



Administer BlueXP

BlueXP setup and administration

NetApp
October 25, 2024

This PDF was generated from <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-identity-and-access-management.html> on October 25, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Administer BlueXP 1
 - Identity and access management 1
 - BlueXP accounts 30
 - Enable single sign-on by using identity federation with BlueXP 43
 - Connectors 48
 - Credentials and subscriptions 67
 - Monitor BlueXP operations 108

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 permissions to members at specific parts of the hierarchy, which prevents access to resources in other parts of the hierarchy.

BlueXP IAM replaces and enhances the previous functionality provided by BlueXP accounts. [Learn more about the introduction of BlueXP IAM.](#)

BlueXP IAM is supported when using BlueXP in standard mode. If you're using BlueXP in restricted mode or private mode, then you use a BlueXP *account* to manage users and resources.

- [Learn about BlueXP accounts](#)
- [Learn about BlueXP deployment modes](#)

How BlueXP IAM works

BlueXP IAM enables you to grant access to your organization's resources by defining which members have permissions to specific parts of the organization's hierarchy. For example, a member can have project admin permissions for a project that has five associated resources.

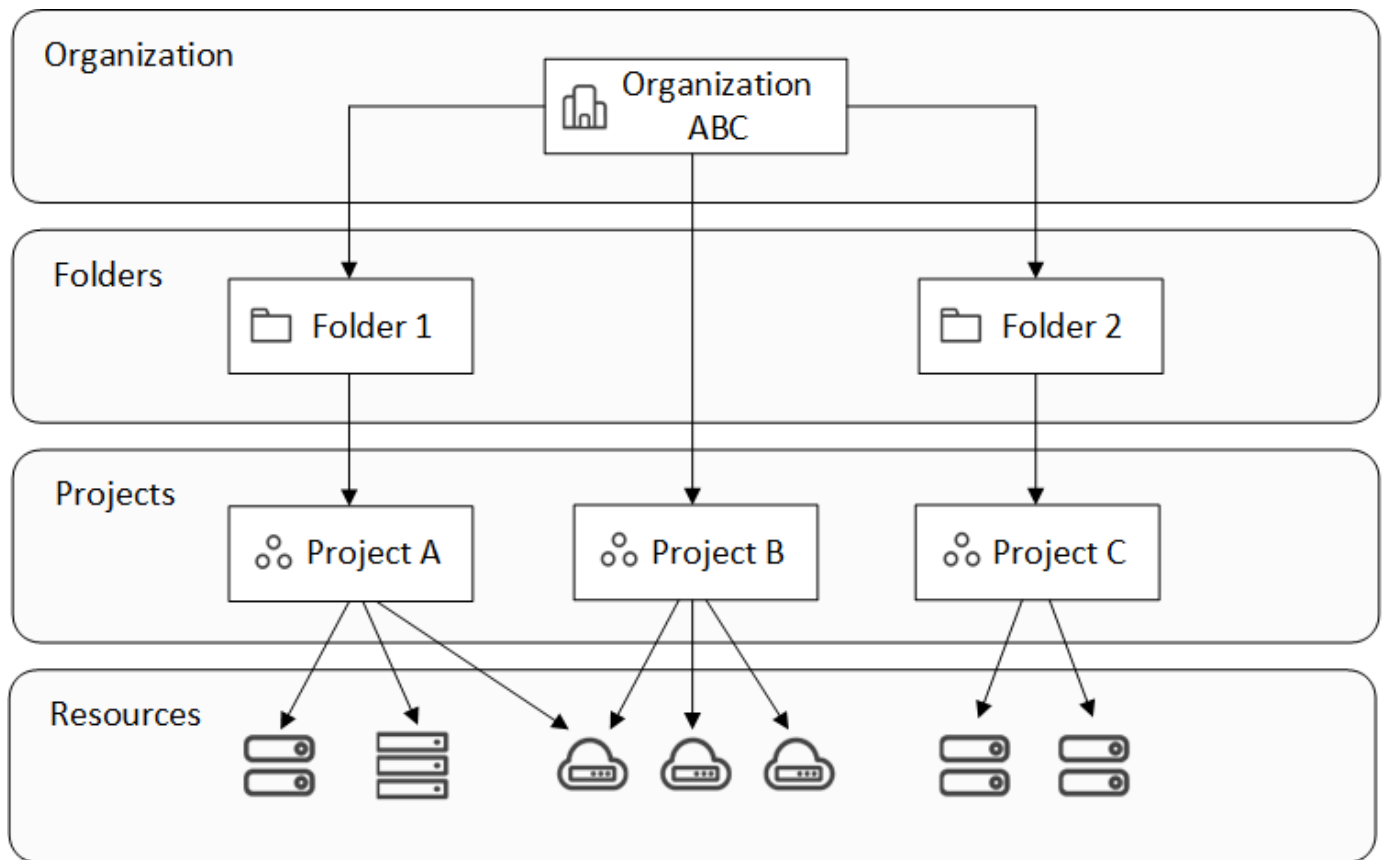
When using BlueXP IAM, you'll manage the following components:

- 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.

When you sign up to BlueXP, you're prompted to create a new 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).

Folders can contain projects, other folders, or a combination of both.

You don't need to create folders. They are 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.



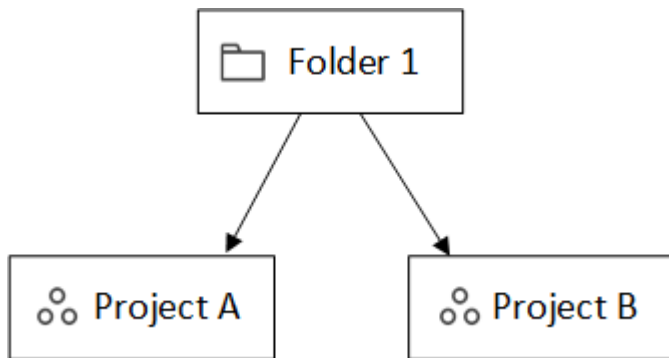
You can also associate a Connector with another folder or project in your organization. [Learn more about using Connectors with BlueXP IAM.](#)

When to associate a resource with a folder

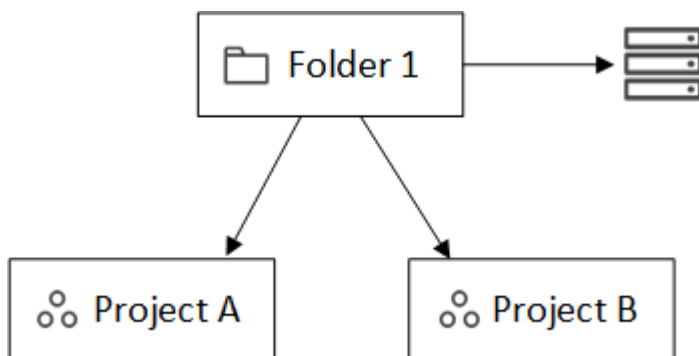
You also have the option to associate a resource with a folder, but this is optional and meets the needs of a specific use case.

An *Organization admin* might associate a resource with a folder so that a *Folder or project admin* can then associate that resource with the appropriate projects that reside in the folder.

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

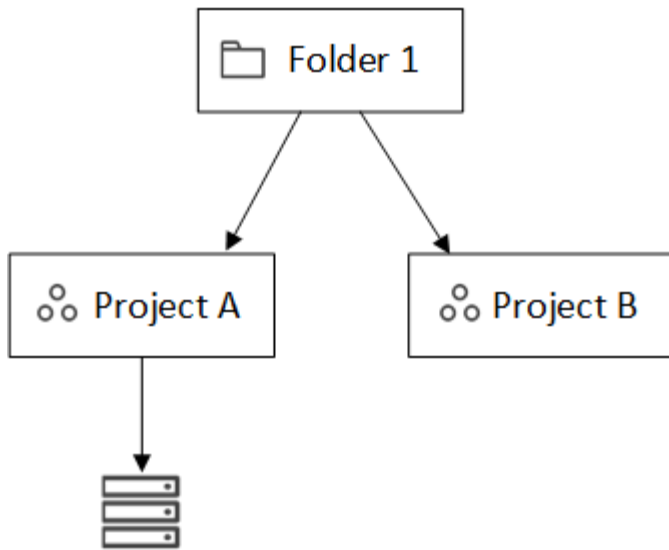


The *Organization admin* can associate a resource with the folder:



Associating the resource with the folder doesn't automatically make that resource accessible from all projects in the folder. But the *Folder or project admin* can then decide which projects that resource should be made available to. After making that decision, the admin can then associate the resource with the right 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.

An organization has at least one user with the *Organization admin* role (the user who creates the organization is automatically assigned this role). 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.

By providing permissions at a specific part of the resource hierarchy, you can restrict access rights to only the resources that a member needs to complete their tasks.

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

Roles that you grant at the organization level are inherited by all folders, projects, and resources in the organization. That means the member has permissions to everything in the organization.

Folders

Roles that you grant at the folder level are inherited by all folders, projects, and resources in the folder.

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

Roles that you grant at the project level are inherited by all resources associated with that project.

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.

Predefined roles

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

[Learn about IAM predefined 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 might want to make a Connector available to use with another project in the following 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 associated with 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.

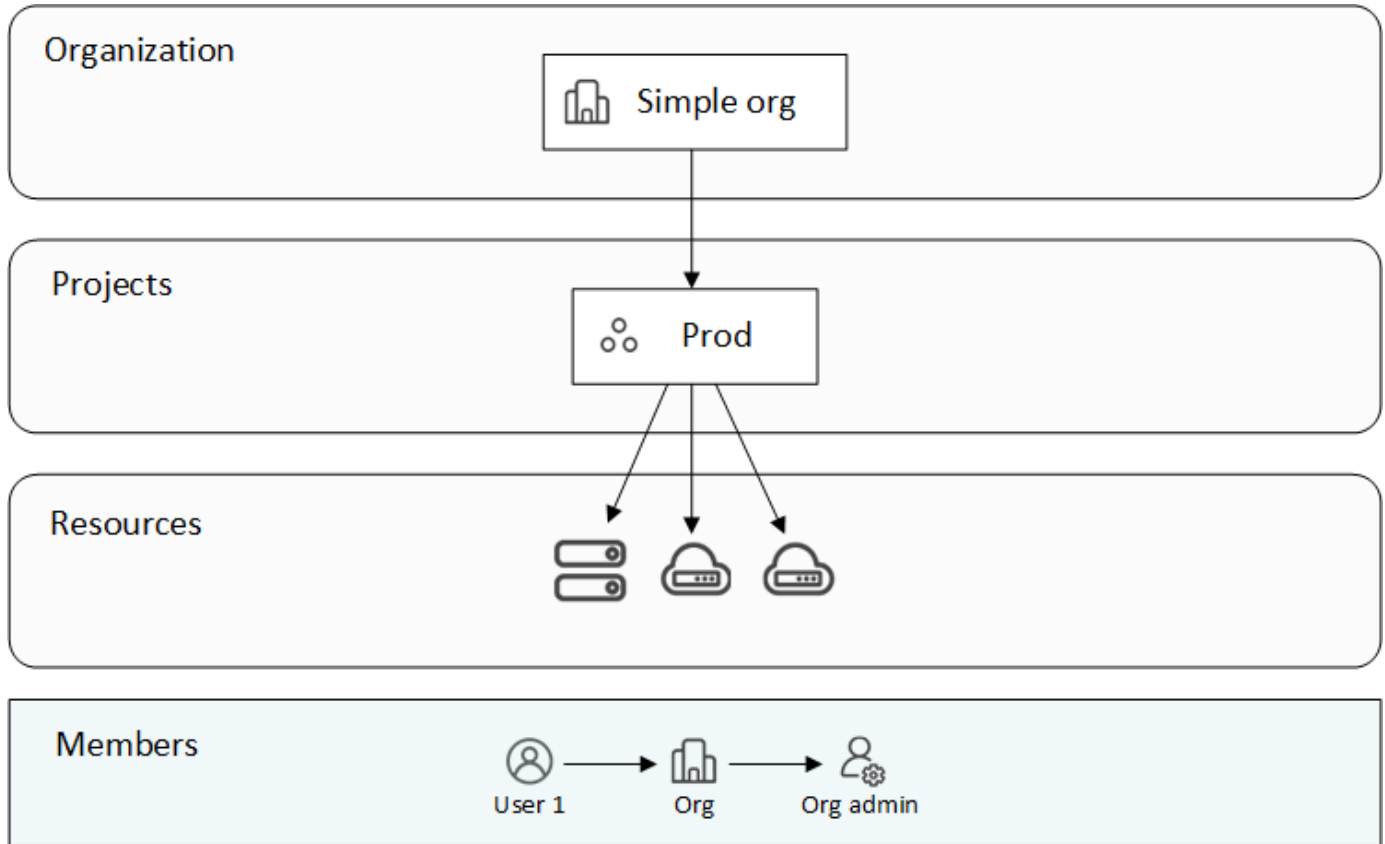
An *Organization admin* might associate a Connector with a folder so that the *Folder or project admin* can make the decision to associate that Connector with the appropriate projects that reside in the folder.

IAM examples

The following examples show how you might set up your organization.

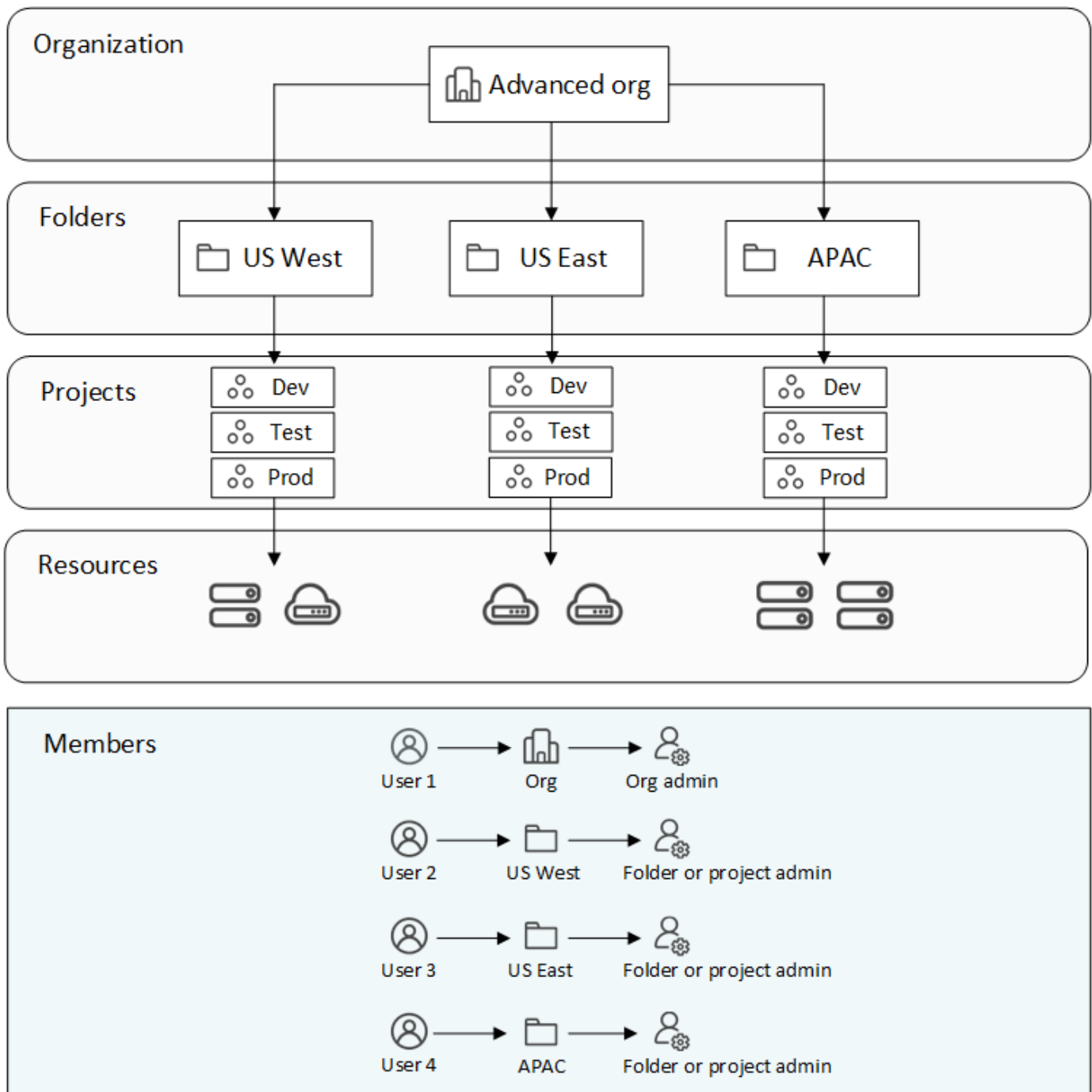
Simple organization

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](#)
- [Predefined BlueXP IAM 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

You can simply use the default project or you can create additional projects and folders that match the hierarchy of your business.

[Learn how to organize your resources with folders and projects.](#)

2

Associate members with your organization

If multiple people in your business need to access and manage resources from BlueXP, you'll need to associate their user accounts with your organization and provide the appropriate permissions across your resource hierarchy. 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 *working environments*. A working environment represents a storage system that organization members manage from within a project. For example, a Cloud Volumes ONTAP system or an on-premises ONTAP cluster.

Learn how to create or discover resources from the BlueXP canvas:

- [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 the resource is managed by a Connector, then you also need to create an association between the project and the associated Connector.

- [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

The depth of your organization's hierarchy can go down to 7 levels. As a result, you can create nested folders down to 6 levels. The last nested folder can then include projects at the seventh level of the hierarchy.

The following image illustrates the maximum depth of your organization's 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 only select from the resources that are associated with the parent of the folder or project. If the parent is the organization, then you can choose from any resource in the organization. If the parent is a folder, then you can only select from the resources that are associated with the folder.

[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**.


Result

BlueXP creates the folder or project and associates the specified resources and members.

View the resources and members 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.

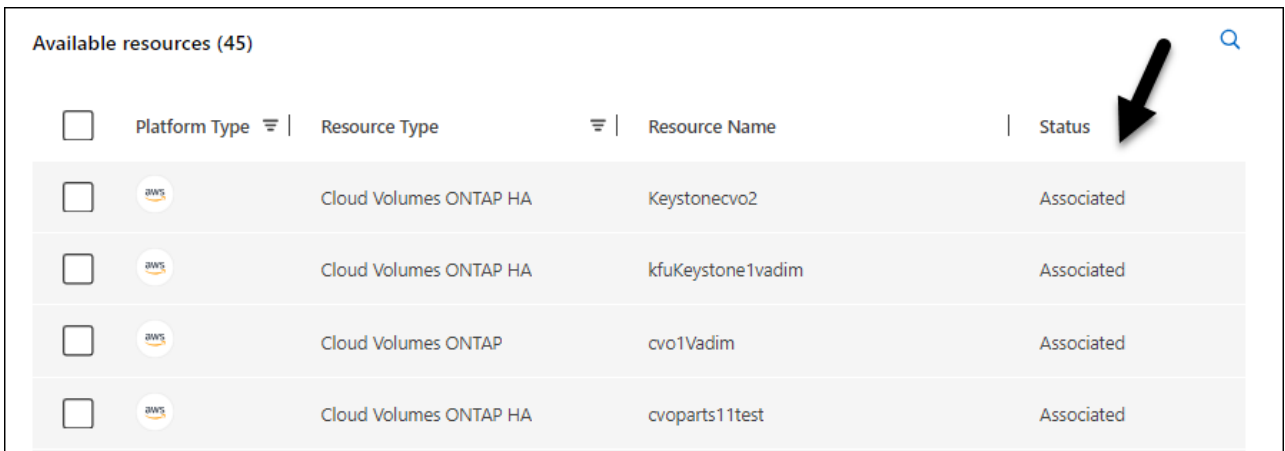
Steps

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, view details about associated resources and member access:

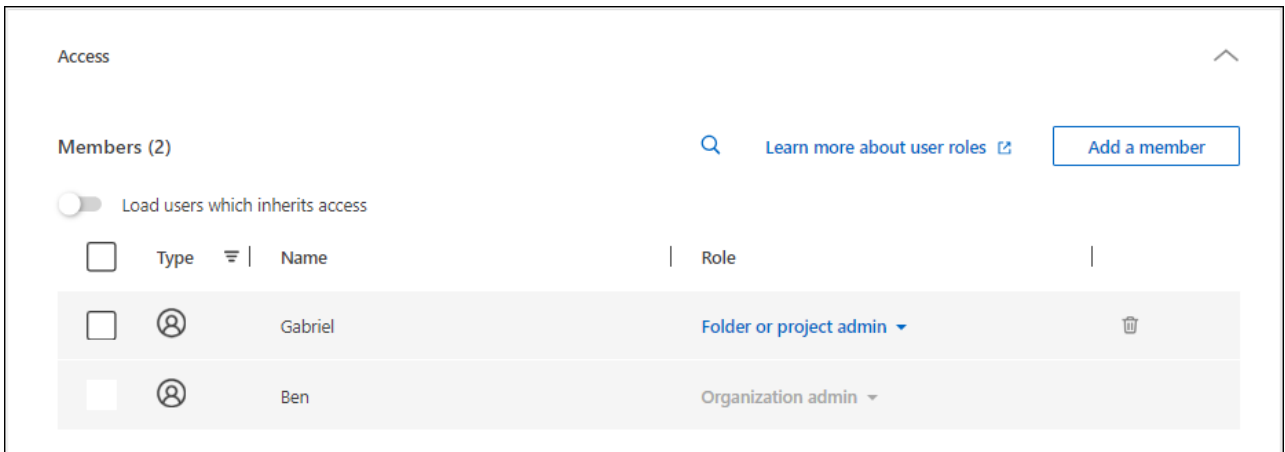
- Select **Resources** to view the associated resources. In the table, the **Status** column identifies the resources that are associated with the folder or project.



