# Administer BlueXP

BlueXP setup and administration

NetApp
August 29, 2025

# Table of Contents

Administer BlueXP . . . 1

Identity and access management . . . 1

Learn about BlueXP identity and access management . . . 1

Get started with BlueXP identity and access management . . . 8

Organize your resources in BlueXP IAM with folders and projects . . . 9

Add BlueXP members and service accounts . . . 14

Use roles to manage user access to resources . . . 19

Manage the resource hierarchy in your BlueXP organization . . . 20

Associate a BlueXP Connector with other folders and projects . . . 23

Switch between BlueXP organizations, projects, and Connectors . . . 24

Organization and project IDs . . . 26

Monitor or audit IAM activity from the BlueXP timeline . . . 27

BlueXP access roles . . . 28

Identity federation . . . 40

Enable single sign-on by using identity federation with BlueXP . . . 40

Domain verification . . . 42

Configure federations . . . 43

Manage federations in BLueXP . . . 50

Import your federation to BlueXP . . . 52

Connectors . . . 52

Maintain the Connector VM and operating system . . . 52

Install a CA-signed certificate for web-based console access . . . 55

Configure a Connector to use a proxy server . . . 57

Require the use of IMDSv2 on Amazon EC2 instances . . . 64

Manage connector upgrades . . . 66

Work with multiple Connectors . . . 68

Troubleshoot the Connector . . . 69

Uninstall and remove the Connector . . . 72

Default configuration for the Connector . . . 74

Enforce ONTAP permissions for ONTAP Advanced View (ONTAP System Manager) . . . 76

Credentials and subscriptions . . . 77

AWS . . . 77

Azure . . . 91

Google Cloud . . . 105

Manage NSS credentials associated with BlueXP . . . 111

Manage credentials associated with your BlueXP login . . . 116

Monitor BlueXP operations . . . 118

Audit user activity from the BlueXP timeline . . . 118

Monitor activities using the Notification Center . . . 119

# Administer BlueXP

## Identity and access management

### Learn about BlueXP identity and access management

BlueXP identity and access management (IAM) enables you to organize and control access to your NetApp resources. You can organize your resources according to your organization's hierarchy. For example, you can organize resources by geographical location, site, or business unit. You can then assign IAM roles to members at specific parts of the hierarchy, which prevents access to resources in other parts of the hierarchy.

- Learn about BlueXP deployment modes

#### How BlueXP IAM works

BlueXP IAM lets you grant resource access by assigning users access roles to specific parts of the hierarchy. For example, a member can be assigned the Folder or project admin role for a project with five resources.

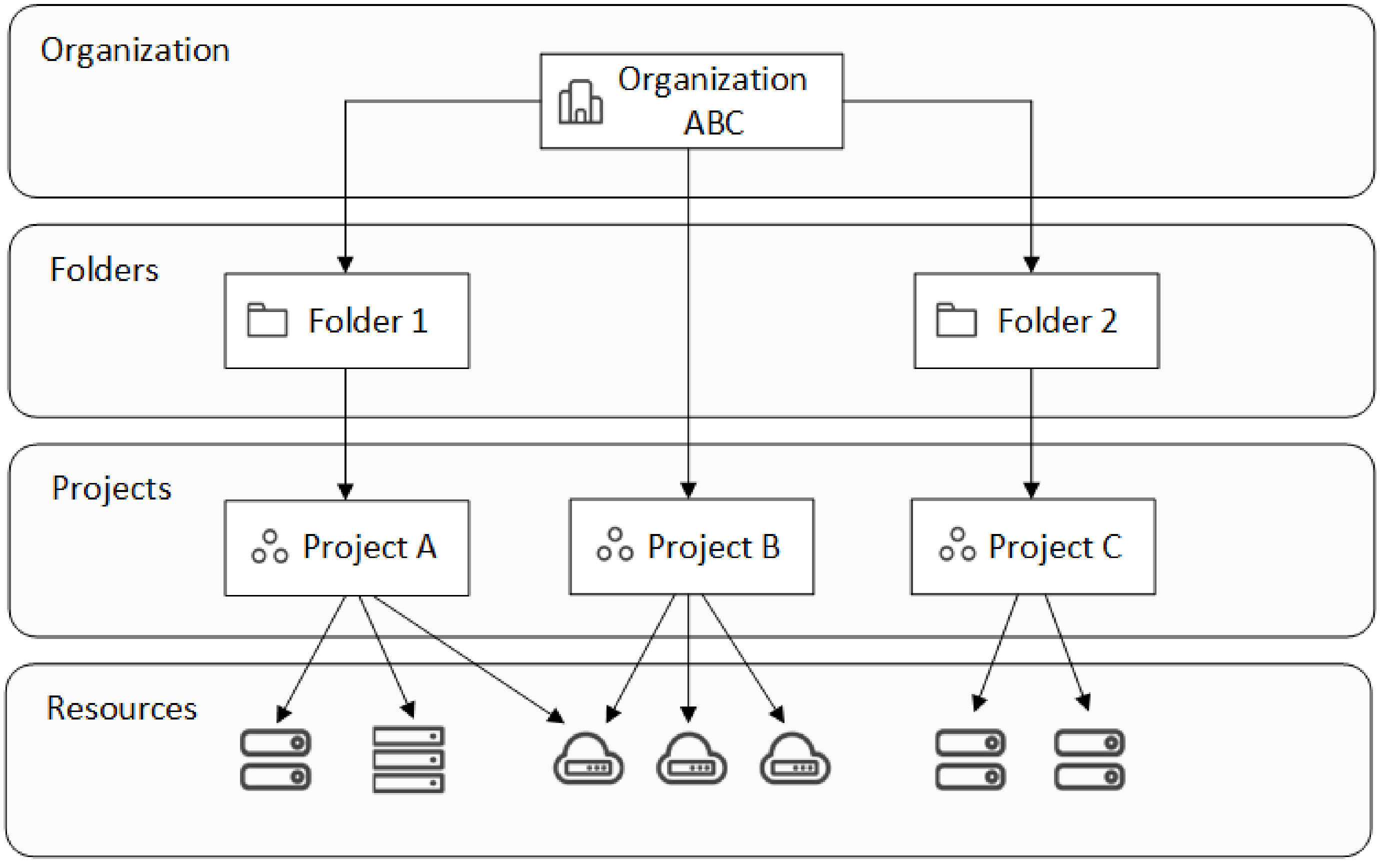
When using BlueXP IAM, you'll manage the following components:

- The organization
- Folders
- Projects
- Resources
- Members
- Roles and permissions
- Connectors

BlueXP resources are organized hierarchically:

- The organization is the top of the hierarchy.
- Folders are children of the organization or of another folder.
- Projects are children of the organization or of a folder.
- Resources are associated with one or more folders or projects.

The following image illustrates this hierarchy at a basic level.



#### Organization

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

#### Folders

A *folder* enables you to group related projects together and separate them from other projects in your organization. For example, a folder might represent a geographical location (EU or US East), a site (London or Toronto), or a business unit (engineering or marketing).

olders can contain projects, other folders, or both. Creating folders is optional.

#### Projects

A *project* represents a workspace in BlueXP that organization members access from the BlueXP canvas in order to manage resources. For example, a project can include a Cloud Volumes ONTAP system, an on-premises ONTAP cluster, or an FSx for ONTAP file system.

An organization can have one or many projects. A project can reside directly underneath the organization or within a folder.

#### Resources

A *resource* is a working environment that you created or discovered in BlueXP.

When you create or discover a resource, the resource is associated with the currently selected project. That might be the only project that you want to associate this resource with. But you can choose to associate the resource with additional projects in your organization.

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

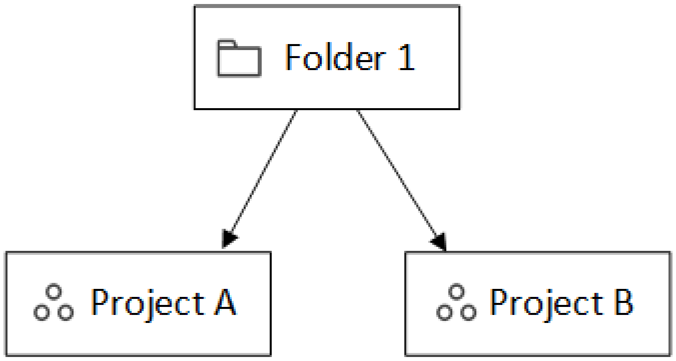
> You can also associate a Connector with another folder or project in your organization. Learn more about using Connectors with BlueXP IAM.

### When to associate a resource with a folder

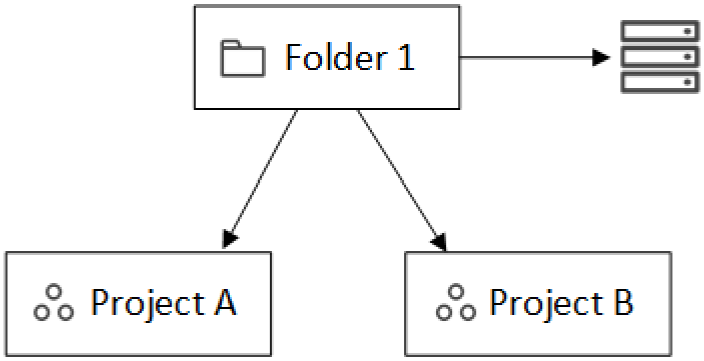
You also have the option to associate a resource with a folder, but this is optional and meets the needs of a specific use case.

An *Organization administrator* might associate a resource with a folder to allow a *Folder or project administrator* to link that resource to the appropriate projects in the folder.

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

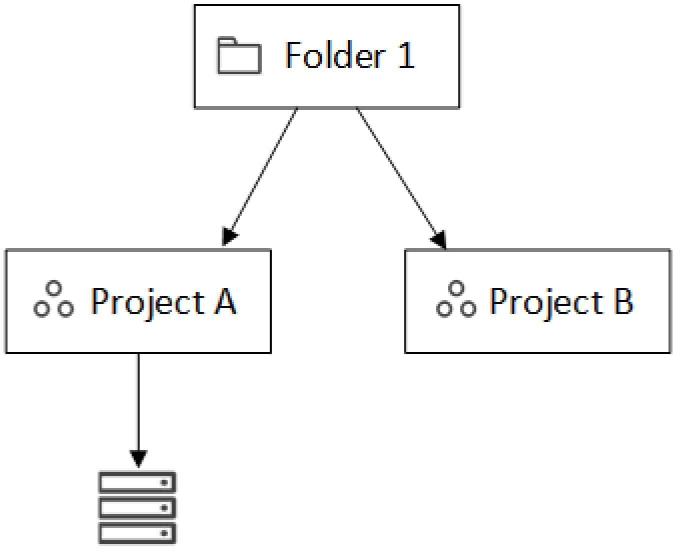


The *Organization admin* can associate a resource with the folder:



Associating a resource with a folder doesn't 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.

#### 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.

Each organization includes at least one user with the *Organization admin* role (BlueXP automatically assigns this role to the user who creates the organization). You can add other members to the organization and assign different permissions across different levels of the resource hierarchy.

#### Roles and permissions

In BlueXP IAM, you don’t grant permissions directly to organization members. Instead, you grant each member a role. A role contains a set of permissions that enables a member to perform specific actions at a specific level of the resource hierarchy.

Granting permissions at a specific hierarchy level restricts access to the resources a member needs and the services that they can use with those resources.

### Where you can assign roles in the hierarchy

When you associate a member with a role, you need to select 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.

### Role inheritance

When you assign a role, the role is inherited down the organization hierarchy:

**Organization**

Granting a member an access role at the organization level gives them permissions to all folders, projects, and resources.

**Folders**

When you grant an access role at the folder level, all folders, projects, and resources in the folder inherit that role.

For example, if you assign a role at the folder level and that folder has three projects, the member will have permissions to those three projects and any associated resources.

**Projects**

When you grant an access role at the project level, all resources associated with that project inherit that role.

### Multiple roles

You can assign each organization member a role at different levels of the organization hierarchy. It can be the same role or a different role. For example, you can assign a member role A for project 1 and project 2. Or you can assign a member role A for project 1 and role B for project 2.

### Access roles

BlueXP supports several predefined roles that you can assign to the members of your organization.

Learn about access roles.

#### Connectors

When an *Organization admin* creates a Connector, BlueXP automatically associates that Connector with the organization and the currently selected project. The *Organization admin* automatically has access to that Connector from anywhere in the organization. But if you have other members in your organization with different roles, those members can only access that Connector from the project in which it was created, unless you associate that Connector with other projects.

You make a Connector available for another project in these cases:

- You want to allow members in your organization to use an existing Connector to create or discover additional working environments in another project
- You associated an existing resource with another project and that resource is managed by a Connector

  If a resource that you associate with an additional project is discovered using a BlueXP Connector, then you also need to associate the Connector with the project that the resource is now associated with.Otherwise, the Connector and its associated resource aren’t accessible from the BlueXP canvas by members who don’t have the *Organization admin* role.

You can create an association from the **Connectors** page in BlueXP IAM:

- Associate a Connector with a project

  When you associate a Connector with a project, that Connector is accessible from the BlueXP canvas when viewing the project.

- Associate a Connector with a folder

  Associating a Connector with a folder doesn’t automatically make that Connector accessible from all projects in the folder. Organization members can’t access a Connector from a project until you associate the Connector with that specific project.

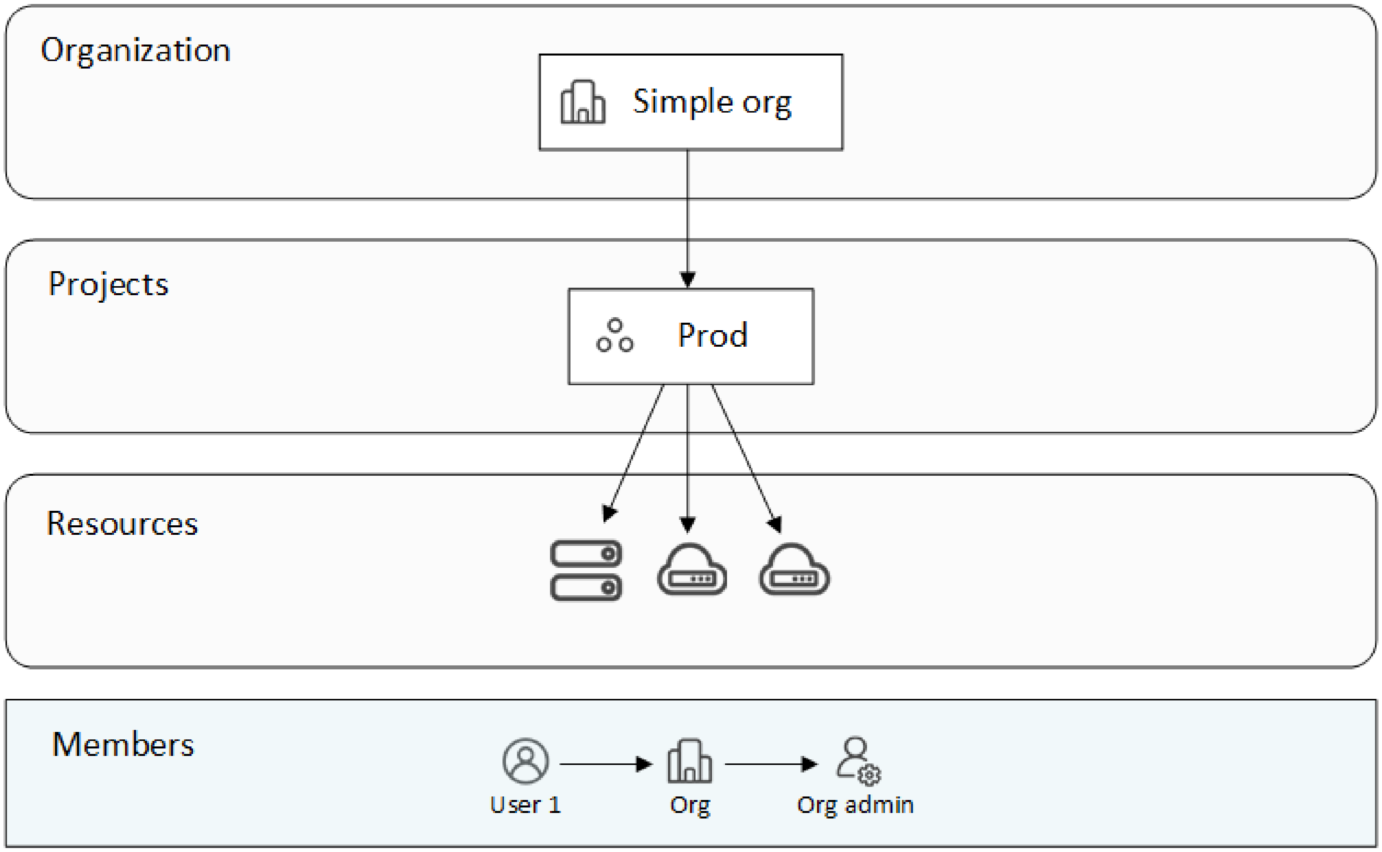
  An *Organization admin* might associate a Connector with a folder so that the *Folder or project admin* can make the decision to associate that Connector with the appropriate projects that reside in the folder.

### IAM examples

These examples demonstrate how you might set up your organization.

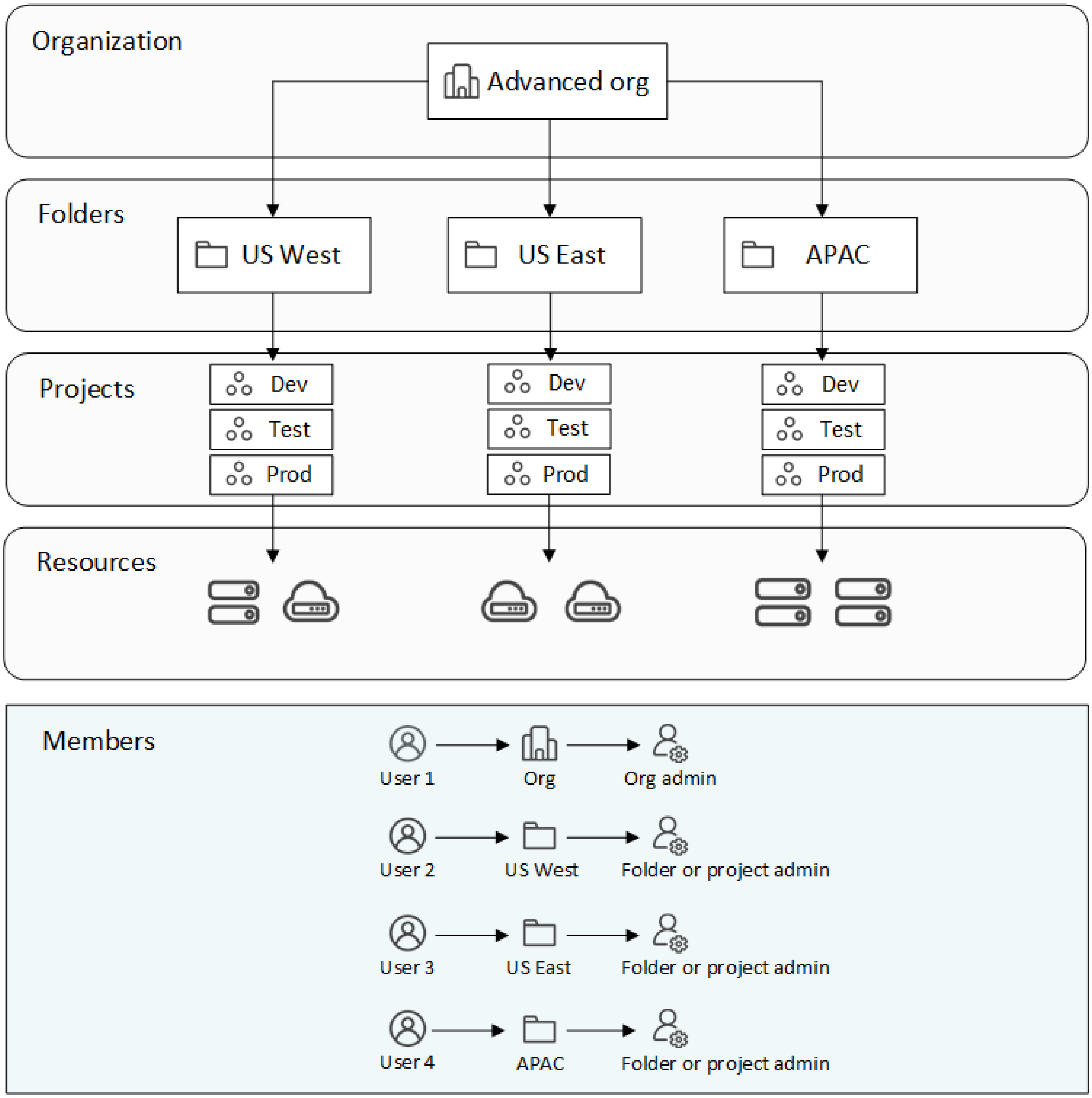
#### Simple organization

The following diagram shows a simple example of an organization that uses the default project and no folders. A single member manages the entire organization.



#### Advanced organization

The following diagram shows an organization that uses folders to organize the projects for each geographic location in the business. Each project has its own set of associated resources. The members include an organization admin and an admin for each folder in the organization.



### What you can do with BlueXP IAM

The following examples describe how you might use IAM to manage your BlueXP organization:

- Grant specific roles to specific members so that they can only complete the required tasks.
- Modify member permissions because they moved departments or because they have additional responsibilities.
- Remove a user who left the company.
- Add folders or projects to your hierarchy because a new business unit has added NetApp storage.
- Associate a resource with another project because that resource has capacity that another team can utilize.

- View the resources that a member can access.
- View the members and resources associated with a specific project.

### Where to go next

- Get started with BlueXP IAM
- Organize your resources in BlueXP with folders and projects
- Manage BlueXP members and their permissions
- Manage the resource hierarchy in your BlueXP organization
- Associate Connectors with folders and projects
- Switch between BlueXP projects and organizations
- Rename your BlueXP organization
- Monitor or audit IAM activity
- BlueXP access roles
- Learn about the API for BlueXP IAM

## Get started with BlueXP identity and access management

When you sign up to BlueXP, you’re prompted to create a new organization. The organization includes one member (an Organization admin) and one default project. To set up BlueXP 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 must have **Organization admin** permissions to administer the entire organization from BlueXP IAM. If you have **Folder or project admin** permissions, you can only administer the folders and projects for which you have permissions.

Follow these steps to set up a new BlueXP organization. The order in which you complete these steps might be different, depending on your organization’s needs.

### 1 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.

### 2 Associate members with your organization

If multiple people in your business need access to BlueXP, associate their user accounts with your organization and assign the necessary permissions. You also have the option to add service accounts to your organization.

Learn how to manage members and their permissions.

### 3 Add or discover resources

Add or discover resources in BlueXP as *the working environments*. Organization members manage a working environment, which represents a storage system, 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**

When you create or discover a resource in BlueXP, that resource is automatically associated with the project that was selected when you created or discovered the working environment. If you want to make that resource available to another project in your organization, then you'll need to create an association between them. If a Connector manages the resource, associate the Connector with the respective project.S

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

**Related information**

- Learn about BlueXP identity and access management
- Learn about the API for BlueXP IAM

## Organize your resources in BlueXP IAM with folders and projects

BlueXP identity and access management (IAM) enables you to organize your NetApp resources using projects and folders. A *project* represents a workspace in BlueXP that organization members access to manage *resources* (for example, a Cloud Volumes ONTAP system). A *folder* groups related projects together. After you organize your resources into folders and projects, you can grant granular access to resources by providing organization members with permissions to specific folders and projects.

### Add a folder or project

When you create your BlueXP organization, it includes a single project. You can create additional projects to manage your organization's resources. You can optionally create folders to group related projects together.

**About this task**

Your organization's resource hierarchy can have up to 7 levels, with nested folders down to 6 levels and projects at the seventh level.

The following image illustrates the maximum depth of your organization's resource hierarchy:

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. From the **Organization** page, select **Add folder or project**.
3. Select **Folder** or **Project**.
4. Provide details about the folder or project:
   - **Name and location**: Enter a name and choose a location in the hierarchy for the folder or project. A folder or project can reside directly underneath the organization or within a folder.
   - **Resources**: Select the resources that you want to associate with this folder or project.

     You can select resources associated with the parent folder or project: all resources for an organization parent, or folder-specific resources for a folder parent.

     Learn when you might associate a resource with a folder.
   - **Access**: View the members who will have access to the folder or project based on the existing permissions already defined in your resource hierarchy.

     If needed, select **Add a member** to specify additional organization members who should have access to the folder or project and then select a role. A role defines the permissions that members have for the folder or project.

     Learn about predefined IAM roles.
5. Select **Add**.

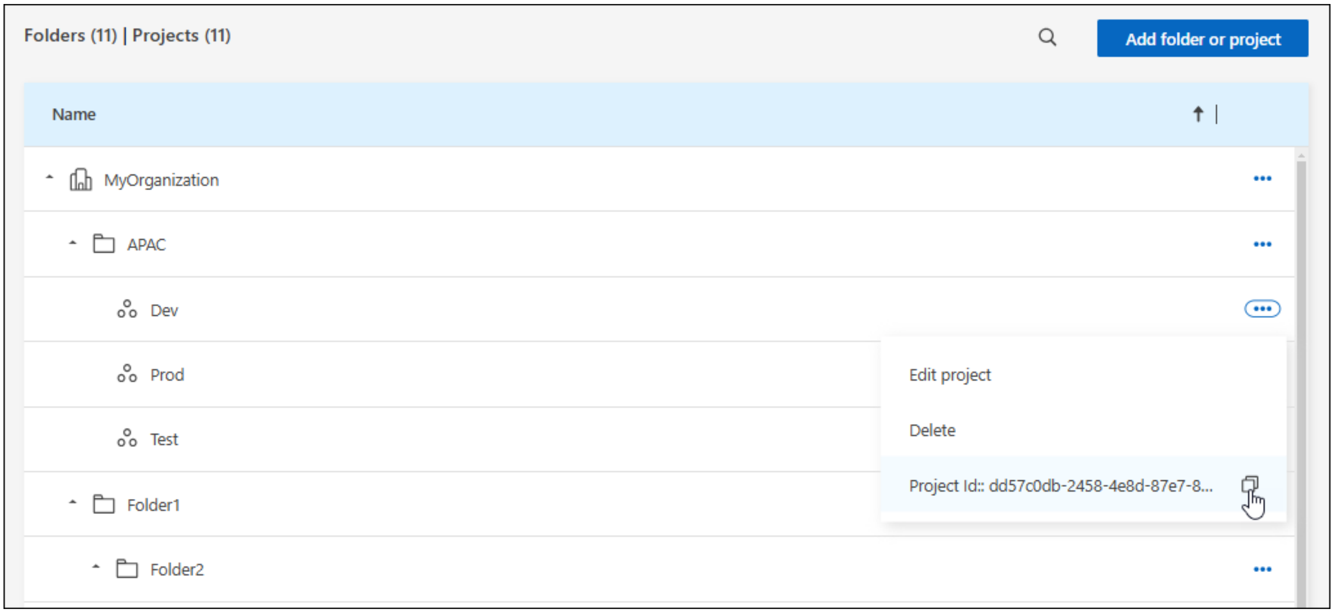
### Obtain the ID for a project

If you're using the BlueXP API, you might need to obtain the ID for a project. For example, when creating a Cloud Volumes ONTAP working environment.

**Steps**

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

   The system displays the project ID.
2. To copy the ID, select the copy button.



Project Id:: dd57c0db-2458-4e8d-87e7-8...

### Rename a folder or project

If needed, you can change the name of your folders and projects.

#### 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

You can delete the folders and projects that you no longer need.

#### Before you begin

- The folder or project must not have any associated resources. Learn how to disassociate resources.
- A folder must not contain any subfolders or projects. You need to delete those folders and projects first.

#### Steps

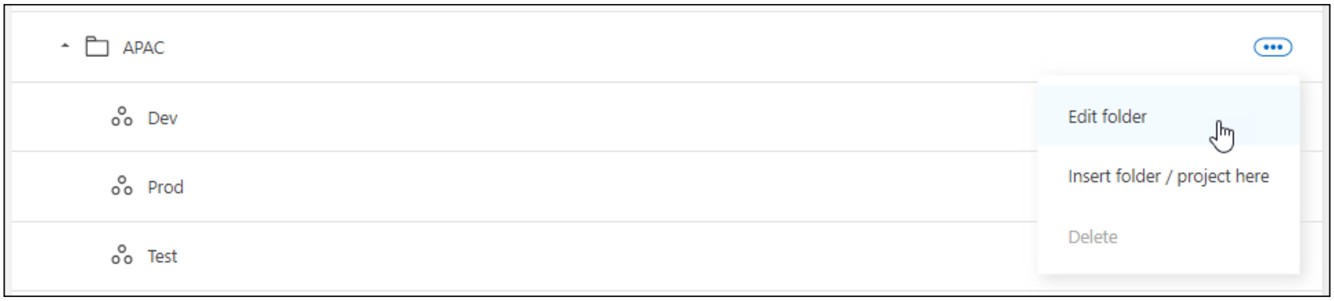
1. From the **Organization** page, navigate to a project or folder in the table, select ••• and then select **Delete**.
2. Confirm that you want to delete the folder or project.

### View the resources associated with a folder or project

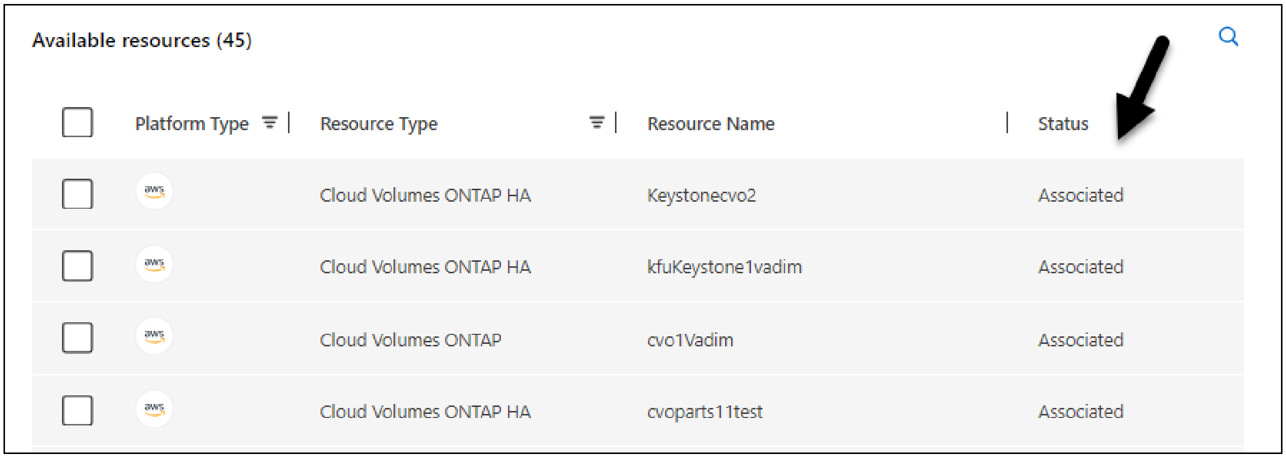
To verify that your resources are organized appropriately and accessible to the right members in your organization, you can view which resources and members are associated with a folder or project.

#### 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.



Available resources (45)

| □ | Platform Type | Resource Type | Resource Name | Status |
|---|---|---|---|---|
| □ | aws | Cloud Volumes ONTAP HA | Keystonecvo2 | Associated |
| □ | aws | Cloud Volumes ONTAP HA | kfuKeystone1vadim | Associated |
| □ | aws | Cloud Volumes ONTAP | cvo1Vadim | Associated |
| □ | aws | Cloud Volumes ONTAP HA | cvoparts11test | Associated |

### Modify the resources associated with a folder or project

Members with permissions for a folder or project can access its associated resources.

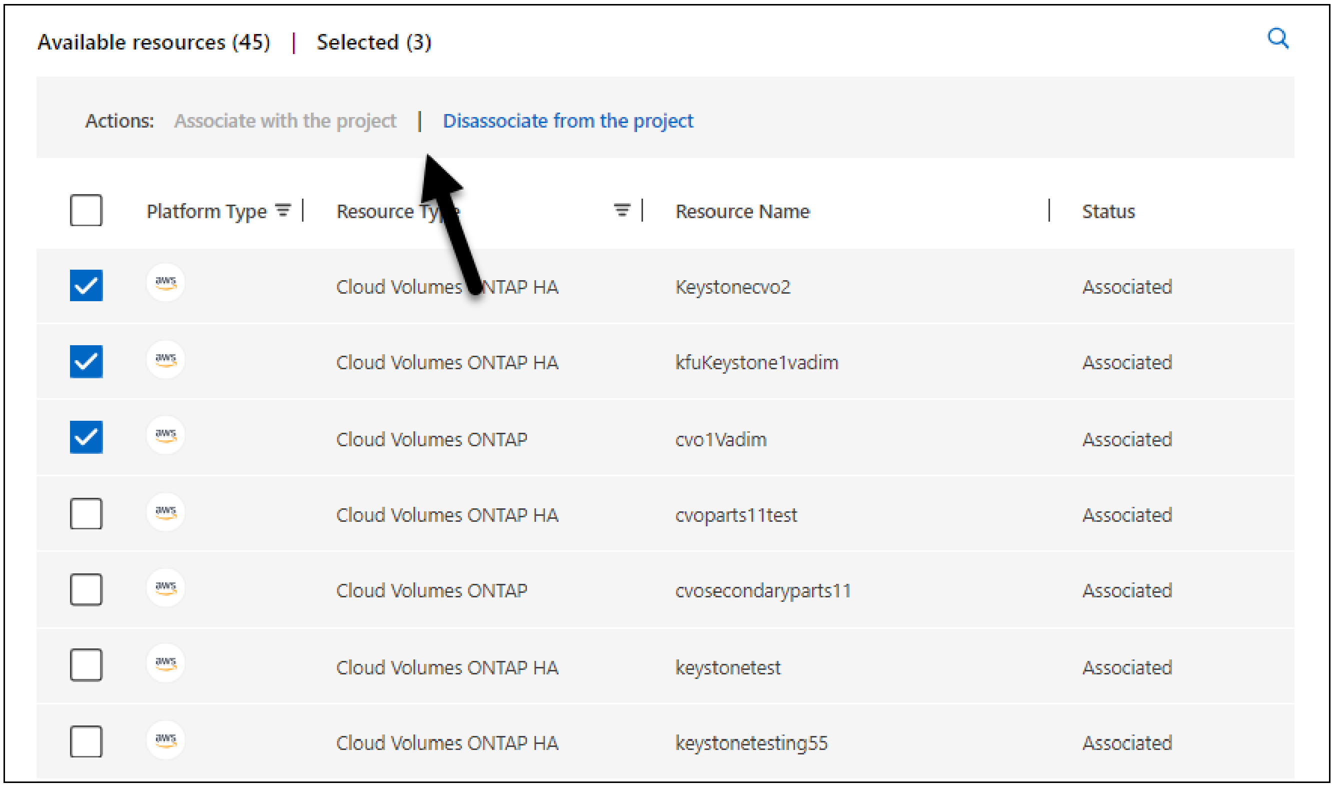
#### Before you begin

Learn when you might associate a resource with a folder.

