is currently associated with a Cloud Volumes ONTAP system. You first need to attach those systems to a different NSS account.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to delete, select ••• and then select **Delete**.
4. Select **Delete** to confirm.

Learn about NetApp Console agents

You use a Console agent to connect NetApp Console to your infrastructure and securely orchestrate storage solutions across AWS, Azure, Google Cloud, or on-premises environments, as well as use data protection services.

A Console agent enables you to:

- Orchestrate storage management tasks from the NetApp Console such as provisioning Cloud Volumes ONTAP, setting up storage volumes, using data classification, and more.
- Authenticate using your cloud provider's IAM roles for subscription billing integration
- Use advanced data services (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience, and NetApp Cloud Tiering)
- Use the Console in restricted mode.

If you don't need advanced orchestration or data protection, you can centrally manage on-premises ONTAP clusters and cloud-native storage services without deploying an agent. Monitoring and data mobility tools are also available.

The following table shows which features and services you can use with and without a Console agent.

	Available with agent	Available without agent
Supported Storage systems:		
Amazon FSx for ONTAP	Yes (discovery and management features)	Yes (discovery only)
Amazon S3 storage	Yes	No
Azure Blob storage	Yes	Yes
Azure NetApp Files	Yes	Yes
Cloud Volumes ONTAP	Yes	No
E-Series systems	Yes	No
Google Cloud NetApp Volumes	Yes	Yes
Google Cloud storage buckets	Yes	No
StorageGRID systems	Yes	No
On-premises ONTAP cluster (advanced management and discovery)	Yes (advanced management and discovery)	No (basic discovery only)
Available storage management services:		
Alerts	Yes	No
Automation hub	Yes	Yes
Digital Advisor (Active IQ)	Yes	No
License and subscription management	Yes	No
Economic efficiency	Yes	No
Home page dashboard metrics	Yes[2]	No
Lifecycle planning	Yes	No[1]
Sustainability	Yes	No
Software updates	Yes	Yes

	Available with agent	Available without agent
NetApp Workloads	Yes	Yes
Available data services:		
NetApp Backup and Recovery	Yes	No
Data Classification	Yes	No
NetApp Cloud Tiering	Yes	No
NetApp Copy and Sync	Yes	No
NetApp Disaster Recovery	Yes	No
NetApp Ransomware Resilience	Yes	No
NetApp Volume Caching	Yes	No

[1] You can view Lifecycle planning without a Console agent, but a Console agent is required to initiate actions.

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

Console agents must be operational at all times

Console agents are a fundamental part of the NetApp Console. It's your responsibility (the customer) to ensure that relevant agents are up, operational, and accessible at all times. The Console can handle short agent outages, but you must fix infrastructure failures quickly.

This documentation is governed by the EULA. Operating the product outside the documentation may impact its functionality and your EULA rights.

Supported locations

You can install agents in the following locations:

- Amazon Web Services
- Microsoft Azure

  Deploy a Console agent in Azure in the same region as the Cloud Volumes ONTAP systems it manages. Alternatively, deploy it in the Azure region pair. This ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts. Learn how Cloud Volumes ONTAP uses an Azure Private Link

- Google Cloud

  To use the Console and data services with Google Cloud, deploy your agent in Google Cloud.

- On your premises

Communication with cloud providers

The agent uses TLS 1.3 for all communication to AWS, Azure, and Google Cloud.

Restricted mode

To use the Console in restricted mode, you install a Console agent and access the Console interface that's running locally on the Console agent.

Learn about NetApp Console deployment modes.

How to install a Console agent

You can install a Console agent directly from the Console, from your cloud provider's marketplace, or by manually installing the software on your own Linux host or in your VCenter environment.

- Learn about NetApp Console deployment modes
- Get started with NetApp Console in standard mode
- Get started with NetApp Console in restricted mode

Cloud provider permissions

You need specific permissions to create the Console agent directly from the NetApp Console and another set of permissions for the Console agent itself. If you create the Console agent in AWS or Azure directly from the Console, then the Console creates the Console agent with the permissions that it needs.

When using the Console in standard mode, how you provide permissions depends on how you plan to create the Console agent.

To learn how to set up permissions, refer to the following:

- Standard mode
  - Agent installation options in AWS
  - Agent installation options in Azure
  - Agent installation options in Google Cloud
  - Set up cloud permissions for on-premises deployments
- Set up permissions for restricted mode

To view the exact permissions that the Console agent needs for day-to-day operations, refer to the following pages:

- Learn how the Console agent uses AWS permissions
- Learn how the Console agent uses Azure permissions
- Learn how the Console agent uses Google Cloud permissions

It's your responsibility to update the Console agent policies as new permissions are added in subsequent releases. The release notes list new permissions.

Agent upgrades

NetApp updates agent software monthly to add features and improve stability. Some Console features, like Cloud Volumes ONTAP and on-premises ONTAP cluster management, rely on the Console agent version and settings.

When you install your agent in the cloud, the Console agent updates automatically if it has internet access.