Available resources (45)

<input type="checkbox"/>	Platform Type	Resource Type	Resource Name	Status
<input type="checkbox"/>		Cloud Volumes ONTAP HA	Keystonecvo2	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	kfuKeystone1vadim	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP	cvo1Vadim	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	cvoparts11test	Associated



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



Access

Members (2) [Learn more about user roles](#) [Add a member](#)

☐ Load users which inherits access

<input type="checkbox"/>	Type	Name	Role
<input type="checkbox"/>		Gabriel	Folder or project admin
<input type="checkbox"/>		Ben	Organization admin

What's next?

If needed, you can [modify the associated resources](#) or [modify member access](#).

Modify the resources associated with a folder or project

You can modify the resources that are associated with a folder or project by associating or disassociating a resource. For example, you might want to associate a resource with another project because that resource has capacity that another team can utilize.

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

<input type="checkbox"/>	Platform Type	Resource Type	Resource Name	Status
<input checked="" type="checkbox"/>		Cloud Volumes ONTAP HA	Keystonecvo2	Associated
<input checked="" type="checkbox"/>		Cloud Volumes ONTAP HA	kfuKeystone1vadim	Associated
<input checked="" type="checkbox"/>		Cloud Volumes ONTAP	cvo1Vadim	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	cvoparts11test	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP	cvosecondaryparts11	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	keystonetest	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	keystonetesting55	Associated

5. Select **Apply**

Result

BlueXP associates the resources with the folder or project. Organization members who have permissions for that folder or project can now access the associated resources.

Modify member access to a folder or project

Modify member access to a folder or project to ensure that the right members have access to the resources associated with the 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, select **Access**.

BlueXP displays the list of members who have access to the 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.

If a role was provided at a higher level of the hierarchy (at the folder or organization level), then you

should consider whether to change the role at the lower level or the higher level. For example, if you assigned the *Folder or project admin* role at the folder level, changing the role at the project level to lower-level permissions won't alter the permissions for the member. Because roles are inherited down the organization hierarchy, the member would still have admin permissions at the project level.

[Learn more about role inheritance.](#)

- **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.

If member access was provided at a higher level of the hierarchy (at the folder or organization level), then you can't remove member access when viewing this folder or project. You need to switch to that part of the hierarchy. Alternatively, you can [manage permissions from the Members page](#).

4. Select **Apply**.

Result

BlueXP updates the members who have access to the folder or project.

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**.

Result

BlueXP updates the name of the folder or project.

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.

Result

BlueXP deletes the folder or project. That folder or project is no longer available to organization members.

Related information

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

Add BlueXP IAM members and manage their permissions

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.



To ensure that you don't lose access to your BlueXP organization, it's a best practice to have two members with the Organization admin role.

About this task

When a *Folder or project admin* views the **Members** page, the page displays all members in the organization. However, a member with this role can only view and manage member permissions for the folders and projects for which they have permissions. [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 typically used by an application to complete specified tasks without human intervention.


User account

Steps

1. If the user hasn't already done so, ask them to go to the [NetApp BlueXP website](#) and sign up.

When the user signs up, they should complete the **Sign up** page, verify their email address, and then log in. When prompted to create an organization, the user should close out of BlueXP and let you know that they've created their user account. 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.
- If you select the organization or a folder, the member will have permissions to everything that resides within the organization or folder.
- **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.
 - If you selected the organization, you can choose from any role other than **Folder or project admin**.
 - If you selected a folder or project, you can choose from any role other than **Organization admin**.
- **Add role**: If you want to provide access to additional folders or projects within your organization, select **Add role**, specify another folder or project, and then choose a role.

[Learn about predefined IAM roles.](#)

6. Select **Add**.

Result


BlueXP adds the user to the organization.

What's next?

The user should receive an email from NetApp BlueXP. The email includes information that the member can use 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.
- If you select the organization or a folder, the member will have permissions to everything that resides within the organization or folder.
- **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.
 - If you selected the organization, you can choose from any role other than **Folder or project admin**.
 - 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, select **Add role**, specify another folder or project, and then choose a role.
5. Select **Add**.
 6. Download or copy the client ID and client secret.

The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely. Note that you can recreate the client ID and client secret later on as needed.

7. Select **Close**.

Result

BlueXP adds the service account to your organization.


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.


About this task

The **Members** page shows details about two types of members: user accounts and service accounts.

Steps

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

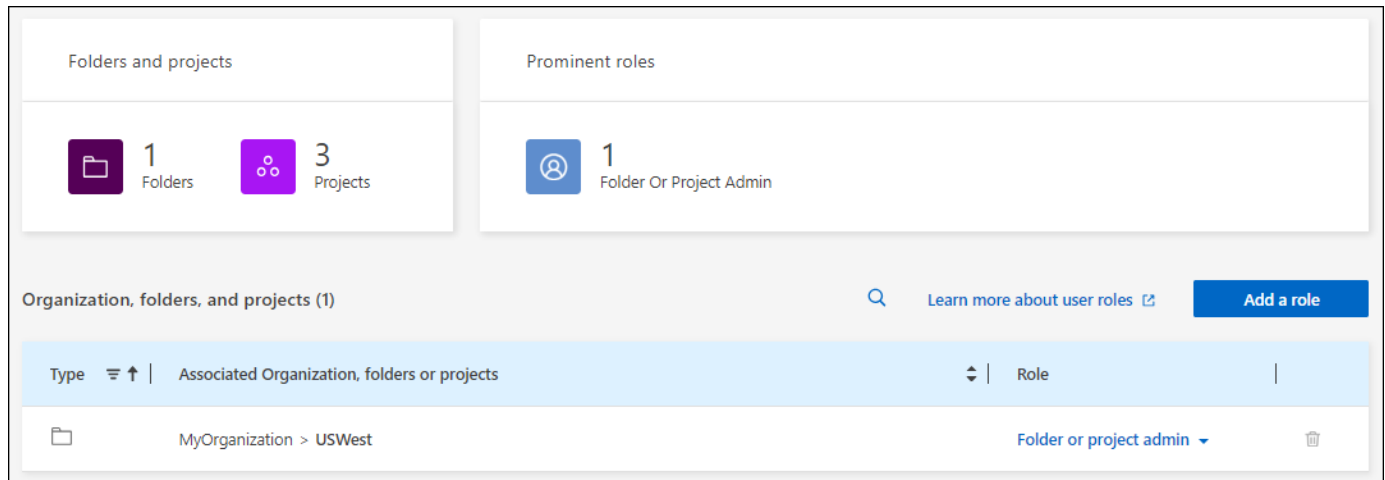
The members of your organization appear in the **Members** table.

3. From the **Members** page, navigate to a member in the table, select  and then select **View details**.


Result

BlueXP displays details about the member, which includes the folders and projects that the member has permissions for across your organization's resource hierarchy.

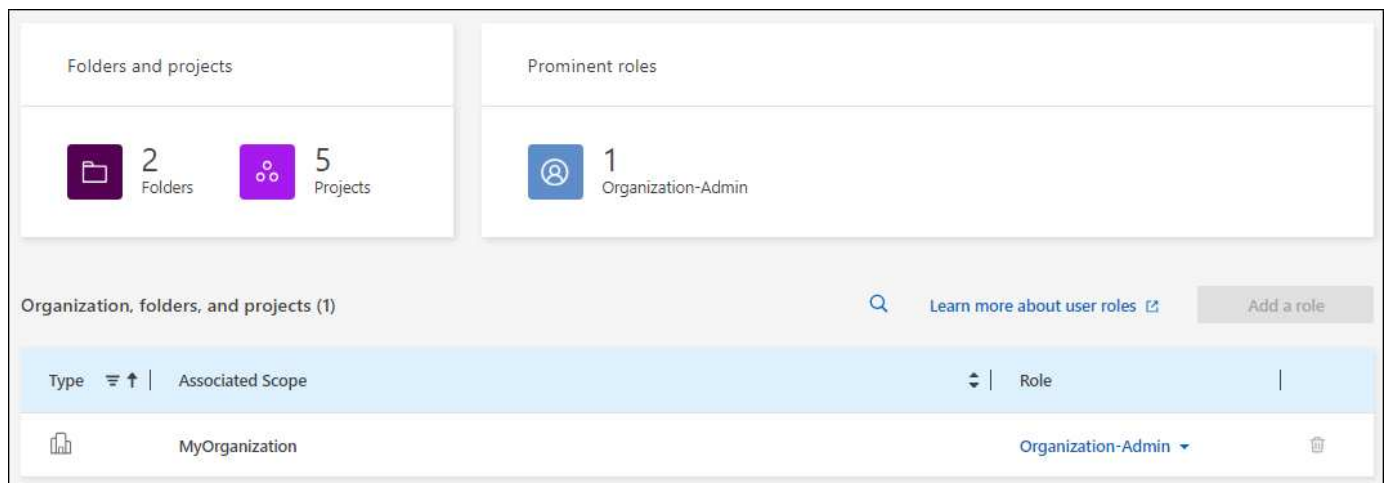
Here's an example of a member who is assigned the *Folder or project admin* role for a folder, which provides permissions to the three projects in the folder.




The screenshot displays the 'Members' page in the BlueXP console. It features two main sections: 'Folders and projects' and 'Prominent roles'. The 'Folders and projects' section shows 1 Folder and 3 Projects. The 'Prominent roles' section shows 1 role: 'Folder Or Project Admin'. Below these sections is a table titled 'Organization, folders, and projects (1)'. The table has columns for 'Type', 'Associated Organization, folders or projects', and 'Role'. The first row shows a folder icon, 'MyOrganization > USWest', and the role 'Folder or project admin'. There are also search, 'Learn more about user roles', and 'Add a role' buttons.

Type	Associated Organization, folders or projects	Role
	MyOrganization > USWest	Folder or project admin

Here's another example that shows a member who has the Organization admin role, which gives the user access to all resources in the organization.



The screenshot displays the 'Members' page in the BlueXP console. It features two main sections: 'Folders and projects' and 'Prominent roles'. The 'Folders and projects' section shows 2 Folders and 5 Projects. The 'Prominent roles' section shows 1 role: 'Organization-Admin'. Below these sections is a table titled 'Organization, folders, and projects (1)'. The table has columns for 'Type', 'Associated Scope', and 'Role'. The first row shows a folder icon, 'MyOrganization', and the role 'Organization-Admin'. There are also search, 'Learn more about user roles', and 'Add a role' buttons.

Type	Associated Scope	Role
	MyOrganization	Organization-Admin

Related information

[View all of the members associated with a specific folder or project.](#)

Manage a member's permissions

A role defines the permissions assigned to a member at the organization, folder, or project level. Each organization member can have a role assigned 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 role B for project 2.



A member who is assigned the Organization admin role can't be assigned any additional roles. They already have permissions across the entire organization.

Add a role to a member

Provide a member with additional permissions in your organization by adding roles that apply to the organization, folder, or project level.

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 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.
 - If you selected the organization, you can choose from any role other than **Folder or project admin**.
 - 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, select **Add role**, specify another folder or project, and then choose a role.

3. Select **Add new roles**.

Result

BlueXP adds the roles. The member now has permissions for the resources in the organization, folder, or project that you selected.

Change from one role to another

If you need to modify a member's permissions, you can change the role that's associated with that member at the organization, folder, or project level.

If you need to change the roles for multiple members in your organization, you can use a bulk action to complete the changes all at once.

One member

Steps

1. From the **Members** page, navigate to a member in the table, select **...** and then select **View details**.
2. In the table, navigate to the organization, folder, or project and then select a new role.

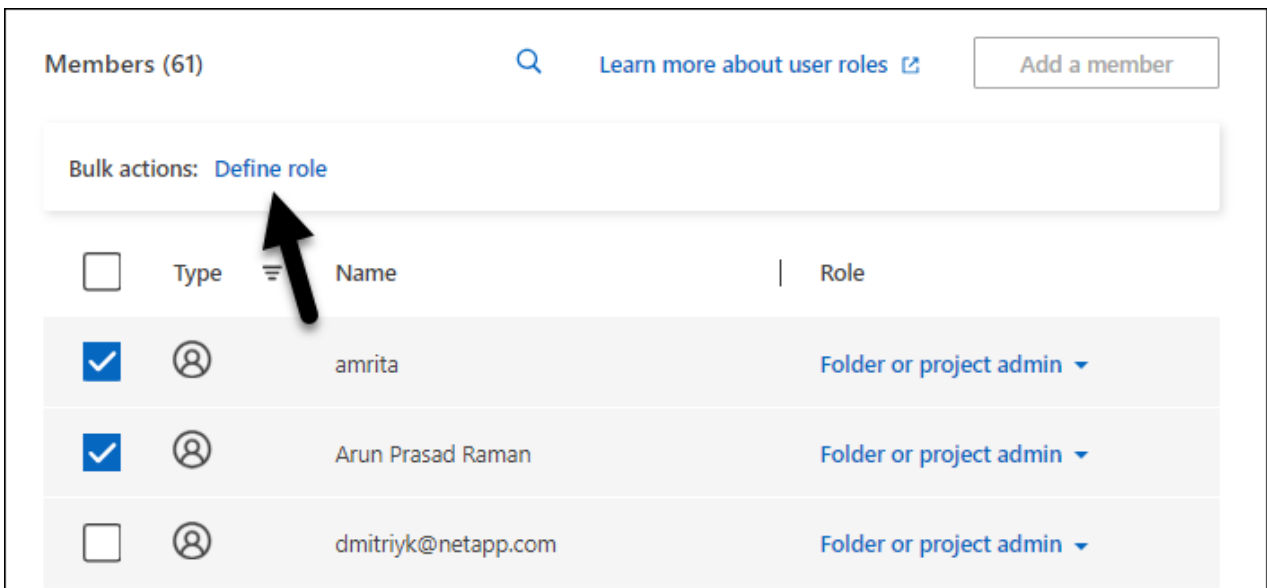
Result

BlueXP updates the roles associated with that member at the organization, folder, and project level.

Multiple members

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select **...** and then select **Edit organization**, **Edit folder**, or **Edit project**.
2. On the **Edit** page, select **Access**.
3. Select all members or individually select two or more members.
4. Select **Define role**.



5. Select the role that you'd like to assign to the members and then select **Define**.

Result

BlueXP updates the roles for all of the members that you selected.

Remove permissions for a folder or project

You can remove a member's permissions to a specific folder or project by removing their role.



About this task

If a member has permissions in your organization to *only* one folder or project, you can't remove that role. You have two choices:

- If you want the member to have permissions to another part of the resource hierarchy, you need to add that role first and then delete the existing role.

- If you don't want the member to have permissions to anything, then you can simply remove the member 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, navigate to the folder or project level and then select 

Result

BlueXP removes permissions for that member at the folder or project level.



Recreate the credentials for a service account

You can recreate the credentials (client ID and client secret) for a service account at any time. You might recreate the credentials if you lost them or if your business requires that you rotate security credentials after a period of time.

About this task

Recreating the credentials deletes the existing credentials for the service account and then creates new credentials. You will not be able to 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.

The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.

6. Select **Close**.

Result

A new client ID and client secret are now associated with the service account.


Remove a member from your organization

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

About this task

This task doesn't delete the member's BlueXP account or NetApp Support Site account. It simply removes the member and their associated permissions from your organization.

Steps

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

Result

BlueXP removes the member. If that member logs in to BlueXP again, they no longer have access to your BlueXP organization.

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](#)


Manage the resource hierarchy in your BlueXP organization

When you use BlueXP identity and access management (IAM) to 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 working environment that BlueXP already manages.

View the resources in your organization

To start managing your resource hierarchy, you should be aware of the resources that are associated with your organization.

Steps

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

Result

The resources associated with your organization display in the **Resources** table.

What's next?

To find a specific resource, you can [search and filter the contents of the table](#).

After you've found the resource that you're looking for, you can complete any of the following actions:

- [View the folders and projects that are associated with the resource](#)
- [Associate the resource with additional folders and projects](#)
- [Remove the resource from a folder or project](#)

Find specific resources in your organization

If you have a large number of resources in your organization, you can use the search and filter options to find a specific resource.

Steps

1. From the **Resources** page, select **Advanced Search & Filtering**.
2. 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.

3. Select **Search**.

Result

The contents of the Resources table refreshes to show the resources that match your search and filter selections.

Associate a resource with folders and projects

If you want to make a resource available to another folder or project in your organization, then you'll need to create an association between the folder or project and the resource.

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**.

Result

BlueXP associates the resource with the selected folders and projects.

- 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 the resource that you associated is discovered using a BlueXP Connector and you have other members in your organization, then you also need to associate the Connector with the project that the resource is now associated with. Otherwise, the Connector and it's associated resource aren't accessible from the BlueXP canvas by members who don't have 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.




Steps

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

Result

BlueXP displays the folders and projects that are associated with the resource.

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

Folders (0) Project (1)		Associate to folder or project
Type	Associated folders or projects	
	MyOrganization	
	MyOrganization > Project1	

What's next?

- You can [associate the resource with an additional project or folder](#).
- You can [remove the resource from a specific folder or project](#).
- 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. After you remove the association, organization members can no longer manage the resource from the folder or project.

About this task

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**.

Result

BlueXP removes the association. Members can no longer access the resource from that folder or project.

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

A Connector is required to manage several types of working environments from BlueXP. 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. 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 from BlueXP identity and access management (IAM).


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.](#)
- Due to a known issue, the Connectors page in BlueXP IAM displays any old Connectors that you previously removed from BlueXP.

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.

To find a specific Connector, you can use the search that's above the table and filter the contents of the table by selecting a specific part of the resource hierarchy.

4. To first view the folders and projects that the Connector is associated with, 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**.

Result

BlueXP associates the Connector with the selected folders and projects. Members who have permissions for those folders and projects now have the ability to select that 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.



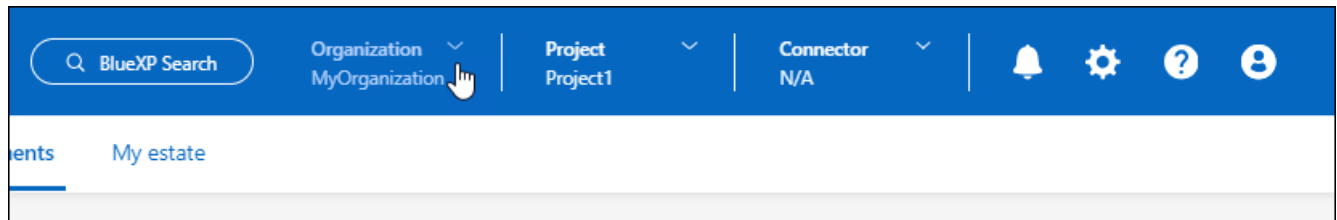
You might belong to multiple organizations if you were invited to join another organization or if you created an additional organization yourself. You can create an additional organization by using the API. [Learn how to create a new organization](#)

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

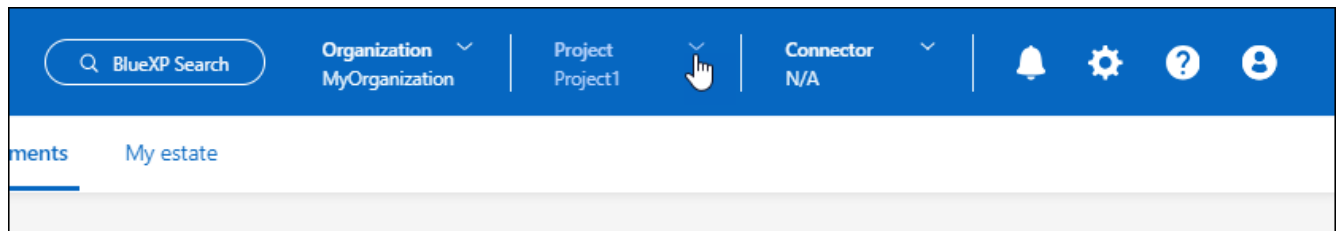
If your organization includes multiple projects and you have access to those projects, you can switch between them at any time.