#### 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. Depending on the resources that you selected, select either **Associate with the project** or **Disassociate from the project**.



Available resources (45) | Selected (3)

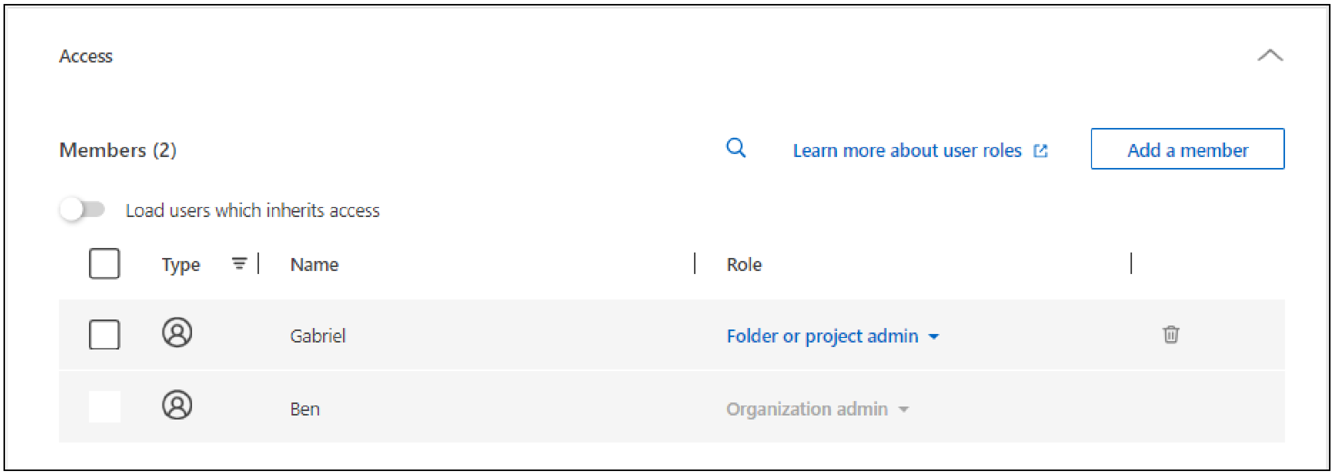
Actions: Associate with the project | Disassociate from the project

| ☐ | Platform Type | Resource Type | Resource Name | Status |
|---|---|---|---|---|
| ☑ | aws | Cloud Volumes ONTAP HA | Keystonecvo2 | Associated |
| ☑ | aws | Cloud Volumes ONTAP HA | kfuKeystone1vadim | Associated |
| ☑ | aws | Cloud Volumes ONTAP | cvo1Vadim | Associated |
| ☐ | aws | Cloud Volumes ONTAP HA | cvoparts11test | Associated |
| ☐ | aws | Cloud Volumes ONTAP | cvosecondaryparts11 | Associated |
| ☐ | aws | Cloud Volumes ONTAP HA | keystonetest | Associated |
| ☐ | aws | Cloud Volumes ONTAP HA | keystonetesting55 | Associated |

5. Select **Apply**

### View members associated with a folder or project

- Select **Access** to view the members who have access to the folder or project.



Access

Members (2)

Load users which inherits access

| ☐ | Type | Name | Role |
|---|---|---|---|
| ☐ | ○ | Gabriel | Folder or project admin ▾ |
|  | ○ | Ben | Organization admin ▾ |

### Modify member access to a folder or project

Modify member access to ensure the right members can access the associated resources.

Member access provided at a higher hierarchy level cannot be changed at lower levels. You need to switch to that part of the hierarchy and update the member's permissions there. Alternatively, you can manage permissions from the Members page.

Learn more about role inheritance.

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

## Add BlueXP members and service accounts

BlueXP identity and access management (IAM) enables you to add members to your organization and assign them one or more roles across your resource hierarchy. A *role* contains a set of permissions that enables a member to perform specific actions at a specific level of the resource hierarchy. You can associate new user accounts and service accounts, manage member roles, and more.

> Ensure two members have the Organization admin role to avoid losing access to your BlueXP organization.

To manage users and their permissions, you must be assigned one of the following roles:

- Organization admin

  Users with this role can manage all members

- Folder or project admin

  Users with this role can manage members only of a designated folder or project

  ```
  _Folder or project admin_ can view all members on the *Members* page but
  manage permissions only for folders and projects they have access to.
  xref:{relative_path}reference-iam-predefined-roles.html[Learn more about
  the actions that a _Folder or project admin_ can complete].
  ```

### Add members to your organization

You can add two types of members to your organization: a user account and a service account. A service account is used by applications to perform tasks via the BlueXP API without human intervention. A user account is typically used by a person to log in to BlueXP and manage resources.

Users must sign up for BlueXP before being added to an organization or assigned a role. However, you can create service accounts directly from BlueXP.

To manage users and their permissions, you must have the **Organization admin** role or the **Folder or project admin** role. Remember that users with the **Folder or project admin** role can only manage members for the folder or projects of which they have admin permissions.

**User account**

**Steps**

1. Direct the user to visit NetApp BlueXP website to sign up.

   Once users sign up, they complete the **Sign up** page, check their email, and log in. If BlueXP prompts users to create an organization, they close it and notify you of their account creation. You can then add the user to your existing BlueXP organization.

   Learn how to sign up to BlueXP.

2. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
3. Select **Members**.
4. Select **Add a member**.
5. To add the member, complete the steps in the dialog box:
   - **Entity Type**: Keep **User** selected.
   - **User's email**: Enter the user's email address that is associated with the BlueXP login that they created.
   - **Select an organization, folder, or project**: 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 admin permissions.
     - Selecting an organization or folder grants the member permissions to all its contents.
   - **Select a category** and 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.
     - If you selected a folder or project, you can choose from any role other than **Organization admin**.

       Learn about access roles.
   - **Add role**: If you want to provide access to additional folders or projects within your organization or grant the user further permissions in the selected area, select **Add role**, specify another folder or project or a different role category and then choose a role.
6. Select **Add**.

   NetApp BlueXP sends the user an email with information on how to access BlueXP.

**Service account**

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select **Members**.
3. Select **Add a member**.
4. To add the member, complete the steps in the dialog box:
   - **Entity Type**: Select **Service account**.

  - **Service account name**: Enter a name for the service account.
  - **Select an organization, folder, or project**: 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 admin permissions.
    - Selecting an organization or folder grants the member permissions to all its contents.
  - **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.
    - If you selected a folder or project, you can choose from any role other than **Organization admin**.

      Learn about predefined IAM roles.
  - **Add role**: If you want to provide access to additional folders or projects within your organization or grant the user further permissions in the selected area, select **Add role**, specify another folder or project or a different role category and then choose a role.

5. Download or copy the client ID and client secret.

   BlueXP displays the client secret only once. Copy or download it and store it securely.Note that you can recreate the client ID and client secret later on as needed.

6. Select **Close**.

### View organization members

You can view a list of all members in your BlueXP organization. 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 BlueXP resources.

You can view both user accounts and service accounts from the **Members** page.

ⓘ You can also view all of the members associated with a specific folder or project. Learn more.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
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**.

### Remove a member from your organization

You might need to remove a member from your organization—for example, if they leave your company.

Removing a member removes their permissions but keeps their BlueXP and NetApp Support Site accounts.

**Steps**

1. From the **Members** page, navigate to a member in the table, select ••• then select **Delete user**.
2. Confirm that you want to remove the member from your organization.

### Recreate the credentials for a service account

Create new credentials if lost or when updating security credentials becomes necessary.

**About this task**

When you recreate the credentials, you delete the existing credentials for the service account and create new ones. You cannot use the previous credentials.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
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.

   BlueXP displays the client secret only once. Copy or download it and store it securely.

### Manage a user’s multi-factor authentication (MFA)

If a user has loses access to their MFA device, you can either remove or disable their MFA configuration.

If you remove their MFA configuration, the user needs to set up MFA again when they log in to BlueXP. If the user has only lost access to their MFA device temporarily, they can use the recovery code that they saved when they set up MFA to log in to BlueXP.

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 BlueXP.

> ⓘ You must have an email address in the same domain as the affected user to manage that user’s multi-factor authentication.

**Steps**

1. In the upper right of the console, select ⚙ > **Identity & Access Management**.
2. Select **Members**.

   The members of your organization appear in the **Members** table.

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.

**Related information**

- Learn about BlueXP identity and access management

- Get started with BlueXP IAM
- Predefined BlueXP IAM roles
- Learn about the API for BlueXP IAM

## Use roles to manage user access to resources

Within BlueXP, you can assign roles to users based on what they need to do and where.

Users with the **Organization admin** or **Folder or project admin** role have the responsibility of assigning roles to other users. You can assign access roles on a project or folder basis. For example, you can assign a user the Ransomware protection admin role for one project and the SnapCenter admin role for a different project. Alternatively, if a user needs the Classification admin role for all projects within a specific folder, you can give them this role at the folder level.

Use access roles to assign access to storage resources based on the specific tasks that users need to perform. For example, if a user needs to interact with ransomware protection services, they must be given an access role that includes either viewing or administrative permissions for the ransomware protection service for the project for which the access role is granted.

Assign roles to users based on your IAM strategy for enhanced security. IAM roles ensure users have only the access they need.

> Remember that you can’t directly grant access to resources. Assign resources to projects first. Consider setting up your resource hierarchy before assigning users access. Learn how to organize your resources in BlueXP IAM with folders and projects.

### View roles(s) assigned to a member

When you add a member to your organization, you are prompted to assign them a role. You can members to 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.

### 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 protection admin role for an organization. In that example, the user would be able to perform ransomware protection tasks on all projects within your organization.

Your access role strategy should align with the way you have organized your NetApp resources.

> A member who is assigned the Organization admin role can’t be assigned any additional roles. They already have permissions across the entire organization. A member with the Folder or project role can’t be assigned any other roles within the folder or project where they have that role already. Both of these roles provide access to all services within the scope that they are assigned.

**Steps**

1. From the **Members** page, navigate to a member in the table, select ••• and then select **Add a role**.
2. 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.

Learn about access roles.
* **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.

1. Select **Add new roles**.

### Change a member’s assigned role

You can change the assigned roles for a member should you need to adjust the access for a user.

> 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. 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 change the member’s assigned role and select **View** in the **Role** column to view the roles assigned to this member.
3. 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 this role to a role within the same role category. For example, you can change from one data service role to another. Confirm the change.
   b. To unassign a member’s role, select 🗑 next to the role to unassign the member the respective role. You’ll be asked to confirm the removal.

## Manage the resource hierarchy in your BlueXP organization

When you use associate a member with your organization, you provide permissions at the organization, folder, or project level. To ensure that those members have permissions to access the right resources, you'll need to manage the resource hierarchy of your organization by associating resources with specific projects and folders. A *resource* is a storage resource that BlueXP already manages or is aware of.

#### View the resources in your organization

You can view both discovered and undiscovered resources associated with your organization. Undiscovered resources are storage resources identified by digital advisor but not added as working environments.

> ⓘ The IAM resources page excludes Amazon FSx for NetApp ONTAP resources because you cannot associate them with an IAM role. View these resources on their respective canvas or from workloads.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select **Resources** to view the Resources page.
3. Select **Advanced Search & Filtering**.
4. Use any of the available options to find the resource that you're looking for:
   - **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.

**Before you begin**

You should understand how resource association works. Learn about resources, including when to associate a resource with a folder.

**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 in BlueXP.
   - If you associated the resource with a folder, a *Folder or project admin* can now access the resource

from within BlueXP IAM. Learn about associating a resource with a folder.

### After you finish

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

Learn how to associate a Connector with a folder or project.

## View the folders and projects associated with a resource

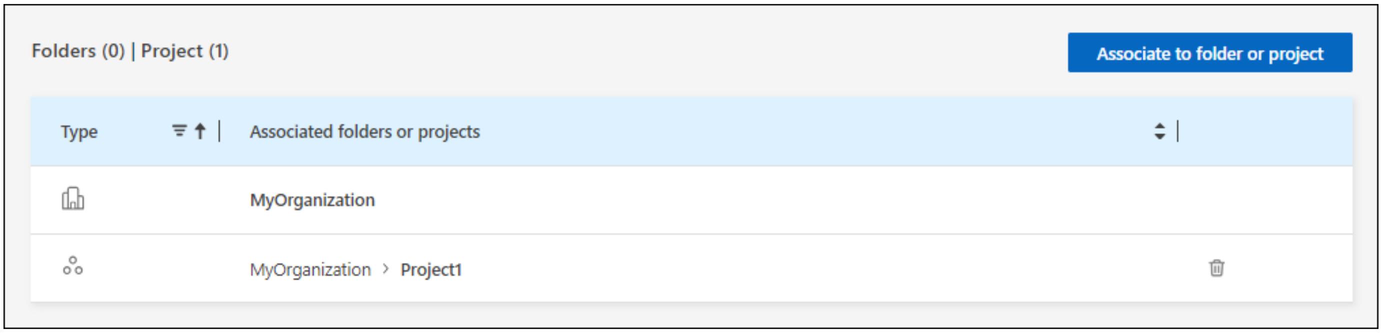
To identify where a resource is available in your organization’s hierarchy, you can view the folders and projects that are associated with that resource.

> If you need to determine 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.



Folders (0) | Project (1)

| Type | Associated folders or projects | |
|---|---|---|
| | MyOrganization | |
| | MyOrganization › Project1 | 🗑 |

> If you need to determine 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.

## Remove a resource from a folder or project

To remove a resource from a folder or project, you need to remove the association between the folder or project and the resource. Removing the association prevents members from managing the resource in the folder or project.

> If you want to remove a discovered resource from the entire organization, you need to remove the working environment from the BlueXP canvas.

### Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **View details**.
2. For the folder or project for which you want to remove the resource, select 🗑
3. Confirm that you want to remove the association by selecting **Delete**.

**Related information**

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

## Associate a BlueXP Connector with other folders and projects

```
When an _Organization admin_ creates a Connector, it is automatcially
associated with currently selected project within the organization.
Although someone with the _Organization admin_  can access to that
Connector from anywhere in the organization. Other members in your
organization can only access that Connector from the project in which it
was created, unless you associate that Connector with other projects.
```

**Before you begin**

You should understand how Connector association works. Learn about using Connectors with BlueXP IAM.

**About this task**

- When a *Folder or project admin* views the **Connectors** page, the page displays all Connectors in the organization. However, a member with this role can only view and associate Connectors with the folders and projects for which they have permissions. Learn more about the actions that a *Folder or project admin* can complete.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select **Connectors**.
3. From the table, find the Connector that you want to associate.

   Use the search above the table to find a specific Connector or filter the table by resource hierarchy.

4. To view the folders and projects linked to the Connector, select ••• and then select **View details**.

   BlueXP displays details about the folders and projects that the Connector is associated with.

5. Select **Associate to folder or project**.
6. Select a folder or project and then select **Accept**.
7. To associate the Connector with an additional folder or project, select **Add a folder or project** and then select the folder or project.
8. Select **Associate Connector**.

**After you finish**

If you want to associate the resources that the Connector manages with the same folders and projects, you can do so from the Resources page.

Learn how to associate a resource with folders and projects.

**Related information**

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

## Switch between BlueXP organizations, projects, and Connectors

You might belong to multiple BlueXP organizations or have permissions to access multiple projects or Connectors within a BlueXP organization. When needed, you can easily switch between organizations, projects, and Connectors to access the resources associated with that organization, project, or Connector.

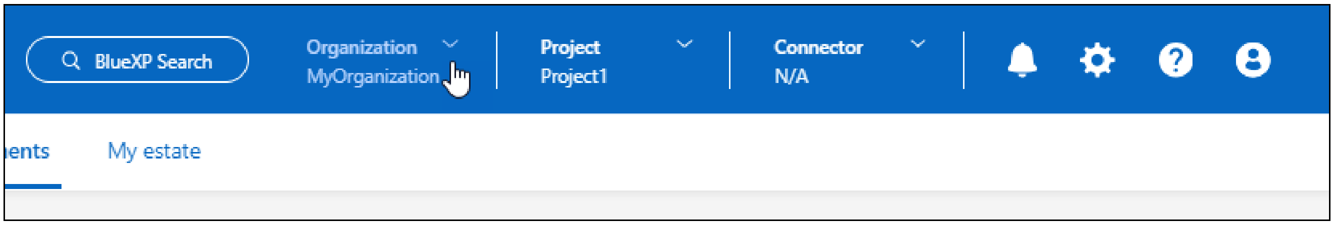
> You might belong to multiple organizations if you were invited to join another organization or if you created an additional organization yourself. You can create an additional organization by using the API. Learn how to create a new organization

### Switch between organizations

If you are a member of multiple organizations, you can switch between them at any time.

**Steps**

1. At the top of BlueXP, select **Organization**.



2. Select another organization and then select **Switch**.

**Result**

BlueXP switches to the selected organization and displays the resources associated with that organization.

### Switch between projects

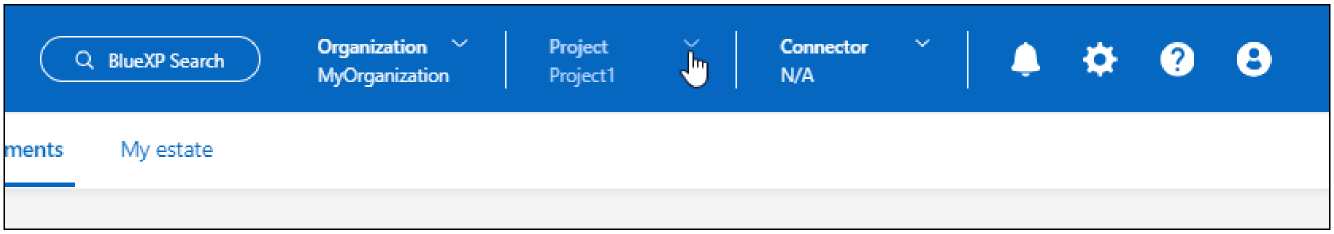
If your organization includes multiple projects and you have access to those projects, you can switch between them at any time.

**Before you begin**

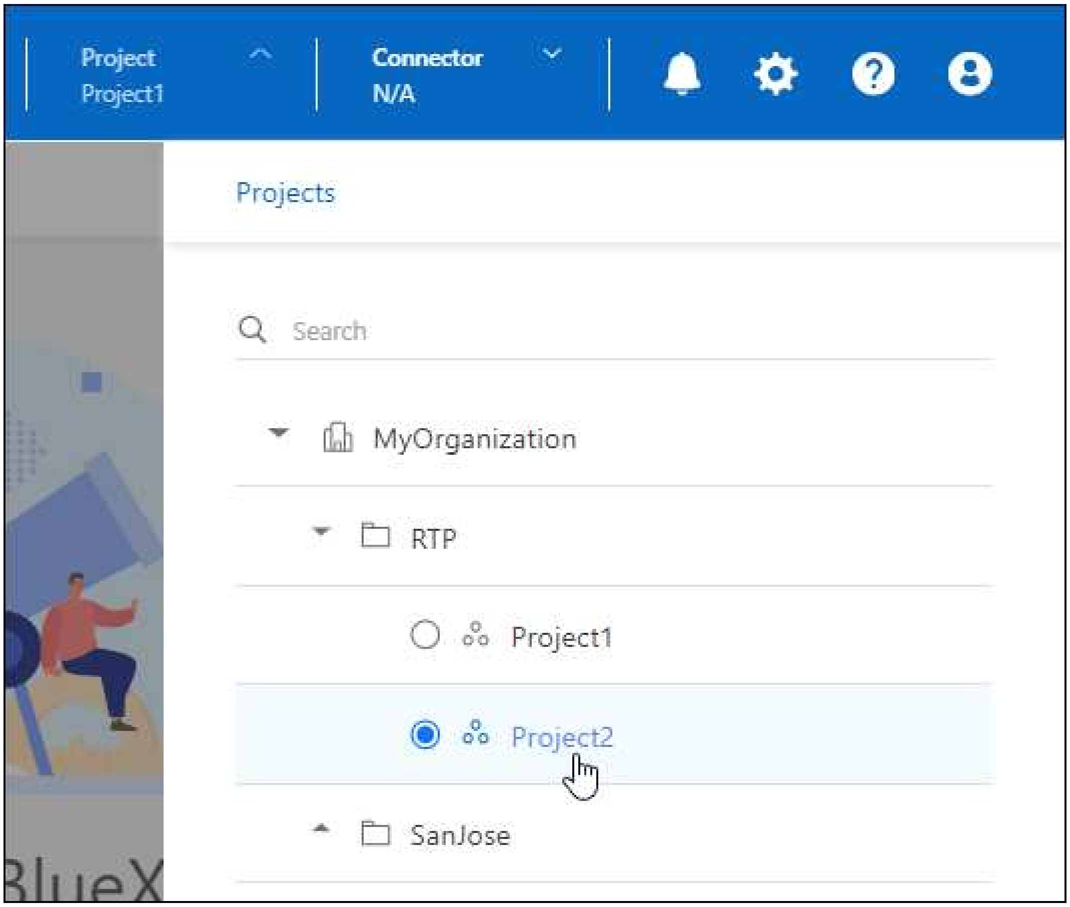
You must be on any page in the BlueXP console other than the BlueXP identity and access management (IAM) pages. You can't switch to another project when viewing any of the IAM pages.

**Steps**

1. At the top of BlueXP, select **Project**.



2. Browse through the folders and projects in your organization, select the project that you want, and then select **Switch**.



**Result**

BlueXP switches to the selected project and displays the resources associated with that project.

### Switch between Connectors

If you have multiple Connectors, you can switch between them to see the working environments that are associated with a specific Connector.

**Steps**

1. At the top of BlueXP, select **Connector**.
2. Select another Connector and then select **Switch**.

**Result**

BlueXP refreshes and shows the working environments associated with the selected Connector.

**Related information**

Associate Connectors with folders and projects.

**Related information**

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

## Organization and project IDs

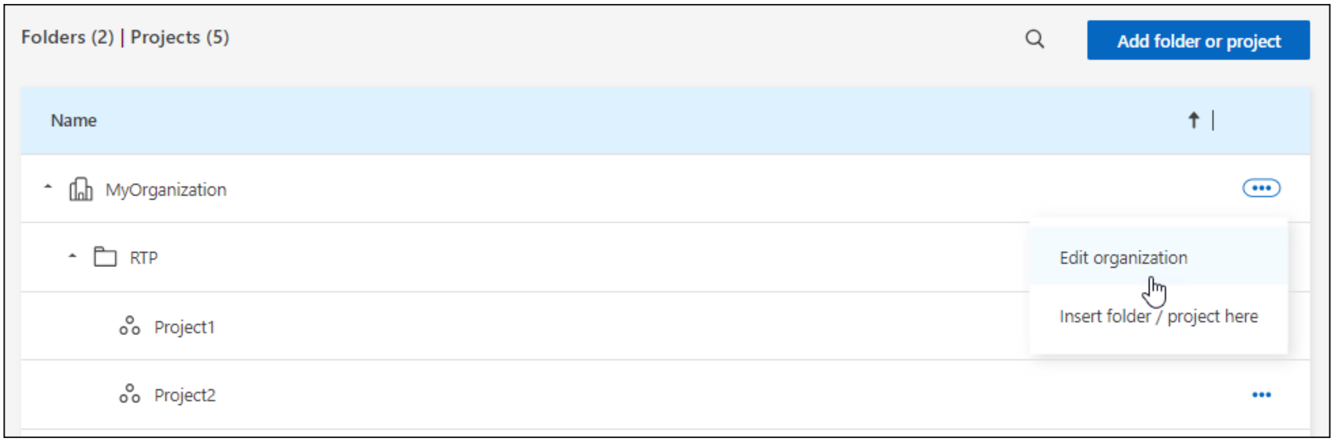
Your BlueXP organization has a name and an ID. You can choose a name for your organization to help identify it in your BlueXP deployment. You may also need to retrieve the organization ID for certain integrations.

### Rename your organization

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

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. From the **Organization** page, navigate to the first row in the table, select ••• and then select **Edit organization**.



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

### Get the organization ID

The organization ID is used for certain integrations with BlueXP.

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

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Organization** tab to view the **Organization** page.

3. 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

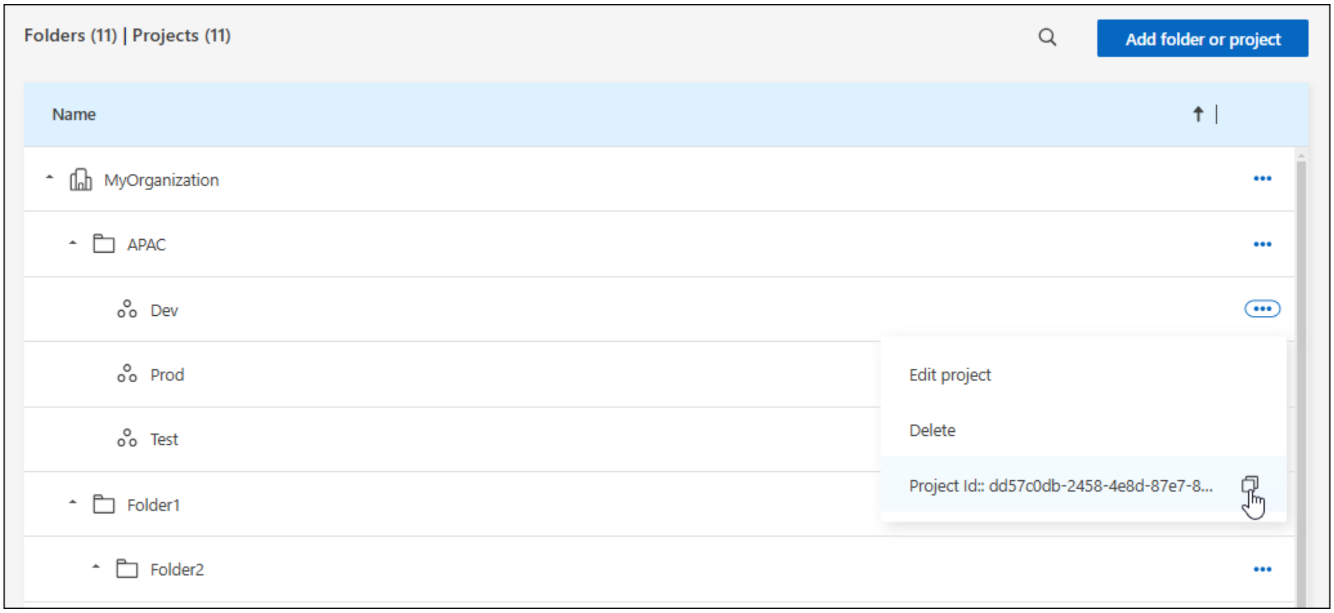
If you're using the BlueXP API, you might need to obtain the ID for a project. For example, when creating a Cloud Volumes ONTAP working environment.

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

## Monitor or audit IAM activity from the BlueXP timeline

If you need to monitor or audit an action that was completed from BlueXP identity and access management (IAM), you can view details from the BlueXP Timeline. For example, you might want to verify who added a member to an organization or that a project was deleted successfully.

#### Steps

1. In the upper right of the BlueXP console, select ⚙ > **Timeline**.
2. From the filters, select **Service** and then select **Tenancy**.
3. Use any of the other filters to change which actions display in the table.

For example, you can use the **User** filter to show actions related to a specific user account.

**Result**

The Timeline updates to show you completed management actions related to BlueXP IAM.

## BlueXP access roles

### Learn about BlueXP access roles

BlueXP identity and access management (IAM) includes 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 all BlueXP administration permissions, including assigning roles and adding users. Platform roles provide access to all BlueXP data services and applications. BlueXP IAM includes two platform roles: Organization admin and Folder or project admin. The main difference between the two BlueXP IAM platform roles is scope.

| 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 BlueXP task and use any data service that does not have an explicit role associated with it.<br>Users with this role organize and manage your BlueXP organization. They create folders and projects, assign roles, add users, and can manage all working environments, if they have the credentials to do so.<br>This is the only access role that can create Connectors. |
| Folder or project admin | Allows a user unrestricted access to specific projects and folders to which they are assigned. Can add members to folders or projects they manage, as well as perform any BlueXP task and use any data service or application on resources within the folder or project they are assigned.<br>Folder or project admins cannot create Connectors. |
| Federation admin | Allows a user create and manage federations with BlueXP, which enables single-sign on (SSO). |
| Federation viewer | Allows a user to view existing federations with BlueXP. Cannot create or manage federations |

#### Application roles

The following is a list of roles in the application category. Each role grants specific permissions within its designated scope. Users who do not have the required application role or a platform role will be unable to access the 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. |
| Keystone admin | Users with the Keystone admin role can create service requests. Allows users to monitor and view consumption, assets, and administrative information 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 montioring 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 working environments. |
| Storage viewer | View storage health and governance functions, as well as view previously discovered storage resources. Cannot discover, modify, or delete existing storage working environments. |
| System health specialist | Administer storage and health and governance functions, all permissions of the Storage admin except cannot modify or delete existing working environments. |

#### 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 the Backup and recovery service. |
| 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 service. |
| Backup and recovery clone admin | Clone applications and data in the Backup and recovery service. |
| Backup and recovery viewer | View Backup and recovery information. |
| Disaster recovery admin | Perform any actions in the Disaster recovery service. |
| Disaster recovery failover admin | Perform failover and migrations. |

| Data service role | Responsibilities |
|---|---|
| Disaster recovery application admin | Create replication plans, modify replication plans, and start test failovers. |
| Disaster recovery viewer | View information only. |
| Classification viewer | Provides the ability to view BlueXP classification scan results.<br>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 a viewer role. |
| Ransomware protection admin | Manage actions on the Protect, Alerts, Recover, Settings, and Reports tabs of the Ransomware protection service. |
| Ransomware protection viewer | View workload data, view alert data, download recovery data, and download reports in the Ransomware protection service. |
| SnapCenter admin | Provides the ability to back up snapshots from on-premises ONTAP clusters using BlueXP backup and recovery for applications. A member who has this role can complete the following actions in BlueXP:<br>* Complete any action from Backup and recovery > Applications<br>* Manage all working environments in the projects and folders for which they have permissions<br>* Use all BlueXP services<br>SnapCenter does not have a viewer role. |

**Related links**

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

### BlueXP platform access roles

Assign platform roles to users to grant permissions to perform administration tasks in BlueXP, assign roles, add users, create Connectors, and manage federations.

#### Example for organization roles in BlueXP 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 BlueXP 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 BlueXP platform role can perform.

#### Organization administration roles

| Task | Organization admin | Folder or project admin |
|---|---|---|
| Create Connectors | Yes | No |
| Create, modify or delete working environments (add or discover new resources using the BlueXP canvas) | 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 Connectors with folders and projects | Yes | No |
| Remove Connectors from a folders and projects | Yes | No |
| Manage Connectors (edit certificates, settings, and so on) | Yes | No |
| Manage credentials from Settings > Credentials | Yes | Yes |
| Create, manage, and view federations | Yes | No |
| Register for support and submit cases through BlueXP | Yes | Yes |
| Use data services | Yes | Yes |
| View the BlueXP timeline 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 |

### Application roles

#### Keystone access roles for BlueXP

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 BlueXP

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 | No |
| Manage alerts | Yes | No |
| Create alerts for self | Yes | Yes |
| **Digital wallet**: | | |
| Can view digital wallet | Yes | Yes |
| **Keystone reports page**: | | |
| Download reports | Yes | Yes |

| Feature and action | Keystone admin | Keystone viewer |
|---|---|---|
| Manage reports | Yes | Yes |
| Create reports for self | Yes | Yes |
| **Service requests**: | | |
| Create service requests | Yes | No |
| View service requests created by any user within the Organization | Yes | Yes |

#### Operational support analyst access role for BlueXP

You can assign the following 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 BlueXP | Yes |
| View the BlueXP timeline and notifications | Yes |
| View, download, and configure alerts | Yes |

#### Storage access roles for BlueXP

You can assign the following roles to users to provide them access to the storage management features in BlueXP that are associated with supported storage resources. You can assign users an administrative role to manage storage or a viewer role for monitoring.

ⓘ These roles are not available from the BlueXP 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

BlueXP services and features:

- Digital advisor
- Software updates
- Economic efficiency
- Sustainability

**Example for storage roles in BlueXP**

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 BlueXP tasks like user management, Connector creation, and cost tools such as the digital wallet.

Within a team of 12, two users are given the **Storage viewer** role which allows them to monitor the storage resources associated with the BlueXP 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 BlueXP, as well as discover storage resources (add working environments). 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 working environments. 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 BlueXP, including user management, Connector creation, and cost management tools like digital wallet, as well as several users with the **Folder or project admin** role who can perform BlueXP administration tasks for the folders and projects they are assigned to.

The following table shows the actions each BlueXP storage role performs.

| Feature and action | Storage admin | System health specialist | Storage viewer |
|---|---|---|---|
| **Canvas**: | | | |
| Discover new resources (create new working environment) | Yes | Yes | No |
| View discovered resources | Yes | Yes | No |
| Delete working environments | Yes | No | No |
| Modify working environments | Yes | No | No |
| **Create Connector** | No | No | No |
| **Digital advisor** | | | |
| View all pages and functions | Yes | Yes | Yes |
| **Digital wallet** | | | |
| View all pages and functions | No | No | No |
| **Software updates** | | | |

| Feature and action | Storage admin | System health specialist | Storage viewer |
|---|---|---|---|
| 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 |
| Install software updates | Yes | Yes | No |
| **Economic efficiency** | | | |
| 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

#### BlueXP backup and recovery roles

You can assign the following roles to users to provide them access to the Backup and recovery service within BlueXP. 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.

Backup and recovery uses the following roles:

- **Backup and recovery super admin**: Perform any actions.
- **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.
- **Backup and recovery clone admin**: Clone applications and data.
- **Backup and recovery viewer**: View backup and recovery information.