Operating system and VM maintenance

Maintaining the operating system on the Console agent host is your (customer's) responsibility. For example, you (customer) should apply security updates to the operating system on the Console agent host by following your company's standard procedures for operating system distribution.

Note that you (customer) don't need to stop any services on the Console gent host when applying minor security updates.

If you (customer) need to stop and then start the Console agent VM, you should do so from your cloud provider's console or by using the standard procedures for on-premises management.

The Console agent must be operational at all times.

Multiple systems and agents

An agent can manage multiple systems and support data services in the Console. You can use a single agent to manage multiple systems based on deployment size and the data services you use.

For large-scale deployments, work with your NetApp representative to size your environment. Contact NetApp Support if you experience issues.

Here are a few examples of agent deployments:

- You have a multicloud environment (for example, AWS and Azure) and you prefer to have one agent in AWS and another in Azure. Each manages the Cloud Volumes ONTAP systems running in those environments.
- A service provider might use one Console organization to provide services for their customers, while using another organization to provide disaster recovery for one of their business units. Each organization needs its own agent.

Learn about NetApp Console identity and access management

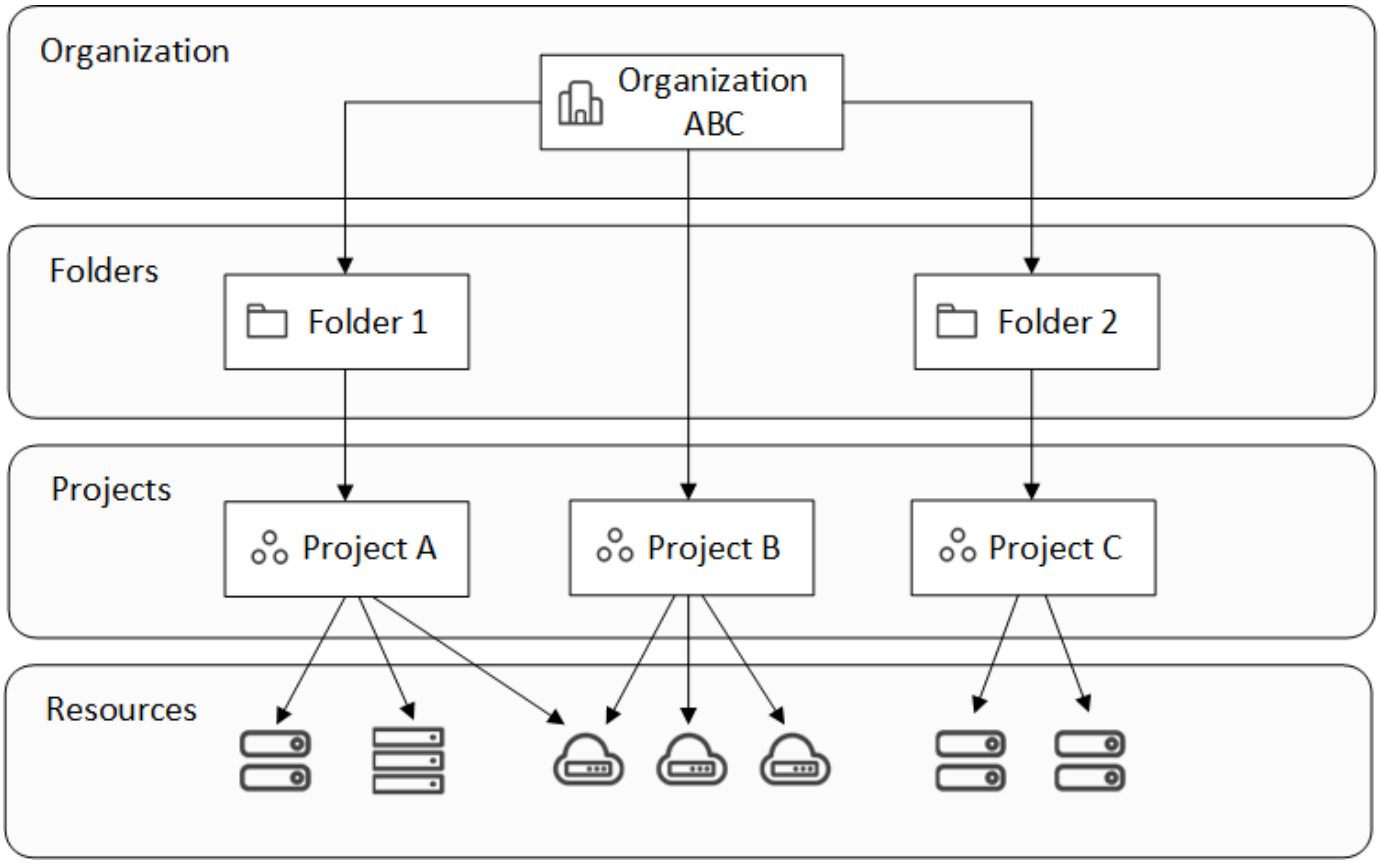
Use NetApp Console's Identity and Access Management (IAM) to organize your NetApp resources and control access according to your business structure—by location, department, or project.

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

Copyright information

Trademark information