Before you begin

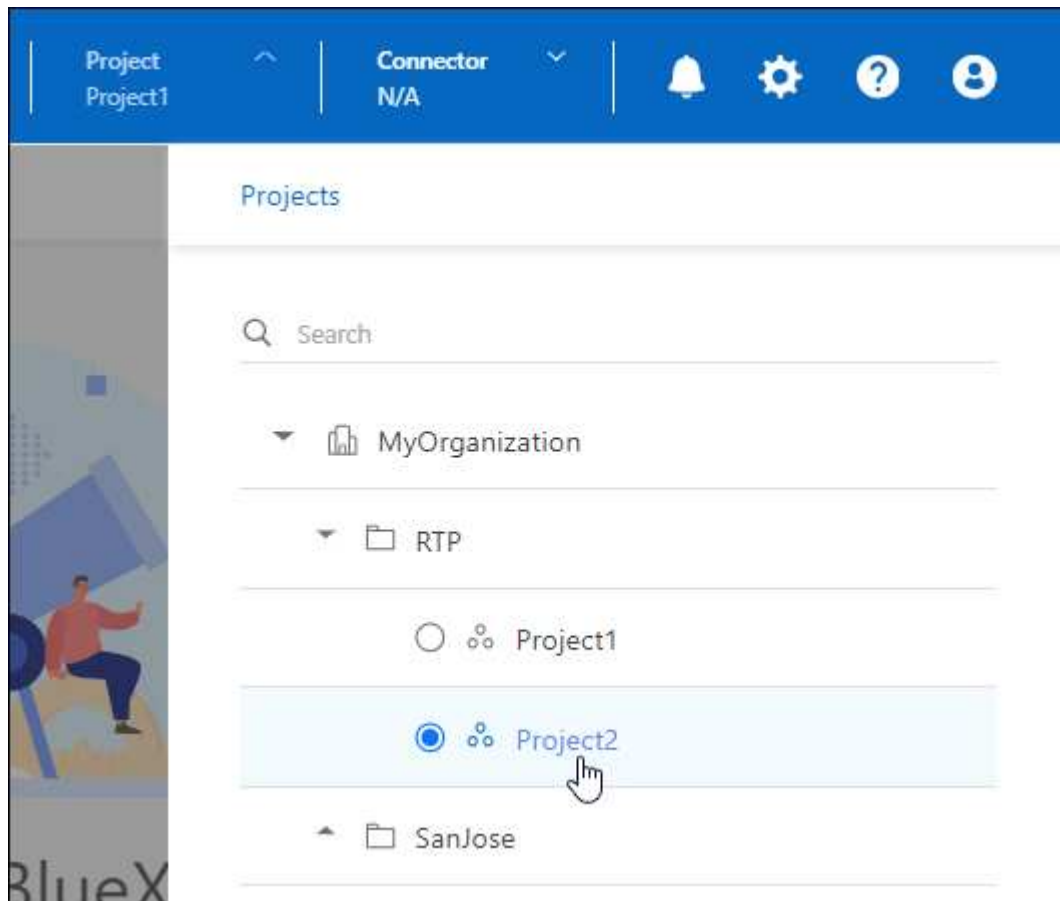
You must be on any page in the BlueXP console other than the BlueXP identity and access management (IAM) pages. You can't switch to another project when viewing any of the IAM pages.

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 link

[Associate Connectors with folders and projects.](#)



Related information

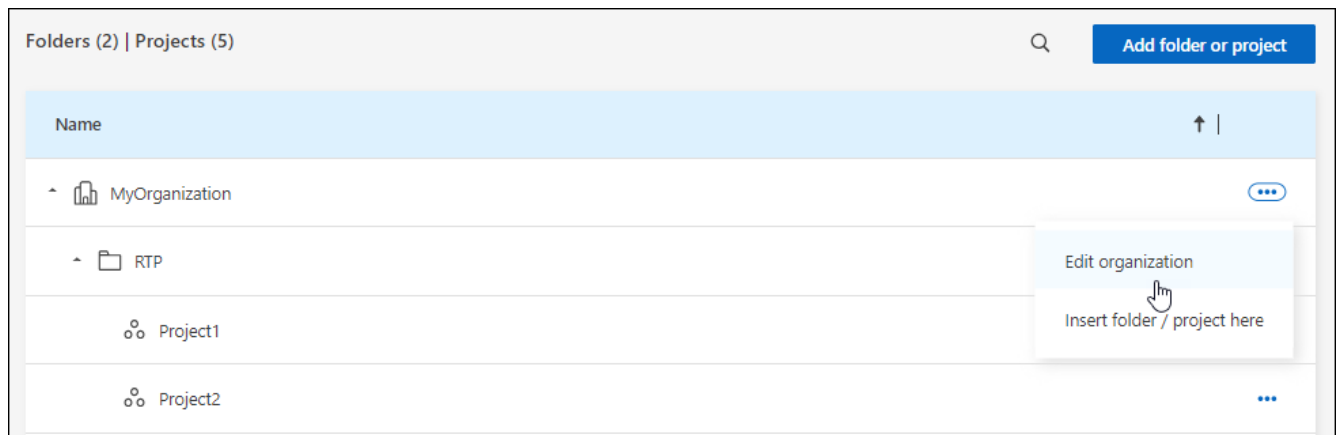
- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Learn about the API for BlueXP IAM](#)

Rename your BlueXP organization

If needed, you can change the name of your BlueXP organization from BlueXP identity and access management (IAM). The organization name appears at the top of the BlueXP web-based console and within the IAM pages.

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**.

Result

BlueXP updates the name of your organization. You should immediately see the updated name at the top of the BlueXP console.

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.

Predefined BlueXP IAM roles and permissions

BlueXP identity and access management (IAM) includes several 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.

Organization admin

Description

Provides full control of the entire BlueXP organization.

Permissions

A member who has this role can complete all actions in BlueXP.

Folder or project admin

Description

Provides full control of one or more projects and folders.

Note that if you assign this role at the folder level, the member has permissions to all projects that are associated with that folder.

Permissions

A member who has this role can complete the following actions in BlueXP:

- Manage all working environments in the projects and folders for which they have permissions
- Use all BlueXP services
- From BlueXP IAM, an admin of a folder can administer the folders, projects, and resources that are children of that folder:
 - Add folders or projects within the folder
 - Edit folders and projects: their names, associated resources, and member access
 - Delete folders and projects
 - Add a user account and associate a role at the folder or project level

- Associate a Connector with a folder or project
- Add a role to a member at the folder or project level
- View resources associated with folders and projects
- Associate viewable resources with additional folders or projects
- Dissociate a resource from a folder or project
- From BlueXP IAM, an admin of a project can administer that project and its associated resources as follows:
 - Edit the project: its name, associated resources, and member access
 - Add a user account and associate a role at the project level
 - Associate a Connector with a project, if the member has admin permissions to other projects that have other associated Connectors
 - Add a role to a member at the project level
 - View resources associated with the project
 - Associate resources with the project, if the member has admin permissions to other projects that have other associated resources
 - Dissociate a resource from the project
 - Delete the project
- Manage credentials from Settings > Credentials
- View the BlueXP timeline
- Register BlueXP for support and submit cases

SnapCenter admin

Description

Provides the ability to back up snapshots from on-premises ONTAP clusters using BlueXP backup and recovery for applications.

Permissions

A member who has this role can complete the following actions in BlueXP:

- Complete any action from Backup and recovery > Applications
- Manage all working environments in the projects and folders for which they have permissions
- Use all BlueXP services

Classification viewer

Description

Provides the ability view BlueXP classification scan results.

Permissions

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.

No other actions are available to a member who has this 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 accounts

Learn about BlueXP accounts

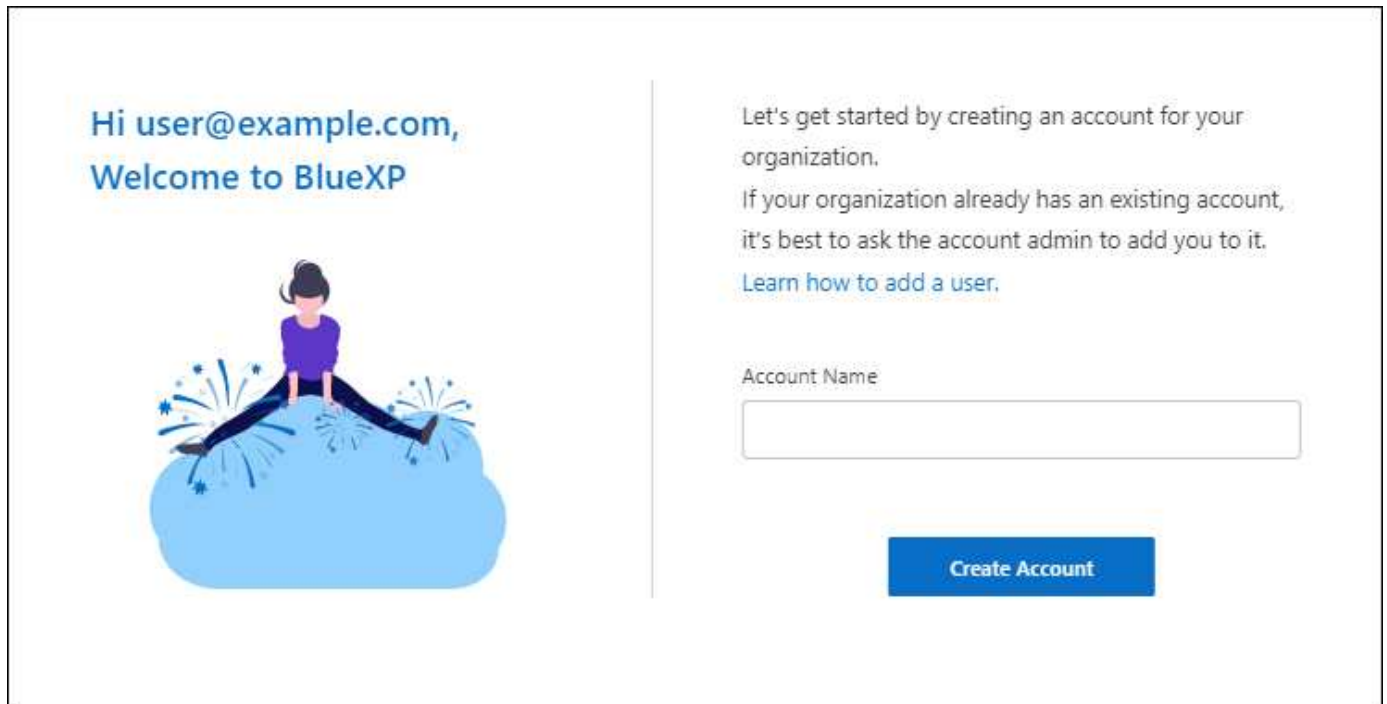
When you use BlueXP in restricted mode or private mode, you'll use a *BlueXP account* to manage users and organize resources in isolated *workspaces*. For example, a group of users can deploy and manage Cloud Volumes ONTAP working environments in a workspace that isn't visible to users who manage working environments in a different workspace.

If you're using BlueXP in standard mode, you won't have a BlueXP account. Instead, you'll have a *BlueXP organization* that you manage using BlueXP identity and access management (IAM).

- [Learn about BlueXP IAM](#)
- [Learn about BlueXP deployment modes](#)

Overview

When you first access BlueXP, you're prompted to select or create an account. For example, you'll see the following screen if you don't have an account yet:

The image shows a user interface for creating a BlueXP account. On the left, there is a greeting: "Hi user@example.com, Welcome to BlueXP" in blue text. Below the text is an illustration of a person in a purple shirt and black pants sitting on a large blue cloud, with small blue starburst effects around them. On the right side, there is instructional text: "Let's get started by creating an account for your organization." followed by "If your organization already has an existing account, it's best to ask the account admin to add you to it." and a link "Learn how to add a user." in blue. Below this text is a text input field labeled "Account Name". At the bottom right, there is a blue button with the text "Create Account" in white.

BlueXP Account Admins can then modify the settings for this account by managing users (members),

workspaces, and Connectors:

The screenshot shows the 'Manage Account: KeystoneTes...' interface. At the top, there are four tabs: 'Overview' (selected), 'Members', 'Workspaces', and 'BlueXP Connector'. Below the tabs, there are three summary cards: '30 Members' (with a person icon), '1 Workspaces' (with a folder icon), and '3 Connectors' (with a plug icon). Below these cards, there are two rows of account details. The first row shows 'KeystoneTest01' as the 'Account Name' with an edit icon, and 'Allow Private Preview' as a toggle switch. The second row shows 'account-Pq7bhQxz' as the 'Account ID' with a copy icon, and 'Allow Third Party Services' as a toggle switch.

[Learn how to manage your BlueXP account.](#)

Members

Members are BlueXP users that you associate with your BlueXP account. Associating a user with an account and one or more workspaces in that account enables those users to create and manage working environments in BlueXP.

When you associate a user, you assign them a role:

- *Account Admin*: Can perform any action in BlueXP.
- *Workspace Admin*: Can create and manage resources in the assigned workspace.
- *Compliance Viewer*: Can only view compliance information for BlueXP classification and generate reports for workspaces that they have permission to access.

[Learn more about these roles.](#)

Workspaces

In BlueXP, a workspace isolates any number of *working environments* from other users in the account. Workspace Admins can't access the working environments in a workspace unless the Account Admin associates the admin with that workspace.

A working environment represents a storage system. For example:

- A Cloud Volumes ONTAP system
- An on-premises ONTAP cluster
- A StorageGRID system

[Learn how to add a workspace.](#)

Connectors

A Connector executes the actions that BlueXP needs to perform in order to manage your data infrastructure. The Connector runs on a virtual machine instance that you deploy in your cloud provider or on an on-premises host that you configured.

You can use a Connector with more than one BlueXP service. For example, if you're using a Connector to manage Cloud Volumes ONTAP, you can use that same Connector with another service like BlueXP tiering.

[Learn more about Connectors.](#)

Examples

The following examples depict how you might set up your accounts.

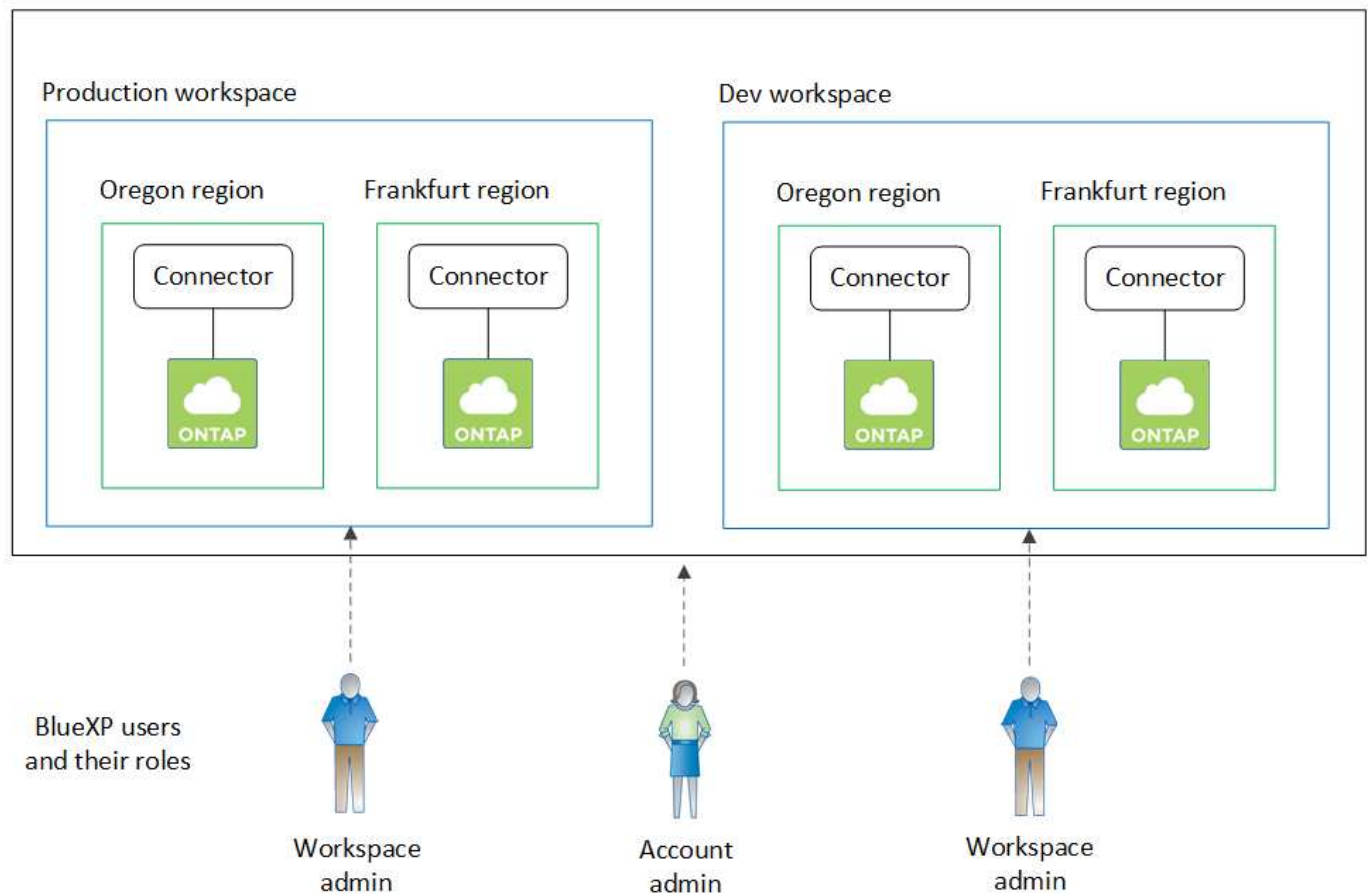


In both example images that follow, the Connector and the Cloud Volumes ONTAP systems don't actually reside *in* the BlueXP account—they're running in a cloud provider. This is a conceptual representation of the relationship between each component.

Multiple workspaces

The following example shows an account that uses two workspaces to create isolated environments. The first workspace is for a production environment and the second is for a dev environment.