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

| Feature and action | Backup and recovery super admin | Backup admin | Restore admin | Clone admin | 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**: | | | | | |

| Feature and action | Backup and recovery super admin | Backup admin | Restore admin | Clone admin | Viewer |
|---|---|---|---|---|---|
| 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 storage buckets | Yes | Yes | Yes | Yes | Yes |
| Create, edit, or delete storage buckets | Yes | Yes | No | No | No |

#### BlueXP disaster recovery roles

You can assign the following roles to users to provide them access to the Diaster recovery within BlueXP. 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 |

| Feature and action | Disaster recovery admin | Disaster recovery failover admin | Disaster recovery application admin | Disaster recovery viewer |
|---|---|---|---|---|
| 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**: | | | | |
| View jobs | Yes | No | Yes | Yes |
| Cancel jobs | Yes | Yes | Yes | No |

#### Ransomware protection access roles for BlueXP

Ransomware roles provide users access to the Ransomware protection service. The two roles are Ransomware protection admin and Ransomware protection viewer. The main difference between the two roles is the actions they can take in Ransomware protection.

The following table shows the actions each BlueXP ransomware protection role can perform.

| Feature and action | Ransomware protection admin | Ransomware protection viewer |
|---|---|---|
| View dashboard and all tabs | Yes | Yes |
| Start free trial | Yes | No |
| Discover workloads | Yes | No |
| **On the Protect tab**: | | |
| Add, modify, or delete policies | Yes | No |
| Protect workloads | Yes | No |
| Identify sensitive data | Yes | No |
| Edit workload protection | Yes | No |

| Feature and action | Ransomware protection admin | Ransomware protection viewer |
|---|---|---|
| View workload details | Yes | Yes |
| Download data | Yes | Yes |
| **On the Alerts tab**: | | |
| View alert details | Yes | Yes |
| Edit incident status | Yes | No |
| View incident details | Yes | Yes |
| Get full list of impacted files | Yes | No |
| Download alerts data | Yes | Yes |
| **On the Recover tab**: | | |
| Download impacted files | Yes | No |
| Restore workload | Yes | No |
| Download recovery data | Yes | Yes |
| Download reports | Yes | Yes |
| **On the Settings tab**: | | |
| Add or modify backup targets | Yes | No |
| Add or modify SIEM targets | Yes | No |
| **On the Reports tab**: | | |
| Download reports | Yes | Yes |

# Identity federation

## Enable single sign-on by using identity federation with BlueXP

Single-sign on (federation) simplifies the login process and enhances security by allowing users to log in to BlueXP using their corporate credentials. You can enable single sign-on (SSO) with your identity provider (IdP) or with the NetApp Support site.

**Required role**

Organization admin, Federation admin, Federation viewer. Learn more about access roles.

### Identity federation with NetApp Support Site

When you federate with the NetApp Support Site, users can login with the same credentials to access BlueXP as you use for the NetApp Support Site, Active IQ Digital Advisor and other apps associated with your NetApp Support Site account. After you set up federation, any new users who create a NetApp Support Site accounts are also be able to access BlueXP.

> ⓘ If you federate with the NetApp Support Site, you can't also federate with your corporate identity management provider. Choose which one works best for your organization.

**Steps**

1. Download and complete the NetApp Federation Request Form.
2. Submit the form to the email address specified in the form.

   The NetApp support team reviews and processes your request.

### Set up a federated connection with your identity provider

You can set up a federated connection with your identity provider to enable single sign-on (SSO) for BlueXP. The process involves configuring your identity provider to trust NetApp as a service provider and then creating the connection in BlueXP.

> ⓘ If you previously configured federation using NetApp Cloud Central (an external application to BlueXP), you'll need to import your federation using the BlueXP Federation page to be able to manage it within BlueXP. Learn how to import your federation.

#### Supported identity providers

NetApp supports the following protocols and identity providers for federation:

**Protocols**

- Security Assertion Markup Language (SAML) identity providers
- Active Directory Federation Services (AD FS)

**Identity providers**

- Microsoft Entra ID
- PingFederate

#### Federation with BlueXP workflow

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can federate with your email domain or with a different domain that you own. To federate with a domain different from your email domain, first verify you own the domain.

**1** **Verify your domain (if not using your email domain)**

To federate with a domain different from your email domain, verify that you own it. You can federate your email domain without any extra steps.

2 **Configure your IdP to trust NetApp as a service provider**

Configure your identity provider to trust NetApp by creating a new application and providing the necessary information, such as the ACS URL, Entity ID or other credential information. Service provider information varies by identity provider, so refer to the documentation for your specific identity provider for details. You'll need to work with your IdP administrator to complete this step.

3 **Create the federated connection in BlueXP**

To create the connection, you need to provide the necessary information from your identity provider, such as the SAML metadata URL or file. This information is used to establish the trust relationship between BlueXP and your identity provider. The information you provide depends on the IdP that you are using. For example, if you're using Microsoft Entra ID, you need to provide the client ID, secret, and domain.

4 **Test your federation in BlueXP**

Test your federated connection before enabling it. The Federation page in BlueXP provides a test option that allows you to verify your test user is able to authenticate successfully. If the test is successful, you can enable the connection.

5 **Enable your connection in BlueXP**

After you enable the connection, users can log in to BlueXP using their corporate credentials.

Review the topic for your respective protocol or IdP to get started:

- Set up a federated connection with AD FS
- Set up a federated connection with Microsoft Entra ID
- Set up a federated connection with PingFederate
- Set up a federated connection with a SAML identity provider

## Domain verification

### Verify the email domain for your federated connection

If you want to federate with a domain that is different than your email domain, you must first verify that you own the domain. You can only use verified domains for federation.

**Required roles**

Organization admin or Federation admin. Learn more about access roles.

Verifying your domain involves adding a TXT record to your domain's DNS settings. This record is used to prove that you own the domain and allows BlueXP to trust the domain for federation. You may need to coordinate with your IT or network administrator to complete this step.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Select **Verify domain ownership**.
5. Enter the domain that you want to verify and select **Continue**.
6. Copy the TXT record that is provided.
7. Go to your domain's DNS settings and configure the TXT value that was provided as a TXT record for your domain. Work with your IT or network administrator if needed.
8. After the TXT record is added, return to BlueXP and select **Verify**.

## Configure federations

### Federate BlueXP with Active Directory Federation Services (AD FS)

Federate your Active Directory Federation Services (AD FS) with BlueXP to enable single sign-on (SSO) for BlueXP. This allows users to log in to BlueXP using their corporate credentials.

**Required roles**

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

> You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.

NetApp supports service provider-initiated (SP-initiated) SSO only. First, configure the identity provider to trust BlueXP as a service provider. Then, create a connection in BlueXP using your identity provider's configuration.

You can set up federation with your AD FS server to enable single sign-on (SSO) for BlueXP. The process involves configuring your AD FS to trust BlueXP as a service provider and then creating the connection in BlueXP.

**Before you begin**

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the Verify your domain in BlueXP topic.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.

   b. Enter the name of the federation you are configuring.

   c. If you choose a verified domain, select the domain from the list.

5. Select **Next**.

6. For your connection method, choose **Protocol** and then select **Active Directory Federation Services (AD FS)**.

7. Select **Next**.

8. Create a Relying Party Trust in your AD FS server. You can use PowerShell or manually configure it on your AD FS server. Consult the AD FS documentation for details on how to create a relying party trust.

   a. Create the trust using PowerShell by using following script:

   ```
   (new-object Net.WebClient -property @{Encoding = [Text.Encoding]
   ::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
   auth0/master/AD FS.ps1") | iex
   AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
   cloud-account.auth0.com/login/callback"
   ```

   b. Alternatively, you can create the trust manually in the AD FS management console. Use the following BlueXP values when creating the trust:

      - When creating the Relying Trust Identifier, use the **YOUR_TENANT** value: `netapp-cloud-account`

      - When you select **Enable support for the WS-Federation**, use the **YOUR_AUTH0_DOMAIN** value: `netapp-cloud-account.auth0.com`

   c. After creating the trust, copy the metadata URL from your AD FS server or download the federation metadata file. You'll need this URL or file to complete the connection in BlueXP.

   NetApp recommends using the metadata URL to let BlueXP automatically retrieve the latest AD FS configuration. If you download the federation metadata file, you will need to update it manually in BlueXP whenever there are changes to your AD FS configuration.

9. Return to BlueXP, and select **Next** to create the connection.

10. Create the connection with AD FS.

    a. Enter the **AD FS URL** that you copied from your AD FS server in the previous step or upload the federation metadata file that you downloaded from your AD FS server.

11. Select **Create connection**. Creating the connection might take a few seconds.

12. Select **Next**.

13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.

14. Select **Next**.

15. On the **Enable federation** page, review the federation details and then select **Enable federation**.

16. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

## Federate BlueXP with Microsoft Entra ID

Federate with your Microsoft Entra ID IdP provider to enable single sign-on (SSO) for BlueXP. This allows users to log in using their corporate credentials.

### Required roles

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

> ⓘ You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can set up a federated connection with Microsoft Entra ID to enable single sign-on (SSO) for BlueXP. The process involves configuring your Microsoft Entra ID to trust BlueXP as a service provider and then creating the connection in BlueXP.

### Before you begin

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the Verify your domain in BlueXP topic.

### Steps

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.

### Domain details

4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
   b. Enter the name of the federation you are configuring.
   c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.

### Connection method

6. For your connection method, choose **Provider** and then select **Microsoft Entra ID**.
7. Select **Next**.

### Configuration instructions

1. Configure your Microsoft Entra ID to trust NetApp as a service provider. You need to do this step on your

Microsoft Entra ID server.

   a. Use the following values when registering your Microsoft Entra ID app to trust BlueXP:

      - For the **Redirect URL** , use `https://services.cloud.netapp.com`
      - For the **Reply URL**, use `https://netapp-cloud-account.auth0.com/login/callback`

   b. Create a client secret for your Microsoft Entra ID app. You'll need to provide the client ID, the client secret, and the Entra ID domain name to complete the federation.

2. Return to BlueXP, and select **Next** to create the connection.

### Create connection

1. Create the connection with Microsoft Entra ID

   a. Enter the client ID and Client secret that you created in the previous step.

   b. Enter the Microsoft Entra ID domain name.

2. Select **Create connection**. The system creates the connection in a few seconds.

### Test and enable the connection

1. Select **Next**.
2. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.
3. Select **Next**.
4. On the **Enable federation** page, review the federation details and then select **Enable federation**.
5. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

### Federate BlueXP with PingFederate

Federate with your PingFederate IdP provider to enable single sign-on (SSO) for BlueXP. This allows users to log in using their corporate credentials.

### Required roles

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

> You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can set up a federated connection with PingFederate to enable single sign-on (SSO) for BlueXP. The process involves configuring your PingFederate server to trust BlueXP as a service provider and then creating the connection in BlueXP.

### Before you begin

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the Verify your domain in BlueXP topic.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.

   b. Enter the name of the federation you are configuring.

   c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Provider** and then select **PingFederate**.
7. Select **Next**.
8. Configure your PingFederate server to trust NetApp as a service provider. You need to do this step on your PingFederate server.
   a. Use the following values when configuring PingFederate to trust BlueXP:
      - For the **Reply URL** or **Assertion Consumer Service (ACS) URL**, use `https://netapp-cloud-account.auth0.com/login/callback`
      - For the **Logout URL**, use `https://netapp-cloud-account.auth0.com/logout`
      - For **Audience/Entity ID**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` where <fed-domain-name-pingfederate> is the domain name for the federation. For example, if your domain is `example.com`, the Audience/Entity ID would be `urn:auth0:netappcloud-account:fed-example-com-pingfederate`.

   b. Copy the PingFederate server URL. You will need this URL when creating the connection in BlueXP.

   c. Download the X.509 certificate from your PingFederate server. It needs to be in Base64-encoded PEM format (.pem, .crt, .cer).
9. Return to BlueXP, and select **Next** to create the connection.
10. Create the connection with PingFederate
    a. Enter the PingFederate server URL that you copied in the previous step.

    b. Upload the X.509 signing certificate. The certificate must be in PEM, CER, or CRT format.
11. Select **Create connection**. The system creates the connection in a few seconds.
12. Select **Next**.
13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.
14. Select **Next**.
15. On the **Enable federation** page, review the federation details and then select **Enable federation**.

16. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

#### Federate with a SAML identity provider

### Federate with your SAML 2.0 IdP provider to enable single sign-on (SSO) for BlueXP. This allows users to log in using their corporate credentials.

**Required role**

Organization admin. Learn more about access roles.

> ⓘ You can federate with your corporate IdP or with the NetApp Support Site. You can't federate with both.

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can set up a federated connection with your SAML 2.0 provider to enable single sign-on (SSO) for BlueXP. The process involves configuring your provider to trust NetApp as a service provider and then creating the connection in BlueXP.

**Before you begin**

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the Verify your domain in BlueXP topic.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Enter your domain details:
   a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
   b. Enter the name of the federation you are configuring.
   c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Protocol** and then select **SAML Identity Provider**.
7. Select **Next**.
8. Configure your SAML identity provider to trust NetApp as a service provider. You need to do this step on your SAML provider server.
   a. Ensure that your IdP has the attribute `email` set to the user's email address. This is required for BlueXP to identify users correctly:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName">
        <saml:AttributeValue xsi:type="xs:string">
email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

   b. Use the following values when registering your SAML application with BlueXP:

      - For the **Reply URL** or **Assertion Consumer Service (ACS) URL**, use `https://netapp-cloud-account.auth0.com/login/callback`
      - For the **Logout URL**, use `https://netapp-cloud-account.auth0.com/logout`
      - For **Audience/Entity ID**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` where <fed-domain-name-saml> is the domain name you want to use for federation. For example, if your domain is `example.com`, the Audience/Entity ID would be `urn:auth0:netapp-cloud-account:fed-example-com-samlp`.

   c. After creating the trust, copy the following values from your SAML provider server:

      - Sign In URL
      - Sign Out URL (optional)

   d. Download the X.509 certificate from your SAML provider server. It needs to be in PEM, CER, or CRT format.

9. Return to BlueXP, and select **Next** to create the connection.
10. Create the connection with SAML.

    a. Enter the **Sign In URL** of your SAML server.

    b. Upload the X.509 certificate that you downloaded from your SAML provider server.

    c. Optionally, enter the **Sign Out URL** of your SAML server.

11. Select **Create connection**. The system creates the connection in a few seconds.
12. Select **Next**.
13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.
14. Select **Next**.
15. On the **Enable federation** page, review the federation details and then select **Enable federation**.
16. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

## Manage federations in BLueXP

You can manage your federation in BlueXP. You can disable it, update expired credentials, as well as disable it if you no longer need it.

> ⓘ If you previously configured federation using NetApp Cloud Central (an external application to BlueXP), you'll need to import your federation using the BlueXP Federation page to be able to manage it within BlueXP. Learn how to import your federation

You can also add a verified domain to an existing federation, which allows you to use multiple domains for your federated connection.

> ⓘ Federation management events such as enabling, disabling, and updating federations display in the Timeline. Learn more about monitoring operations in BlueXP.

**Required roles**

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. Learn more about access roles.

### Enable a federation

If you have created a federation but it is not enabled, you can enable it through the Federation tab in BlueXP. Enabling a federation allows users associated with the federation to log in to BlueXP using their corporate credentials. You must have already created the federation and tested it successfully before enabling it.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu ••• next to the federation that you want to enable and select **Enable**.

### Add a verified domain to an existing federation

You can add a verified domain to an existing federation in BlueXP to use multiple domains with the same identity provider (IdP).

You must have already verified the domain in BlueXP before you can add it to a federation. If you haven't verified the domain yet, you can do so by following the steps in Verify your domain in BlueXP.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Update domains**. The **Update domains** dialog box lists the domain already associated with this federation.
4. Select a verified domain from the list of available domains.
5. Select **Update**. It make take up to 30 seconds for users of the new domain to have federated access to BlueXP.

### Updating an expiring federated connection

You can update the details of a federation in BlueXP. For example, you'll need to update the federation if the credentials such as a certificate or client secret expire. When needed, update the notification date to remind you to update the connection before it expires.

> ⓘ Update BlueXP first before updating your IdP to avoid login issues. Stay logged in to BlueXP during the process.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu (three vertical dots) next to the federation that you want to update and select **Update federation**.
4. Update the details of the federation as needed.
5. Select **Update**.

### Test an existing federation

If you are having trouble with an existing federation, you can test the connection to see if it is working properly. This can help you identify any issues with the federation and troubleshoot them.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Test connection**.
4. Select **Test**. You're prompted to log in with your corporate credentials. If the connection is successful, you will be redirected to the BlueXP console. If the connection fails, you will see an error message indicating the issue with the federation.
5. Select **Done** to return to the **Federation** tab.

### Disable a federation

If you no longer need a federation, you can disable it. This prevents users associated with the federation from logging in to BlueXP using their corporate credentials. You can re-enable the federation later if needed.

You should disable a federation before deleting it. For example, if you are decommissioning the IdP in favor of another IdP or no longer want to use federation. This allows you to re-enable it later if needed.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Disable**.

#### Delete a federation

If you no longer need a federation, you can delete it. This removes the federation from BlueXP and prevents any users associated with the federation from logging in to BlueXP using their corporate credentials. For example, if the IdP is being decommissioned or if the federation is no longer needed. After you delete a federation, you cannot recover it. You must create a new federation.

> ⓘ You must disable a federation before you can delete it. You cannot undelete a federation after you delete it.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu ⋮ next to the federation that you want to add a verified domain to and select **Delete**.

### Import your federation to BlueXP

If you have previously setup federation through NetApp Cloud Central (an external application to BlueXP) the Federation page prompts you to import your existing federated connection to BlueXP to manage it in the new interface. This allows you to take advantage of the latest enhancements without having to recreate your federated connections.

Existing customers who have already set up federated connections to BlueXP can import their existing federations to the new interface. This allows you to manage your federated connections in the new Federations page without having to recreate them.

> ⓘ After you import your existing federation, you can manage the federation from the Federations page. Learn more about managing federations.

**Required role**

Organization admin or Federation admin. Learn more about access roles.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Import Federation**.

# Connectors

## Maintain the Connector VM and operating system

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

If you have an existing Connector, you should be aware of changes to supported Linux operating systems.

### Operating system patches and the Connector

Apply OS security patches without stopping Connector host services.

### VM or instance type

If you create a Connector from BlueXP, it deploys a VM instance in your cloud provider with a default configuration. After you create the Connector, don’t switch to a smaller VM instance with less CPU or RAM.

The following table lists the CPU and RAM requirements:

**CPU**
8 cores or 8 vCPUs

**RAM**
32 GB

Learn about the default configuration for the Connector.

### Monitor the Connector

BlueXP notifies you when the Connector VM is unhealthy, including disk space, RAM, and CPU issues. Monitor these notifications in the Notifications Center within BlueXP or configure email notifications. Occasional increases in disk space, memory, or CPU usage are normal, but if it happens frequently, you should take steps to resolve.

BlueXP notifies you when a Connector resource (CPU, RAM, or disk space) exceeds 90% of its total capacity for 30 consecutive minutes. Afterwards, if the resource usage drops below that threshold, the notification displays as resolved (green) in the Notifications Center.

Work with NetApp support if you have questions about modifying your Connector VM.

Learn more.

| Notification | Action needed |
|---|---|
| Disk space is too high | Review the NetApp Knowledge Base article. |
| CPU usage is too high | Increase the CPU size of the Connector VM in your hyperscaler or on-premises, depending on where you installed it. Alternatively, create additional Connectors and distribute the workload across multiple Connectors. RAM utilization can vary based on your environment, ONTAP workloads, number of Cloud Volumes ONTAP systems, and the data services that you are using. |

| Notification | Action needed |
|---|---|
| RAM usage is too high | Increase the RAM of the Connector VM in your hyperscaler or on-premises, depending on where you installed it. Alternatively, create additional Connectors and distribute the workload across multiple Connectors. RAM utilization can vary based on your environment, ONTAP workloads, number of Cloud Volumes ONTAP systems, and the data services that you are using. |

### Stopping and starting the Connector VM

If you need to, stop and start the Connector VM using your cloud provider's console or standard on-premises procedures.

Be aware that the Connector must be operational at all times.

### Connect to the Linux VM

If you need to connect to the Linux VM that the Connector runs on, use the connectivity options from your cloud provider.

**AWS**

When you create the Connector instance in AWS, provide an AWS access key and secret key. You can use this key pair to SSH to the instance. Use the user name 'ubuntu' for the EC2 Linux instance. For Connectors created prior to May 2023, use the user name 'ec2-user'.

AWS Docs: Connect to your Linux instance

**Azure**

When you create the Connector VM in Azure, you specify a user name and choose to authenticate with a password or SSH public key. Use the authentication method that you chose to connect to the VM.

Azure Docs: SSH into your VM

**Google Cloud**

You can't specify an authentication method when you create a Connector in Google Cloud. However, you can connect to the Linux VM instance using the Google Cloud Console or Google Cloud CLI (gcloud).

Google Cloud Docs: Connect to Linux VMs

### Change the IP address for a Connector

You can change the internal and public IP addresses of the Connector instance assigned by your cloud provider if needed.

**Steps**

1. Follow the instructions from your cloud provider to change the local IP address or public IP address (or both) for the Connector instance.
2. Restart the Connector instance to register a new public IP address with BlueXP.
3. If you changed the private IP address, update the backup location for Cloud Volumes ONTAP configuration files so that the backups are being sent to the new private IP address on the Connector.

Update the backup location for each Cloud Volumes ONTAP system.

a. From the Cloud Volumes ONTAP CLI, set the privilege level to advanced:

```
set -privilege advanced
```

b. Run the following command to display the current backup target:

```
system configuration backup settings show
```

c. Run the following command to update the IP address for the backup target:

```
system configuration backup settings modify -destination <target-
location>
```

#### Edit a Connector’s URIs

You can add and remove the Uniform Resource Identifier (URI) for a Connector.

**Steps**

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Expand the **Connector URIs** bar to view connector URIs.
4. Add and remove URIs and then select **Apply**.

### Install a CA-signed certificate for web-based console access

When you use BlueXP in restricted mode or private mode, the user interface is accessible from the Connector virtual machine that’s deployed in your cloud region or on-premises. By default, BlueXP uses a self-signed SSL certificate to provide secure HTTPS access to the web-based console running on the Connector. If required by your business, you can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate. After you install the certificate, BlueXP uses the CA-signed certificate when users access the web-based console.

#### Before you begin

You need to create a Connector before you can change BlueXP settings. Learn how to create a Connector.

#### Install an HTTPS certificate

Install a certificate signed by a CA for secure access to the web-based console running on the Connector.

**About this task**

You can install the certificate using one of the following options:

- Generate a certificate signing request (CSR) from BlueXP, submit the certificate request to a CA, and then install the CA-signed certificate on the Connector.

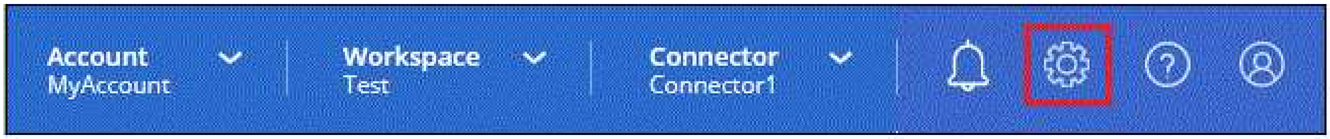
  The key pair that BlueXP uses to generate the CSR is stored internally on the Connector. BlueXP automatically retrieves the same key pair (private key) when you install the certificate on the Connector.

- Install a CA-signed certificate that you already have.

  With this option, the CSR is not generated through BlueXP. You generate the CSR separately and store the private key externally. You provide BlueXP with the private key when you install the certificate.

**Steps**

1. In the upper right of the BlueXP console, select the Settings icon, and select **HTTPS Setup**.

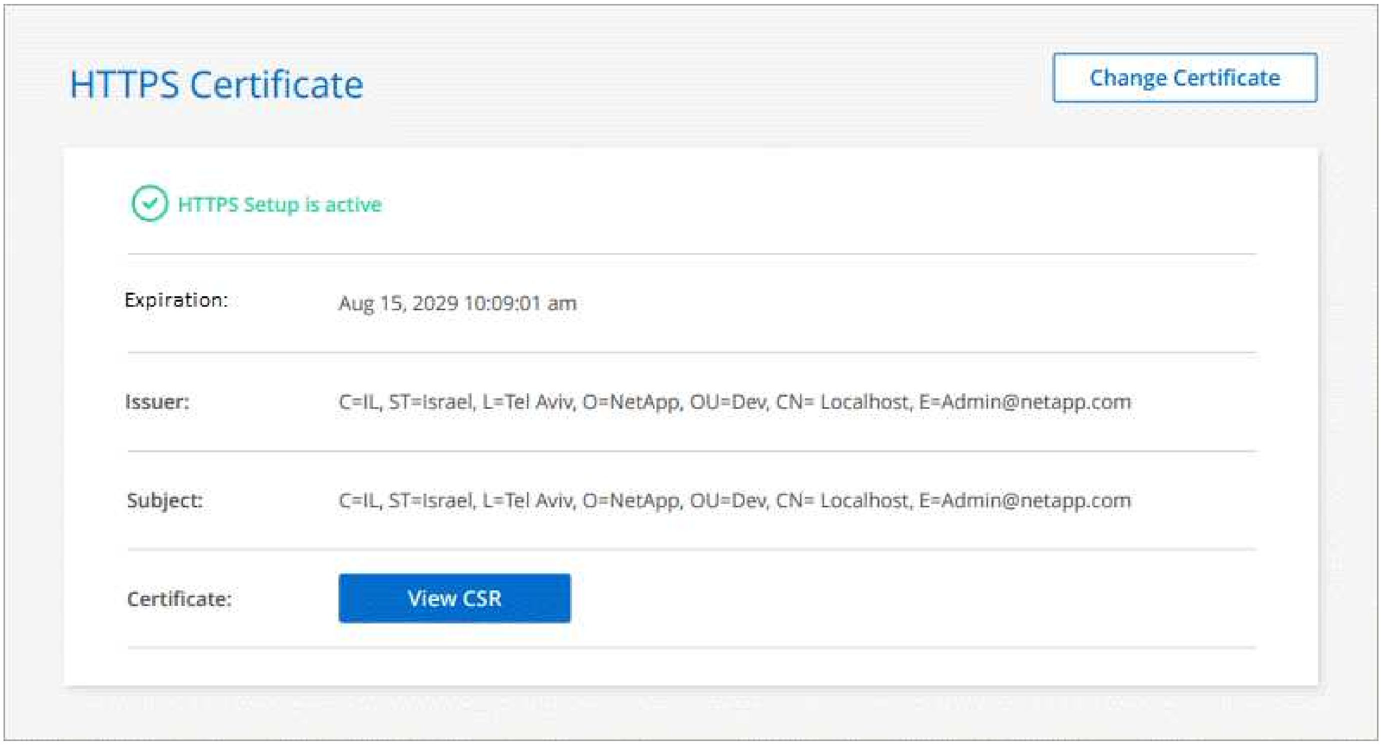


2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

| Option | Description |
|---|---|
| Generate a CSR | a. Enter the host name or DNS of the Connector host (its Common Name), and then select **Generate CSR**.<br>BlueXP displays a certificate signing request.<br>b. Use the CSR to submit an SSL certificate request to a CA.<br>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.<br>c. Upload the certificate file and then select **Install**. |
| Install your own CA-signed certificate | a. Select **Install CA-signed certificate**.<br>b. Load both the certificate file and the private key and then select **Install**.<br>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. |

**Result**

BlueXP now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a Connector that is configured for secure access:



HTTPS Certificate

HTTPS Setup is active

Expiration: Aug 15, 2029 10:09:01 am

Issuer: C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com

Subject: C=IL, ST=Israel, L=Tel Aviv, O=NetApp, OU=Dev, CN= Localhost, E=Admin@netapp.com

Certificate:

#### Renew the BlueXP HTTPS certificate

You should renew the BlueXP HTTPS certificate before it expires to ensure secure access to the BlueXP console. If you don’t renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

**Steps**

1. In the upper right of the BlueXP console, select the Settings icon, and select **HTTPS Setup**.

   Details about the BlueXP certificate displays, including the expiration date.

2. Select **Change Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

**Result**

BlueXP uses the new CA-signed certificate to provide secure HTTPS access.

## Configure a Connector to use a proxy server

If your corporate policies require you to use a proxy server for all communication to the internet, then you need to configure your Connectors to use that proxy server. If you didn’t configure a Connector to use a proxy server during installation, then you can configure the Connector to use that proxy server at any time.

The Connector’s proxy server enables outbound internet access without a public IP or NAT gateway. The proxy server provides outbound connectivity only for the Connector, not for Cloud Volumes ONTAP systems.

If Cloud Volumes ONTAP systems lack outbound internet access, BlueXP configures them to use the Connector’s proxy server. You must ensure that the Connector’s security group allows inbound connections over port 3128. Open this port after deploying the Connector.

If the Connector itself doesn’t have an outbound internet connection, Cloud Volumes ONTAP systems cannot use the configured proxy server.

### Supported configurations

- Transparent proxy servers are supported for Connectors that serve Cloud Volumes ONTAP systems. If you use BlueXP services with Cloud Volumes ONTAP, create a dedicated Connector for Cloud Volumes ONTAP where you can use a transparent proxy server.
- Explicit proxy servers are supported with all Connectors, including those that manage Cloud Volumes ONTAP systems and those that manage BlueXP services.
- HTTP and HTTPS.
- The proxy server can reside in the cloud or in your network.

> ⓘ Once you have configured a proxy, you cannot change the proxy type. If you need to change the proxy type, you remove the Connector and add a new Connector with the new proxy type.

### Enable an explicit proxy on a Connector

When you configure a Connector to use a proxy server, that Connector and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

This operation restarts the Connector. Verify the Connector is idle before proceeding.

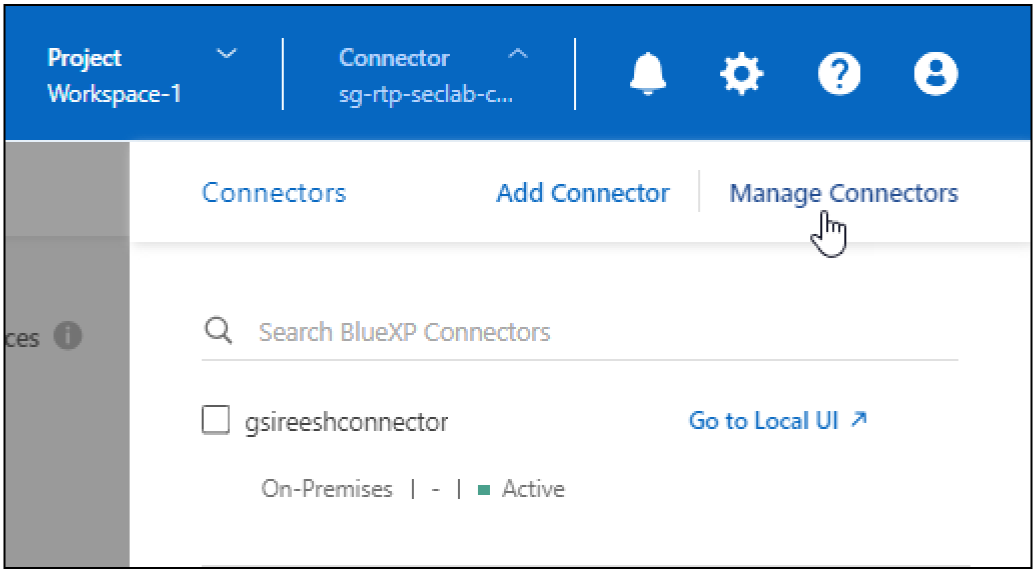
**Steps**

1. Navigate to the **Edit BlueXP Connector** page.

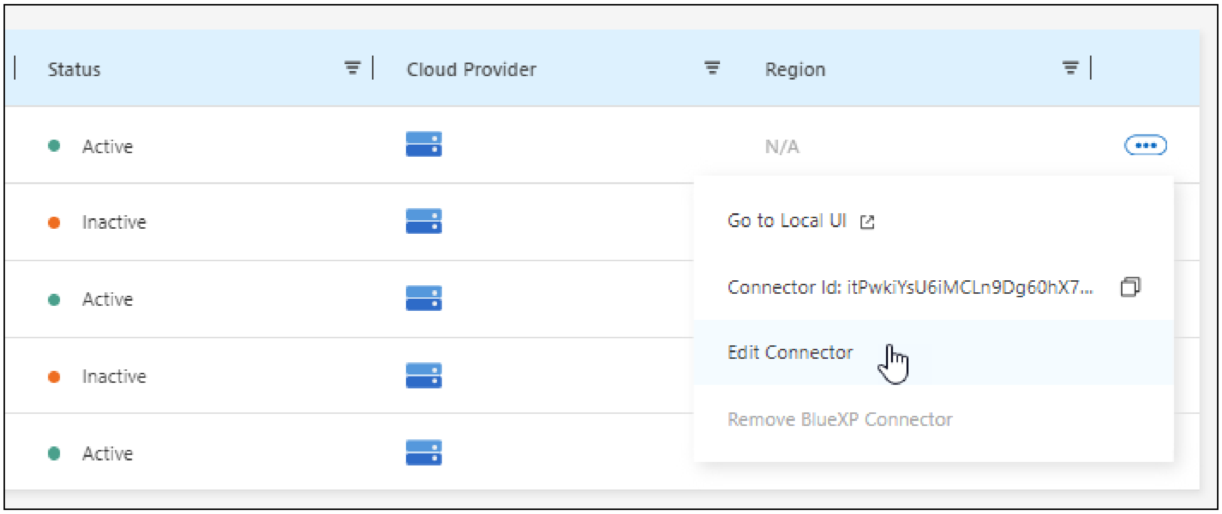
**Standard mode**

a. Select the **Connector** drop-down from the BlueXP header.

b. Select **Manage Connectors**.



c. Select the action menu for a Connector and select **Edit Connector**.

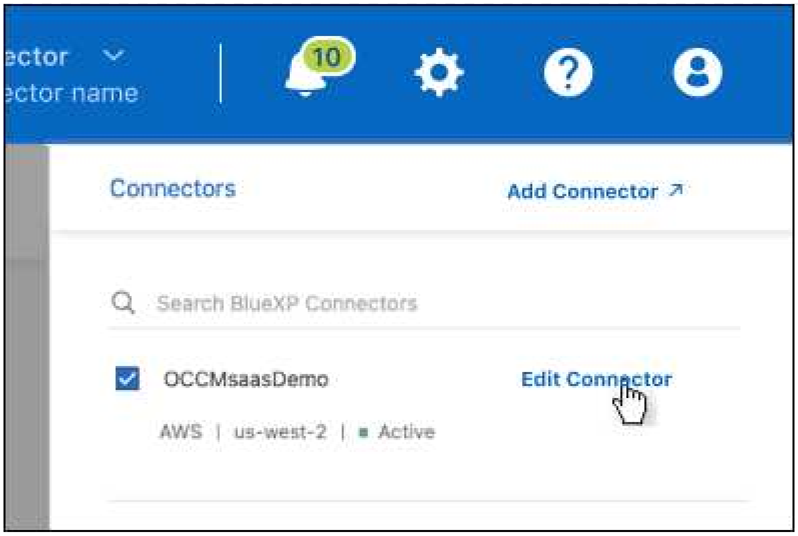


| Status | Cloud Provider | Region |
|---|---|---|
| ● Active | | N/A |
| ● Inactive | | |
| ● Active | | |
| ● Inactive | | |
| ● Active | | |

**Restricted or private mode**

a. Select the **Connector** drop-down from the BlueXP header.

b. Select **Edit Connector**.