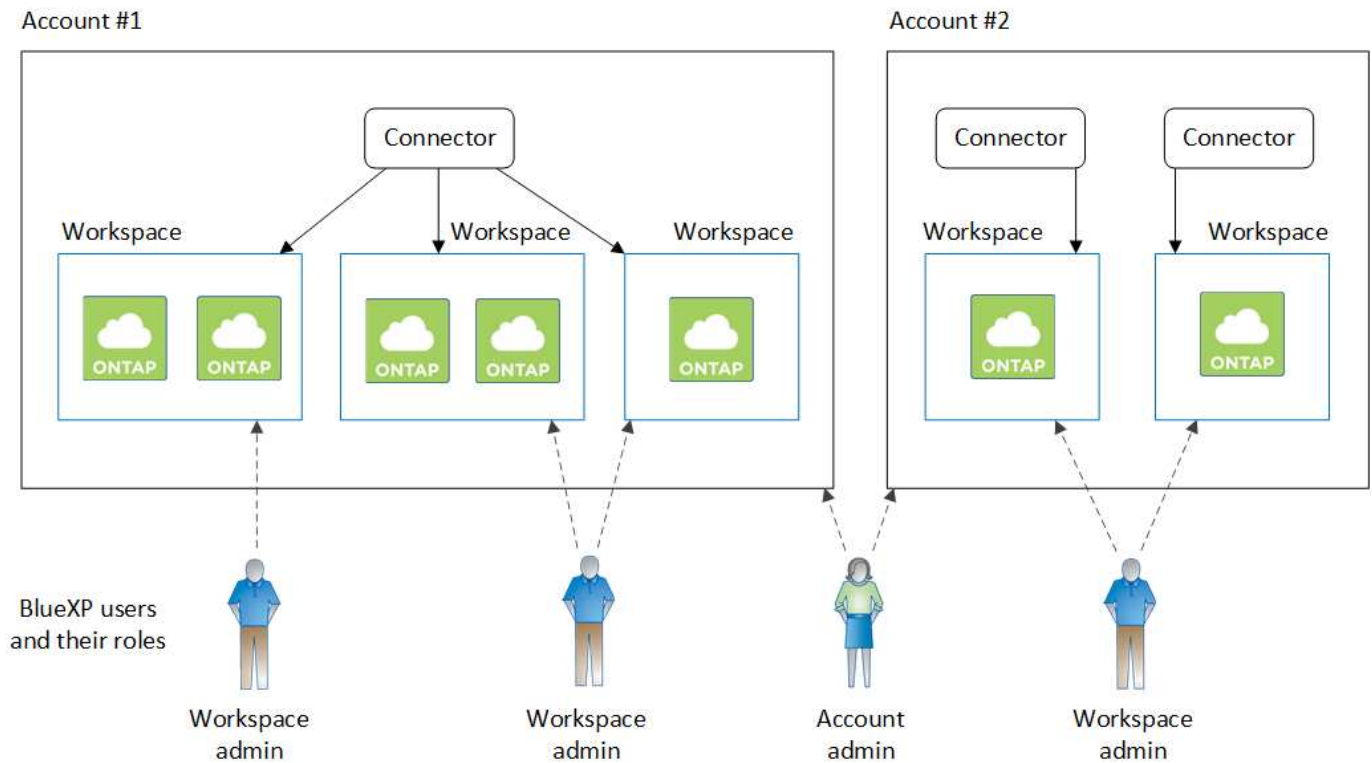
Account



Multiple accounts

Here's another example that shows the highest level of multi-tenancy by using two separate BlueXP accounts. For example, a service provider might use BlueXP in one account to provide services for their customers, while using another account to provide disaster recovery for one of their business units.

Note that account 2 includes two separate Connectors. This might happen if you have systems in separate regions or in separate cloud providers.



Manage your BlueXP account

When you use BlueXP in restricted mode or private mode, you'll use a *BlueXP account* to manage users and organize resources. When you create your account, it only includes a single admin user and a workspace. You can manage the account to fit your needs by adding users, creating service accounts for automation purposes, by adding workspaces, and more.

If you're using BlueXP in standard mode, you won't have a BlueXP account. Instead, you'll have a *BlueXP organization* that you manage using BlueXP identity and access management (IAM).

- [Learn about BlueXP IAM](#)
- [Learn about BlueXP deployment modes](#)

Manage your account with the Tenancy API

If you want to manage your account settings by sending API requests, then you'll need to use the *Tenancy API*. This API is different than the BlueXP API, which you use to create and manage Cloud Volumes ONTAP working environments.

Create and manage users

The user's in your account can access and manage the resources in specific workspaces.

Add users

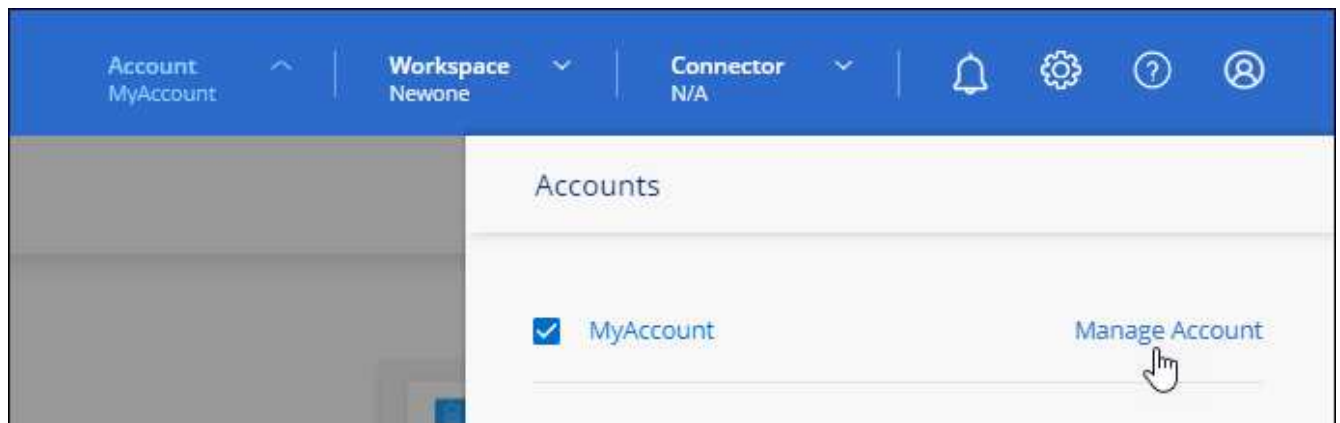
Associate users with your BlueXP account so those users can create and manage working environments in BlueXP.

Steps

1. If the user hasn't already done so, ask the user to go to [NetApp BlueXP website](#) and sign up.
2. From the top of BlueXP, select the **Account** drop-down.



3. Select **Manage Account** next to the currently selected account.



4. From the Members tab, select **Associate User**.
5. Enter the user's email address and select a role for the user:
 - **Account Admin:** Can perform any action in BlueXP.
 - **Workspace Admin:** Can create and manage resources in assigned workspaces.
 - **Compliance Viewer:** Can only view compliance information for BlueXP classification and generate reports for workspaces that they have permission to access.
6. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.



The image shows a web-based dialog box titled "Associate User". At the top, there is a user icon. Below the title, a light blue banner contains the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The main form area has three sections: "User's Email" with a text input field containing "test@netapp.com"; "Role" with a dropdown menu showing "Workspace Admin"; and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (X). At the bottom, there are two buttons: a grey "Cancel" button and a blue "Associate User" button.



Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 X

Cancel Associate User

7. Select **Associate**.

Result

The user should receive an email from NetApp BlueXP titled "Account Association." The email includes the information needed to access BlueXP.

Remove users

Disassociating a user makes it so they can no longer access the resources in a BlueXP account.

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.



2. From the Members tab, select the action menu in the row that corresponds to the user.



3. Select **Disassociate User** and select **Disassociate** to confirm.

Result

The user can no longer access the resources in this BlueXP account.

Manage a Workspace Admin's workspaces

You can associate and disassociate Workspace Admins with workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.



You also need to associate the Connector with workspaces so Workspace Admins can access those workspaces from BlueXP. [Learn how to manage a Connector's workspaces.](#)

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.



2. From the Members tab, select the action menu in the row that corresponds to the user.



3. Select **Manage Workspaces**.
4. Select the workspaces to associate with the user and select **Apply**.

Result

The user can now access those workspaces from BlueXP, as long as the Connector was also associated with the workspaces.

Create and manage service accounts

A service account acts as a "user" that can make authorized API calls to BlueXP for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time.

You give permissions to a service account by assigning it a role, just like any other BlueXP user. You can also associate the service account with specific workspaces in order to control the working environments (resources) that the service can access.

When you create the service account, BlueXP enables you to copy or download a client ID and client secret for the service account. This key pair is used for authentication with BlueXP.

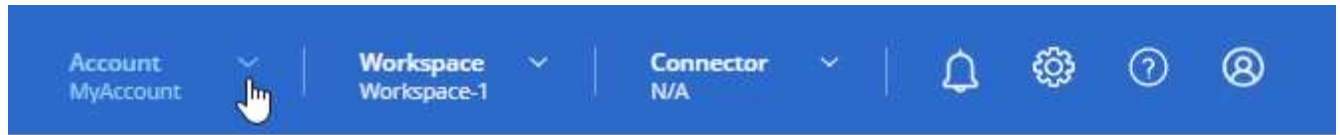
Note that a refresh token is not required for API operations when using a service account. [Learn about refresh tokens](#)

Create a service account

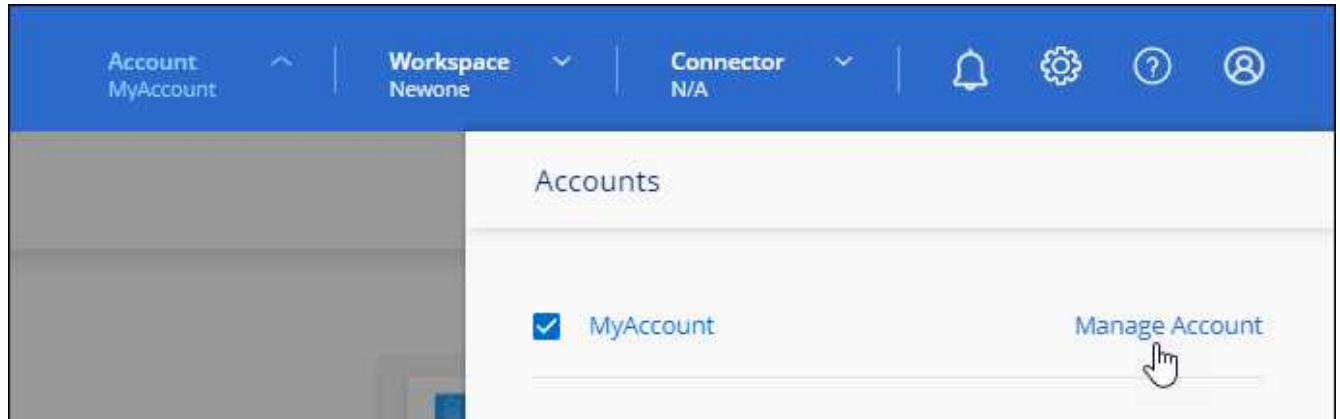
Create as many service accounts as you need to manage the resources in your working environments.

Steps

1. From the top of BlueXP, select the **Account** drop-down.



2. Select **Manage Account** next to the currently selected account.



3. From the Members tab, select **Create Service Account**.
4. Enter a name and select a role. If you chose a role other than Account Admin, choose the workspace to associate with this service account.
5. Select **Create**.
6. Copy or download the client ID and client secret.

The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.

7. Select **Close**.

Obtain a bearer token for a service account

In order to make API calls to the [Tenancy API](#), you'll need to obtain a bearer token for a service account.

[Learn how to create a service account token](#)

Copy the client ID

You can copy a service account's client ID at any time.

Steps

1. From the Members tab, select the action menu in the row that corresponds to the service account.



2. Select **Client ID**.
3. The ID is copied to your clipboard.

Recreate keys

Recreating the key will delete the existing key for this service account and then create a new key. You won't be able to use the previous key.

Steps

1. From the Members tab, select the action menu in the row that corresponds to the service account.



2. Select **Recreate Key**.
3. Select **Recreate** to confirm.
4. Copy or download the client ID and client secret.

The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.

5. Select **Close**.

Delete a service account

Delete a service account if you no longer need to use it.

Steps

1. From the Members tab, select the action menu in the row that corresponds to the service account.



2. Select **Delete**.
3. Select **Delete** again to confirm.

Manage workspaces

Manage your workspaces by creating, renaming, and deleting them. Note that you can't delete a workspace if it contains any resources. It must be empty.

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.
2. Select **Workspaces**.
3. Choose one of the following options:
 - Select **Add New Workspace** to create a new workspace.
 - Select **Rename** to rename the workspace.
 - Select **Delete** to delete the workspace.

If you created a new workspace, you must also add the Connector to that workspace. If you don't add the Connector, then Workspace Admins can't access any of the resources in the workspace. Refer to the following section for more details.

Manage a Connector's workspaces

You need to associate the Connector with workspaces so Workspace Admins can access those workspaces from BlueXP.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in BlueXP by default.

[Learn more about users, workspaces, and Connectors.](#)

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.
2. Select **Connector**.
3. Select **Manage Workspaces** for the Connector that you want to associate.
4. Select the workspaces to associate with the Connector and select **Apply**.

Change your account name

Change your account name at any time to change it to something meaningful for you.

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.
2. In the **Overview** tab, select the edit icon next to the account name.
3. Type a new account name and select **Save**.

Allow private previews

Allow private previews in your account to get access to new services that are made available as a preview in BlueXP.

Services in private preview are not guaranteed to behave as expected and might sustain outages and be missing functionality.

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.
2. In the **Overview** tab, enable the **Allow Private Preview** setting.

Allow third-party services

Allow third-party services in your account to get access to third-party services that are available in BlueXP. Third-party services are cloud services similar to the services that NetApp offers, but they're managed and supported by third-party companies.

Steps

1. From the top of BlueXP, select the **Account** drop-down and select **Manage Account**.
2. In the **Overview** tab, enable the **Allow Third Party Services** setting.

Create another BlueXP account

When you set up BlueXP in restricted mode or private mode, you're prompted to create a *BlueXP account*, which enables you to manage users and organize resources. This account might be all that you need, but if your business requires multiple accounts, then you'll need to create additional accounts by using the Tenancy API.

If you're using BlueXP in standard mode, you won't have a BlueXP account. Instead, you'll have an organization that you manage using BlueXP identity and access management (IAM). [Learn about BlueXP IAM](#).

Steps

1. Use the following API call to create an additional BlueXP account:

```
POST /tenancy/account/{accountName}
```

If you want to enable restricted mode, you need to include the following in the request body:

```
{
  "isSaasDisabled": true
}
```



You can't change the restricted mode setting after BlueXP creates the account. You can't enable restricted mode later and you can't disable it later. It must be set at time of account creation.

[Learn how to use this API call](#)

Related information

- [Learn about BlueXP accounts](#)
- [Learn about BlueXP deployment modes](#)

User roles

When you use BlueXP in restricted mode or private mode, you'll use a *BlueXP account* to manage users. You can provide specific permissions to users in your account by selecting from the following roles: Account Admin, Workspace Admin, Compliance Viewer, and SnapCenter Admin.

If you're using BlueXP in standard mode, you won't have a BlueXP account. Instead, you'll have a *BlueXP organization* that you manage using BlueXP identity and access management (IAM).

- [Learn about BlueXP IAM](#)
- [Learn about BlueXP deployment modes](#)

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
Create Connectors	Yes	No	No	No
Manage working environments	Yes	Yes	No	Yes
Enable services on working environments	Yes	Yes	No	Yes
Use BlueXP services	Yes	Yes	No	Yes
Remove working environments from a workspace	Yes	Yes	No	No
Delete working environments	Yes	Yes	No	No
View data replication status	Yes	Yes	No	No
View the timeline	Yes	Yes	No	No
Switch between workspaces	Yes	Yes	Yes	Yes
View BlueXP classification scan results	Yes	Yes	Yes	No
Receive the Cloud Volumes ONTAP report	Yes	No	No	No

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
Manage BlueXP accounts	Yes	No	No	No
Manage credentials	Yes	Yes	No	No
Modify BlueXP settings	Yes	Yes	No	No
View and manage the Support Dashboard	Yes	Yes	No	No

Related link

[Manage your BlueXP account](#)

Enable single sign-on by using identity federation with BlueXP

Identity federation enables single sign-on with BlueXP so that users can log in using credentials from your corporate identity. To get started, learn how identity federation works with BlueXP and then review an overview of the setup process.

Identity federation with NSS credentials

If you use your NetApp Support Site (NSS) credentials to log in to BlueXP, you should not follow the instructions on this page to set up identity federation. You should do the following instead:

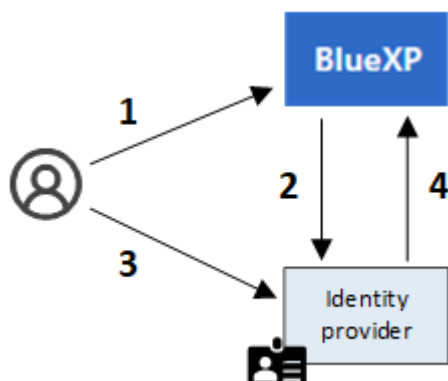
- Download and complete the [NetApp Federation Request Form](#)
- Submit the form to the email address specified in the form

The NetApp Identity and Access Management team will review your request.

How identity federation works

Setting up identity federation creates a trust connection between BlueXP's authentication service provider (auth0) and your own identity management provider.

The following image depicts how identity federation works with BlueXP:



1. A user enters their email address on the BlueXP login page.
2. BlueXP identifies that the email domain is part of a federated connection and sends the authentication request to the identity provider using the trusted connection.

When you set up a federated connection, BlueXP always uses that federated connection for authentication.

3. The user authenticates by using credentials from your corporate directory.
4. Your identity provider authenticates the user's identity and the user is logged in to BlueXP.

Identity federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML) and OpenID Connect (OIDC).

Supported identity providers

BlueXP supports the following identity providers:

- Security Assertion Markup Language (SAML) identity providers
- Microsoft Entra ID
- Active Directory Federation Services (ADFS)
- PingFederate

BlueXP supports service provider initiated (SP-initiated) SSO only. Identity provider initiated (IdP-initiated) SSO is not supported.



Overview of the setup process

Before you set up a connection between BlueXP and your identity management provider, you should understand the steps that you'll need to take so that you can prepare accordingly.

These steps are specific to users who log in to BlueXP using a NetApp cloud login. If you use your NSS credentials to log in to BlueXP, [learn how to set up identity federation with NSS credentials](#).



SAML identity provider

At a high-level, setting up a federated connection between BlueXP and a SAML identity provider includes the following steps:

Step	Completed by	Description
1	Active Directory (AD) admin	<p>Configure your SAML identity provider to enable identity federation with BlueXP.</p> <p>View instructions for your SAML identity provider:</p> <ul style="list-style-type: none"> • ADFS • Okta • OneLogin • PingFederate • SalesForce • SiteMinder • SSOCircle <p>If your identity provider doesn't appear in the list above, follow these generic instructions</p> <div>  <p>Do <i>not</i> complete the steps that describe how to create a connection in auth0. You'll create that connection in the next step.</p> </div>
2	BlueXP admin	<p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin about the identity provider:</p> <ul style="list-style-type: none"> • Sign in URL • An X509 signing certificate (PEM or CER format) • Sign out URL (optional) <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> <div>  <p>Take note of the certificate expiration date. You need to return to the Federation Setup page and update the certificate <i>before</i> it expires. This is your responsibility. BlueXP does not track the expiration date. It's best to work with your AD team to get alerted on time.</p> </div>
3	AD admin	Complete the configuration on the identity provider using the parameters shown on the Federation Setup page after finishing step 2.
4	BlueXP admin	<p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p>

Microsoft Entra ID


At a high-level, setting up a federated connection between BlueXP and Microsoft Entra ID includes the following steps:

Step	Completed by	Description
1	AD admin	<p>Configure Microsoft Entra ID to enable identity federation with BlueXP.</p> <p>View instructions for registering the application with Microsoft Entra ID</p> <div><p>Do <i>not</i> complete the steps that describe how to create a connection in auth0. You'll create that connection in the next step.</p></div>
2	BlueXP admin	<p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin:</p> <ul style="list-style-type: none">• Client ID• Client secret value• Microsoft Entra ID domain <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> <div><p>Take note of the secret key expiration date. You need to return to the Federation Setup page and update the certificate <i>before</i> it expires. This is your responsibility. BlueXP does not track the expiration date. It's best to work with your AD team to get alerted on time.</p></div>
3	AD admin	<p>Complete the configuration in Microsoft Entra ID using the parameters shown on the Federation Setup page after finishing step 2.</p>
4	BlueXP admin	<p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p>

ADFS


At a high-level, setting up a federated connection between BlueXP and ADFS includes the following steps:


Step	Completed by	Description
1	AD admin	<p>Configure the ADFS server to enable identity federation with BlueXP.</p> <p>View instructions for configuring the ADFS server with auth0</p>

Step	Completed by	Description
2	BlueXP admin	<p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin: the URL for the ADFS server or the federation metadata file.</p> <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> <div>  <p>Take note of the certificate expiration date. You need to return to the Federation Setup page and update the certificate <i>before</i> it expires. This is your responsibility. BlueXP does not track the expiration date. It's best to work with your AD team to get alerted on time.</p> </div>
3	AD admin	Complete the configuration on the ADFS server using the parameters shown on the Federation Setup page after finishing step 2.
4	BlueXP admin	<p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p>

PingFederate

At a high-level, setting up a federated connection between BlueXP and a PingFederate server includes the following steps:

Step	Completed by	Description
1	AD admin	<p>Configure your PingFederate server to enable identity federation with BlueXP.</p> <p>View instructions for creating a connection</p> <div>  <p>Do <i>not</i> complete the steps that describe how to create a connection in auth0. You'll create that connection in the next step.</p> </div>

Step	Completed by	Description
2	BlueXP admin	<p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin:</p> <ul style="list-style-type: none"> • The URL for the PingFederate server • An X509 signing certificate (PEM or CER format) <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> <div>  <p>Take note of the certificate expiration date. You need to return to the Federation Setup page and update the certificate <i>before</i> it expires. This is your responsibility. BlueXP does not track the expiration date. It's best to work with your AD team to get alerted on time.</p> </div>
3	AD admin	Complete the configuration on the PingFederate server using the parameters shown on the Federation Setup page after finishing step 2.
4	BlueXP admin	<p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p>

Updating a federated connection

After the BlueXP admin enables a connection, the admin can update the connection at any time from the [NetApp Federation Setup page](#)

For example, you might need to update the connection by uploading a new certificate.

The BlueXP admin who created the connection is the only authorized user who can update the connection. If you'd like to add additional admins, contact NetApp Support.

Connectors

Maintain the Connector VM and operating system

Maintaining the operating system on the Connector host is your responsibility. For example, you 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

You don't need to stop any services on the Connector host when applying OS security patches.

VM or instance type

If you created a Connector directly from BlueXP, BlueXP deployed a virtual machine instance in your cloud provider using a default configuration. After you create the Connector, you should not change to a smaller VM instance that has less CPU or RAM.

The CPU and RAM requirements are as follows:

CPU

8 cores or 8 vCPUs

RAM

32 GB

[Learn about the default configuration for the Connector.](#)

Stopping the starting the Connector VM

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

[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, you can do so by using the connectivity options available from your cloud provider.

AWS

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](#)

Azure

When you created the Connector VM in Azure, you specified a user name and chose 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

If it's required for your business, you can change the internal IP address and public IP address of the Connector instance that is automatically assigned by your cloud provider.

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. If you changed the public IP address and you need to connect to the local user interface running on the Connector, restart the Connector instance to register the new 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.

You'll need to 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

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

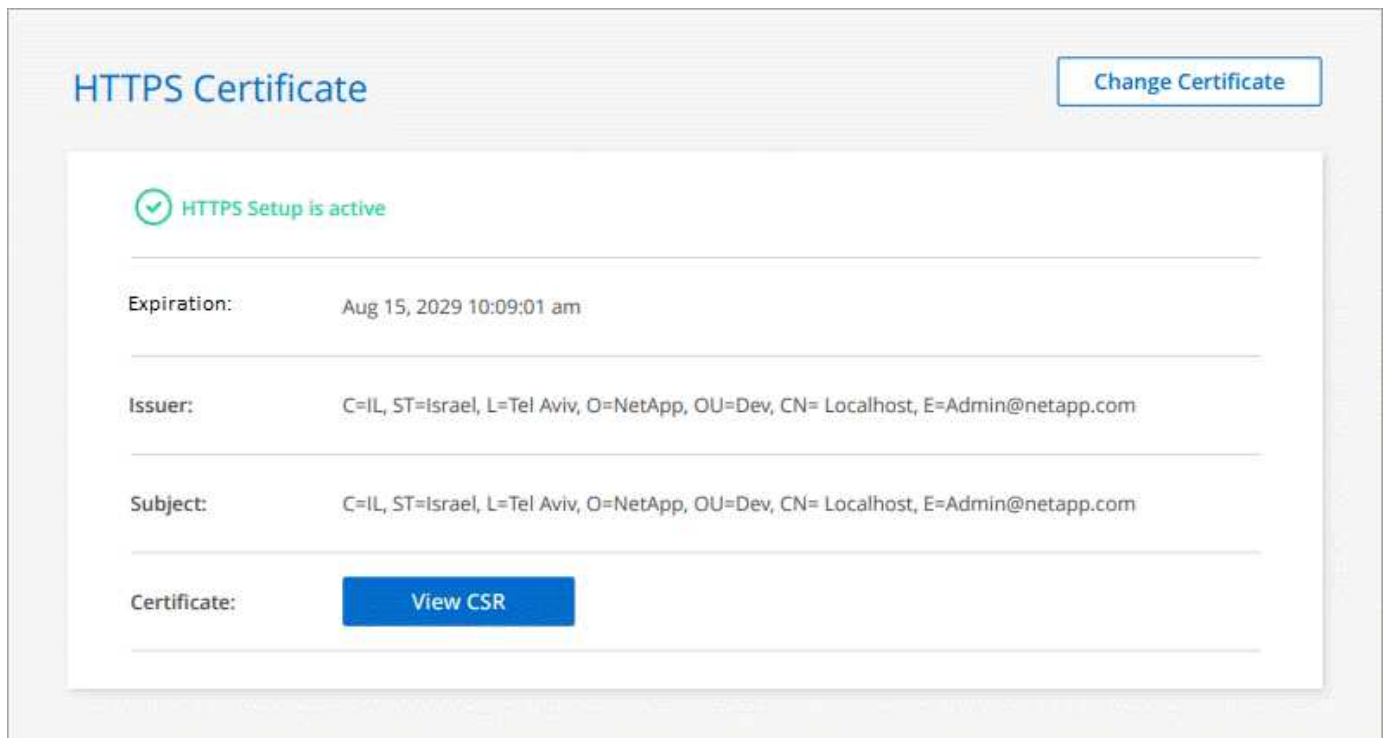


2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

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

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:



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.

Configuring the Connector to use a proxy server provides outbound internet access if a public IP address or a NAT gateway isn't available. This proxy server provides only the Connector with an outbound connection. It doesn't provide any connectivity for Cloud Volumes ONTAP systems.

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those Cloud Volumes ONTAP systems to use a proxy server that's included

with the Connector. The only requirement is to ensure that the Connector's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Connector.

Supported configurations

- BlueXP supports HTTP and HTTPS.
- The proxy server can be in the cloud or in your network.
- BlueXP does not support transparent proxy servers.

Enable a 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.

Note that this operation restarts the Connector. Ensure that the Connector isn't performing any operations before you proceed.

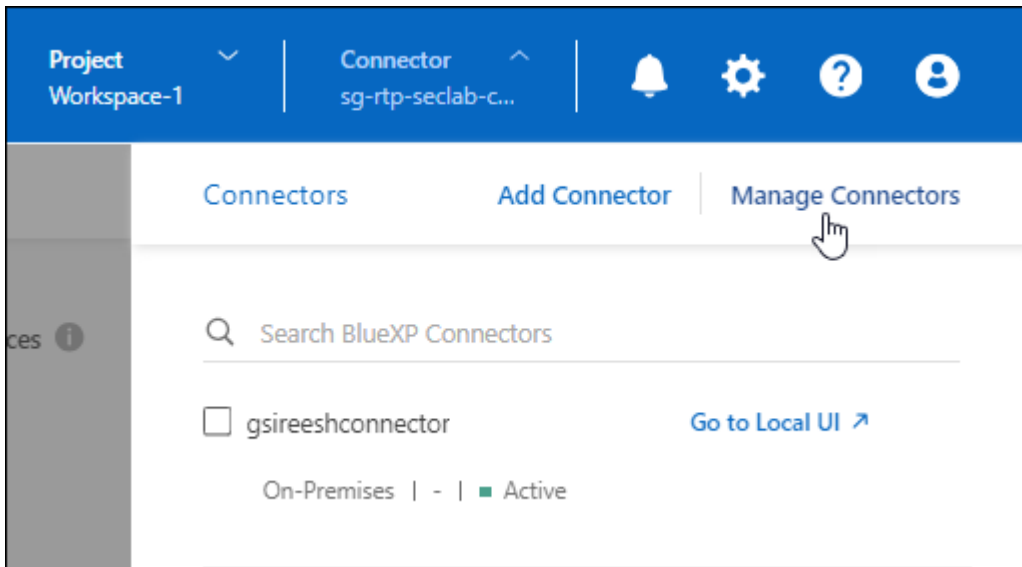
Steps

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

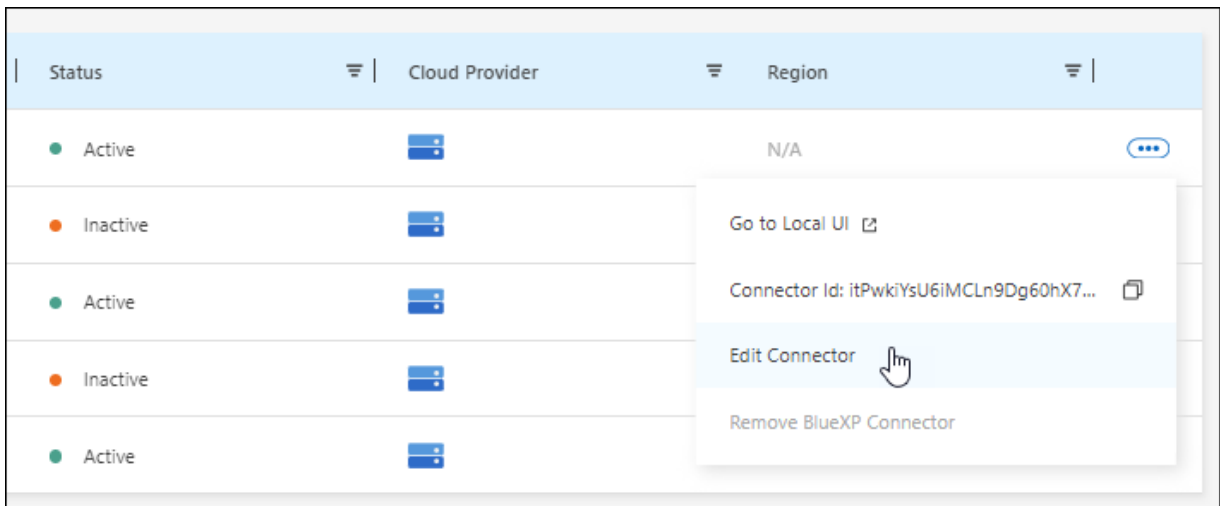
How you navigate depends on whether you're using BlueXP in standard mode (accessing the BlueXP interface from the SaaS website) or using BlueXP in restricted mode or private mode (accessing the BlueXP interface locally from the Connector host).

Standard mode

- Select the **Connector** drop-down from the BlueXP header.
- Select **Manage Connectors**.

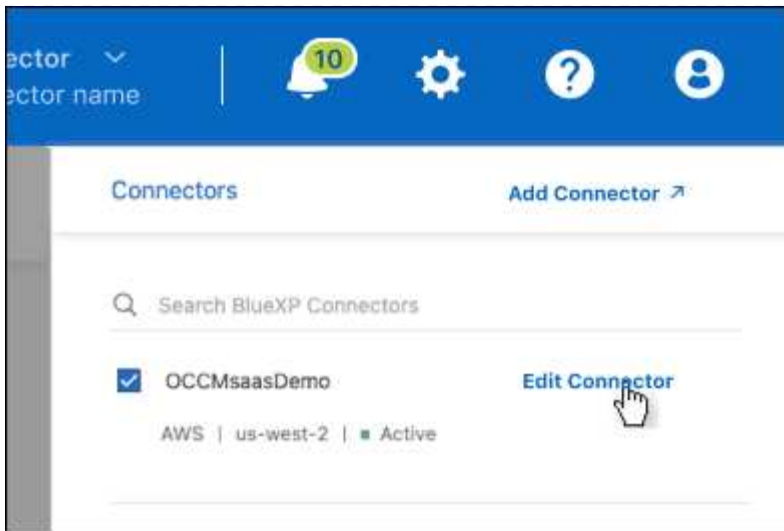


- Select the action menu for a Connector and select **Edit Connector**.



Restricted or private mode

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



2. Select **HTTP Proxy Configuration**.
3. Set up the proxy:
 - a. Select **Enable Proxy**.
 - b. Specify the server using the syntax `http://address:port` or `https://address:port`
 - c. 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.

- d. Select **Save**.

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. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

If you disabled the use of Azure Private Links with Cloud Volumes ONTAP and are using service endpoints instead, then you must 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](#)

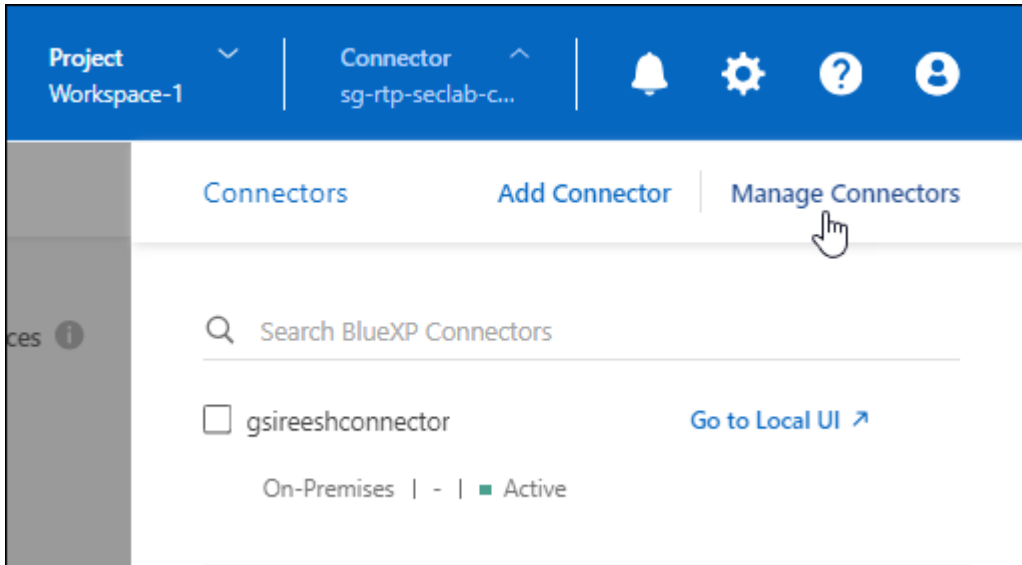
Steps

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

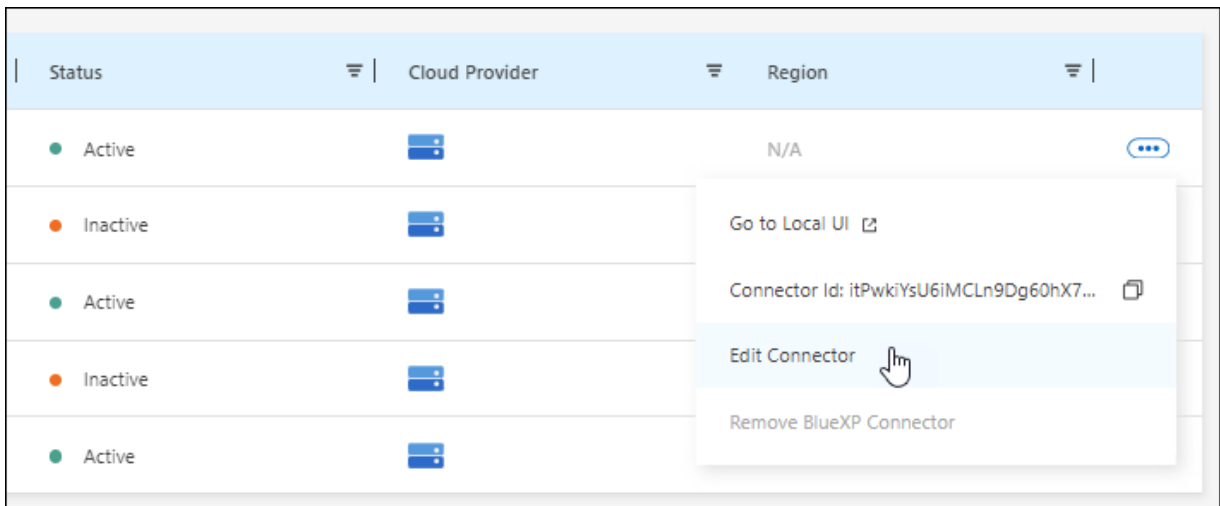
How you navigate depends on whether you're using BlueXP in standard mode (accessing the BlueXP interface from the SaaS website) or using BlueXP in restricted mode or private mode (accessing the BlueXP interface locally from the Connector host).

Standard mode

- Select the **Connector** drop-down from the BlueXP header.
- Select **Manage Connectors**.

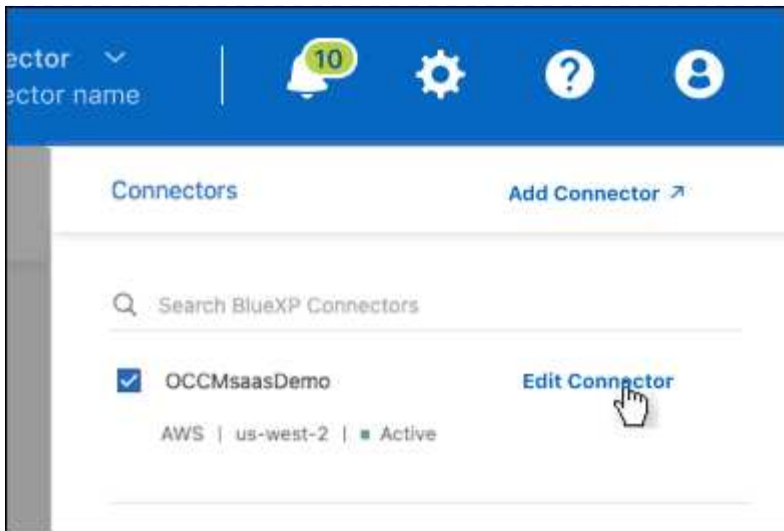


- Select the action menu for a Connector and select **Edit Connector**.



Restricted or private mode

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

Upgrade a Connector when using private mode

If you are using BlueXP in private mode, you can upgrade the Connector when a newer version is available from the NetApp Support Site.



When you use BlueXP in standard mode or restricted mode, you don't need to manually upgrade the Connector. BlueXP automatically upgrades a Connector to the latest release, as long as the Connector has outbound internet access to obtain the software update.

About this task

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.

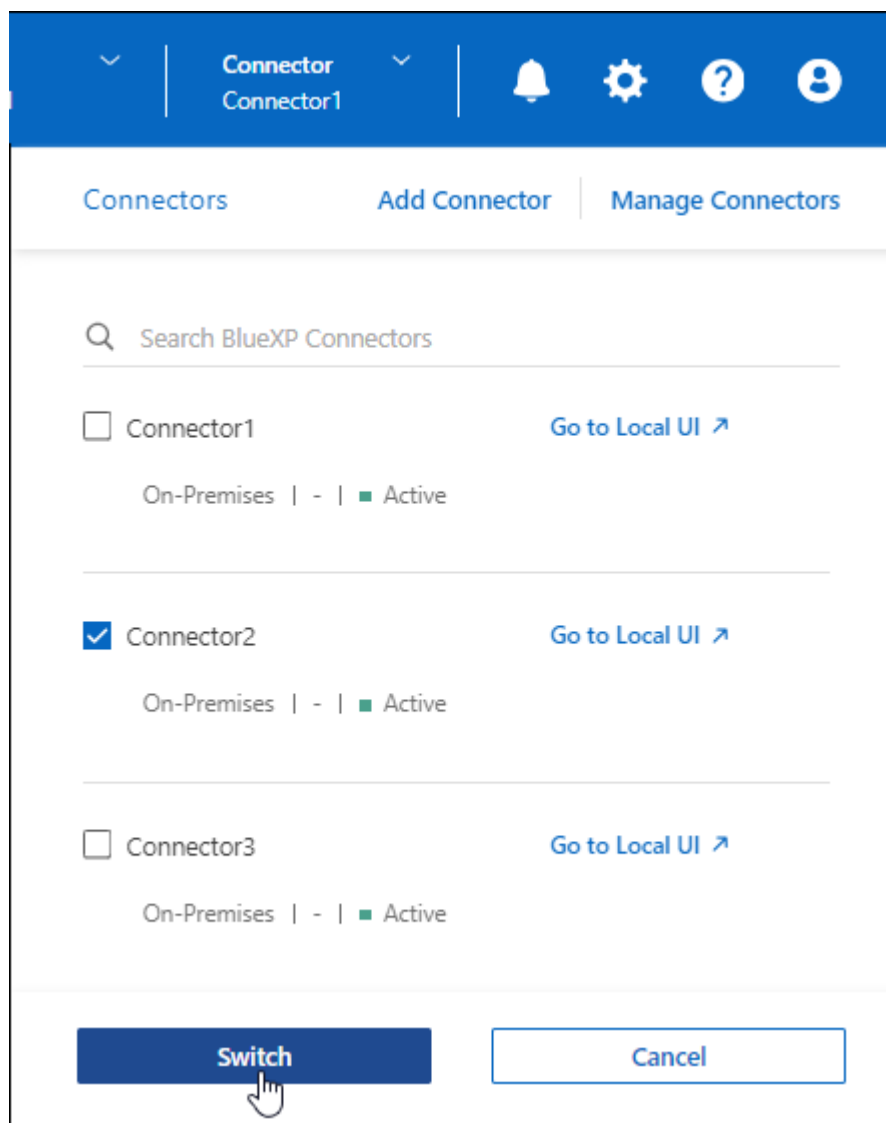
Switch between Connectors

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**.