2. Select **HTTP Proxy Configuration**.
3. Select **Explicit proxy** in the Configuration type field.
4. Select **Enable Proxy**.
5. Specify the server using the syntax http://*address:port* or https://*address:port*
6. Specify a user name and password if basic authentication is required for the server.

   Note the following:

   - The user can be a local user or domain user.
   - For a domain user, you must enter the ASCII code for the \ as follows: domain-name%92user-name

     For example: netapp%92proxy

   - BlueXP doesn't support passwords that include the @ character.
7. Select **Save**.

### Enable a transparent proxy on a Connector

Only Cloud Volumes ONTAP supports using a transparent proxy on the Connector. If you use BlueXP services in addition to Cloud Volumes ONTAP, you should create a separate Connector to use for data services or to use for Cloud Volumes ONTAP.

Before enabling a transparent proxy, ensure that the following requirements are met:

- The Connector is installed on the same network as the transparent proxy server.
- TLS inspection is enabled on the proxy server.
- You have a certificate in PEM format that matches the one used on the transparent proxy server.
- You do not use the Connector for any NetApp data services other than Cloud Volumes ONTAP.

To configure an existing Connector to use a transparent proxy server, you use the Connector maintenance tool that is available through the command line on the Connector host.

When you configure a proxy server, the Connector restarts. Verify the Connector is idle before proceeding.

**Steps**

Ensure that you have a certificate file in PEM format for the proxy server. If you do not have a certificate, contact your network administrator to obtain one.

1. Open a command-line interface on the Connector host.
2. Navigate to the Connector maintenance tool directory: `/opt/application/netapp/service-manager-2/connector-maint-console`
3. Run the following command to enable the transparent proxy, where `/home/ubuntu/<certificate-file>.pem` is the directory and name certificate file that you have for the proxy server:

   ```
   ./connector-maint-console proxy add -c /home/ubuntu/<certificate-
   file>.pem
   ```

   Ensure that the certificate file is in PEM format and resides in the same directory as the command or specify the full path to the certificate file.

   ```
   ./connector-maint-console proxy add -c /home/ubuntu/<certificate-
   file>.pem
   ```

#### Modify the transparent proxy for the Connector

You can update a Connector's existing transparent proxy server by using the `proxy update` command or remove the transparent proxy server by using the `proxy remove` command. For more information, review the documentation for Connector maintenance console.

ⓘ Once you have configured a proxy, you cannot change the proxy type. If you need to change the proxy type, you remove the Connector and add a new Connector with the new proxy type.

### Update the Connector proxy if it loses access to the internet

If the proxy configuration for your network changes, your Connector might lose access to the internet. For example, if someone changes the password for the proxy server or updates the certificate. In this case, you'll need to access the UI from the Connector host directly and update the settings. Ensure you have network access to the Connector host and that you can log into the BlueXP UI.

### Enable direct API traffic

If you configured a Connector to use a proxy server, you can enable direct API traffic on the Connector in order to send API calls directly to cloud provider services without going through the proxy. Connectors running in AWS, Azure, or Google Cloud support this option.

If you disable Azure Private Links with Cloud Volumes ONTAP and use service endpoints, enable direct API traffic. Otherwise, the traffic won't be routed properly.

Learn more about using an Azure Private Link or service endpoints with Cloud Volumes ONTAP

**Steps**

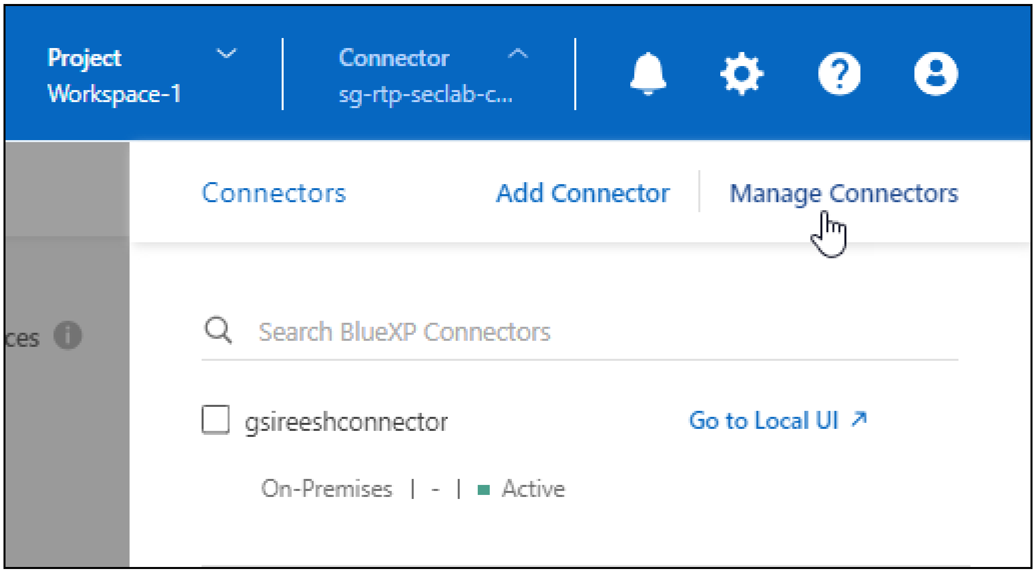
1. Navigate to the **Edit BlueXP Connector** page:

Navigation depends on your BlueXP mode. In standard mode, access the interface from the SaaS website. In restricted or private mode, access it locally from the Connector host.

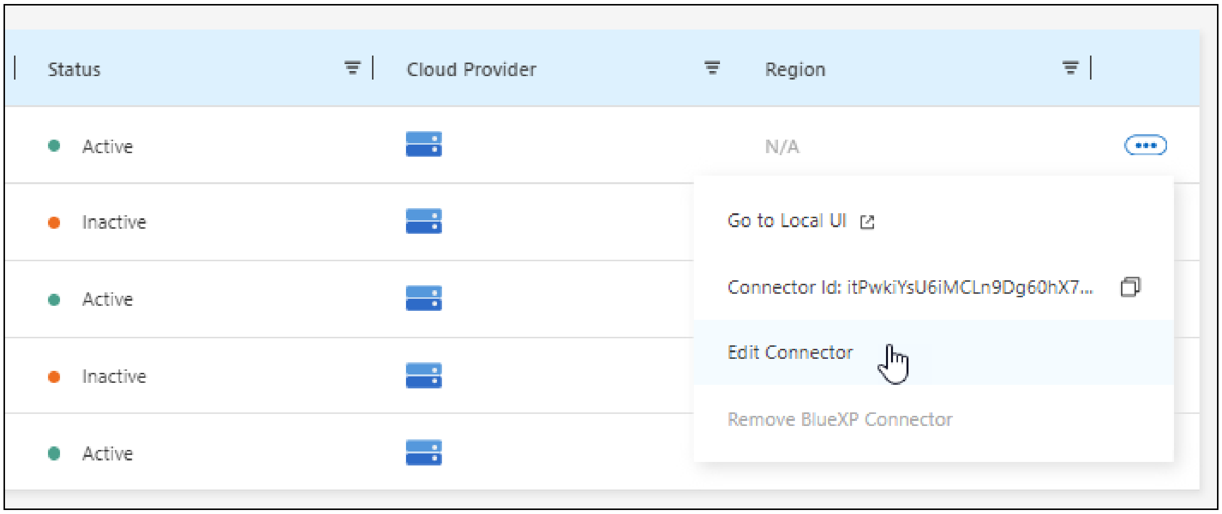
**Standard mode**

a. Select the **Connector** drop-down from the BlueXP header.

b. Select **Manage Connectors**.



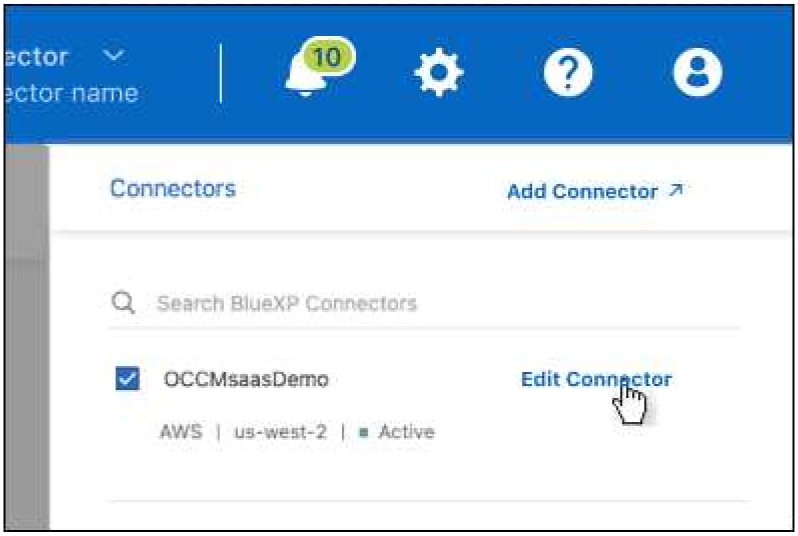
c. Select the action menu for a Connector and select **Edit Connector**.



**Restricted or private mode**

a. Select the **Connector** drop-down from the BlueXP header.

b. Select **Edit Connector**.



2. Select **Support Direct API Traffic**.
3. Select the checkbox to enable the option and then select **Save**.

## Require the use of IMDSv2 on Amazon EC2 instances

BlueXP supports the Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) with the Connector and with Cloud Volumes ONTAP (including the mediator for HA deployments). In most cases, IMDSv2 is automatically configured on new EC2 instances. IMDSv1 was enabled prior to March 2024. If required by your security policies, you might need to manually configure IMDSv2 on your EC2 instances.

**Before you begin**

- The Connector version must be 3.9.38 or later.
- Cloud Volumes ONTAP must be running one of the following versions:
  - 9.12.1 P2 (or any subsequent patch)
  - 9.13.0 P4 (or any subsequent patch)
  - 9.13.1 or any version after this release
- This change requires you to restart the Cloud Volumes ONTAP instances.
- These steps require the use of the AWS CLI because you must change the response hop limit to 3.

**About this task**

IMDSv2 provides enhanced protection against vulnerabilities. Learn more about IMDSv2 from the AWS Security Blog

The Instance Metadata Service (IMDS) is enabled as follows on EC2 instances:

- For new Connector deployments from BlueXP or using Terraform scripts, IMDSv2 is enabled by default on the EC2 instance.
- If you launch a new EC2 instance in AWS and then manually install the Connector software, IMDSv2 is also enabled by default.
- If you launch the Connector from the AWS Marketplace, IMDSv1 is enabled by default. You can manually

configure IMDSv2 on the EC2 instance.

- For existing Connectors, IMDSv1 is still supported but you can manually configure IMDSv2 on the EC2 instance if you prefer.
- For Cloud Volumes ONTAP, IMDSv1 is enabled by default on new and existing instances. You can manually configure IMDSv2 on the EC2 instances if you prefer.

**Steps**

1. Require the use of IMDSv2 on the Connector instance:

   a. Connect to the Linux VM for the Connector.

      When you created the Connector instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance. The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was ec2-user).

      AWS Docs: Connect to your Linux instance

   b. Install the AWS CLI.

      AWS Docs: Install or update to the latest version of the AWS CLI

   c. Use the `aws ec2 modify-instance-metadata-options` command to require the use of IMDSv2 and to change the PUT response hop limit to 3.

      **Example**

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

   > The `http-tokens` parameter sets IMDSv2 to required. When `http-tokens` is required, you must also set `http-endpoint` to enabled.

2. Require the use of IMDSv2 on Cloud Volumes ONTAP instances:

   a. Go to the Amazon EC2 console

   b. From the navigation pane, select **Instances**.

   c. Select a Cloud Volumes ONTAP instance.

   d. Select **Actions > Instance settings > Modify instance metadata options**.

   e. On the **Modify instance metadata options** dialog box, select the following:

      - For **Instance metadata service**, select **Enable**.
      - For **IMDSv2**, select **Required**.
      - Select **Save**.

   f. Repeat these steps for other Cloud Volumes ONTAP instances, including the HA mediator.

   g. Stop and start the Cloud Volumes ONTAP instances

**Result**

The Connector instance and Cloud Volumes ONTAP instances are now configured to use IMDSv2.

## Manage connector upgrades

When you use standard mode or restricted mode, BlueXP automatically upgrades your Connector to the latest release, as long as the Connector has outbound internet access to obtain the software update.
If you need to manually manage when the connector is upgraded, you can disable automatic upgrades for standard mode or restricted mode.

> ⓘ When running BlueXP in private mode, you must always upgrade the connector yourself.

### Disable automatic upgrades

Disabling auto-upgrade for your connector consists of two steps. First you need to ensure that your Connector is healthy and up-to-date. Then you'll edit a configuration file to turn off the automatic upgrade feature.

> ⓘ You can only disable automatic upgrades if you have connector version 3.9.48 or higher.

#### Verify the health of your connector

You should verify that your connector is stable and all containers running on your connector VM are healthy and running. After you disable automatic upgrades, your connector VM stops checking for new services or upgrade packages.

Use one of the following commands to verify your connector. All services should have a status of *Running*. If this isn't the case, contact NetApp support before disabling auto-upgrade.

**Docker**

```
docker ps -a
```

**Podman**

```
podman ps -a
```

#### Disable auto-upgrade for the connector

You disable automatic upgrades by setting the *isUpgradeDisabled* flag in the *com/opt/application/netapp/service-manager-2/config.json* file. By default, this flag is set to false and your connector is automatically upgraded. You can set this flag to true to disable automatic upgrades. You should be familiar with JSON syntax before completing this step.

To re-enable auto-upgrade, use these steps and set the *isUpgradeDisabled* flag to false.

**Steps**

1. Ensure you have verified that your connector is up-to-date and healthy.
2. Create a backup copy of the */opt/application/netapp/service-manager-2/config.json* file to ensure you can

revert your changes.

3. Edit the */opt/application/netapp/service-manager-2/config.json* file and change the value of the *isUpgradeDisabled* flag to true.

   ```
     "isUpgradeDisabled": true,
   ```

4. Save your file.
5. Restart the service manager 2 service by running the following command:

   ```
   systemctl restart netapp-service-manager.service
   ```

6. Run the following command and verify that the Connector status shows as *active(running)*:

   –

   ```
   systemctl status netapp-service-manager.service
   ```

#### Upgrade the connector

The Connector needs to restart during the upgrade process so the web-based console will be unavailable during the upgrade.

**Steps**

1. Download the Connector software from the NetApp Support Site.

   Be sure to download the offline installer for private networks without internet access.

2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

   ```
   chmod +x /path/BlueXP-Connector-Offline-<version>
   ```

   Where <version> is the version of the Connector that you downloaded.

4. Run the installation script:

   ```
   sudo /path/BlueXP-Connector-Offline-<version>
   ```

   Where <version> is the version of the Connector that you downloaded.

5. After the upgrade is complete, you can verify the Connector’s version by going to **Help > Support > Connector**.

## Work with multiple Connectors

If you use multiple Connectors, BlueXP enables you to switch between those Connectors directly from the console. You can also manage a single working environment with multiple Connectors.

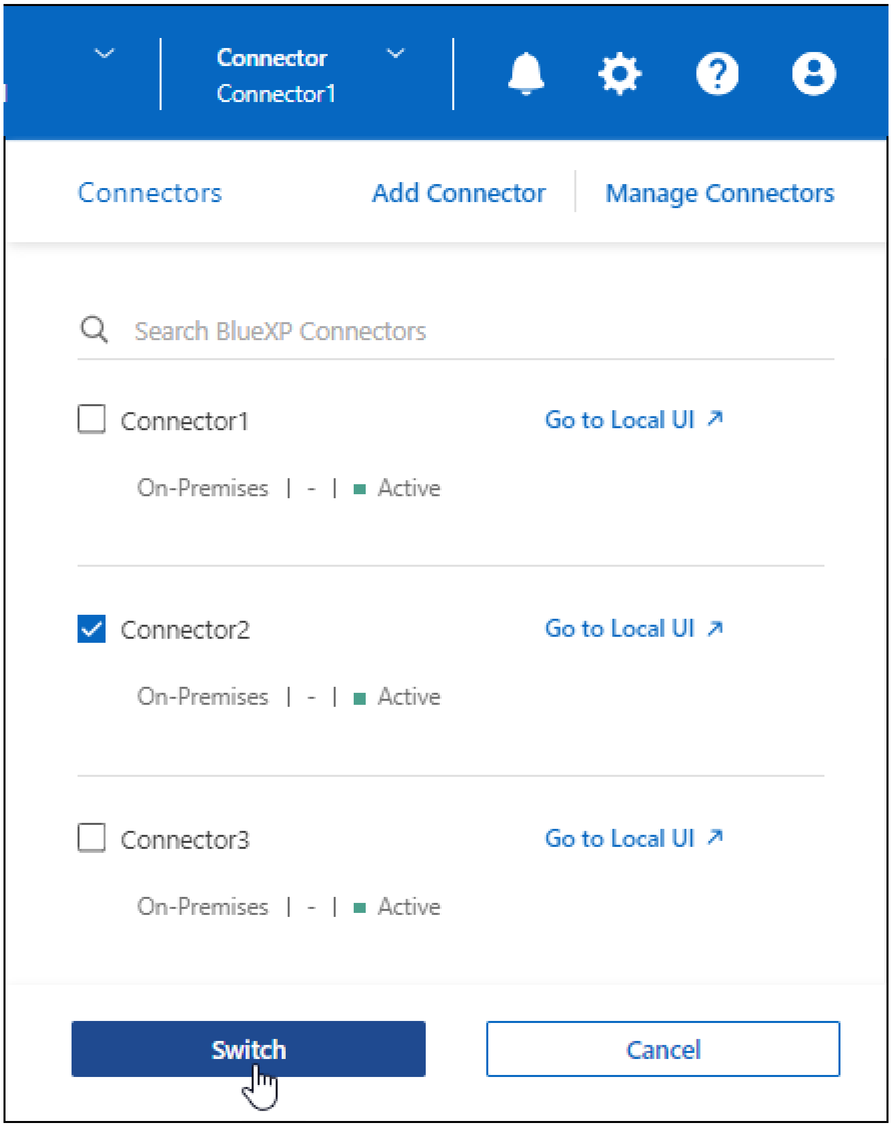
### Switch between Connectors

If you have multiple Connectors, you can switch between them to see the Working Environments that are associated with a specific Connector.

For example, let's say that you're working in a multi-cloud environment. You might have one Connector in AWS and another in Google Cloud. You'd need to switch between those Connectors to manage the Cloud Volumes ONTAP systems running in those clouds.

#### Step

1. Select the **Connector** drop-down, select another Connector, and then select **Switch**.



☐ Connector1
On-Premises | - | 🟩 Active

☑ Connector2
On-Premises | - | 🟩 Active

☐ Connector3
On-Premises | - | 🟩 Active

#### Result

BlueXP refreshes and shows the Working Environments associated with the selected Connector.

### Set up a disaster recovery configuration

You can manage a working environment with multiple Connectors at the same time for disaster recovery purposes. If one Connector goes down, you can switch to the other Connector to immediately manage the working environment.

**Steps**

1. Switch to the other Connector that you want to manage with the working environment.
2. Discover the existing working environment.
    - Add existing Cloud Volumes ONTAP systems to BlueXP
    - Discover ONTAP clusters
3. If you’re managing a Cloud Volumes ONTAP working environment, select **Settings > Connector Settings** and set the Capacity Management Mode to **Manual Mode**.

    To avoid contention issues, only the main Connector should be set to **Automatic Mode**.

    Learn more about the capacity management mode

## Troubleshoot the Connector

To troubleshoot issues with the Connector, you can work with NetApp Support who might ask for your system ID, Connector version, or the latest AutoSupport messages. You can also view the NetApp Knowledge Base to troubleshoot issues yourself.

**Related information**

Get help from NetApp Support.

### Find the system ID for a Connector

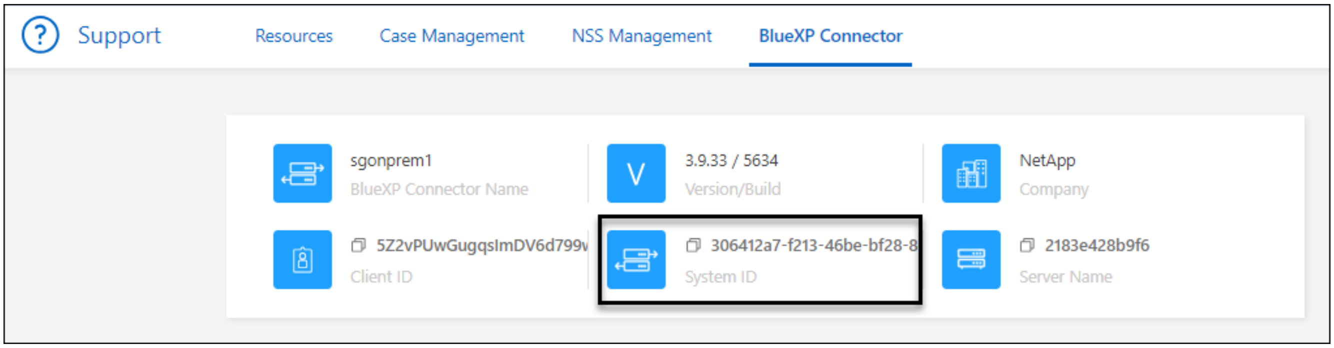
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

**Steps**

1. In the upper right of the BlueXP console, select the Help icon.
2. Select **Support > BlueXP Connector**.

    The system ID appears at the top of the page.

    **Example**



sgonprem1
BlueXP Connector Name

3.9.33 / 5634
Version/Build

NetApp
Company

5Z2vPUwGugqsImDV6d799v
Client ID

306412a7-f213-46be-bf28-8
System ID

2183e428b9f6
Server Name

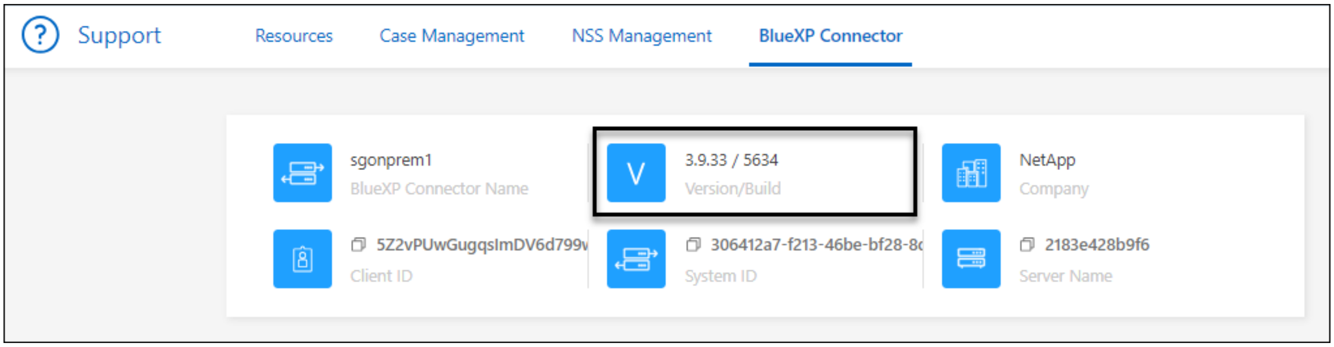
### View a Connector’s version

You can view the version of your Connector to verify that the Connector automatically upgraded to the latest release or because you need to share it with your NetApp representative.

#### Steps

1. In the upper right of the BlueXP console, select the Help icon.
2. Select **Support > BlueXP Connector**.

   The version displays at the top of the page.



sgonprem1
BlueXP Connector Name

3.9.33 / 5634
Version/Build

NetApp
Company

5Z2vPUwGugqsImDV6d799v
Client ID

306412a7-f213-46be-bf28-8c
System ID

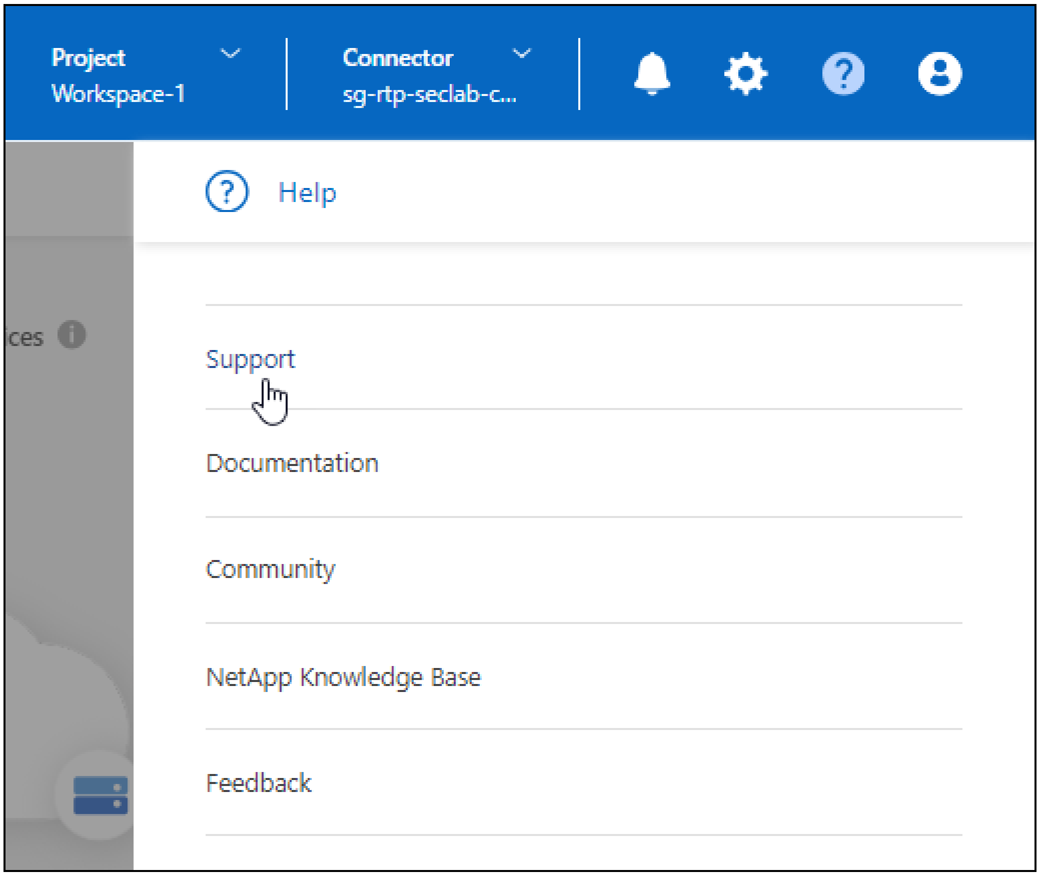
2183e428b9f6
Server Name

### Download or send an AutoSupport message

If you’re having problems, NetApp personnel might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

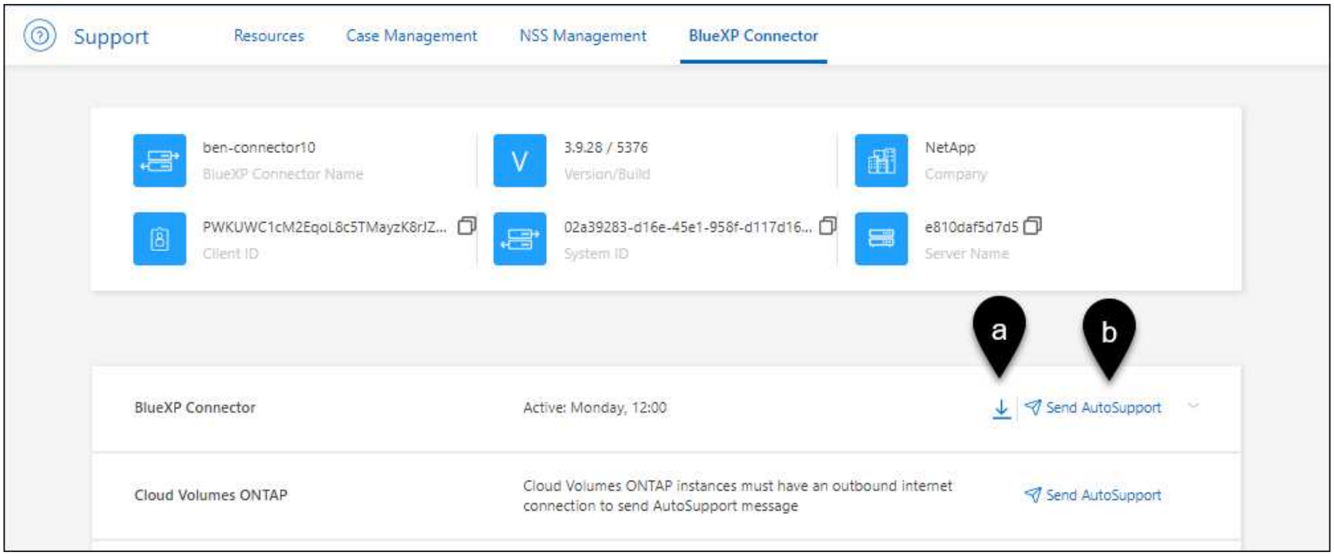
#### Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **BlueXP Connector**.
3. Depending on how you need to send the information to NetApp support, choose one of the following options:
    a. Select the option to download the AutoSupport message to your local machine. You can then send it to NetApp Support using a preferred method.
    b. Select **Send AutoSupport** to directly send the message to NetApp Support.

    BlueXP may take up to five hours to send AutoSupport messages due to load balancing. For urgent communication, download the file and send it manually.



BlueXP Connector Name: ben-connector10

Version/Build: 3.9.28 / 5376

Company: NetApp

Client ID: PWKUWC1cM2EqoL8c5TMayzK8rJZ...

System ID: 02a39283-d16e-45e1-958f-d117d16...

Server Name: e810daf5d7d5

BlueXP Connector — Active: Monday, 12:00

Cloud Volumes ONTAP — Cloud Volumes ONTAP instances must have an outbound internet connection to send AutoSupport message

### Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the BlueXP API.

**Step**

1. Submit a PUT request to /occm/config with the following JSON as body:

   ```
   {
     "maxDownloadSessions": 32
   }
   ```

   The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

   Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

Learn more about the /occm/config API call

### Get help from the NetApp Knowledge Base

View troubleshooting information created by the NetApp Support team.

## Uninstall and remove the Connector

Uninstall the Connector software to troubleshoot issues or to permanently remove the software from the host. The steps that you need to use depends on the deployment mode that you're using. Once a Connector has been removed from your environment, you can remove it from BlueXP.

Learn about BlueXP deployment modes.

### Uninstall the Connector when using standard or restricted mode

If you're using standard mode or restricted mode (in other words, the Connector host has outbound connectivity), then you should follow the steps below to uninstall the Connector software.

**Steps**

1. Connect to the Linux VM for the Connector.
2. From the Linux host, run the uninstallation script:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   *silent* runs the script without prompting you for confirmation.

### Uninstall the Connector when using private mode

If you're using private mode (where the Connector host has *no* outbound connectivity), follow the steps below to uninstall the Connector software.

**Step**

1. Connect to the Linux VM for the Connector.
2. From the Linux host, run the following commands:

```
/opt/application/netapp/ds/cleanup.sh
rm -rf /opt/application/netapp/
```

3. From the Linux host, delete old, unused container image files to free space in the /var directory for re-installation.

**Podman**

```
podman system prune --all
```

**Docker**

```
docker system prune -a
```

### Remove Connectors from BlueXP

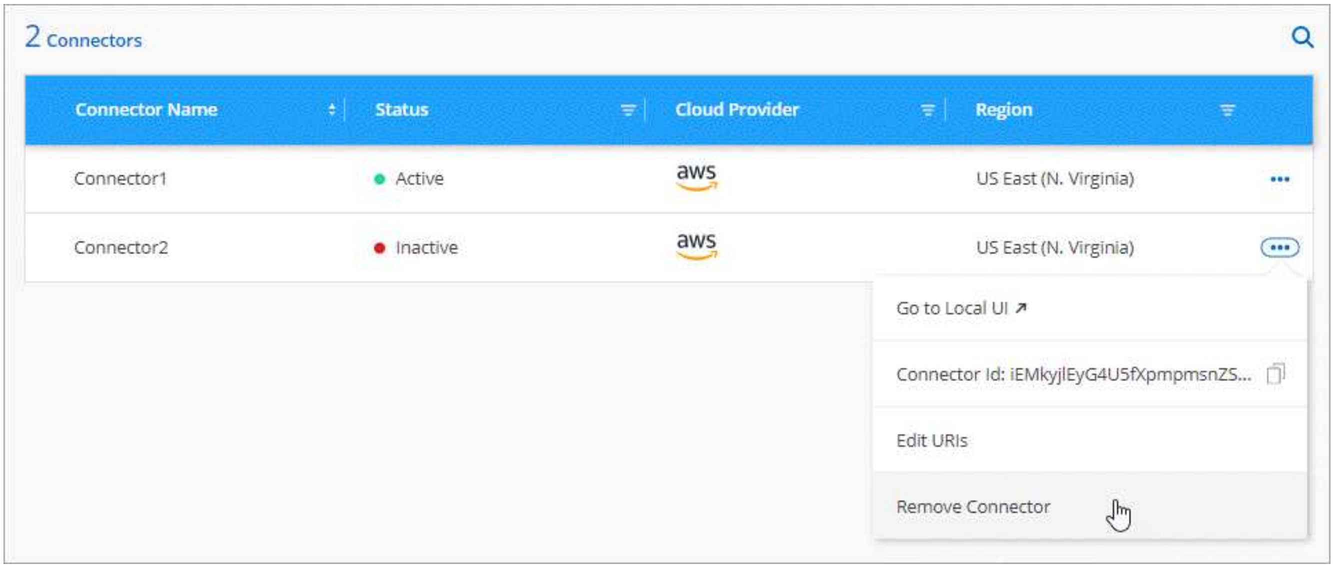
If a Connector is inactive, you can remove it from the list of Connectors in BlueXP. You might do this if you delete the Connector virtual machine or if you uninstall the Connector software.

Note the following about removing a Connector:

- This action doesn't delete the virtual machine.
- This action can't be reverted—once you remove a Connector, you can't add it back.

**Steps**

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu for an inactive Connector and select **Remove Connector**.