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 link

[Get help from NetApp Support.](#)

Find the system ID for a Connector

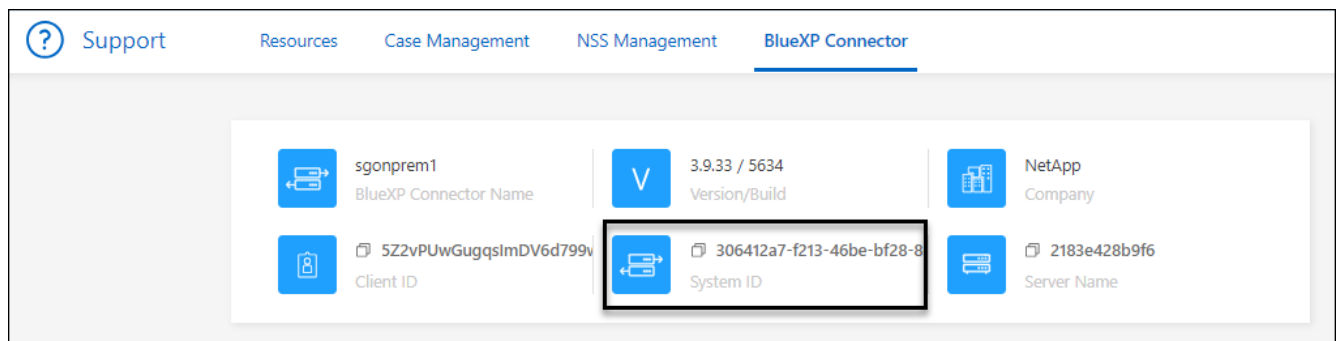
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

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



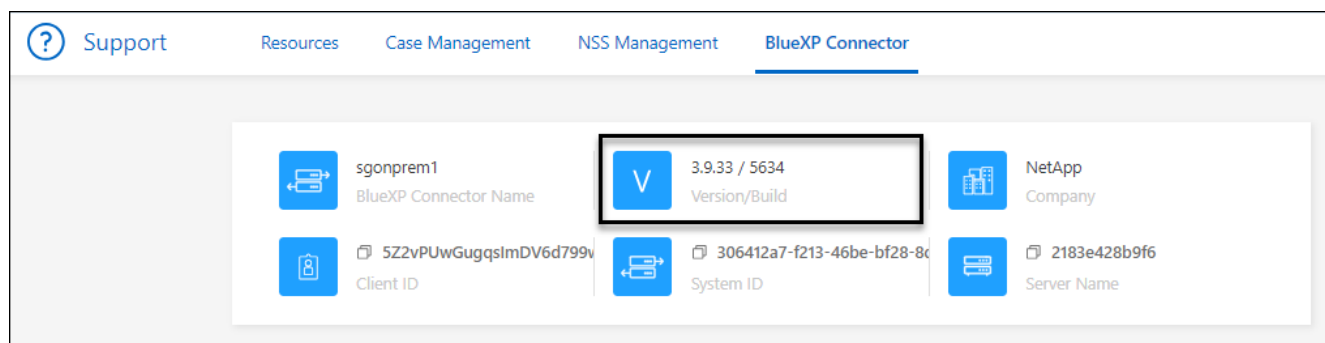
View a Connector's version

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.

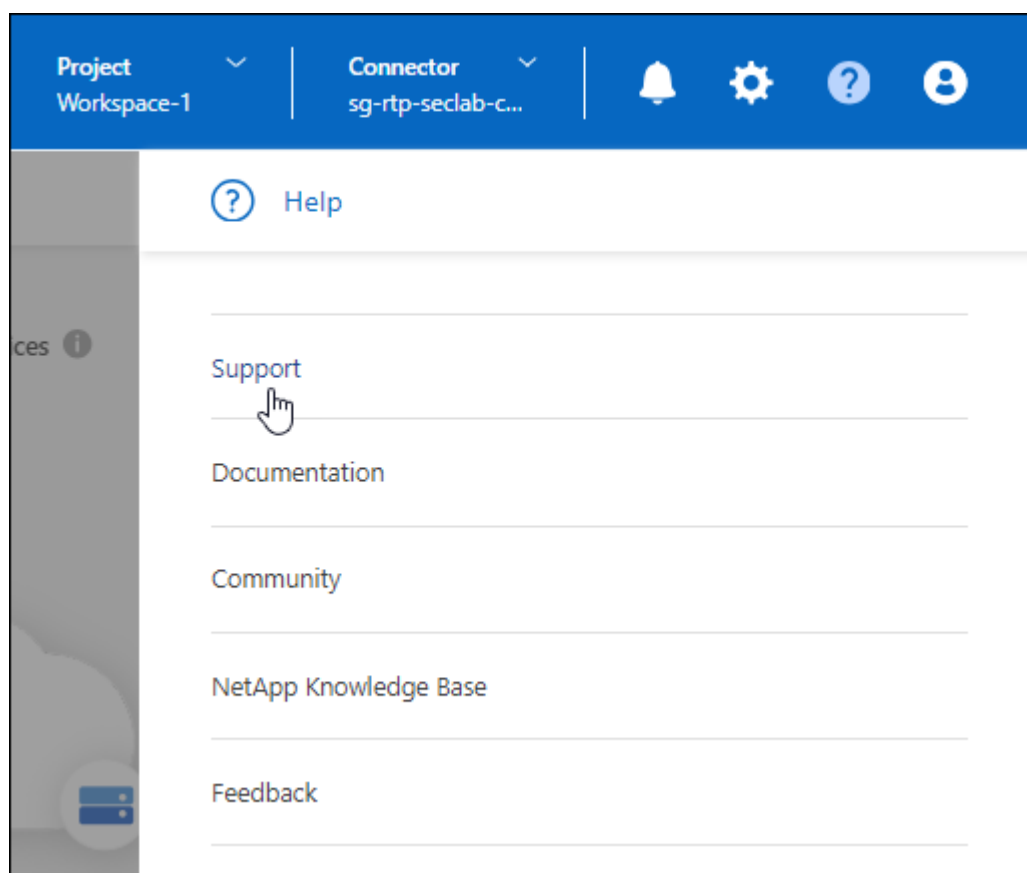


Download or send an AutoSupport message

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

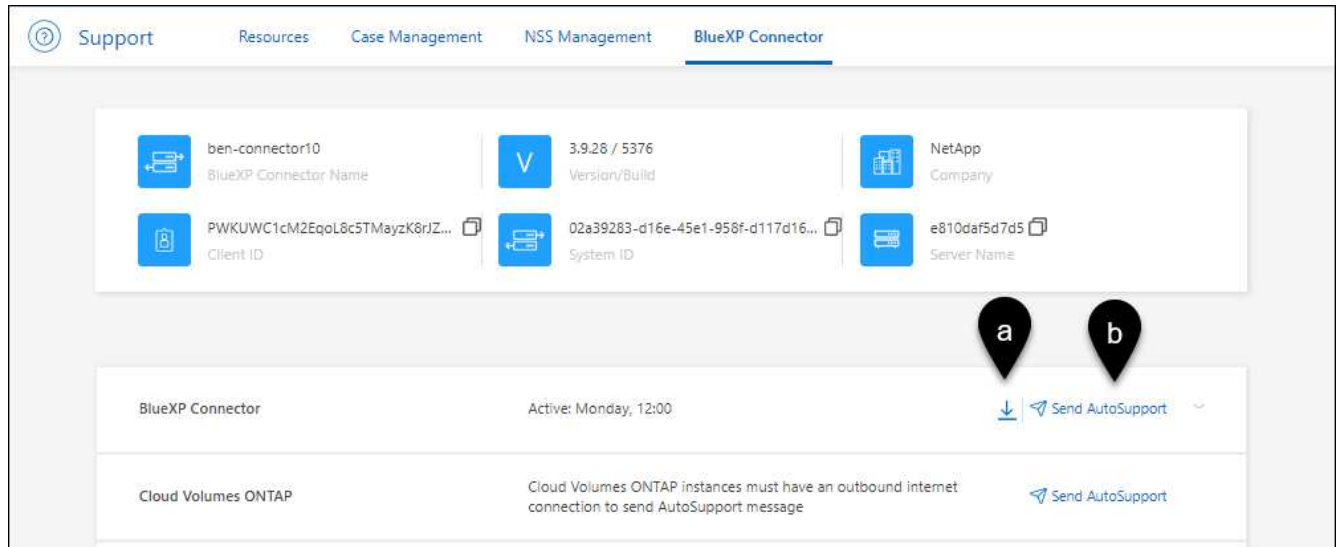
Steps

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.



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 BlueXP in 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.

Result

The Connector software is now uninstalled from the Linux host.