2 Connectors

| Connector Name | Status | Cloud Provider | Region |
|---|---|---|---|
| Connector1 | ● Active | aws | US East (N. Virginia) |
| Connector2 | ● Inactive | aws | US East (N. Virginia) |

4. Enter the name of the Connector to confirm and then select **Remove**.

## Default configuration for the Connector

You might want to learn more about the Connector’s configuration before you deploy it, or if you need to troubleshoot any issues.

### Default configuration with internet access

The following configuration details apply if you deployed the Connector from BlueXP, from your cloud provider’s marketplace, or if you manually installed the Connector on an on-premises Linux host that has internet access.

#### AWS details

If you deployed the Connector from BlueXP or from the cloud provider’s marketplace, note the following:

- The EC2 instance type is t3.2xlarge.
- The operating system for the image is Ubuntu 22.04 LTS.

  The operating system does not include a GUI. You must use a terminal to access the system.
- The installation includes Docker Engine, which is the required container orchestration tool.
- The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was ec2-user).
- The default system disk is a 100 GiB gp2 disk.

#### Azure details

If you deployed the Connector from BlueXP or from the cloud provider’s marketplace, note the following:

- The VM type is Standard_D8s_v3.
- The operating system for the image is Ubuntu 22.04 LTS.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The installation includes Docker Engine, which is the required container orchestration tool.
- The default system disk is a 100 GiB premium SSD disk.

#### Google Cloud details

If you deployed the Connector from BlueXP, note the following:

- The VM instance is n2-standard-8.
- The operating system for the image is Ubuntu 22.04 LTS.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The installation includes Docker Engine, which is the required container orchestration tool.
- The default system disk is a 100 GiB SSD persistent disk.

#### Installation folder

The Connector installation folder resides in the following location:

/opt/application/netapp/cloudmanager

#### Log files

Log files are contained in the following folders:

- /opt/application/netapp/cloudmanager/log
  or
- /opt/application/netapp/service-manager-2/logs (starting with new 3.9.23 installations)

  The logs in these folders provide details about the Connector.

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  The logs in this folder provide details about cloud services and the BlueXP service that runs on the Connector.

#### Connector service

- The BlueXP service is named occm.
- The occm service is dependent on the MySQL service.

  If the MySQL service is down, then the occm service is down too.

#### Ports

The Connector uses the following ports on the Linux host:

- 80 for HTTP access
- 443 for HTTPS access

### Default configuration without internet access

The following configuration applies if you manually installed the Connector on an on-premises Linux host that doesn’t have internet access. Learn more about this installation option.

- The Connector installation folder resides in the following location:

  /opt/application/netapp/ds

- Log files are contained in the following folders:

  /var/lib/docker/volumes/ds_occmdata/_data/log

  The logs in this folder provide details about the Connector and docker images.

- All services are running inside docker containers

  The services are dependent on the docker runtime service running

- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
  - 443 for HTTPS access

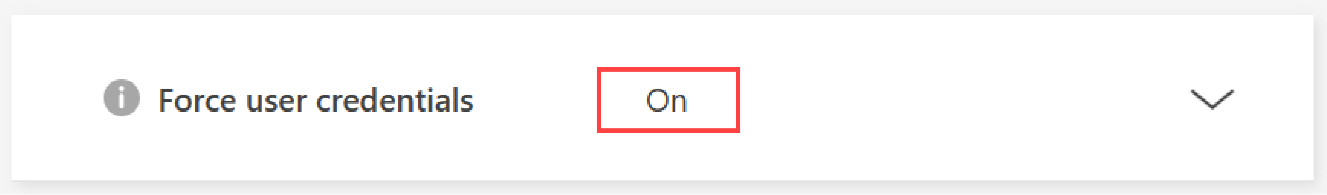
## Enforce ONTAP permissions for ONTAP Advanced View (ONTAP System Manager)

By default, the Connector credentials allow users to access the Advanced View (ONTAP System Manager). You can prompt users for their ONTAP credentials instead. This ensures that a user’s ONTAP permissions are applied when they work with ONTAP clusters in both Cloud Volumes ONTAP and ONTAP on-premises clusters.

ⓘ You must have the Organization admin role to edit Connector settings.

**Steps**

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu in the row that corresponds to the Connector you want to edit.
4. Expand the **Force Credentials** option.
5. Select the checkbox to enable the **Force Credentials** option and then select **Save**.
6. Check if the **Force Credentials** option is enabled.



Force user credentials On

# Credentials and subscriptions

## AWS

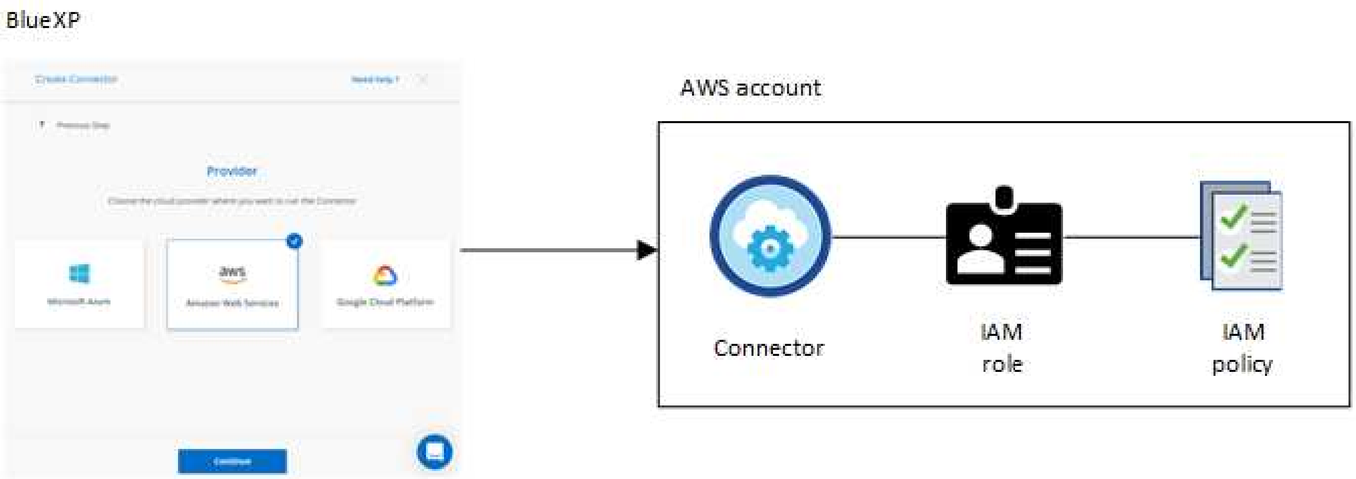
### Learn about AWS credentials and permissions in BlueXP

Learn how BlueXP uses AWS credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more AWS accounts in BlueXP. For example, you might want to learn about when to add additional AWS credentials to BlueXP.

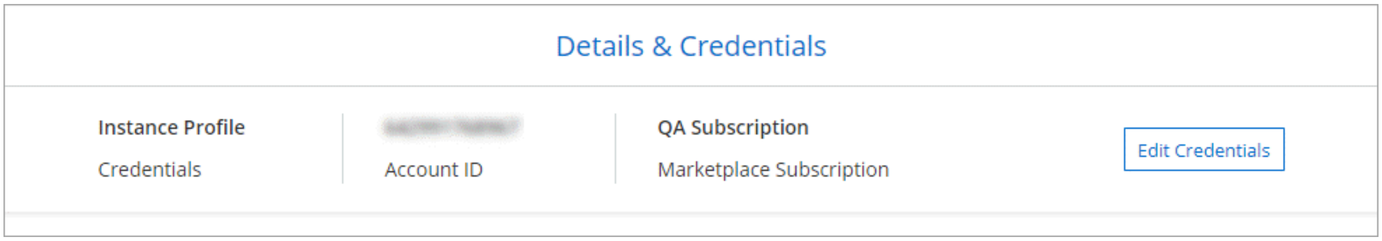
#### Initial AWS credentials

When you deploy a Connector from BlueXP, you need to provide the ARN of an IAM role or access keys for an IAM user. The authentication method that you use must have the required permissions to deploy the Connector instance in AWS. The required permissions are listed in the Connector deployment policy for AWS.

When BlueXP launches the Connector instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides the Connector with permissions to manage resources and processes within that AWS account. Review how BlueXP uses the permissions.



If you create a new working environment for Cloud Volumes ONTAP, BlueXP selects these AWS credentials by default:



Details & Credentials

Instance Profile
Credentials

[redacted]
Account ID

QA Subscription
Marketplace Subscription

You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

#### Additional AWS credentials

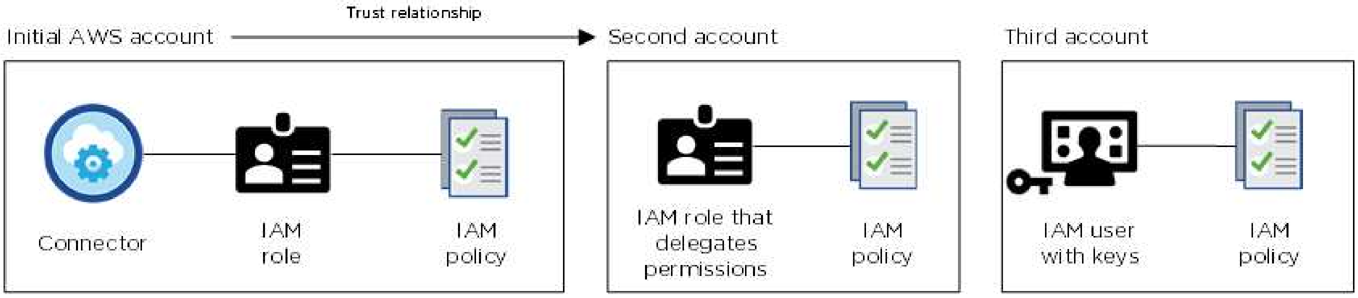
You might add additional AWS credentials to BlueXP in the following cases:

- To use your existing BlueXP Connector with an additional AWS account
- To create a new Connector in a specific AWS account
- To create and manage FSx for ONTAP file systems

Review the sections below for more details.

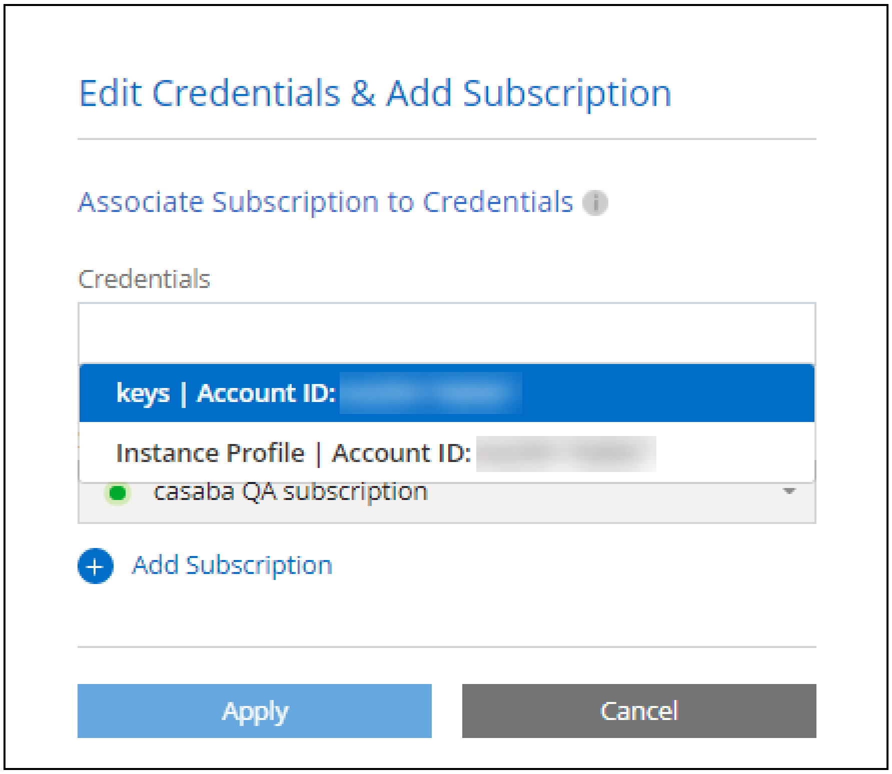
### Add AWS credentials to use a Connector with another AWS account

If you want to use BlueXP with additional AWS accounts, then you can either provide AWS keys for an IAM user or the ARN of a role in a trusted account. The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:



You would then add the account credentials to BlueXP by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP working environment:



Edit Credentials & Add Subscription

Associate Subscription to Credentials

Credentials

keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

casaba QA subscription

Learn how to add AWS credentials to an existing Connector.

#### Add AWS credentials to create a Connector

Adding new AWS credentials to BlueXP provides the permissions needed to create a Connector.

Learn how to add AWS credentials to BlueXP for creating a Connector

#### Add AWS credentials for FSx for ONTAP

Adding new AWS credentials to BlueXP provides the permissions needed to create and manage an FSx for ONTAP working environment.

Learn how to add AWS credentials to BlueXP for Amazon FSx for ONTAP

##### Credentials and marketplace subscriptions

The credentials that you add to a Connector must be associated with an AWS Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or through an annual contract, and to use other BlueXP services.

Learn how to associate an AWS subscription.

Note the following about AWS credentials and marketplace subscriptions:

- You can associate only one AWS Marketplace subscription with a set of AWS credentials
- You can replace an existing marketplace subscription with a new subscription

##### FAQ

The following questions are related to credentials and subscriptions.

### How can I securely rotate my AWS credentials?

As described in the sections above, BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a regular interval. This is a completely manual process.

### Can I change the AWS Marketplace subscription for Cloud Volumes ONTAP working environments?

Yes, you can. When you change the AWS Marketplace subscription that's associated with a set of credentials, all existing and new Cloud Volumes ONTAP working environments will be charged against the new subscription.

Learn how to associate an AWS subscription.

### Can I add multiple AWS credentials, each with different marketplace subscriptions?

All AWS credentials that belong to the same AWS account will be associated with the same AWS Marketplace subscription.

If you have multiple AWS credentials that belong to different AWS accounts, then those credentials can be associated with the same AWS Marketplace subscription or with different subscriptions.

### Can I move existing Cloud Volumes ONTAP working environments to a different AWS account?

No, it's not possible to move the AWS resources associated with your Cloud Volumes ONTAP working environment to a different AWS account.

### How do credentials work for marketplace deployments and on-premisesdeployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in AWS from the AWS Marketplace and you can manually install the Connector software on your own Linux host.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up an IAM role for the BlueXP system, but you can provide permissions using AWS access keys.

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

- Standard mode
  - Set up permissions for an AWS Marketplace deployment
  - Set up permissions for on-premisesdeployments
- Set up permissions for restricted mode
- Set up permissions for private mode

### Manage AWS credentials and marketplace subscriptions for BlueXP

Add and manage AWS credentials so that you deploy and manage cloud resources in your AWS accounts from BlueXP. If you manage multiple AWS Marketplace subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

#### Overview

You can add AWS credentials to an existing Connector or directly to BlueXP:

- Add additional AWS credentials to an existing Connector

  Add AWS credentials to a Connector to manage resources in your cloud environment. Learn how to add AWS credentials to a Connector.

- Add AWS credentials to BlueXP for creating a Connector

  Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create a Connector. Learn how to add AWS credentials to BlueXP.

- Add AWS credentials to BlueXP for FSx for ONTAP

  Add new AWS credentials to BlueXP to create and manage FSx for ONTAP. Learn how to set up permissions for FSx for ONTAP

#### How to rotate credentials

BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. Learn more about AWS credentials and permissions.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice because it’s automatic and it’s secure.

Rotate AWS access keys regularly by updating them in BlueXP. This process is manual.

#### Add additional credentials to a Connector

Add additional AWS credentials to a Connector so that it has the permissions needed to manage resources and processes within your public cloud environment. You can either provide the ARN of an IAM role in another account or provide AWS access keys.

If you’re just getting started with BlueXP, Learn how BlueXP uses AWS credentials and permissions.

### Grant permissions

Provide required permissions before adding AWS credentials to a Connector. The permissions allow the Connector to manage resources and processes within that AWS account. You can provide the permissions with the the ARN of a role in a trusted account or AWS keys.

> ⓘ If you deployed a Connector from BlueXP, BlueXP automatically added AWS credentials for the account in which you deployed the Connector. This ensures the necessary permissions are in place for managing resources. Learn about AWS credentials and permissions.

#### Choices

- Grant permissions by assuming an IAM role in another account
- Grant permissions by providing AWS keys

#### Grant permissions by assuming an IAM role in another account

You can set up a trust relationship between the source AWS account in which you deployed the Connector instance and other AWS accounts by using IAM roles. You would then provide BlueXP with the ARN of the IAM roles from the trusted accounts.

If the Connector is installed on-premises, you can’t use this authentication method. You must use AWS keys.

#### Steps

1. Go to the IAM console in the target account in which you want to provide the Connector with permissions.
2. Under Access Management, select **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the account where the Connector instance resides.
   - Create the required policies by copying and pasting the contents of the IAM policies for the Connector.
3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP later on.

#### Result

The account now has the required permissions. You can now add the credentials to a Connector.

#### Grant permissions by providing AWS keys

If you want to provide BlueXP with AWS keys for an IAM user, then you need to grant the required permissions to that user. The BlueXP IAM policy defines the AWS actions and resources that BlueXP is allowed to use.

You must use this authentication method if the Connector is installed on-premises. You can’t use an IAM role.

#### Steps

1. From the IAM console, create policies by copying and pasting the contents of the IAM policies for the Connector.

   AWS Documentation: Creating IAM Policies
2. Attach the policies to an IAM role or an IAM user.
   - AWS Documentation: Creating IAM Roles
   - AWS Documentation: Adding and Removing IAM Policies

#### Result

The account now has the required permissions. You can now add the credentials to a Connector.

#### Add the credentials

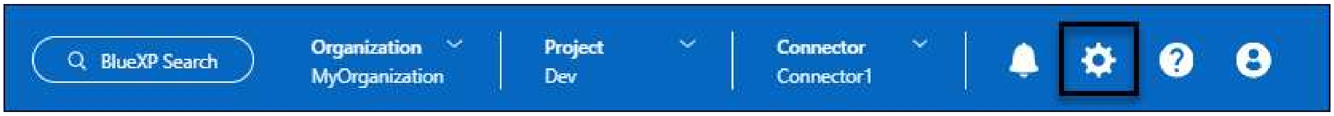
After you provide an AWS account with the required permissions, you can add the credentials for that account to an existing Connector. This enables you to launch Cloud Volumes ONTAP systems in that account using the same Connector.

**Before you begin**

If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes and then add you add the credentials.

**Steps**

1. Use the top navigation bar to elect the Connector to which you want to add credentials.
2. In the upper right of the console, select the Settings icon, and select **Credentials**.



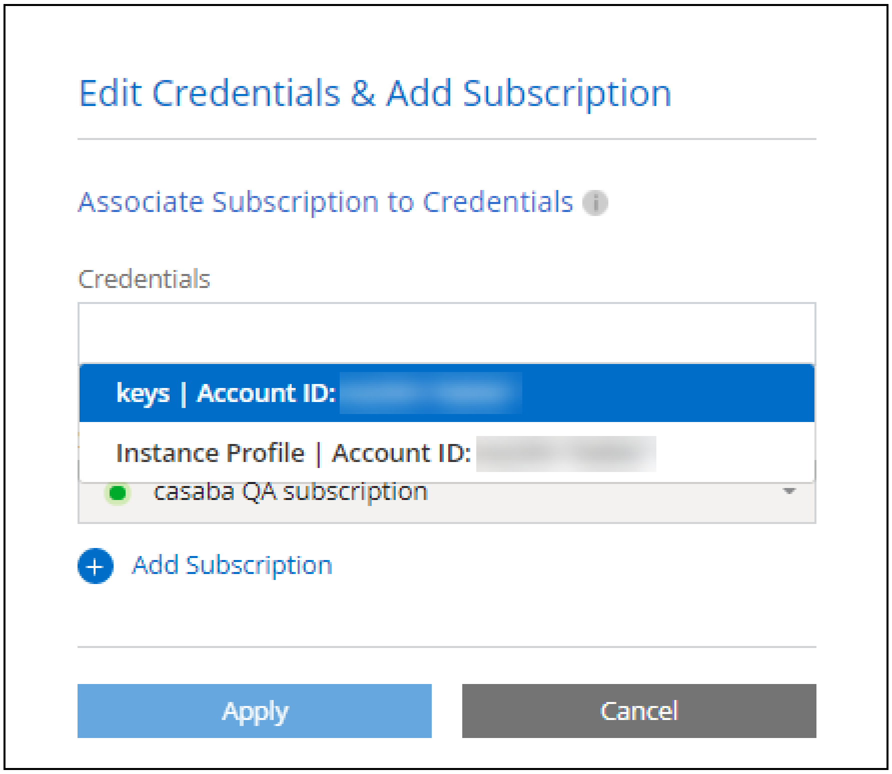
3. On the **Organization credentials** or **Account credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > Connector**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of a trusted IAM role, or enter an AWS access key and secret key.
   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

      To pay for services at an hourly rate (PAYGO) or with an annual contract, you must associate AWS credentials with your AWS Marketplace subscription.

   d. **Review**: Confirm the details about the new credentials and select **Add**.

**Result**

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:



Edit Credentials & Add Subscription

Associate Subscription to Credentials

Credentials

keys | Account ID: [redacted]

Instance Profile | Account ID: [redacted]

casaba QA subscription

**Add credentials to BlueXP for creating a Connector**

Add AWS credentials by providing the ARN of an IAM role that gives the permissions needed to create a Connector. You can choose these credentials when creating a new Connector.

### Set up the IAM role

Set up an IAM role that enables the BlueXP software as a service (SaaS) layer to assume the role.

**Steps**

1. Go to the IAM console in the target account.
2. Under Access Management, select **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the BlueXP SaaS: 952013314444
   - For Amazon FSx for NetApp ONTAP specifically, edit the **Trust relationships** policy to include "AWS": "arn:aws:iam::952013314444:root".

     For example, the policy should look like this:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Refer to AWS Identity and Access Management (IAM) documentation for more information on cross account resource access in IAM.

- Create a policy that includes the permissions required to create a Connector.
  - View the permissions needed for FSx for ONTAP
  - View the Connector deployment policy

3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP in the next step.

**Result**

The IAM role now has the required permissions. You can now add it to BlueXP.

### Add the credentials

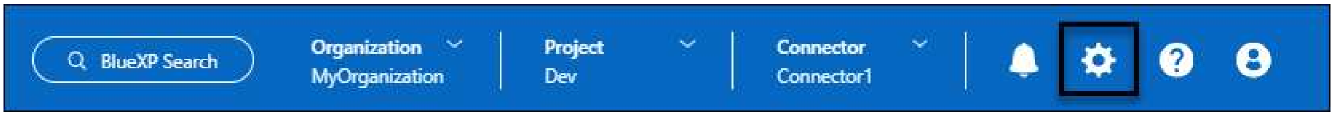
After you provide the IAM role with the required permissions, add the role ARN to BlueXP.

**Before you begin**

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

**Steps**

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.



2. On the **Organization credentials** or **Account credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > BlueXP**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.
   c. **Review**: Confirm the details about the new credentials and select **Add**.

#### Add credentials to BlueXP for Amazon FSx for ONTAP

For details, refer to the BlueXP documentation for Amazon FSx for ONTAP

#### Configure an AWS subscription

After you add your AWS credentials, you can configure an AWS Marketplace subscription with those credentials. The subscription enables you to pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or using an annual contract, and to pay for other data services.

There are two scenarios in which you might configure an AWS Marketplace subscription after you've already added the credentials:

- You didn't configure a subscription when you initially added the credentials.
- You want to change the AWS Marketplace subscription that is configured to the AWS credentials.

  Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

### Before you begin

You need to create a Connector before you can configure a subscription. Learn how to create a Connector.

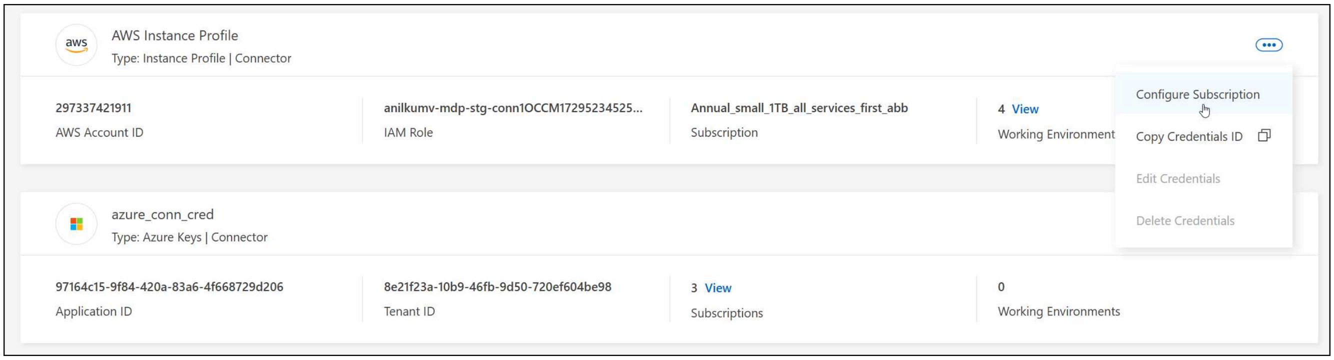
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

Subscribe to NetApp Intelligent Services from the AWS Marketplace

### Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

   You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.



AWS Instance Profile
Type: Instance Profile | Connector

AWS Account ID: 297337421911
IAM Role: anilkumv-mdp-stg-conn1OCCM17295234525...
Subscription: Annual_small_1TB_all_services_first_abb
Working Environment: 4 View

azure_conn_cred
Type: Azure Keys | Connector

Application ID: 97164c15-9f84-420a-83a6-4f668729d206
Tenant ID: 8e21f23a-10b9-46fb-9d50-720ef604be98
Subscriptions: 3 View
Working Environments: 0

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
   a. Select **View purchase options**.
   b. Select **Subscribe**.

c. Select **Set up your account**.

   You'll be redirected to the BlueXP website.

d. From the **Subscription Assignment** page:

   - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
   - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

     BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

     For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

   - Select **Save**.

#### Associate an existing subscription with your organization or account

When you subscribe to from the AWS Marketplace, the last step in the process is to associate the subscription with your organization. If you didn't complete this step, then you can't use the subscription with your organization or account.

- Learn about BlueXP deployment modes
- Learn about BlueXP identity and access management

Follow the steps below if you subscribed to NetApp intelligent data services from the AWS Marketplace, but you missed the step to associate the subscription with your account.

**Steps**

1. Go to the digital wallet to confirm that you didn't associate your subscription with your BlueXP organization or account.

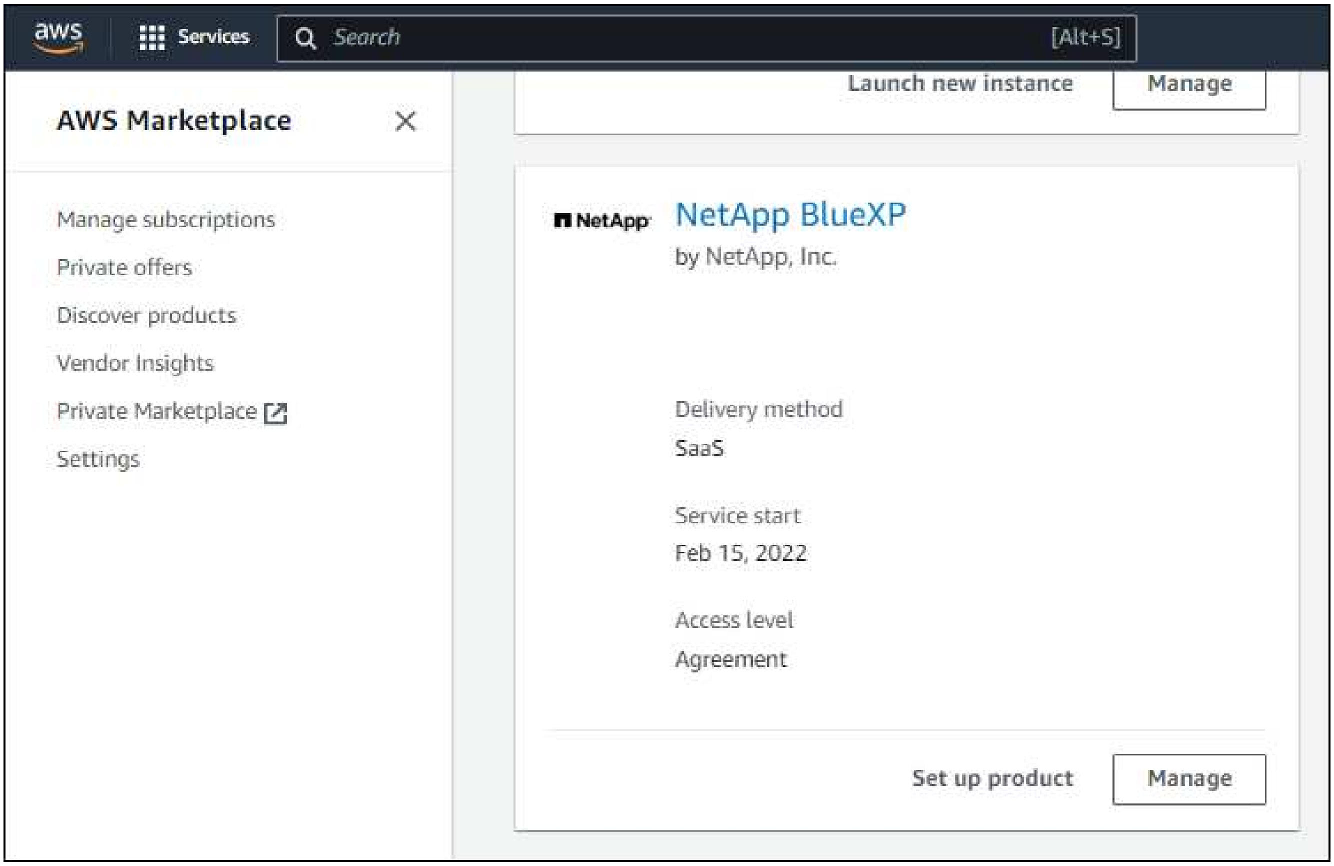
   a. From the navigation menu, select **Governance > Digital wallet**.

   b. Select **Subscriptions**.

   c. Verify that your subscription doesn't appear.

      You'll only see the subscriptions that are associated with the organization or account that you're currently viewing. If you don't see your subscription, proceed with the following steps.

2. Log in to the AWS Console and navigate to **AWS Marketplace Subscriptions**.
3. Find the NetApp Intelligent Data Services subscription.



Delivery method
SaaS

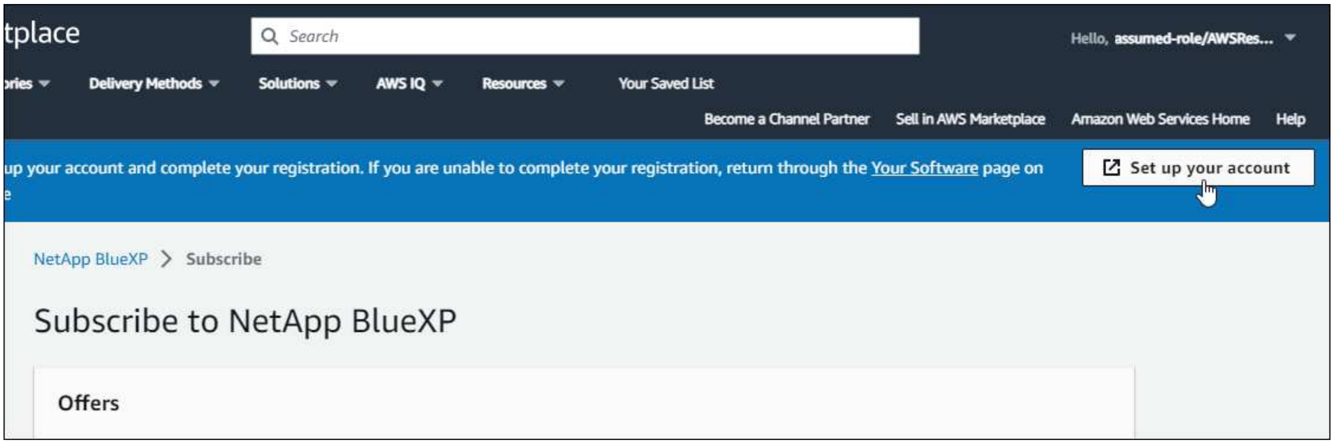
Service start
Feb 15, 2022

Access level
Agreement

4. Select **Set up product**.

   The subscription offer page should load in a new browser tab or window.

5. Select **Set up your account**.



up your account and complete your registration. If you are unable to complete your registration, return through the Your Software page on e

Subscribe to NetApp BlueXP

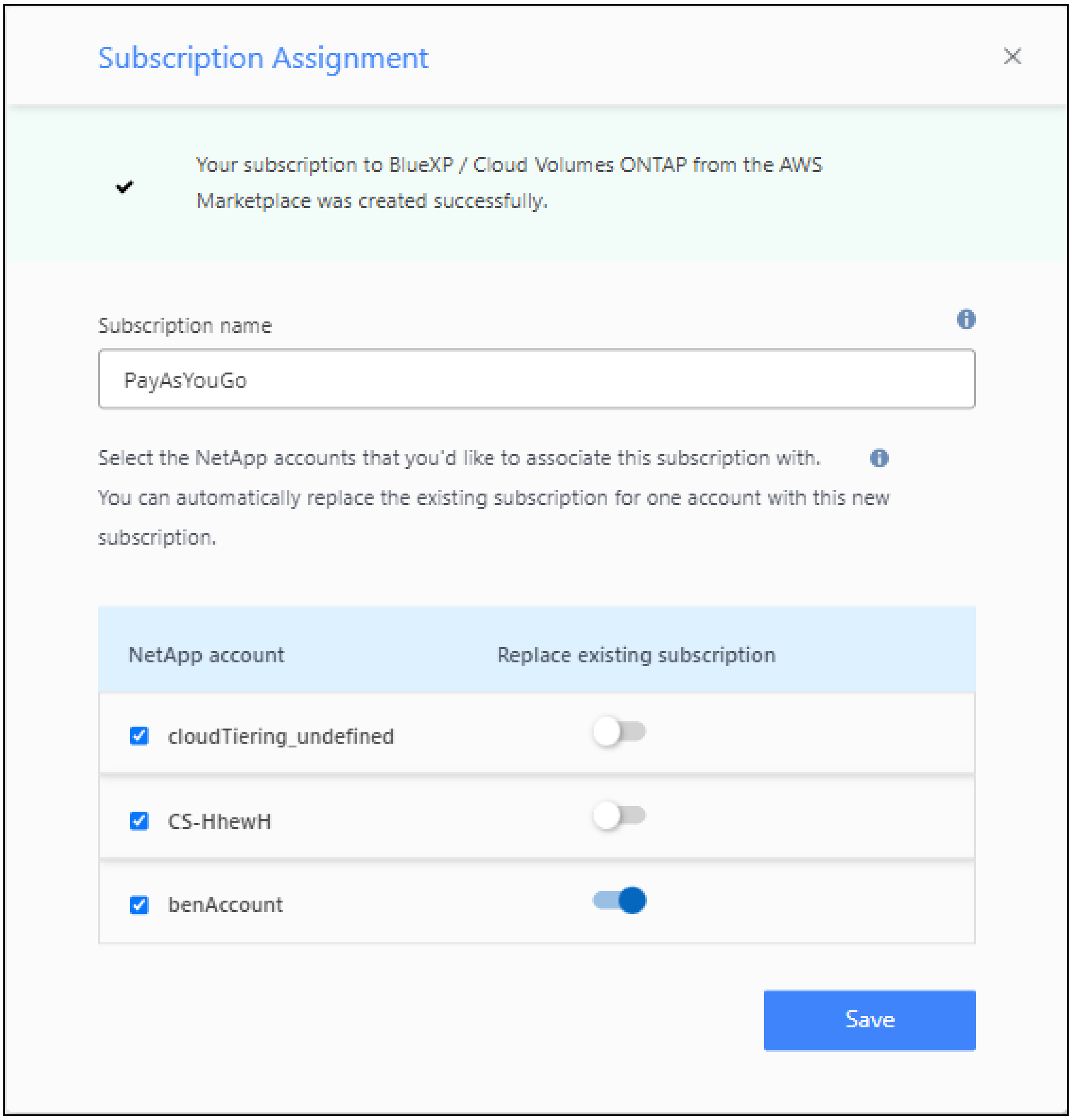
   The **Subscription Assignment** page on netapp.com should load in a new browser tab or window.

   Note that you might be prompted to log in to BlueXP first.

6. From the **Subscription Assignment** page:
   - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
   - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.



Subscription Assignment

✓ Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name

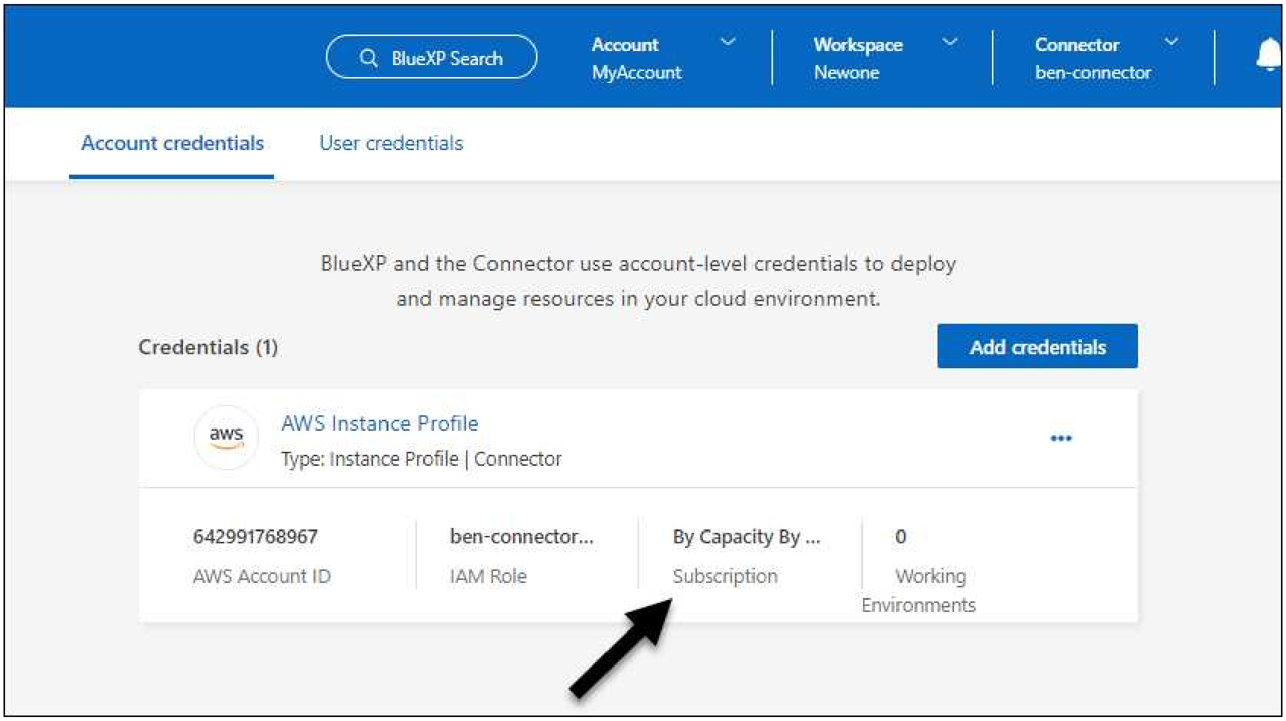
PayAsYouGo

Select the NetApp accounts that you'd like to associate this subscription with. You can automatically replace the existing subscription for one account with this new subscription.

| NetApp account | Replace existing subscription |
|---|---|
| ☑ cloudTiering_undefined | ○ |
| ☑ CS-HhewH | ○ |
| ☑ benAccount | ● |

7. Go to the digital wallet to confirm that the subscription is associated with your organization or account.
    a. From the navigation menu, select **Governance > Digital wallet**.
    b. Select **Subscriptions**.
    c. Verify that your subscription appears.
8. Confirm that the subscription is associated with your AWS credentials.
    a. In the upper right of the console, select the Settings icon, and select **Credentials**.
    b. On the **Organization credentials** or **Account credentials** page, verify that the subscription is associated with your AWS credentials.

Here's an example.



BlueXP and the Connector use account-level credentials to deploy and manage resources in your cloud environment.

Credentials (1)

AWS Instance Profile
Type: Instance Profile | Connector

| | | | |
|---|---|---|---|
| 642991768967 | ben-connector... | By Capacity By ... | 0 |
| AWS Account ID | IAM Role | Subscription | Working Environments |

#### Edit credentials

Edit your AWS credentials by changing the account type (AWS keys or assume role), by editing the name, or by updating the credentials themselves (the keys or the role ARN).

> You can't edit the credentials for an instance profile that is associated with a Connector instance or an Amazon FSx for ONTAP instance. You can only rename the credentials for an FSx for ONTAP instance.

**Steps**

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

#### Delete credentials

If you no longer need a set of credentials, you can delete them. You can only delete credentials that aren't associated with a working environment.

> You can't delete the credentials for an instance profile that is associated with a Connector instance.

**Steps**

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.

3. Select **Delete** to confirm.

## Azure

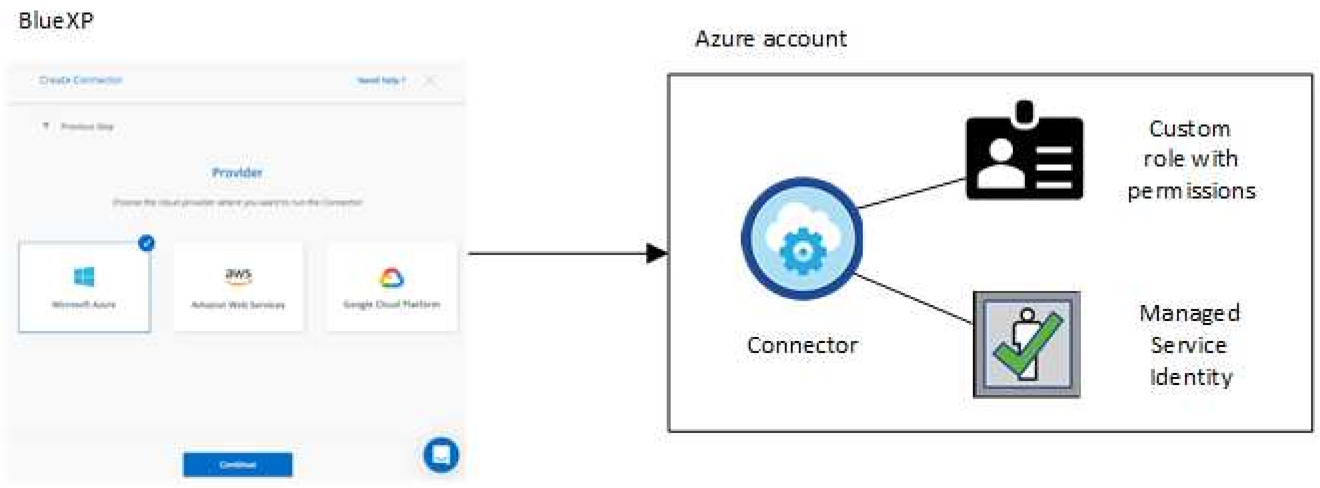
### Learn about Azure credentials and permissions in BlueXP

Learn how BlueXP uses Azure credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more Azure subscriptions. For example, you might want to learn when to add additional Azure credentials to BlueXP.

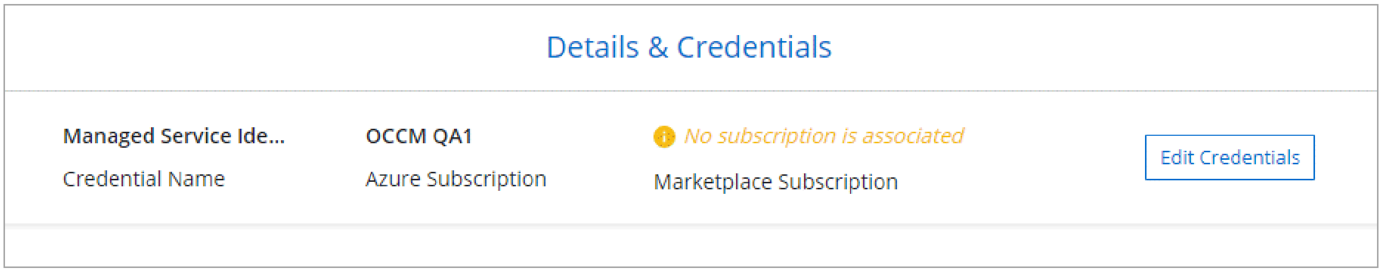
#### Initial Azure credentials

When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector virtual machine. The required permissions are listed in the Connector deployment policy for Azure.

When BlueXP deploys the Connector virtual machine in Azure, it enables a system-assigned managed identity on the virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides BlueXP with the permissions required to manage resources and processes within that Azure subscription. Review how BlueXP uses the permissions.



If you create a new working environment for Cloud Volumes ONTAP, BlueXP selects these Azure credentials by default:



Details & Credentials

Managed Service Ide...
Credential Name

OCCM QA1
Azure Subscription

No subscription is associated
Marketplace Subscription

Edit Credentials

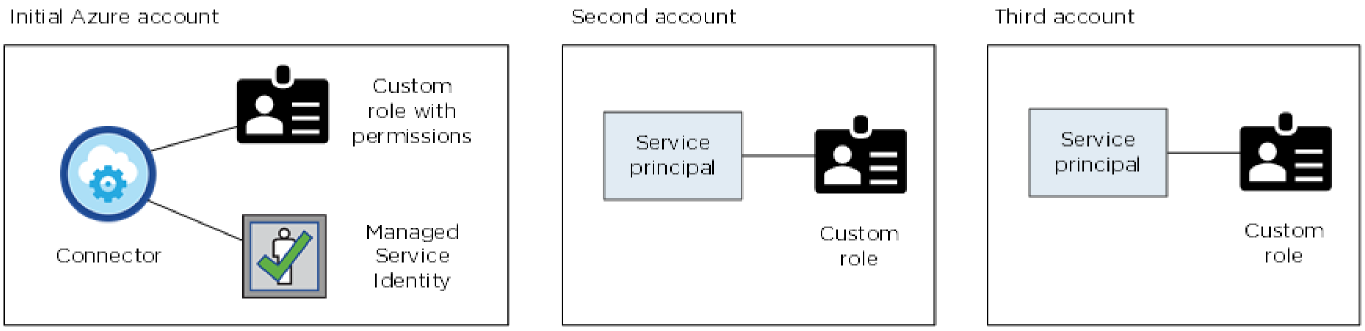
You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

### Additional Azure subscriptions for a managed identity

The system-assigned managed identity assigned to the Connector VM is associated with the subscription in which you launched the Connector. If you want to select a different Azure subscription, then you need to associate the managed identity with those subscriptions.

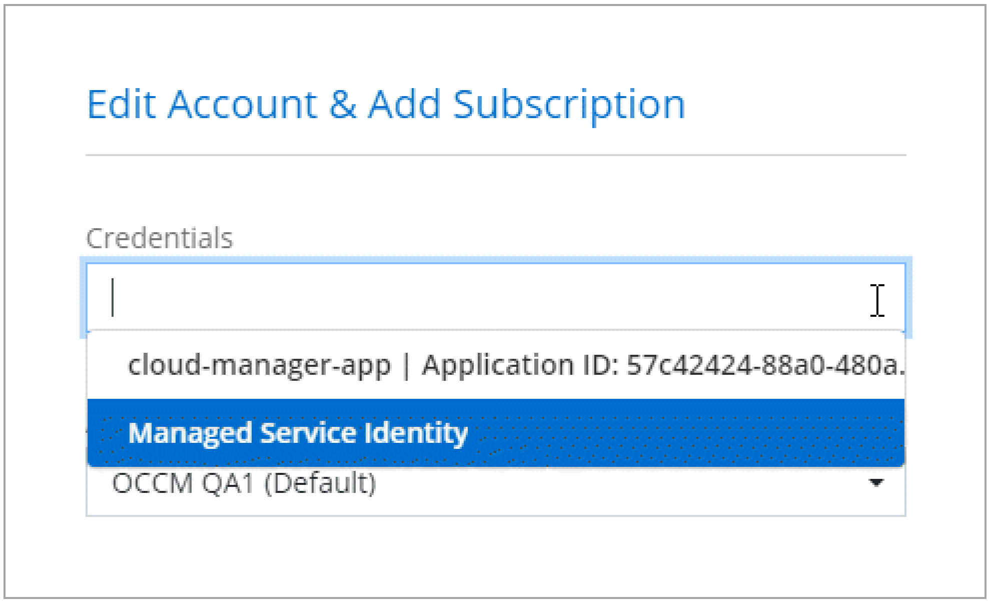
### Additional Azure credentials

If you want to use different Azure credentials with BlueXP, then you must grant the required permissions by creating and setting up a service principal in Microsoft Entra ID for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:



You would then add the account credentials to BlueXP by providing details about the AD service principal.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP working environment:


Edit Account & Add Subscription

Credentials

cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

### Credentials and marketplace subscriptions

The credentials that you add to a Connector must be associated with an Azure Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or through an annual contract, and to use other BlueXP services.

Learn how to associate an Azure subscription.

Note the following about Azure credentials and marketplace subscriptions:

- You can associate only one Azure Marketplace subscription with a set of Azure credentials
- You can replace an existing marketplace subscription with a new subscription

#### FAQ

The following question is related to credentials and subscriptions.

### Can I change the Azure Marketplace subscription for Cloud Volumes ONTAP working environments?

Yes, you can. When you change the Azure Marketplace subscription that’s associated with a set of Azure credentials, all existing and new Cloud Volumes ONTAP working environments will be charged against the new subscription.

Learn how to associate an Azure subscription.

### Can I add multiple Azure credentials, each with different marketplace subscriptions?

All Azure credentials that belong to the same Azure subscription will be associated with the same Azure Marketplace subscription.

If you have multiple Azure credentials that belong to different Azure subscriptions, then those credentials can be associated with the same Azure Marketplace subscription or with different marketplace subscriptions.

### Can I move existing Cloud Volumes ONTAP working environments to a different Azure subscription?

No, it’s not possible to move the Azure resources associated with your Cloud Volumes ONTAP working environment to a different Azure subscription.

### How do credentials work for marketplace deployments and on-premisesdeployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in Azure from the Azure Marketplace, and you can install the Connector software on your own Linux host.

If you use the Marketplace, you can provide permissions by assigning a custom role to the Connector VM and to a system-assigned managed identity, or you can use a Microsoft Entra service principal.

For on-premises deployments, you can’t set up a managed identity for the Connector, but you can provide permissions by using a service principal.

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

- Standard mode
  - Set up permissions for an Azure Marketplace deployment
  - Set up permissions for on-premisesdeployments
- Set up permissions for restricted mode
- Set up permissions for private mode

### Manage Azure credentials and marketplace subscriptions for BlueXP

Add and manage Azure credentials so that BlueXP has the permissions that it needs to deploy and manage cloud resources in your Azure subscriptions. If you manage multiple

Azure Marketplace subscriptions, you can assign each one of them to different Azure credentials from the Credentials page.

Follow the steps on this page if you need to use multiple Azure credentials or multiple Azure Marketplace subscriptions for Cloud Volumes ONTAP.

#### Overview

There are two ways to add additional Azure subscriptions and credentials in BlueXP.

1. Associate additional Azure subscriptions with the Azure managed identity.
2. If you want to deploy Cloud Volumes ONTAP using different Azure credentials, grant Azure permissions using a service principal and add its credentials to BlueXP.

#### Associate additional Azure subscriptions with a managed identity

BlueXP enables you to choose the Azure credentials and Azure subscription in which you want to deploy Cloud Volumes ONTAP. You can’t select a different Azure subscription for the managed identity profile unless you associate the managed identity with those subscriptions.

##### About this task

A managed identity is the initial Azure account when you deploy a Connector from BlueXP. When you deployed the Connector, BlueXP created the BlueXP Operator role and assigned it to the Connector virtual machine.

##### Steps

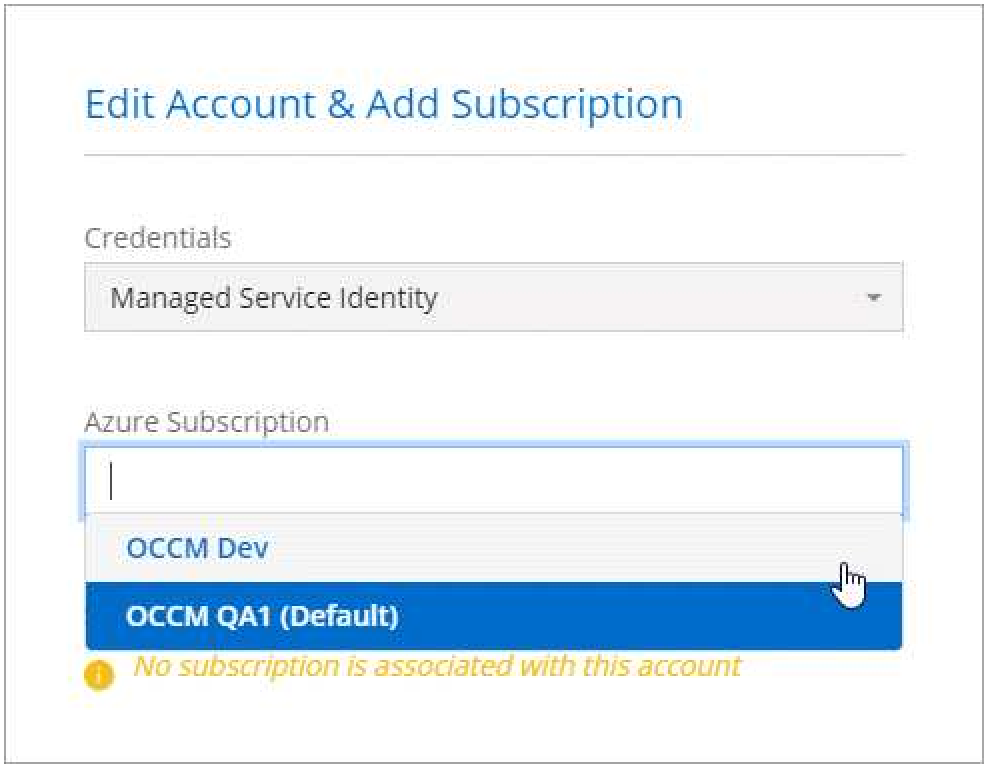
1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Select **Access control (IAM)**.
   a. Select **Add** > **Add role assignment** and then add the permissions:
      - Select the **BlueXP Operator** role.

        > ⓘ BlueXP Operator is the default name provided in the Connector policy. If you chose a different name for the role, then select that name instead.

      - Assign access to a **Virtual Machine**.
      - Select the subscription in which the Connector virtual machine was created.
      - Select the Connector virtual machine.
      - Select **Save**.
4. Repeat these steps for additional subscriptions.

##### Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions for the managed identity profile.



Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

No subscription is associated with this account

**Add additional Azure credentials to BlueXP**

When you deploy a Connector from BlueXP, BlueXP enables a system-assigned managed identity on the virtual machine that has the required permissions. BlueXP selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP.

> An initial set of credentials isn’t added if you manually installed the Connector software on an existing system. Learn about Azure credentials and permissions.

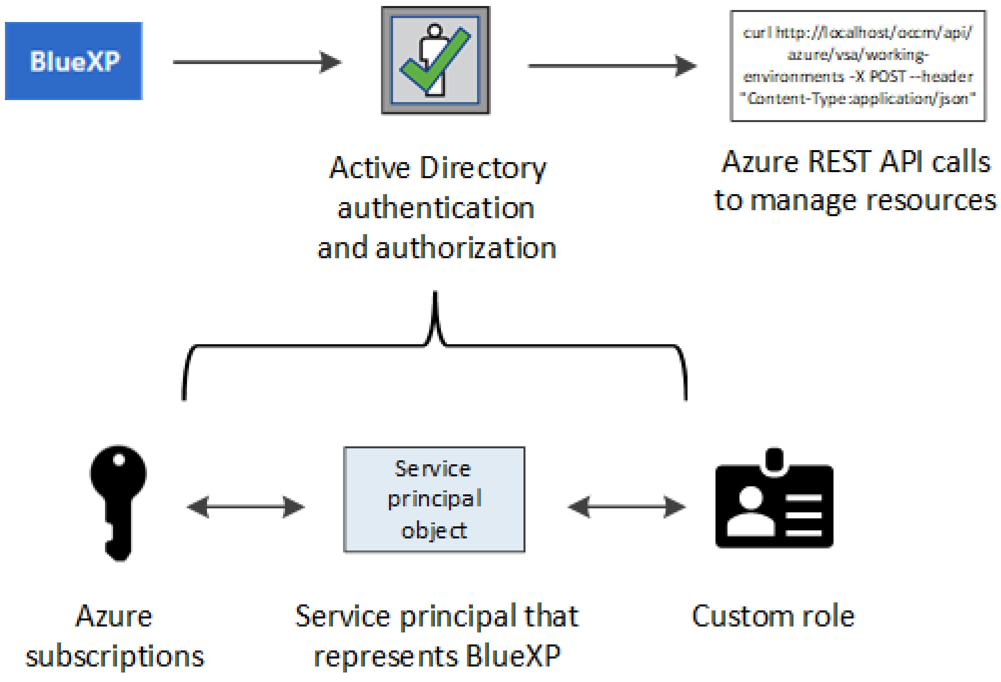
If you want to deploy Cloud Volumes ONTAP using *different* Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Microsoft Entra ID for each Azure account. You can then add the new credentials to BlueXP.

### Grant Azure permissions using a service principal

BlueXP needs permissions to perform actions in Azure. You can grant the required permissions to an Azure account by creating and setting up a service principal in Microsoft Entra ID and by obtaining the Azure credentials that BlueXP needs.

**About this task**

The following image depicts how BlueXP obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents BlueXP in Microsoft Entra ID and is assigned to a custom role that allows the required permissions.


BlueXP
Active Directory authentication and authorization
Azure REST API calls to manage resources
Service principal object
Azure subscriptions
Service principal that represents BlueXP
Custom role

```
curl http://localhost/occm/api/azure/vsa/working-environments -X POST --header "Content-Type:application/json"
```

### Steps

1. Create a Microsoft Entra application.
2. Assign the application to a role.
3. Add Windows Azure Service Management API permissions.
4. Get the application ID and directory ID.
5. Create a client secret.

### Create a Microsoft Entra application

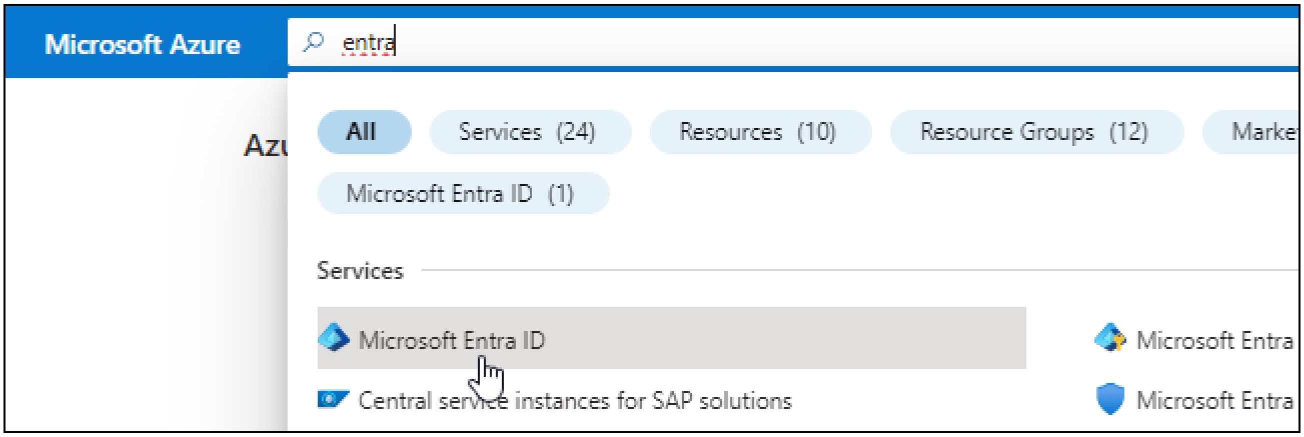
Create a Microsoft Entra application and service principal that BlueXP can use for role-based access control.

### Steps

1. Ensure that you have permissions in Azure to create an Active Directory application and to assign the application to a role.

   For details, refer to Microsoft Azure Documentation: Required permissions

2. From the Azure portal, open the **Microsoft Entra ID** service.



3. In the menu, select **App registrations**.
4. Select **New registration**.
5. Specify details about the application:
    - **Name**: Enter a name for the application.
    - **Account type**: Select an account type (any will work with BlueXP).
    - **Redirect URI**: You can leave this field blank.
6. Select **Register**.

    You’ve created the AD application and service principal.

**Result**

You’ve created the AD application and service principal.

### Assign the application to a role

You must bind the service principal to one or more Azure subscriptions and assign it the custom "BlueXP Operator" role so BlueXP has permissions in Azure.

**Steps**

1. Create a custom role:

    Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to Azure documentation

    a. Copy the contents of the custom role permissions for the Connector and save them in a JSON file.

    b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

    You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

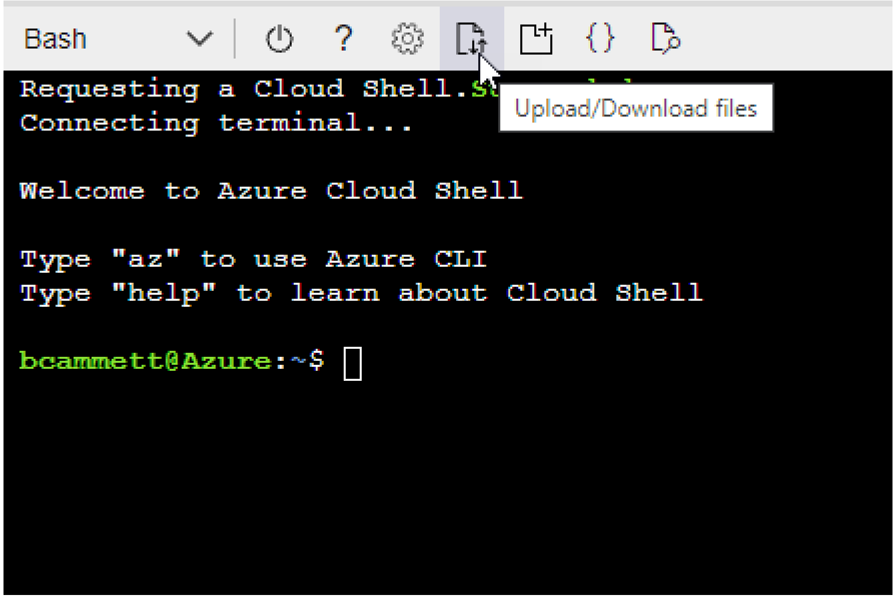
    **Example**

    ```
    "AssignableScopes": [
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
    "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
    ```

    c. Use the JSON file to create a custom role in Azure.

    The following steps describe how to create the role by using Bash in Azure Cloud Shell.

    - Start Azure Cloud Shell and choose the Bash environment.
    - Upload the JSON file.



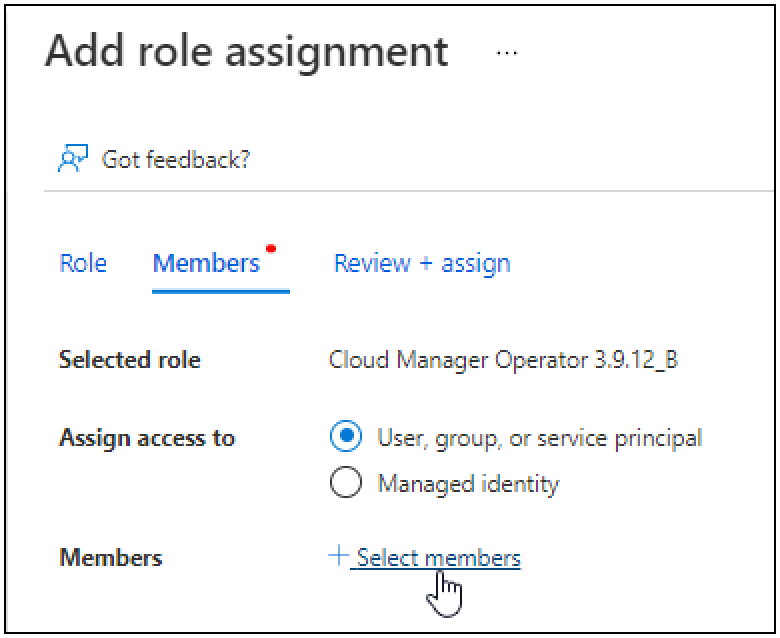
```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

- Use the Azure CLI to create the custom role:

```
az role definition create --role-definition Connector_Policy.json
```

You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

2. Assign the application to the role:
   a. From the Azure portal, open the **Subscriptions** service.
   b. Select the subscription.
   c. Select **Access control (IAM) > Add > Add role assignment**.
   d. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.
   e. In the **Members** tab, complete the following steps:
      - Keep **User, group, or service principal** selected.
      - Select **Select members**.



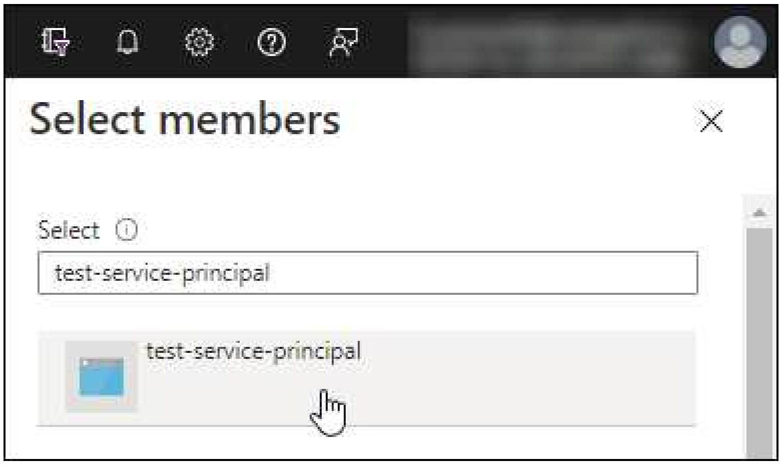
Selected role: Cloud Manager Operator 3.9.12_B

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

- Search for the name of the application.

  Here's an example:



Select: test-service-principal

test-service-principal

- Select the application and select **Select**.
- Select **Next**.

f. Select **Review + assign**.

   The service principal now has the required Azure permissions to deploy the Connector.

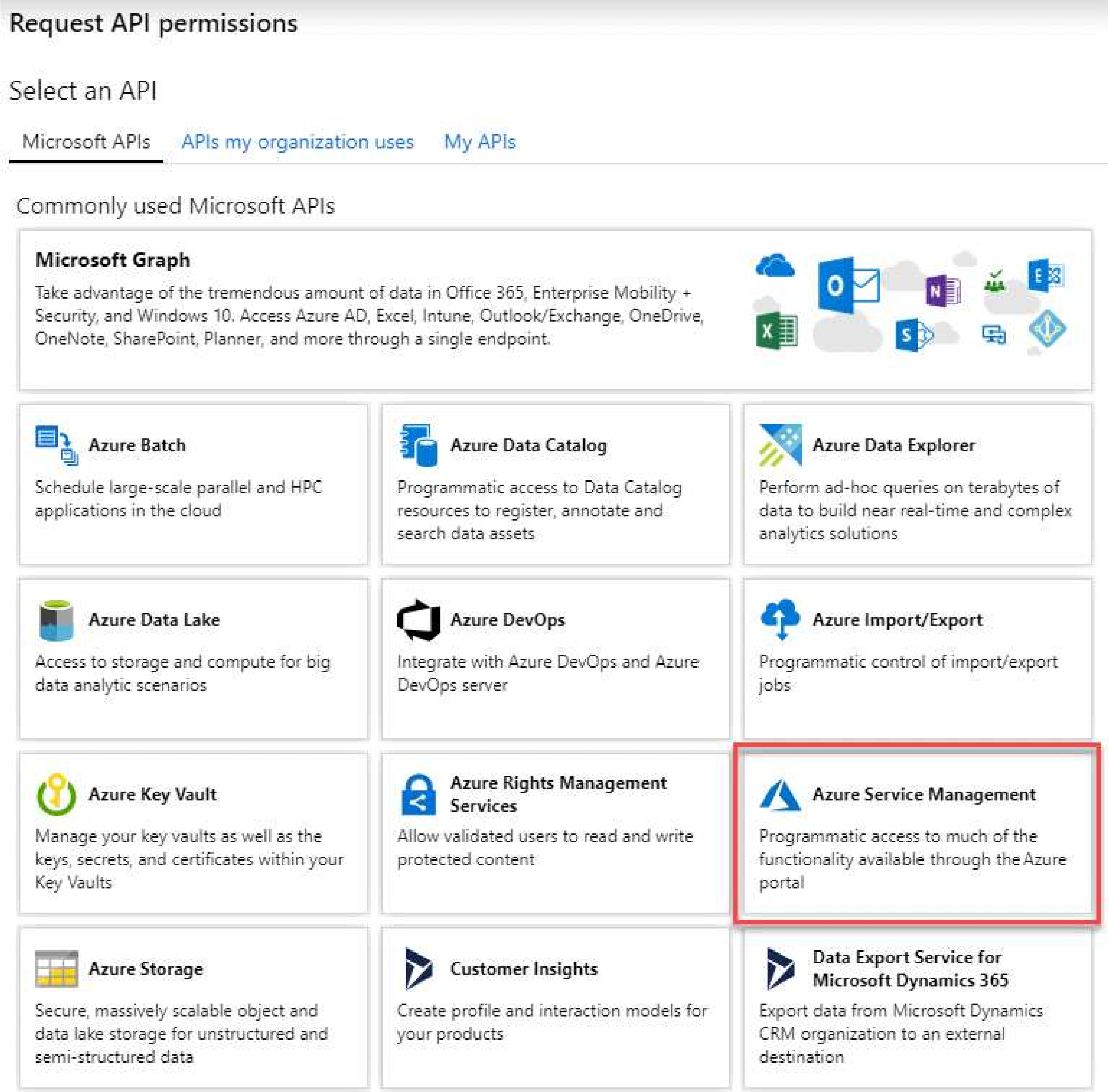
   If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

### Add Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

**Steps**

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.



Request API permissions

Select an API

Commonly used Microsoft APIs

**Microsoft Graph**
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

**Azure Batch**
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**
Access to storage and compute for big data analytic scenarios

**Azure DevOps**
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**
Programmatic control of import/export jobs

**Azure Key Vault**
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**
Allow validated users to read and write protected content

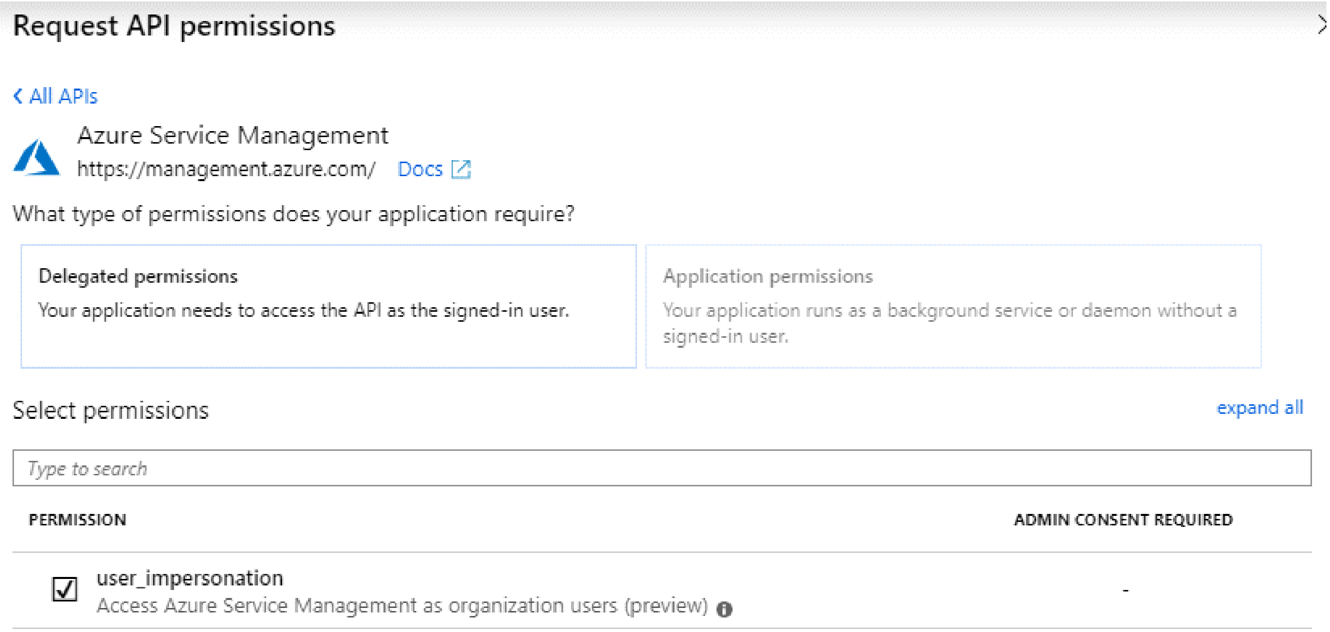
**Azure Service Management**
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**
Export data from Microsoft Dynamics CRM organization to an external destination

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.



Request API permissions

< All APIs

Azure Service Management
https://management.azure.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

expand all

*Type to search*

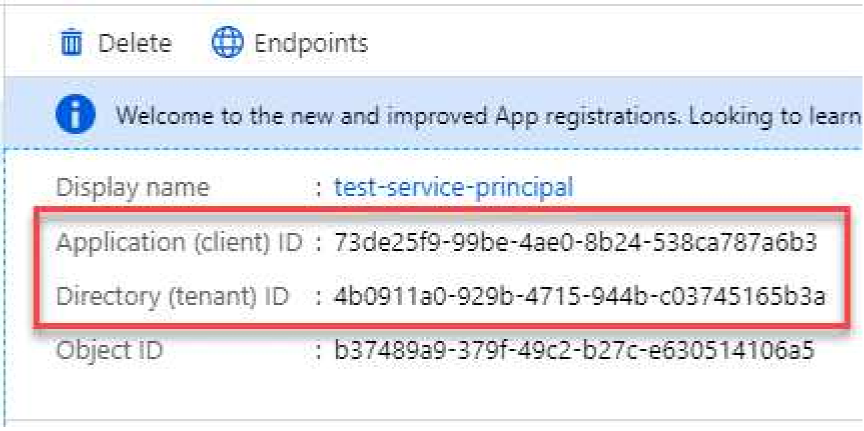
| PERMISSION | ADMIN CONSENT REQUIRED |
|---|---|
| ☑ user_impersonation<br>Access Azure Service Management as organization users (preview) | - |

### Get the application ID and directory ID

When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

#### Steps

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal
Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a
Object ID : b37489a9-379f-49c2-b27c-e630514106a5

When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

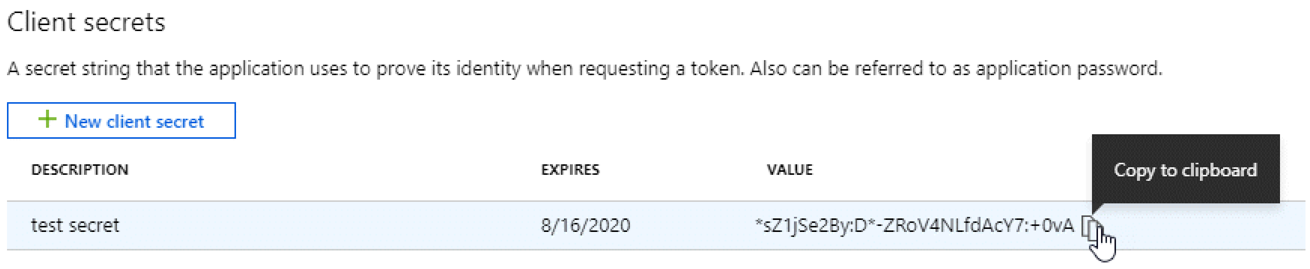
### Create a client secret

You need to create a client secret and then provide BlueXP with the value of the secret so BlueXP can use it to authenticate with Microsoft Entra ID.

#### Steps

1. Open the **Microsoft Entra ID** service.

2. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Select **Add**.
6. Copy the value of the client secret.



Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| DESCRIPTION | EXPIRES | VALUE |
|---|---|---|
| test secret | 8/16/2020 | *sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA |

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

**Result**

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you add an Azure account.

### Add the credentials to BlueXP

After you provide an Azure account with the required permissions, you can add the credentials for that account to BlueXP. Completing this step enables you to launch Cloud Volumes ONTAP using different Azure credentials.

**Before you begin**

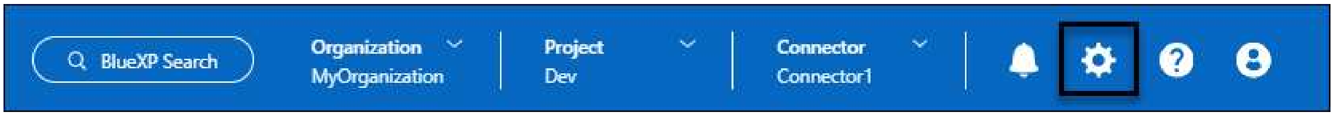
If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

**Before you begin**

You need to create a Connector before you can change BlueXP settings. Learn how to create a Connector.

**Steps**

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.



2. Select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Microsoft Azure > Connector**.
   b. **Define Credentials**: Enter information about the Microsoft Entra service principal that grants the required permissions:
      - Application (client) ID
      - Directory (tenant) ID

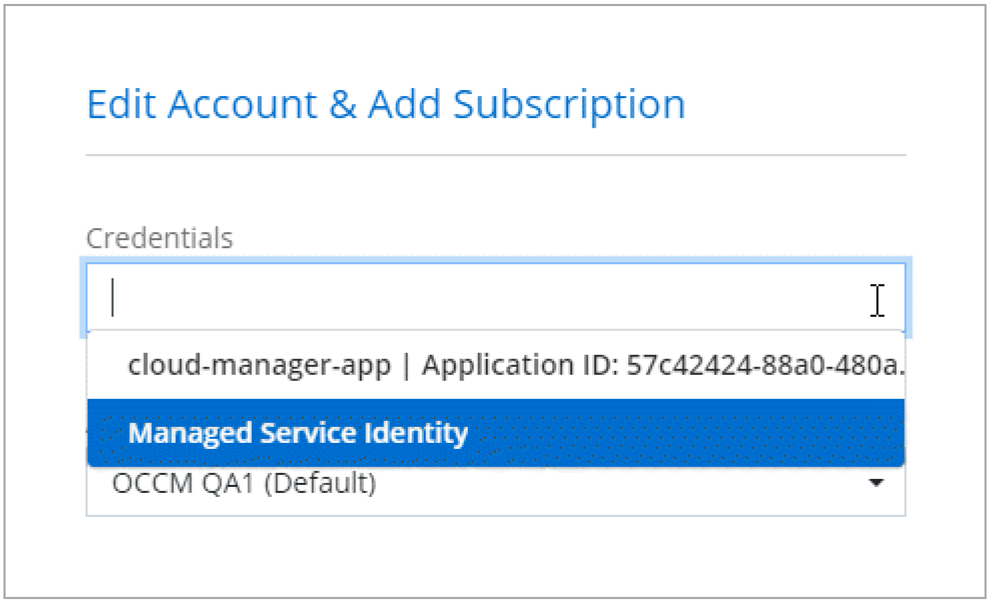
        - Client Secret

   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

   d. **Review**: Confirm the details about the new credentials and select **Add**.

**Result**

You can now switch to different set of credentials from the Details and Credentials page when creating a new working environment



Edit Account & Add Subscription

Credentials

cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

#### Manage existing credentials

Manage the Azure credentials that you've already added to BlueXP by associating a Marketplace subscription, editing credentials, and deleting them.

### Associate an Azure Marketplace subscription to credentials

After you add your Azure credentials to BlueXP, you can associate an Azure Marketplace subscription to those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other BlueXP services.

There are two scenarios in which you might associate an Azure Marketplace subscription after you've already added the credentials to BlueXP:

- You didn't associate a subscription when you initially added the credentials to BlueXP.
- You want to change the Azure Marketplace subscription that is associated with Azure credentials.

  Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

**Before you begin**

You need to create a Connector before you can change BlueXP settings. lLearn how to create a Connector.

**Steps**

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

   You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
   a. If prompted, log in to your Azure account.
   b. Select **Subscribe**.
   c. Fill out the form and select **Subscribe**.
   d. After the subscription process is complete, select **Configure account now**.

      You'll be redirected to BlueXP.

   e. From the **Subscription Assignment** page:
      - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
      - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

        BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

        For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

      - Select **Save**.

        The following video shows the steps to subscribe from the Azure Marketplace:

        Subscribe to NetApp Intelligent Services from the Azure Marketplace

### Edit credentials

Edit your Azure credentials in BlueXP by modifying the details about your Azure service credentials. For example, you might need to update the client secret if a new secret was created for the service principal application.

#### Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

#### Delete credentials

If you no longer need a set of credentials, you can delete them from BlueXP. You can only delete credentials that aren't associated with a working environment.

**Steps**

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

## Google Cloud

### Learn about Google Cloud projects and permissions

Learn how BlueXP uses Google Cloud credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more Google Cloud projects. For example, you might want to learn about the service account that's associated with the Connector VM.

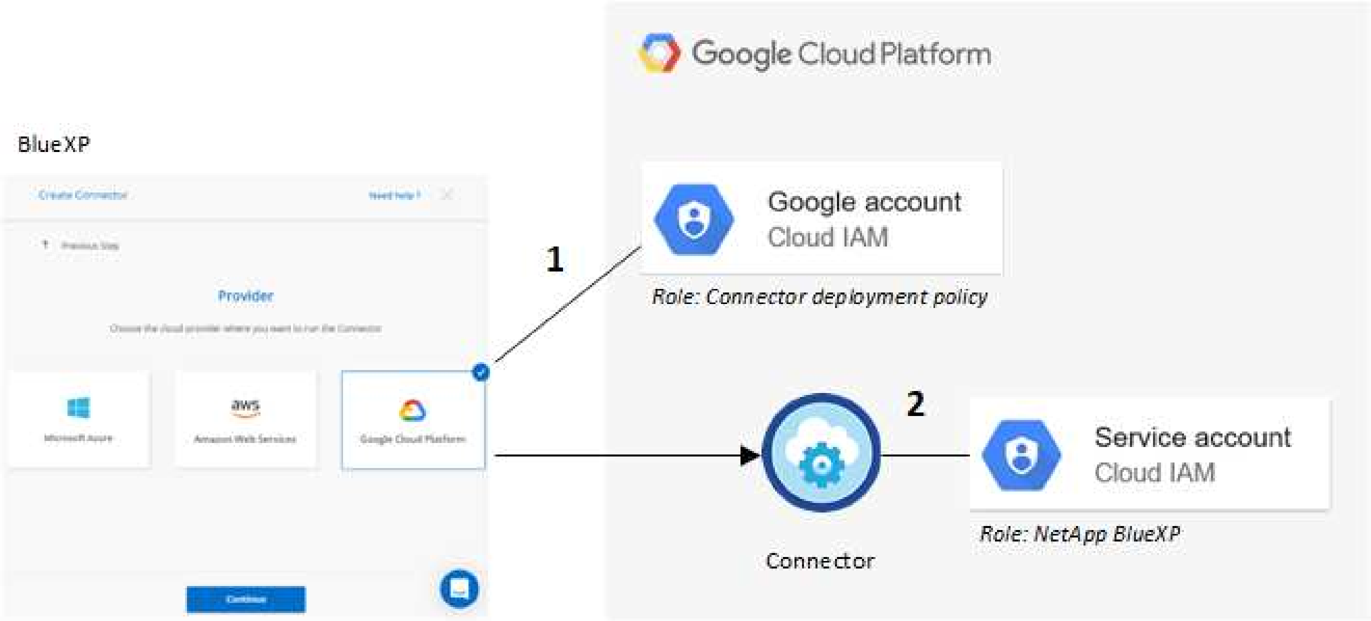
#### Project and permissions for BlueXP

Before you can use BlueXP to manage resources in your Google Cloud project, you must first deploy a Connector. The Connector can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy a Connector directly from BlueXP:

1. You need to deploy a Connector using a Google account that has permissions to launch the Connector VM instance from BlueXP.
2. When deploying the Connector, you are prompted to select a service account for the VM instance. BlueXP gets permissions from the service account to create and manage Cloud Volumes ONTAP systems, to manage backups using BlueXP backup and recovery, and more. Permissions are provided by attaching a custom role to the service account.

The following image depicts the permission requirements described in numbers 1 and 2 above:



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

- Set up Google Cloud permissions for standard mode
- Set up permissions for restricted mode
- Set up permissions for private mode

#### Credentials and marketplace subscriptions

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials for the Google Cloud service account in the project in which the Connector resides. These credentials must be associated with a Google Cloud Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) and use other BlueXP services.

Learn how to associate a Google Cloud Marketplace subscription.

Note the following about Google Cloud credentials and marketplace subscriptions:

- Only one set of Google Cloud credentials can be associated with a Connector
- You can associate only one Google Cloud Marketplace subscription with the credentials
- You can replace an existing marketplace subscription with a new subscription

#### Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as the Connector, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Connector service account and role to that project.

- Learn how to set up the service account
- Learn how to deploy Cloud Volumes ONTAP in Google Cloud and select a project

### Manage Google Cloud credentials and subscriptions for BlueXP

You can manage the Google Cloud credentials that are associated with the Connector

VM instance by associating a marketplace subscription and by troubleshooting the subscription process. Both of these tasks ensure that you can use your marketplace subscription to pay for data services.

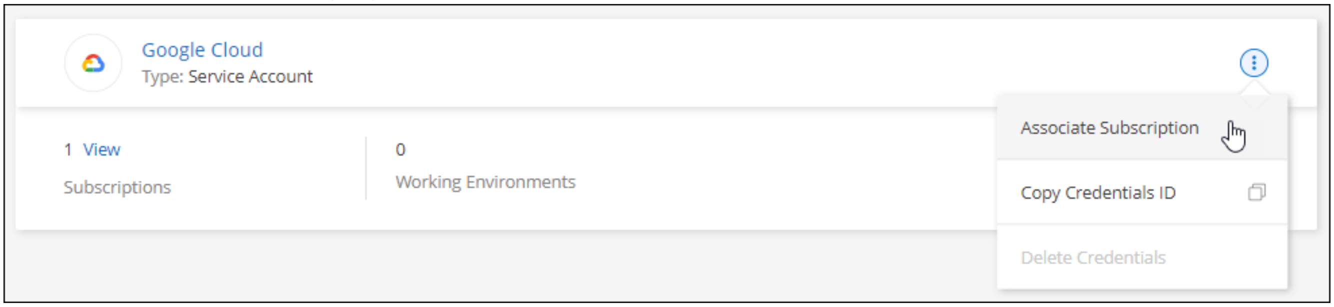
#### Associate a Marketplace subscription with Google Cloud credentials

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials that are associated with the Connector VM instance. At any time, you can change the Google Cloud Marketplace subscription that is associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other data services.

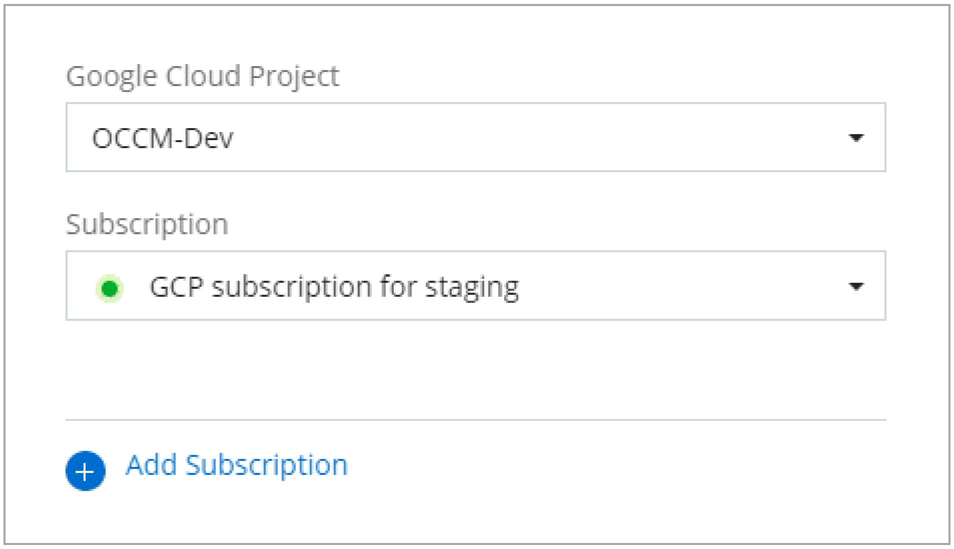
Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

**Steps**

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.
+new screenshot needed (TS)



3. To configure an existing subscription with the selected credentials, select a Google Cloud project and subscription from the drop-down list, and then select **Configure**.



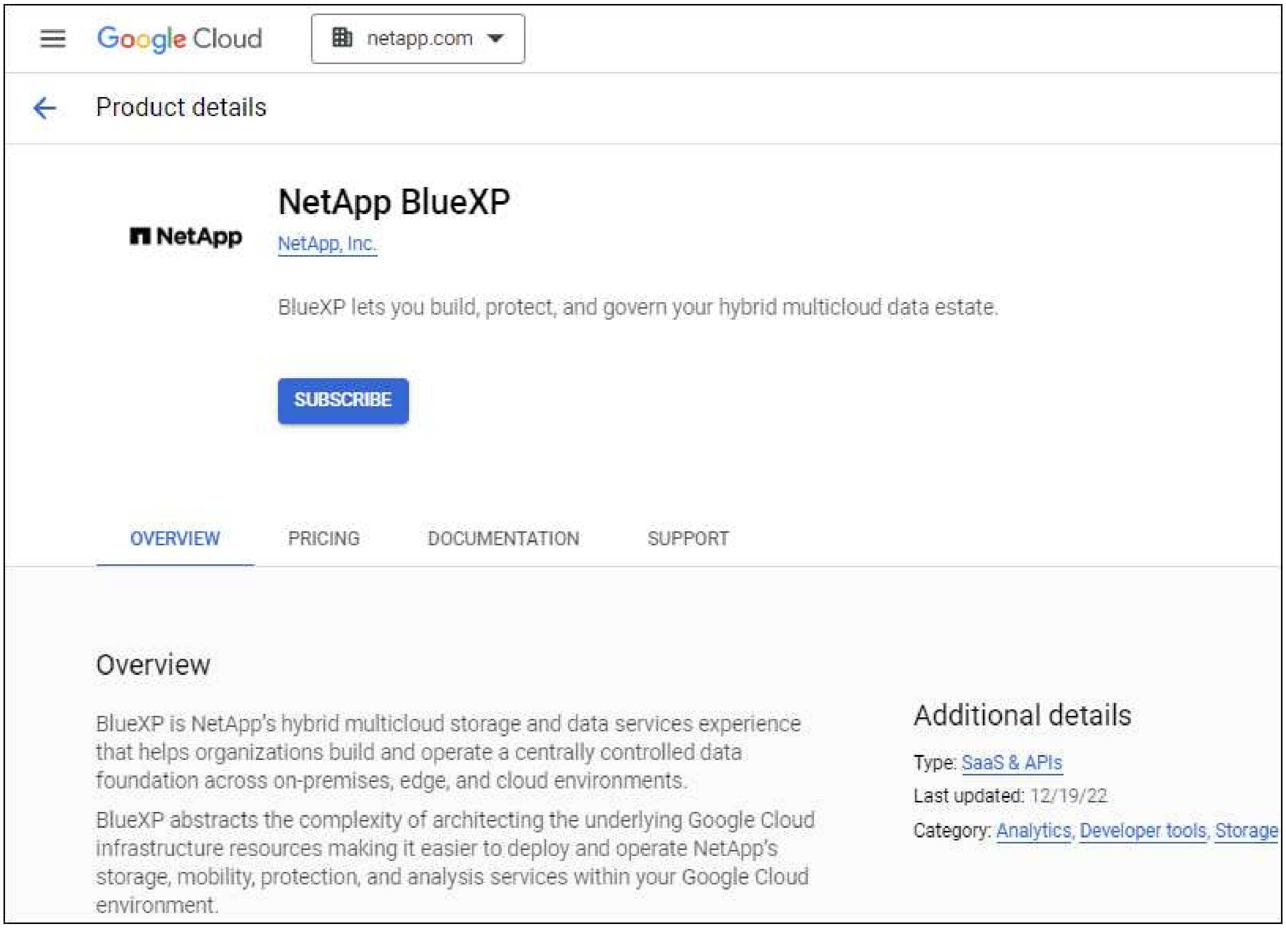
Google Cloud Project: OCCM-Dev

Subscription: GCP subscription for staging

4. If you don’t already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.

ⓘ Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a BlueXP login.

a. After you’re redirected to the NetApp Intelligent Services page on the Google Cloud Marketplace, ensure that the correct project is selected at the top navigation menu.



NetApp BlueXP

NetApp, Inc.

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

Overview

BlueXP is NetApp’s hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp’s storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

Type: SaaS & APIs

Last updated: 12/19/22

Category: Analytics, Developer tools, Storage

b. Select **Subscribe**.

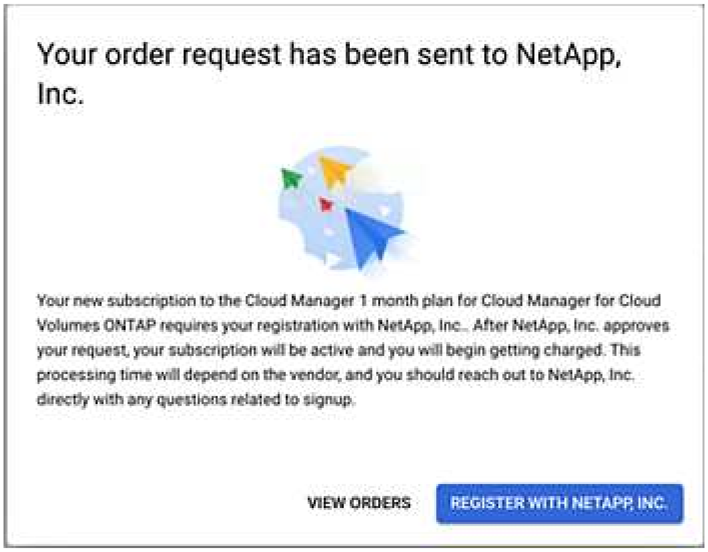
c. Select the appropriate billing account and agree to the terms and conditions.

d. Select **Subscribe**.

   This step sends your transfer request to NetApp.

e. On the pop-up dialog box, select **Register with NetApp, Inc.**

   This step must be completed to link the Google Cloud subscription with your BlueXP organization or account. The process of linking a subscription isn’t complete until you are redirected from this page and then sign in to BlueXP.



Your order request has been sent to NetApp, Inc.

Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

f. Complete the steps on the **Subscription Assignment** page:

> ⓘ If someone from your organization has already subscribed to the NetApp BlueXP subscription from your billing account, then you will be redirected to the Cloud Volumes ONTAP page on the BlueXP website instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

- Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

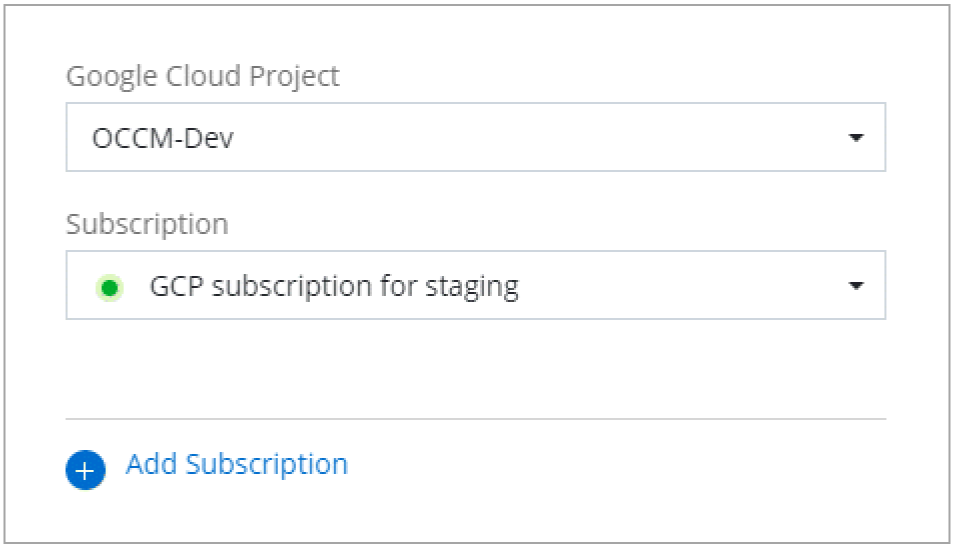
  BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

  For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.
- Select **Save**.

  The following video shows the steps to subscribe from the Google Cloud Marketplace:

  Subscribe to BlueXP from the Google Cloud Marketplace

g. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.



Google Cloud Project

OCCM-Dev

Subscription

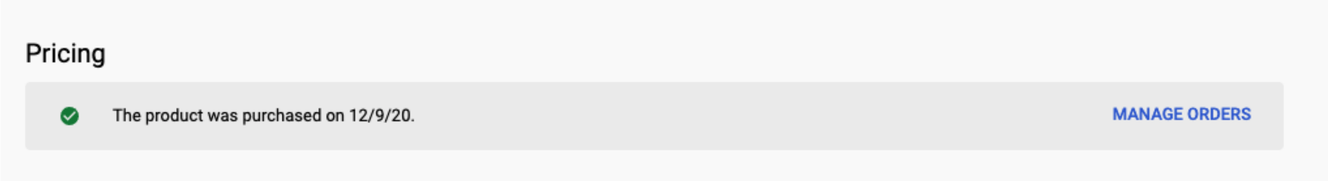
● GCP subscription for staging

#### Troubleshoot the Marketplace subscription process

Sometimes subscribing to NetApp Intelligent Services through the Google Cloud Marketplace can become fragmented due to incorrect permissions or accidentally not following the redirection to the BlueXP website. If this happens, use the following steps to complete the subscription process.

**Steps**

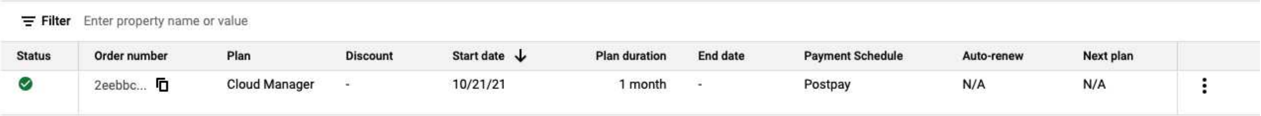
1. Navigate to the NetApp BlueXP page on the Google Cloud Marketplace to check on the state of the order. If the page states **Manage on Provider**, scroll down and select **Manage Orders**.



Pricing

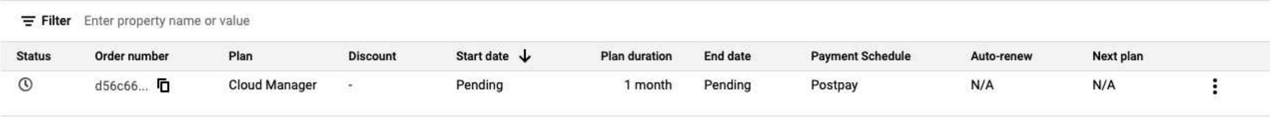
✓ The product was purchased on 12/9/20.

   - If the order shows a green check mark and this is unexpected, somebody else from the organization using the same billing account might already be subscribed. If this is unexpected or you require the details of this subscription, contact your NetApp sales team.



| Status | Order number | Plan | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan |
|---|---|---|---|---|---|---|---|---|---|
| ✓ | 2eebbc... | Cloud Manager | - | 10/21/21 | 1 month | - | Postpay | N/A | N/A |

   - If the order shows a clock and **Pending** status, go back to the marketplace page and choose **Manage on Provider** to complete the process as documented above.



| Status | Order number | Plan | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan |
|---|---|---|---|---|---|---|---|---|---|
| 🕓 | d56c66... | Cloud Manager | - | Pending | 1 month | Pending | Postpay | N/A | N/A |

## Manage NSS credentials associated with BlueXP

Associate a NetApp Support Site account with your BlueXP organization to enable key workflows for Cloud Volumes ONTAP. These NSS credentials are associated with the entire BlueXP organization.

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

- Learn about BlueXP deployment modes
- Learn about BlueXP identity and access management

### Overview

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

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

  Providing your NSS account is required so that BlueXP 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 BlueXP account serial number. Users who belong to the BlueXP organization or account 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 BlueXP from the Support Dashboard within BlueXP.

When you have added your NSS account, BlueXP can use this information for things like license downloads, software upgrade verification, and future support registrations.