Uninstall the Connector when using private mode

If you're using BlueXP in private mode (in other words, the Connector host has *no* outbound connectivity), then you should 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/ds
```

Result

The Connector software is now uninstalled from the Linux host.

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 deleted the Connector virtual machine or if you uninstalled 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 from BlueXP, 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**.



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

Result

BlueXP removes the Connector from its records.

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

Credentials and subscriptions

AWS

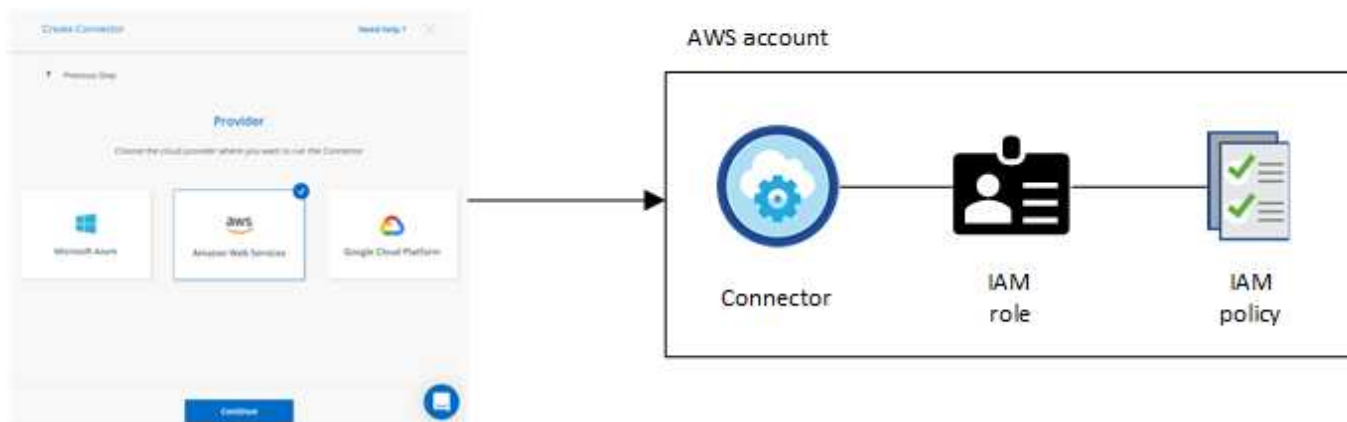
Learn about AWS credentials and permissions

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		QA Subscription	Edit Credentials
Credentials	Account ID	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

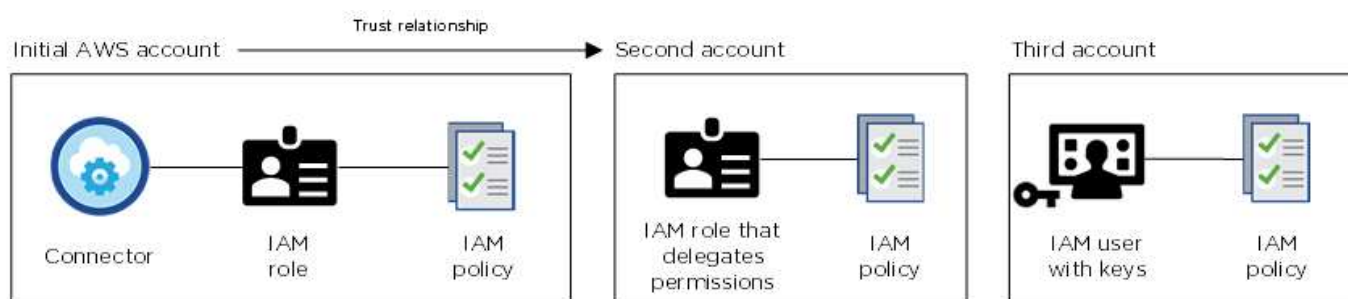
There are two ways to add additional AWS credentials:

- You can add AWS credentials to an existing Connector
- You can add AWS credentials directly to BlueXP

Review the sections below for more details.

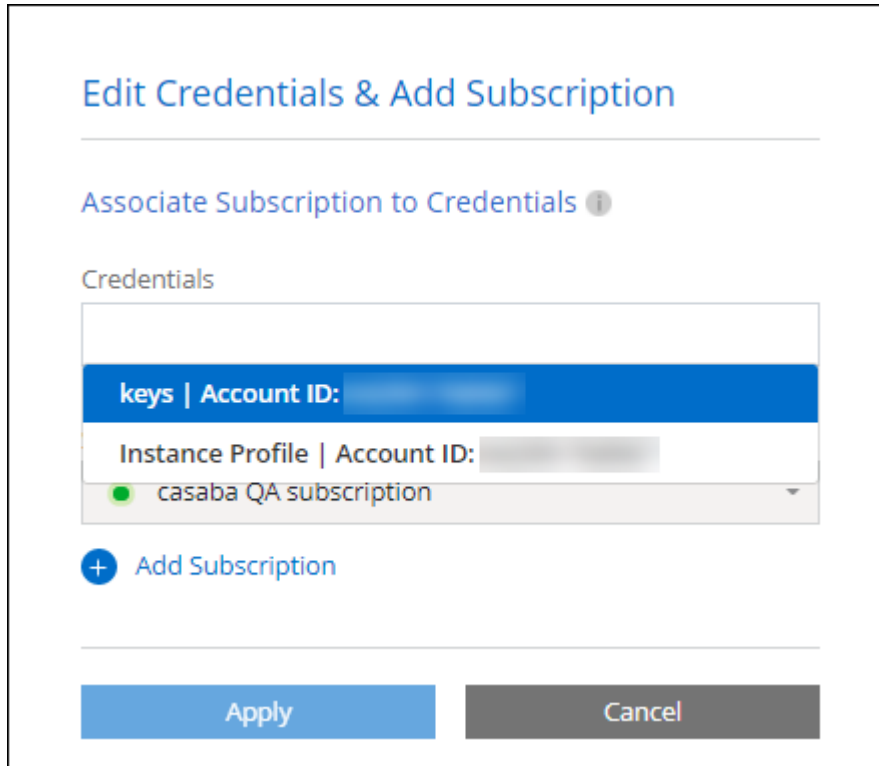
Add AWS credentials to an existing Connector

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

+ Add Subscription

Apply

Cancel

[Learn how to add AWS credentials to an existing Connector.](#)

Add AWS credentials directly to BlueXP

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

- [Learn how to add AWS credentials to BlueXP for Amazon FSx for ONTAP](#)
- [Learn how to add AWS credentials to BlueXP for creating a Connector](#)

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-prem deployments?

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-prem deployments](#)

- [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 BlueXP has the permissions that it needs to deploy and manage cloud resources in your AWS accounts. 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

Adding AWS credentials to an existing Connector provides the permissions needed to manage resources and processes within your public 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

Adding new AWS credentials to BlueXP gives BlueXP the permissions needed 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.

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.

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

Before you add AWS credentials to a Connector, you need to provide the required permissions. The permissions enable BlueXP to manage resources and processes within that AWS account. How you provide

the permissions depends on whether you want to provide BlueXP with 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 initial account is not added if you deployed the Connector from the AWS Marketplace or if you manually installed the Connector software on an existing system. [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 before you add the credentials to BlueXP.

Steps

1. Ensure that the correct Connector is currently selected in BlueXP.
2. In the upper right of the BlueXP 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 BlueXP services at an hourly rate (PAYGO) or with an annual contract, AWS credentials must be associated with an 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 Subscription

Apply Cancel

Add credentials to BlueXP for creating a Connector

Add AWS credentials to BlueXP by providing the ARN of an IAM role that gives BlueXP 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
- 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**.

Result

You can now use the credentials when creating a new Connector.

Add credentials to BlueXP for Amazon FSx for ONTAP

For details, refer to the [BlueXP documentation for Amazon FSx for ONTAP](#)

Associate an AWS subscription

After you add your AWS credentials to BlueXP, you can associate 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 use other BlueXP services.

There are two scenarios in which you might associate an AWS 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 AWS Marketplace subscription that is associated with 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 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 the action menu for a set of credentials and then select **Associate 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 **Associate**.
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**.

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

[Subscribe to BlueXP from the AWS Marketplace](#)

Associate an existing subscription with your organization or account

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



If you're using BlueXP in standard mode, you'll have a *BlueXP organization*, which you manage using BlueXP identity and access management (IAM). But if you're using BlueXP in restricted mode or private mode, then you'll have a *BlueXP account*.

- [Learn about BlueXP deployment modes](#)
- [Learn about BlueXP identity and access management](#)
- [Learn about BlueXP accounts](#)

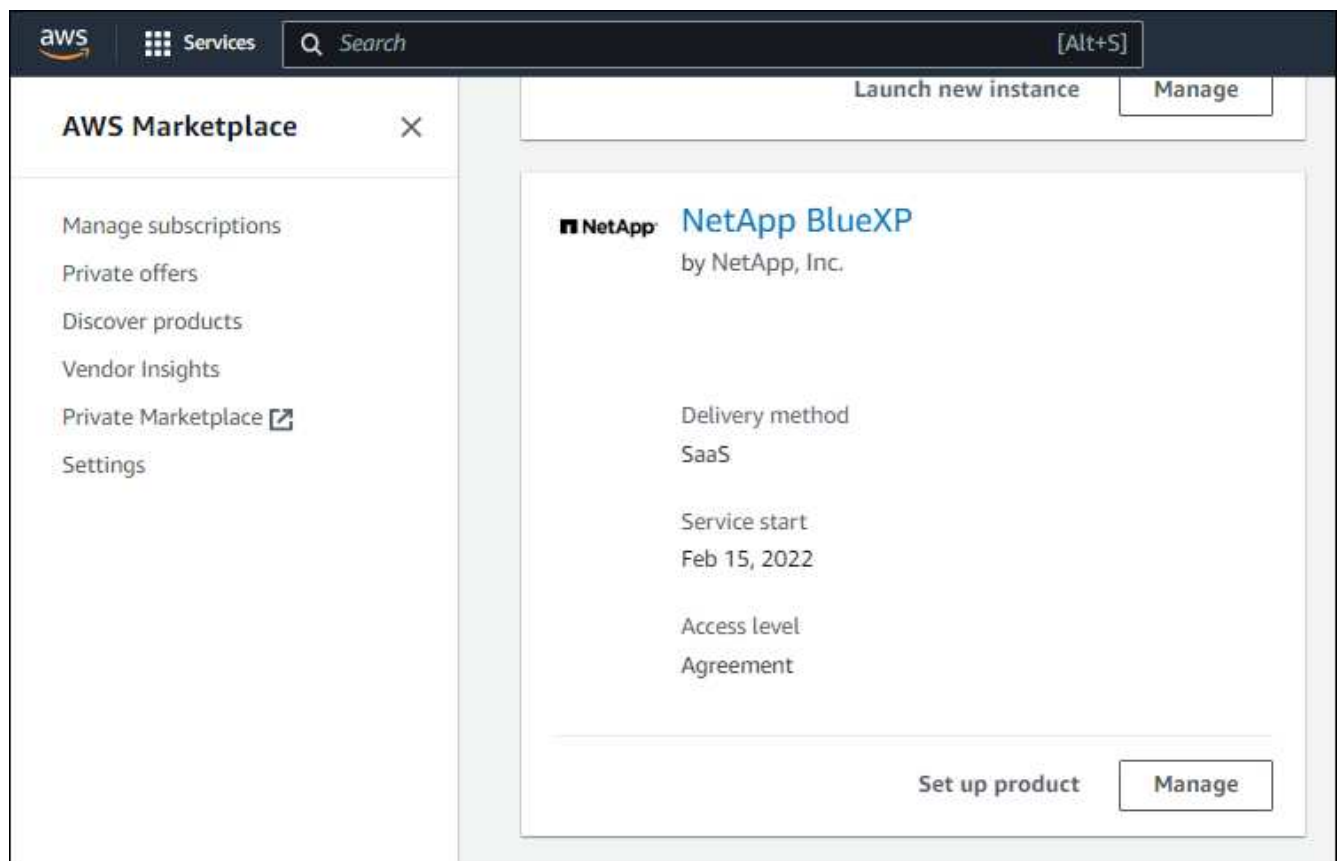
Follow the steps below if you subscribed to BlueXP from the AWS Marketplace, but you missed the step to associate the subscription with your account.

Steps

1. Go to the BlueXP digital wallet to confirm that you didn't associate your subscription with your BlueXP organization or account.
 - a. From the BlueXP navigation menu, select **Governance > Digital wallet**.
 - b. Select **Subscriptions**.
 - c. Verify that your BlueXP 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.

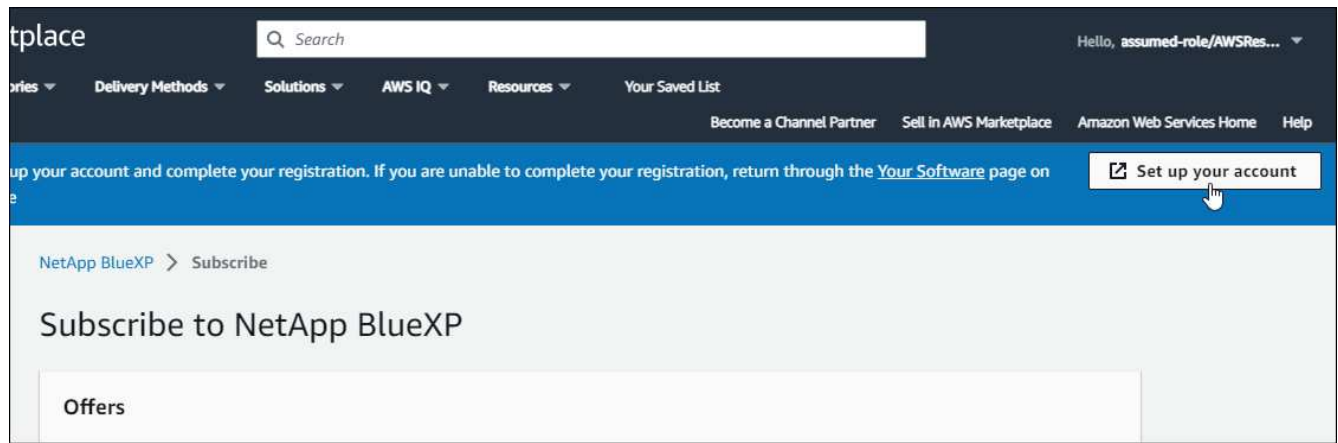
2. Log in to the AWS Console and navigate to **AWS Marketplace Subscriptions**.
3. Find the NetApp BlueXP subscription.



4. Select **Set up product**.

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

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



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

Select the NetApp accounts that you'd like to associate this subscription with.

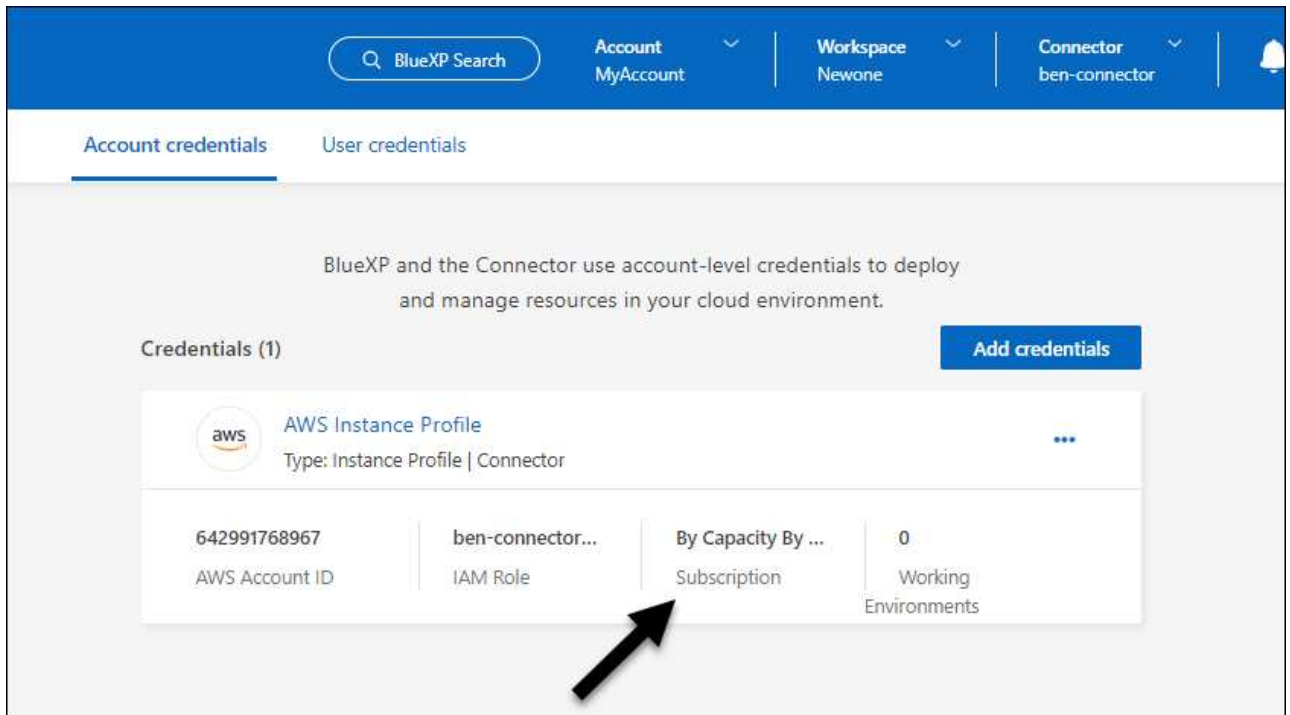
You can automatically replace the existing subscription for one account with this new subscription.

NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

Save

7. Go to the BlueXP digital wallet to confirm that the subscription is associated with your BlueXP organization or account.
 - a. From the BlueXP navigation menu, select **Governance > Digital wallet**.
 - b. Select **Subscriptions**.
 - c. Verify that your BlueXP subscription appears.
8. Confirm that the subscription is associated with your AWS credentials.
 - a. In the upper right of the BlueXP 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.



Edit credentials

Edit your AWS credentials in BlueXP 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.

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.



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 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.

Azure

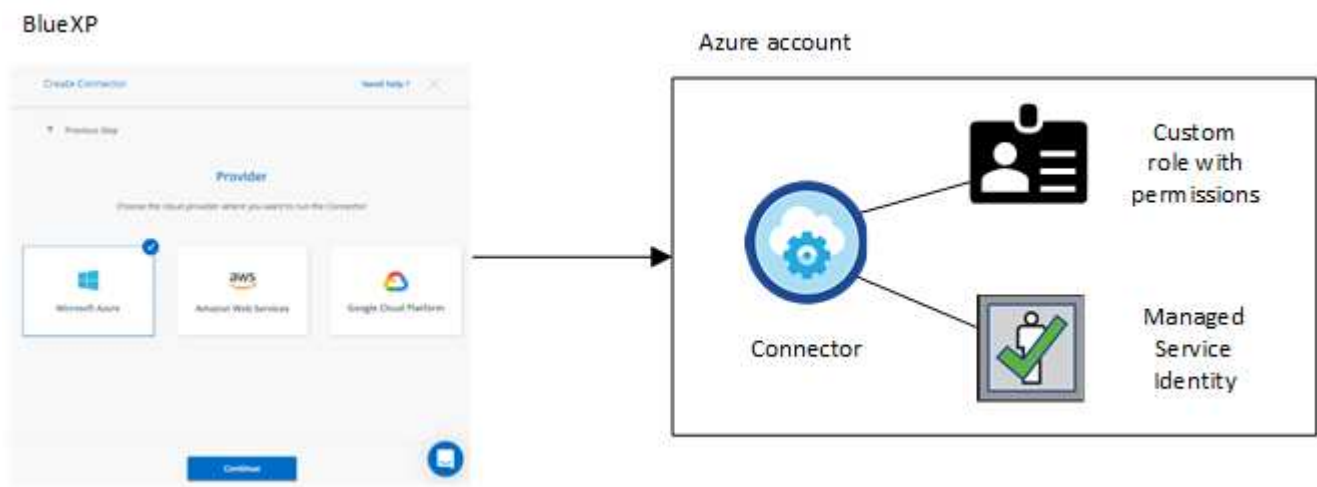
Learn about Azure credentials and permissions

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 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...	OCCM QA1	No subscription is associated	Edit Credentials
Credential Name	Azure Subscription		
	Marketplace Subscription		

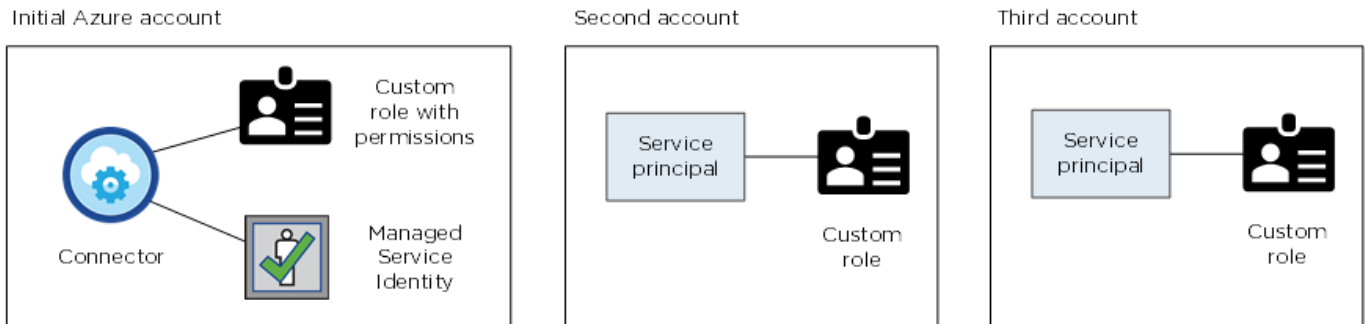
You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

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](#).

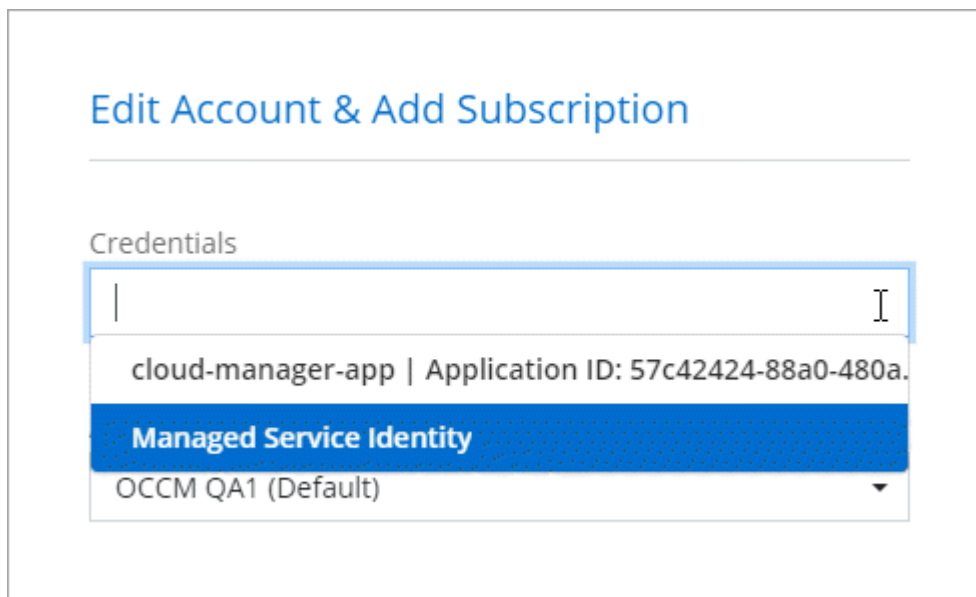
Additional Azure credentials