You can associate multiple NSS accounts with your BlueXP 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 the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management > Add NSS Account**.
3. Select **Continue** to be redirected to a Microsoft login page.
4. 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 BlueXP notification center if your NSS credential has expired. Learn about the Notification Center.

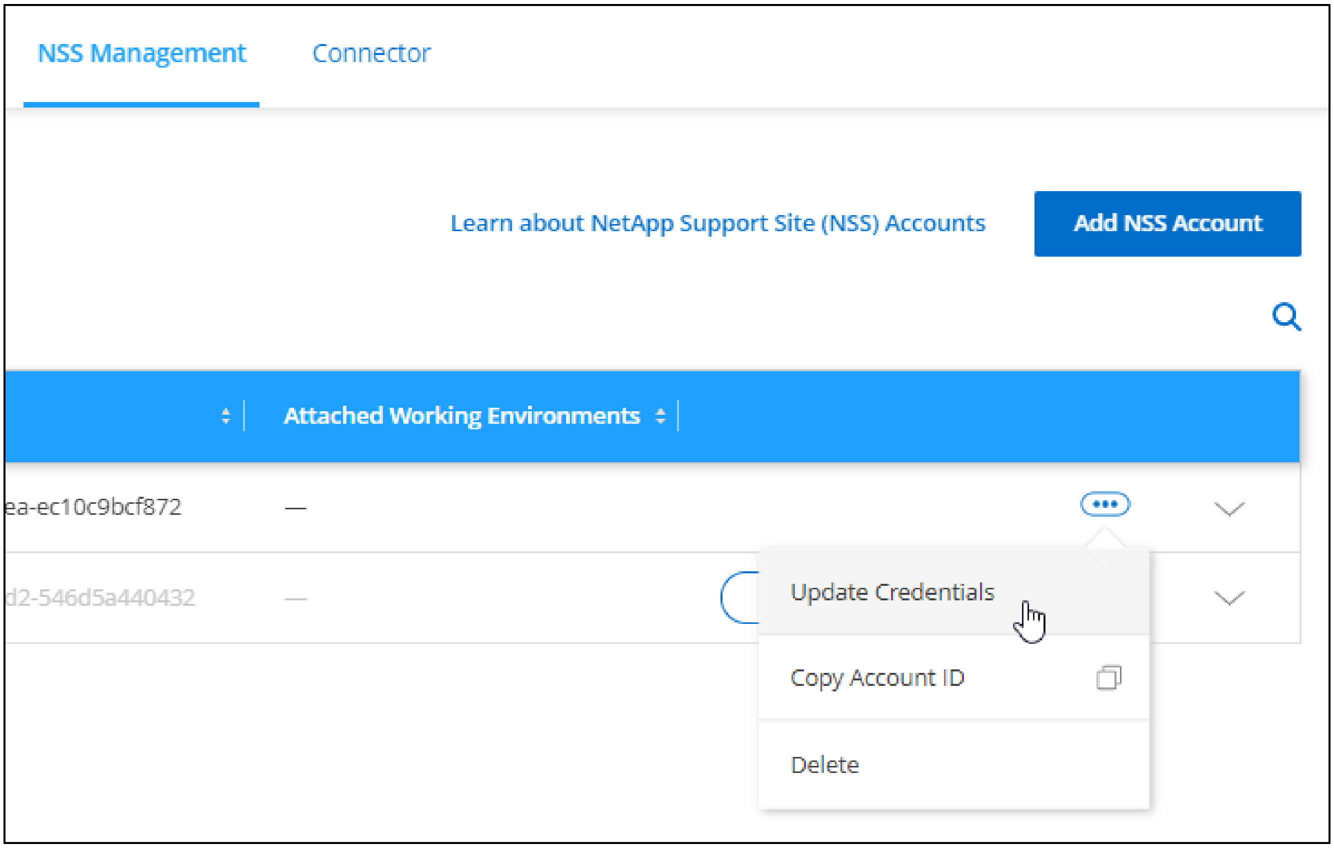
Expired credentials can disrupt the following, but are not limited to:

- License updates in digital wallet, which means 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 BlueXP organization. For example, if the person associated with your NSS account has left your company.

#### Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **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.

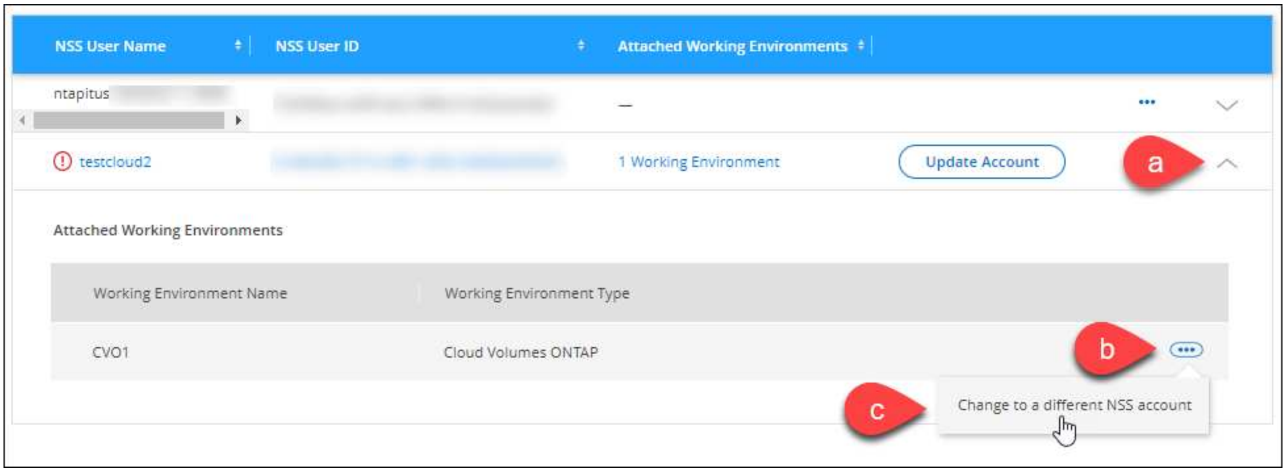
### Attach a working environment to a different NSS account

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 BlueXP.

#### Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **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 working environment is currently associated with.
   b. For the working environment that you want to change the association for, select •••
   c. Select **Change to a different NSS account**.



| NSS User Name | NSS User ID | Attached Working Environments | | |
|---|---|---|---|---|
| ntapitus [redacted] | [redacted] | – | | ••• |
| testcloud2 | [redacted] | 1 Working Environment | Update Account | |

Attached Working Environments

| Working Environment Name | Working Environment Type |
|---|---|
| CVO1 | Cloud Volumes ONTAP |

Change to a different NSS account

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

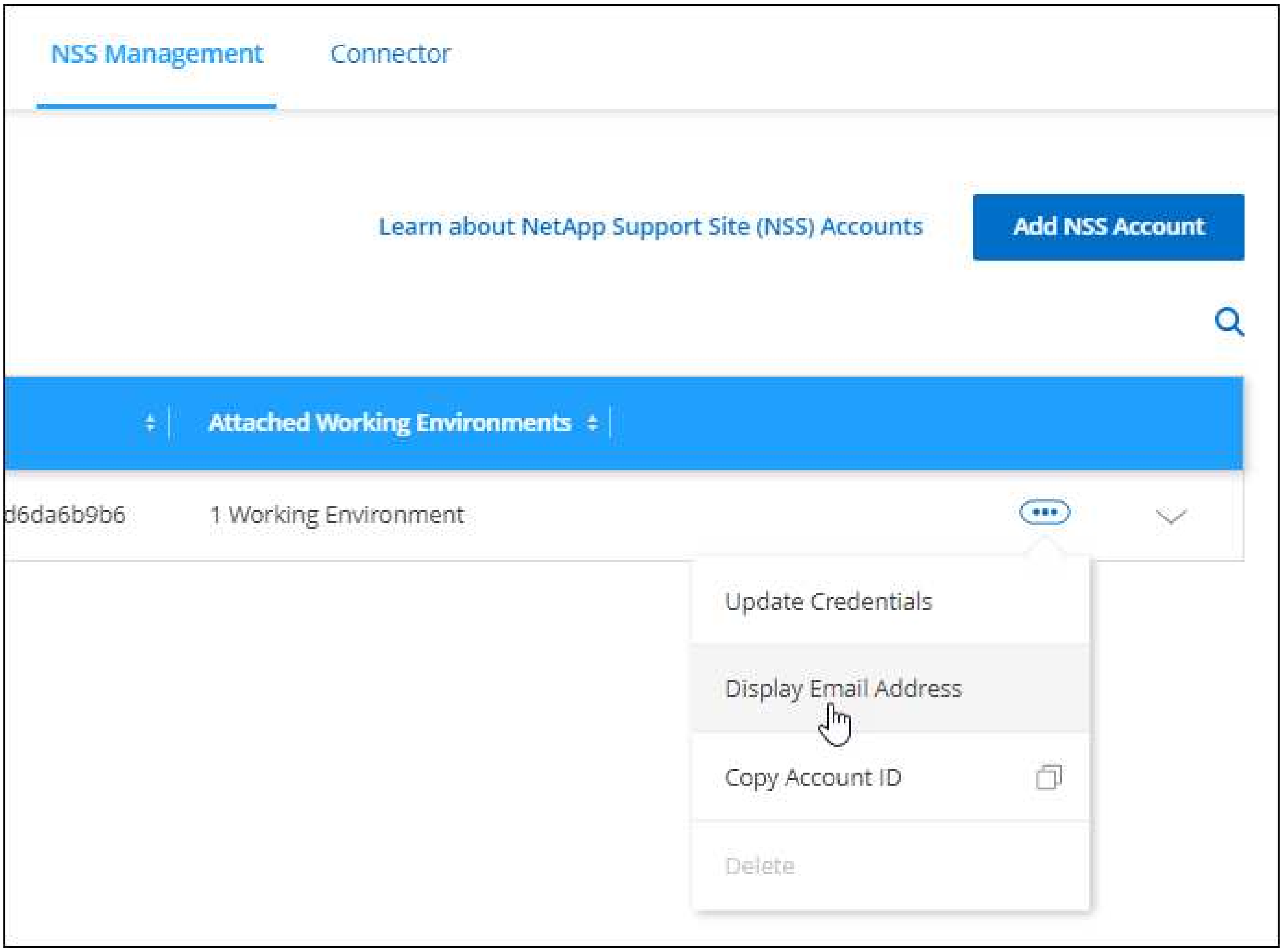
### Display the email address for an NSS account

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, BlueXP 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 the upper right of the BlueXP console, select the Help icon, and select **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.



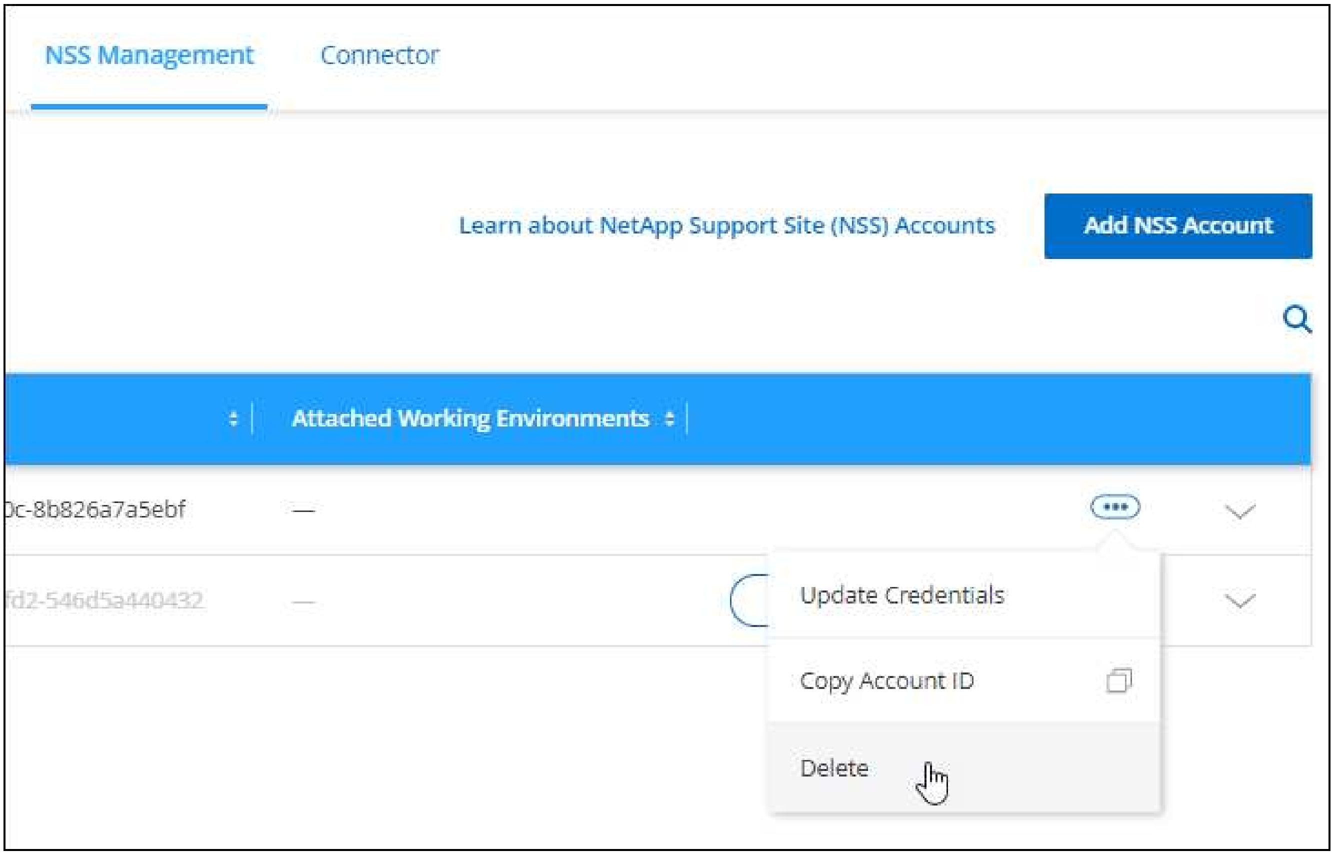
### Remove an NSS account

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

You can’t delete an account that is currently associated with a Cloud Volumes ONTAP working environment. You first need to attach those working environments to a different NSS account.

#### Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **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.

## Manage credentials associated with your BlueXP login

Depending on the actions that you've taken in BlueXP, you might have associated ONTAP credentials and NetApp Support Site (NSS) credentials with your BlueXP user login. You can view and manage those credentials in BlueXP after you've associated them. For example, if you change the password for these credentials, then you'll need to update the password in BlueXP.

### ONTAP credentials

Users need ONTAP admin credentials to discover ONTAP clusters in BlueXP. However, ONTAP System Manager access depends on whether or not you are using a Connector.

**Without a Connector**

Users are prompted to enter their ONTAP credentials to access ONTAP System Manager for the cluster. Users can choose to save these credentials in BlueXP which means they won't be prompted to enter them each time. User credentials are only visible to the respective user and can be managed from the User credentials page.

**With a Connector**

By default, users are not prompted to enter their ONTAP credentials to access ONTAP System Manager. However, a BlueXP administrator (with the Organization admin role) can configure BlueXP to prompt users to enter their ONTAP credentials. When this setting is enabled, users need enter their ONTAP credentials each time.

Learn more.

### NSS credentials

The NSS credentials associated with your BlueXP login enable support registration, case management, and access to Digital Advisor.

- When you access **Support > Resources** and register for support, you're prompted to associate NSS credentials with your BlueXP login.

  This registers your organization or account for support and activates support entitlement. Only one user in your BlueXP organization or account must associate a NetApp Support Site account with their BlueXP login to register for support and activate support entitlement. After this is completed, the **Resources** page shows that your account is registered for support.

  Learn how to register for support

- When you access **Support > Case Management**, you're prompted to enter your NSS credentials, if you haven't already done so. This page enables you to create and manage the support cases associated with your NSS account and with your company.
- When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials.

Note the following about the NSS account associated with your BlueXP login:

- The account is managed at the user level, which means it isn't viewable by other users who log in.
- There can be only one NSS account associated with Digital Advisor and support case management, per user.
- If you're trying to associate a NetApp Support Site account with a Cloud Volumes ONTAP working environment, you can only choose from the NSS accounts that were added to the BlueXP organization or account that you are a member of.

  NSS account-level credentials are different than the NSS account that's associated with your BlueXP login. NSS account-level credentials enable you to deploy Cloud Volumes ONTAP with BYOL, register PAYGO systems, and upgrade its software.

  Learn more about using NSS credentials with your BlueXP organization or account.

### Manage your user credentials

Manage your user credentials by updating the user name and password or by deleting the credentials.

**Steps**

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.
3. If you don't have any user credentials yet, you can select **Add NSS credentials** to add your NetApp Support Site account.
4. Manage existing credentials by choosing the following options from the Actions menu:
   - **Update credentials**: Update the user name and password for the account.
   - **Delete credentials**: Remove the account associated with your BlueXP user account.

**Result**

BlueXP updates your credentials, and you see the changes when accessing the ONTAP cluster, digital advisor, or the Case Management page.

# Monitor BlueXP operations

You can monitor the status of the operations that BlueXP is performing to see if there are any issues that you need to address. You can view the status in the Timeline, the Notification Center, or have notifications sent to your email.

The table compares the Timeline and Notification Center to highlight their features.

| Notification Center | Timeline |
|---|---|
| Shows high level status for events and actions | Provides details for each event or action for further investigation |
| Shows status for the current login session (the information does not appear in the Notification Center after you log off) | Retains status for the last month |
| Shows only actions initiated in the user interface | Shows all actions from the UI or APIs |
| Shows user-initiated actions | Shows all actions, whether user-initiated or system-initiated |
| Filter results by importance | Filter by service, action, user, status, and more |
| Provides the ability to email notifications to users and to others | No email capability |

## Audit user activity from the BlueXP timeline

The Timeline shows the actions that users completed to manage your organization or account. This includes management actions such as associating users, creating working environments, creating Connectors, and more.

The Timeline helps identify who performed an action or its status.

**Steps**

1. In the upper right of the BlueXP console, select ⚙ > **Timeline**.
2. Use the filters above the table to change which actions display in the table.

   For example, you can use the **Service** filter to show actions related to a specific BlueXP service, or you can use the **User** filter to show actions related to a specific user account.

### Download audit logs from the Timeline

You can download the audit logs from the Timeline to a CSV file. This enables you to keep a record of the actions that users performed in your organization. The downloaded CSV file contains all available columns from the Timeline, regardless of which ones you are filtering or displaying in the Timeline.

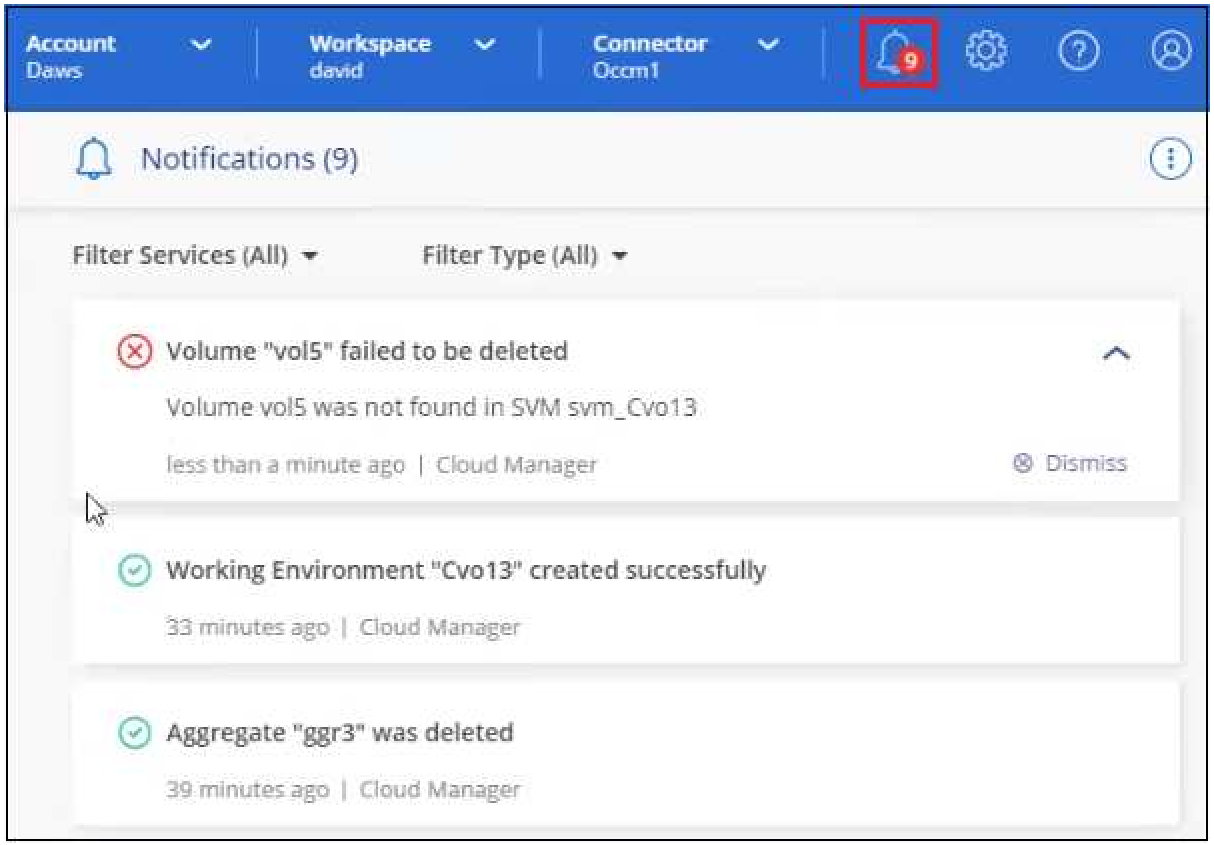
**Steps**

1. In the Timeline, select the download icon in the upper right corner of the table.

## Monitor activities using the Notification Center

Notifications track the progress of your BlueXP operations to verify success. They enable you to view the status for many BlueXP actions that you initiated during your current login session. Not all BlueXP services report information into the Notification Center at this time.

You can display the notifications by selecting the notification bell (🔔) in the menu bar. The color of the little bubble in the bell indicates the highest level severity notification that is active. So if you see a red bubble, it means there’s an important notification that you should look at.



Notifications (9)

Volume "vol5" failed to be deleted

Volume vol5 was not found in SVM svm_Cvo13

less than a minute ago | Cloud Manager

Working Environment "Cvo13" created successfully

33 minutes ago | Cloud Manager

Aggregate "ggr3" was deleted

39 minutes ago | Cloud Manager

You can also configure BlueXP to send certain types of notifications by email so you can be informed of important system activity even when you’re not logged into the system. Emails can be sent to any users who are part of your BlueXP organization or account, or to any other recipients who need to be aware of certain types of system activity. See how to set email notification settings.

### Comparing the Notification Center with BlueXP alerts

The Notification Center enables you to view the status of operations you’ve initiated from BlueXP and set up alert notifications for certain types of system activities. Meanwhile, BlueXP alerts enables you to view issues or potential risks in your ONTAP storage environment related to capacity, availability, performance, protection, and security.

Learn more about BlueXP alerts

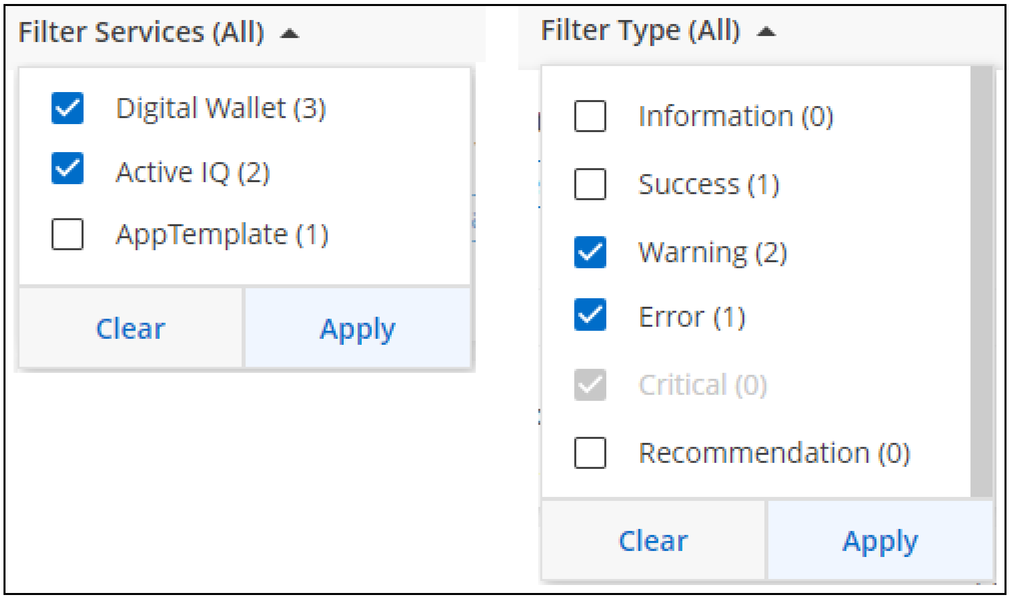
### Notification types

BlueXP classifies notifications into the following categories:

| Notification type | Description |
|---|---|
| Critical | A problem occurred that might lead to service disruption if corrective action is not taken immediately. |
| Error | An action or process ended with failure, or could lead to failure if corrective action is not taken. |
| Warning | An issue that you should be aware of to make sure it does not reach the critical severity. Notifications of this severity do not cause service disruption, and immediate corrective action might not be required. |
| Recommendation | A system recommendation for you to take an action to improve the system or a certain service; for example: costs saving, suggestion for new services, recommended security configuration, etc. |
| Information | A message that provides additional information about an action or process. |
| Success | An action or process completed successfully. |

### Filter notifications

By default you'll see all active notifications in the Notification Center. You can filter the notifications that you see to show only those notifications that are important to you. You can filter by BlueXP "Service" and by notification "Type".



☑ Digital Wallet (3)
☑ Active IQ (2)
□ AppTemplate (1)

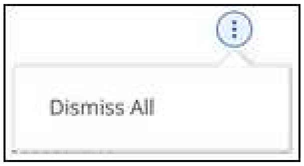
□ Information (0)
□ Success (1)
☑ Warning (2)
☑ Error (1)
☑ Critical (0)
□ Recommendation (0)

For example, if you want to see only "Error" and "Warning" notifications for BlueXP operations, select those entries and you'll see only those types of notifications.

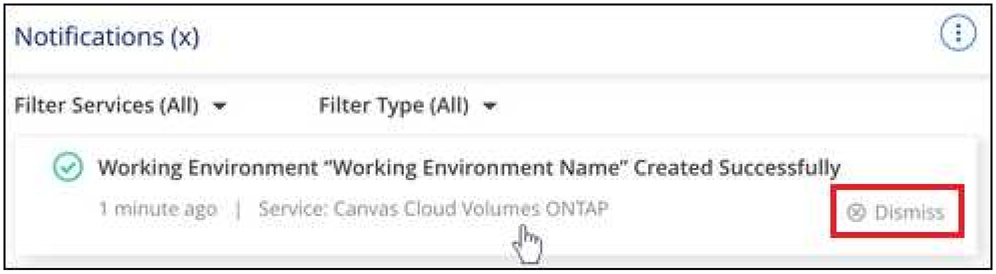
### Dismiss notifications

You can remove notifications from the page if you no longer need to see them. You can dismiss notifications individually or all at once.

To dismiss all notifications, in the Notification Center, select ⋮ and select **Dismiss All**.



To dismiss individual notifications, hover your cursor over the notification and select **Dismiss**.


Notifications (x)
Filter Services (All)
Filter Type (All)
Working Environment "Working Environment Name" Created Successfully
1 minute ago | Service: Canvas Cloud Volumes ONTAP
Dismiss

### Set email notification settings

You can send specific types of notifications by email so you can be informed of important system activity even when you're not logged into BlueXP. Emails can be sent to any users who are part of your BlueXP organization or account, or to any other recipients who need to be aware of certain types of system activity.

- BlueXP sends email notifications for the Connector, digital wallet, copy and sync, and backup and recovery.
- Sending email notifications is not supported when the Connector is installed in a site without internet access.

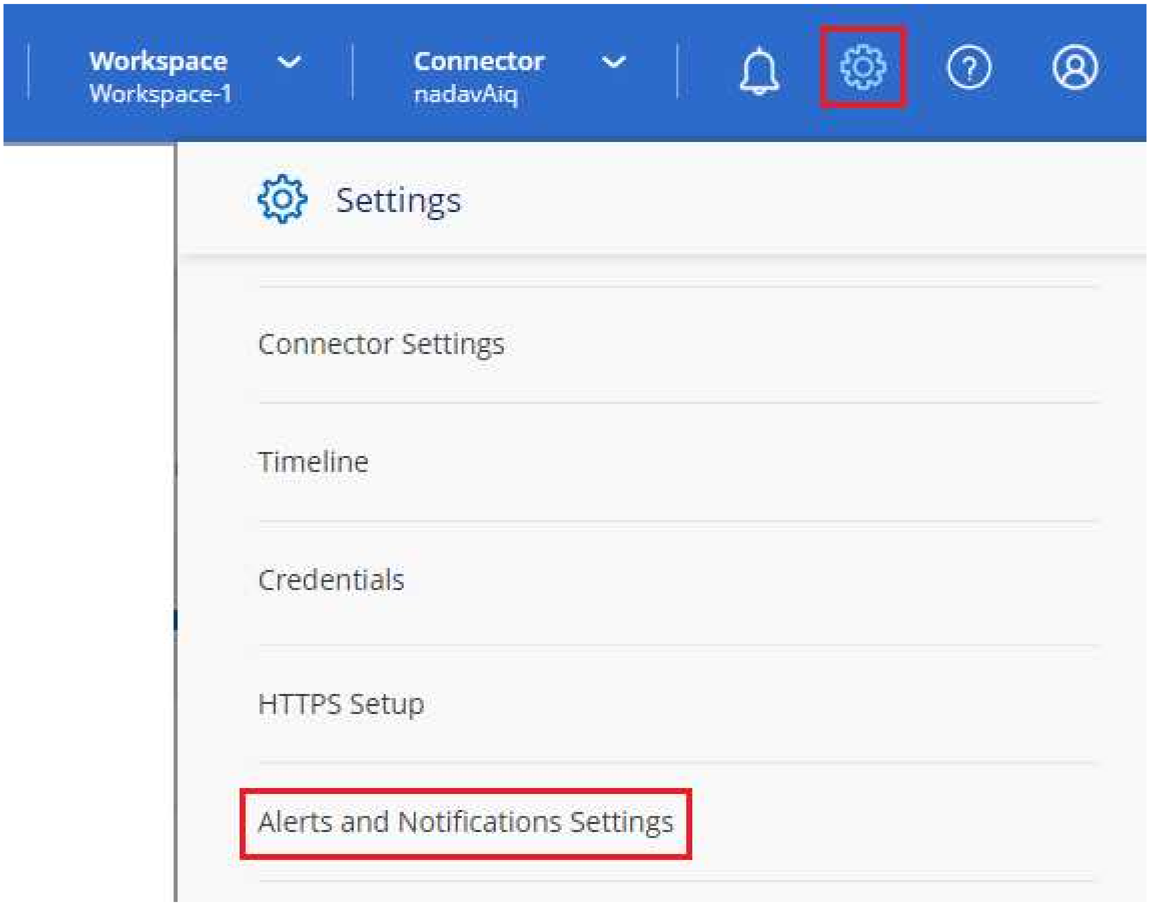
The filters you set in the Notification Center do not determine the types of notifications you'll receive by email. By default, any BlueXP admin will receive emails for all "Critical" and "Recommendation" notifications. These notifications are across all services - you can't choose to receive notifications for only certain services, for example Connectors or BlueXP backup and recovery.

All other users and recipients are configured not to receive any notification emails - so you'll need to configure notification settings for any additional users.

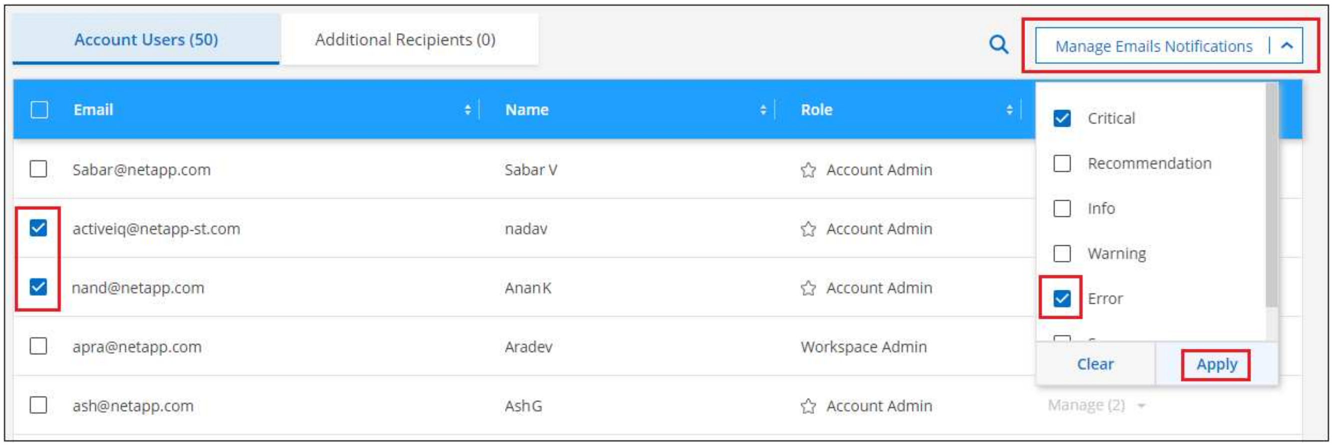
You must have the Organization admin role to customize the notifications settings.

**Steps**

1. From the BlueXP menu bar, select **Settings > Alerts and Notifications Settings**.



2. Select a user, or multiple users, from either the *Users* tab or the *Additional Recipients* tab, and choose the type of notifications to be sent:
   - To make changes for a single user, select the menu in the Notifications column for that user, check the types of Notifications to be sent, and select **Apply**.
   - To make changes for multiple users, check the box for each user, select **Manage Email Notifications**, check the types of Notifications to be sent, and select **Apply**.



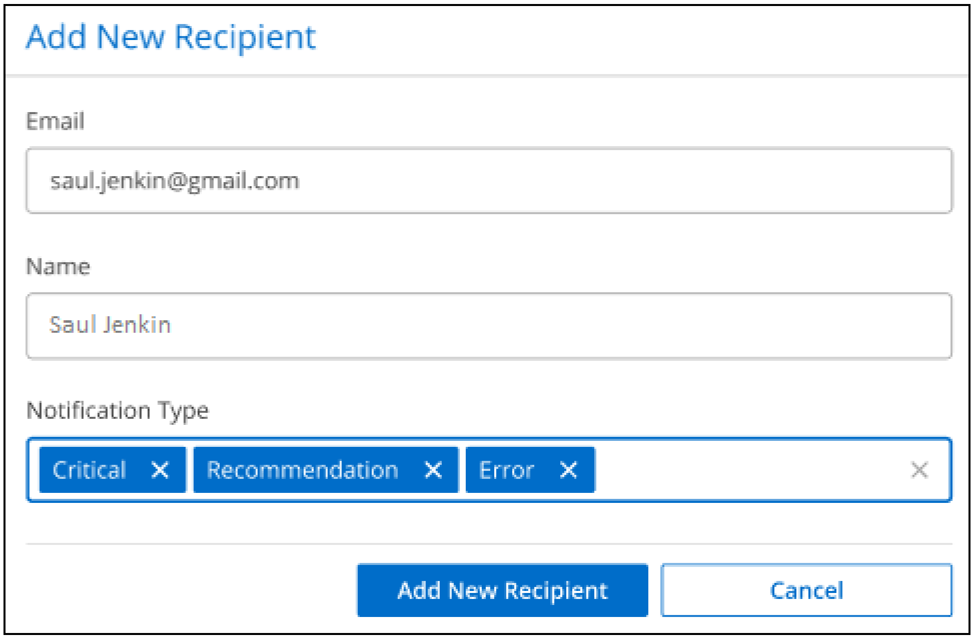
| ☐ | Email | Name | Role | |
|---|---|---|---|---|
| ☐ | Sabar@netapp.com | Sabar V | Account Admin | |
| ☑ | activeiq@netapp-st.com | nadav | Account Admin | |
| ☑ | nand@netapp.com | AnanK | Account Admin | |
| ☐ | apra@netapp.com | Aradev | Workspace Admin | |
| ☐ | ash@netapp.com | AshG | Account Admin | Manage (2) |

### Add additional email recipients

The users who appear in the *Users* tab are populated automatically from the users in your organization or account. You can add email addresses in the *Additional Recipients* tab for other people, or groups, who do not have access to BlueXP, but who need to be notified about certain types of alerts and notifications.

**Steps**

1. From the Alerts and Notifications Settings page, select **Add New Recipients**.



Add New Recipient

Email

saul.jenkin@gmail.com

Name

Saul Jenkin

Notification Type

Critical ✕ Recommendation ✕ Error ✕

2. Enter the name, email address, and select the types of Notifications that recipient will receive, and select **Add New Recipient**.

## Copyright information

## Trademark information