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:



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-prem deployments?

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-prem deployments](#)
- [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.

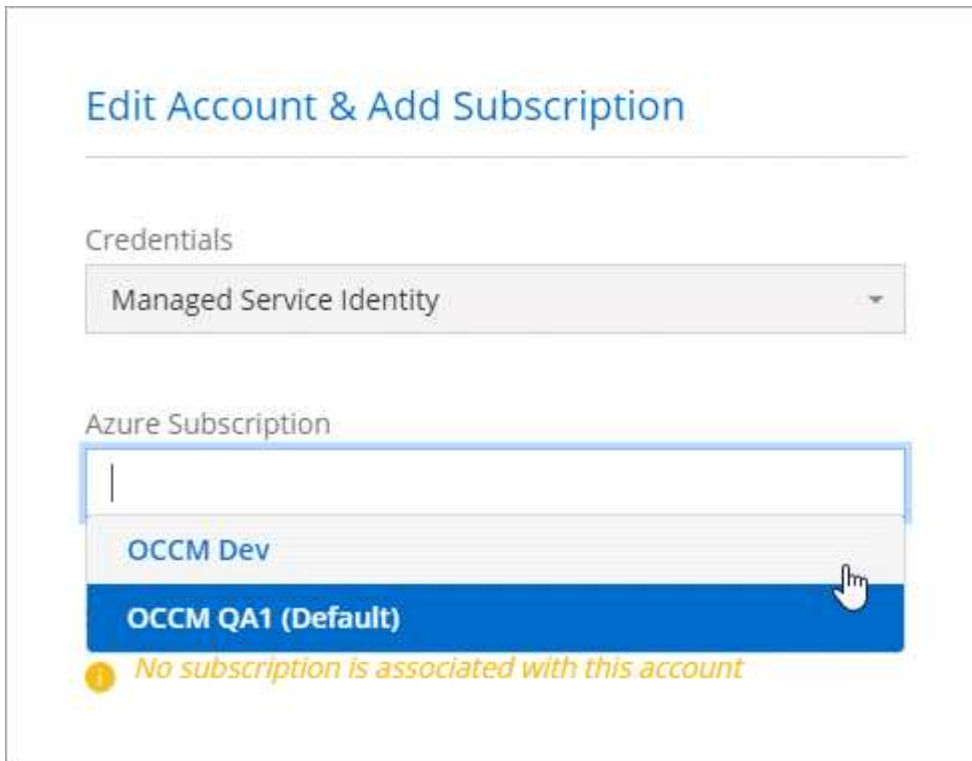


BlueXP Operator is the default name provided in the Connector policy. If you chose a different name for the role, then select that name instead.

- 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

OCCM Dev

OCCM QA1 (Default)

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.



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

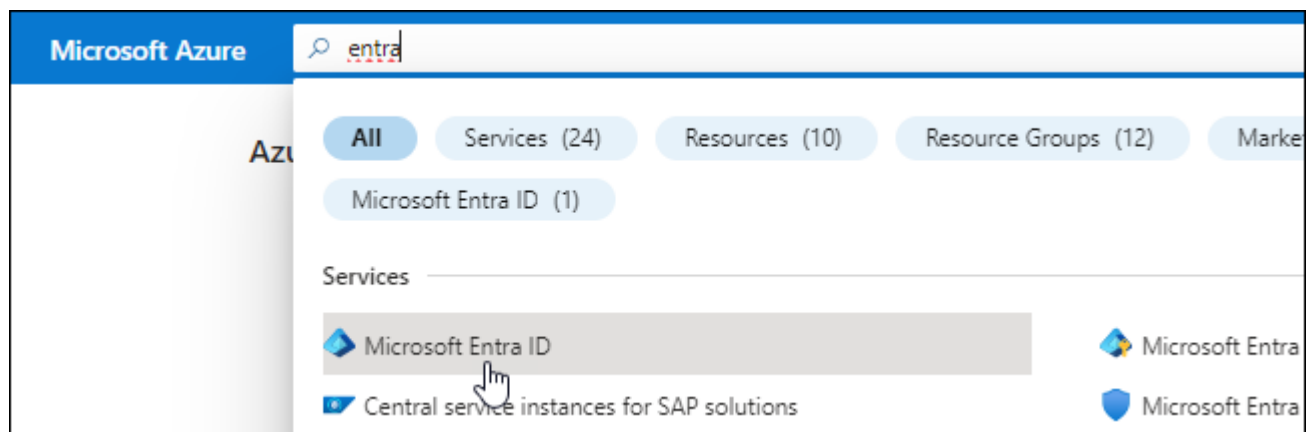
Create a Microsoft Entra application and service principal that BlueXP can use for role-based access control.

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.



- 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**.

Add role assignment ...

[Got feedback?](#)

Role **Members** Review + assign

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 members ✕

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

Microsoft APIs **APIs my organization uses** My APIs

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.

 <p>Azure Batch Schedule large-scale parallel and HPC applications in the cloud</p>	 <p>Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	 <p>Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
 <p>Azure Data Lake Access to storage and compute for big data analytic scenarios</p>	 <p>Azure DevOps Integrate with Azure DevOps and Azure DevOps server</p>	 <p>Azure Import/Export Programmatic control of import/export jobs</p>
 <p>Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	 <p>Azure Rights Management Services Allow validated users to read and write protected content</p>	 <p>Azure Service Management Programmatic access to much of the functionality available through the Azure portal</p>
 <p>Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	 <p>Customer Insights Create profile and interaction models for your products</p>	 <p>Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination</p>

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
<input checked="" type="checkbox"/> user_impersonation 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**.



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.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA

Copy to clipboard

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

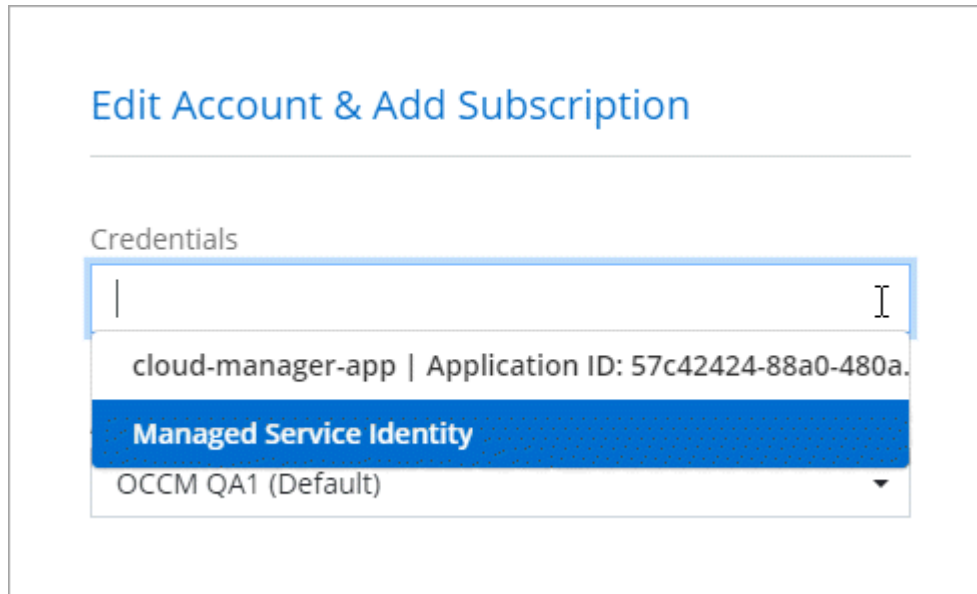
- Client Secret

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](#)



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.

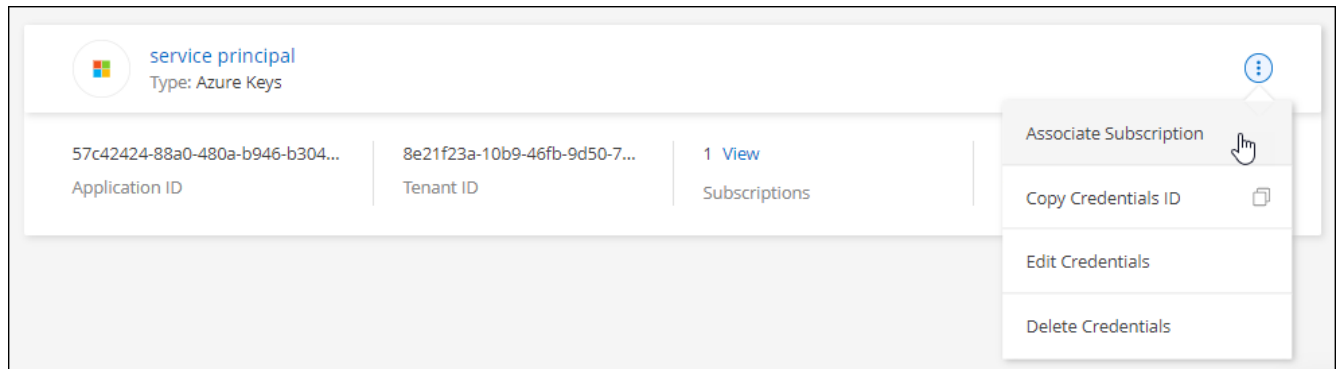
Before you begin

You need to create a Connector before you can change BlueXP settings. [Learn how](#).

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 **Associate 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 **Associate**.
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 the BlueXP website.

- 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 BlueXP 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 BlueXP services.

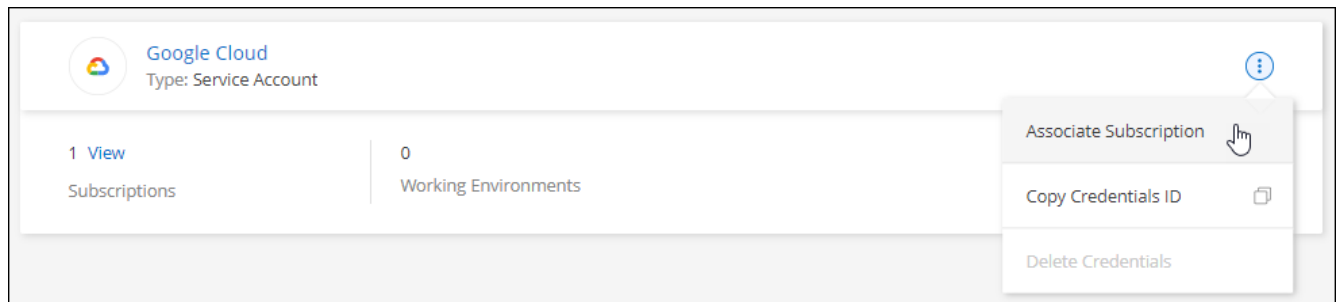
Associate a Marketplace subscription with Google Cloud credentials

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 BlueXP services.

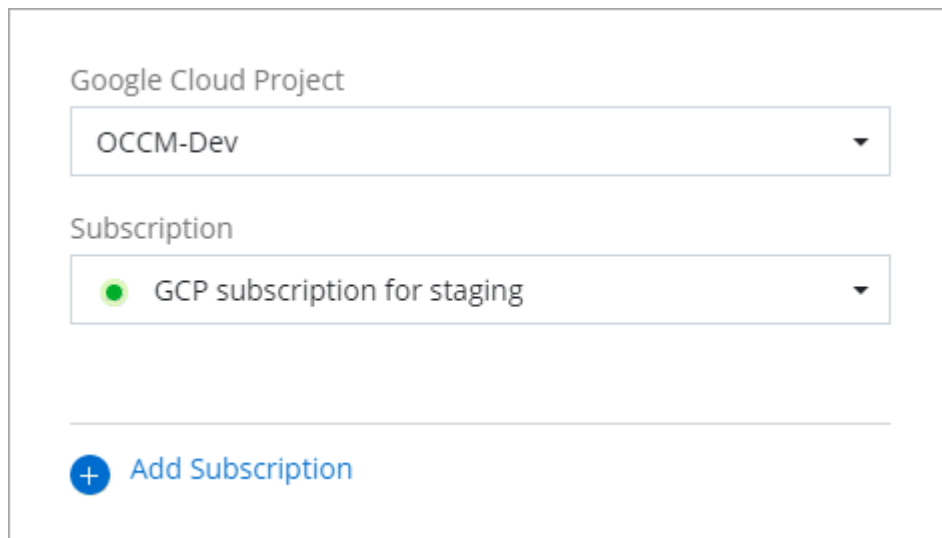
Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

Steps

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



3. To associate the credentials with an existing subscription, select a Google Cloud project and subscription from the down-down list, and then select **Associate**.

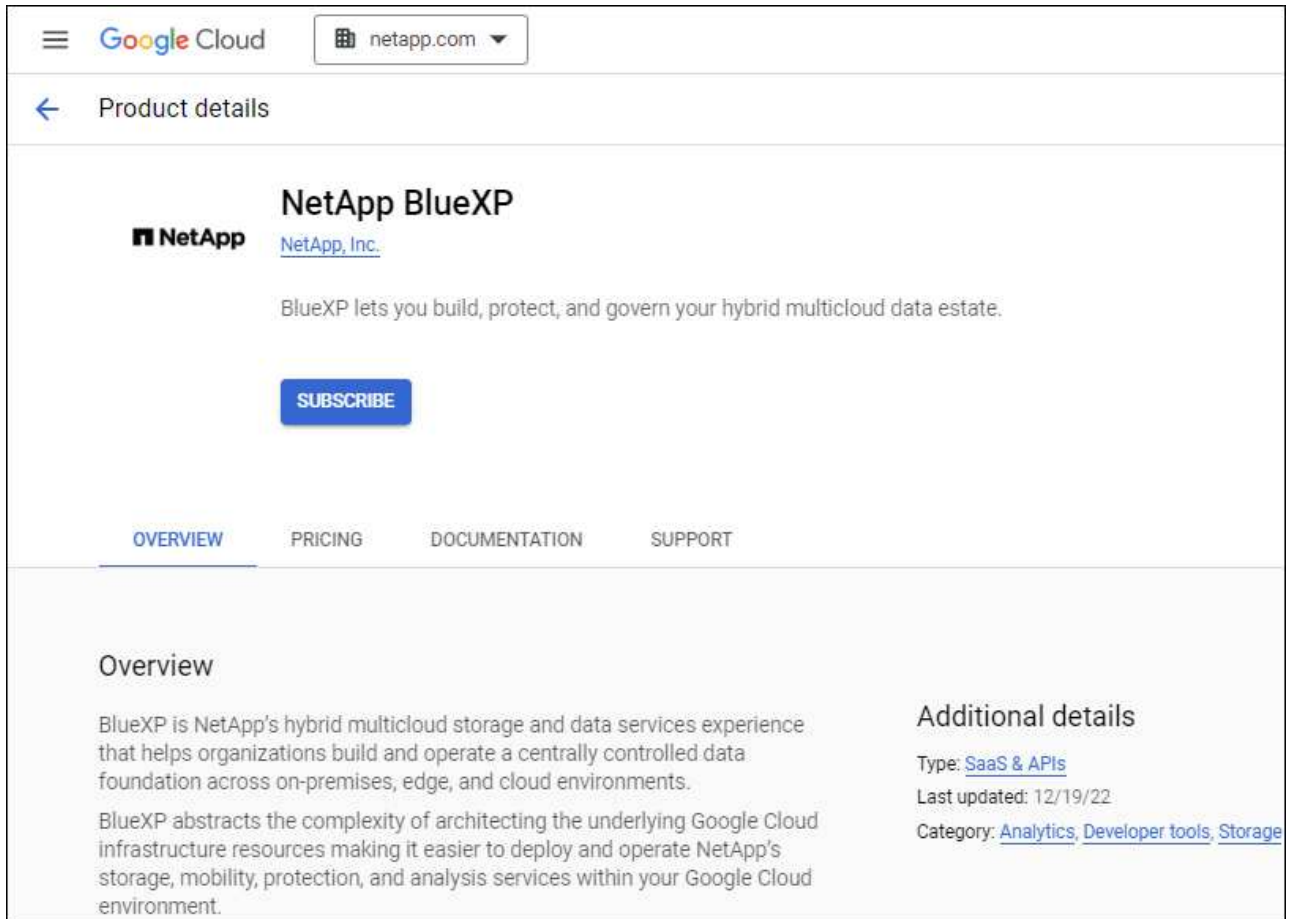


4. If you don't already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.



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 BlueXP page on the Google Cloud Marketplace](#), ensure that the correct project is selected at the top navigation menu.



- 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.



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

 Add Subscription

Troubleshoot the Marketplace subscription process

Sometimes subscribing to BlueXP 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.

[MANAGE ORDERS](#)

- 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.

Filter Enter property name or value										
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.

Filter Enter property name or value										
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 a BlueXP organization or account

Associate a NetApp Support Site account with your BlueXP organization or account to enable key workflows for Cloud Volumes ONTAP. These NSS credentials are associated with the entire BlueXP organization or account.

BlueXP also supports associating one NSS account per BlueXP user account. [Learn how to manage user-level credentials.](#)



If you're using BlueXP in standard mode, you'll have a *BlueXP organization*, which you manage using BlueXP identity and access management (IAM). But if you're using BlueXP in restricted mode or private mode, then you'll have a *BlueXP account*.

- [Learn about BlueXP deployment modes](#)
- [Learn about BlueXP identity and access management](#)
- [Learn about BlueXP accounts](#)

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

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with BlueXP at the BlueXP organization or account level.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

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. 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 specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

Note the following:

- The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

- 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](#)

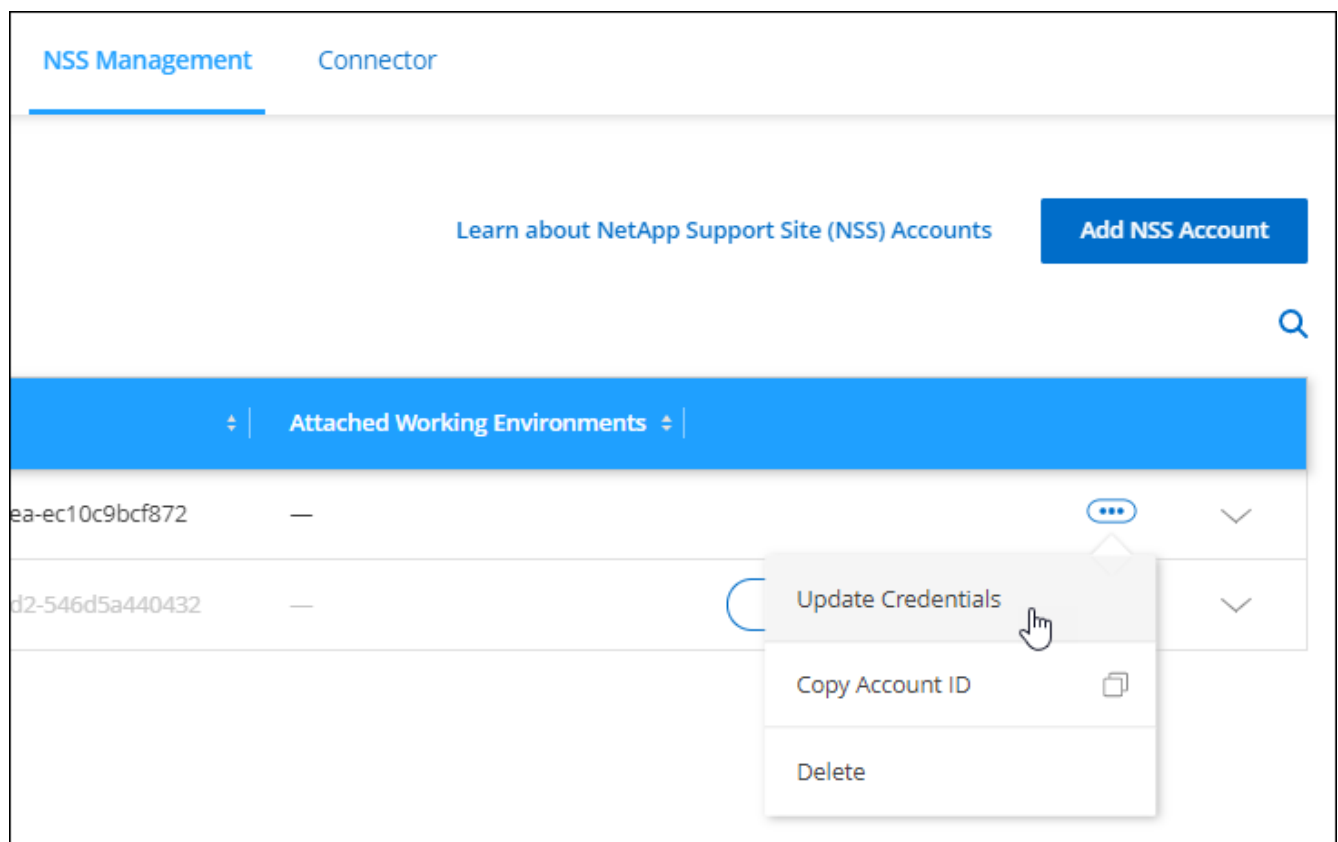
Update NSS credentials

You'll need to update the credentials for your NSS accounts in BlueXP when either of the following happens:

- You change the credentials for the account
- The refresh token associated with your account expires after 3 months

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 specific to support and licensing.

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

authentication process.

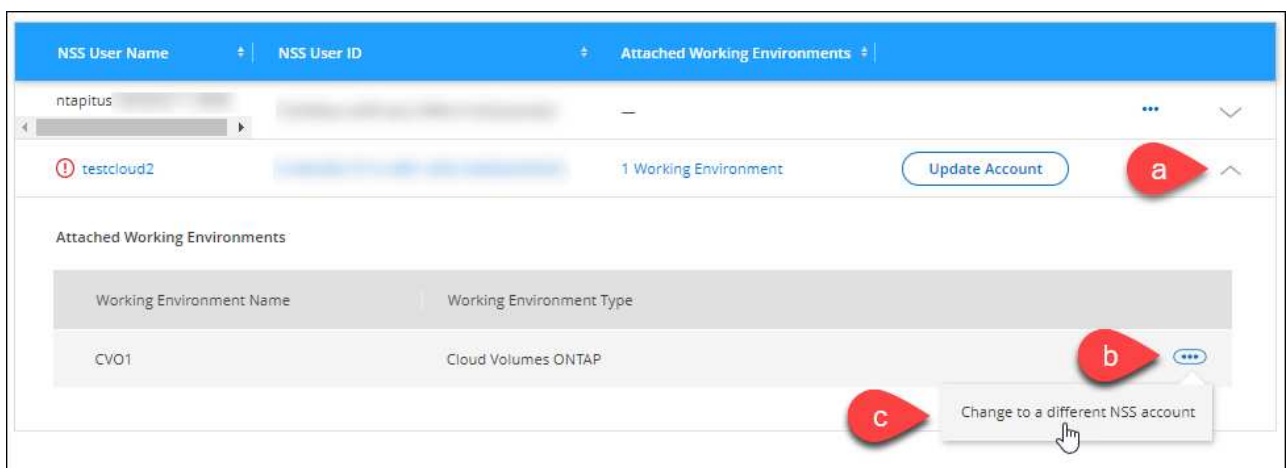
Attach a working environment to a different NSS account

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

This feature is only supported with NSS accounts that are configured to use Microsoft Entra ID adopted by NetApp for identity management. Before you can use this feature, you need select **Add NSS Account** or **Update Account**.

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**.



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

Display the email address for an NSS account

Now that NetApp Support Site accounts use Microsoft Entra ID for authentication services, the NSS user name that displays in BlueXP is typically an identifier generated by Microsoft Entra. As a result, you might not immediately know the email address associated with that account. But BlueXP has an option to show you the associated email address.

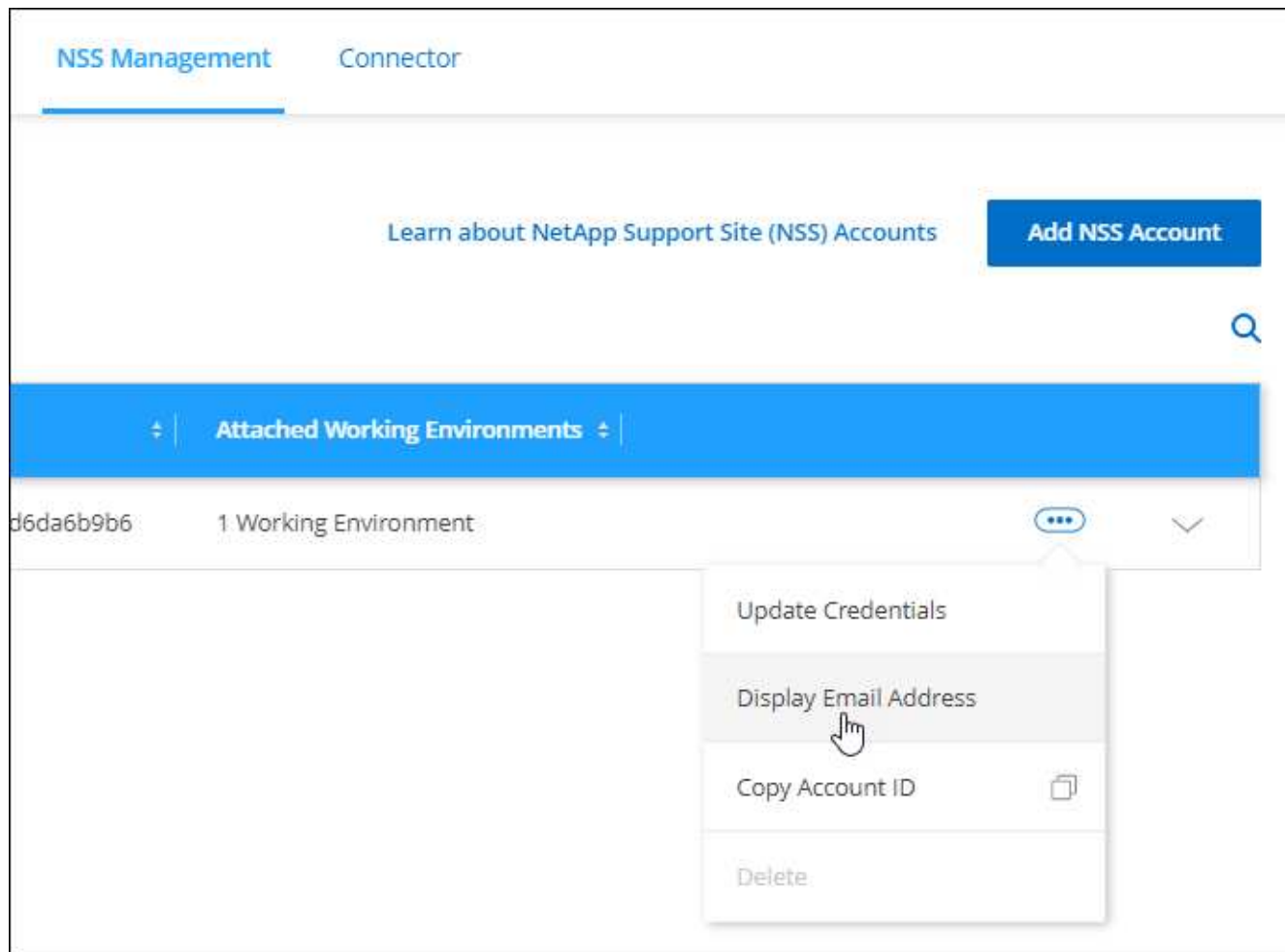


When you go to the NSS Management page, BlueXP generates a token for each account in the table. That token includes information about the associated email address. The token is then removed when you leave the page. The information is never cached, which helps protect your privacy.

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**.



Result

BlueXP displays the NetApp Support Site user name and the associated email address. You can use the copy button to copy the email address.

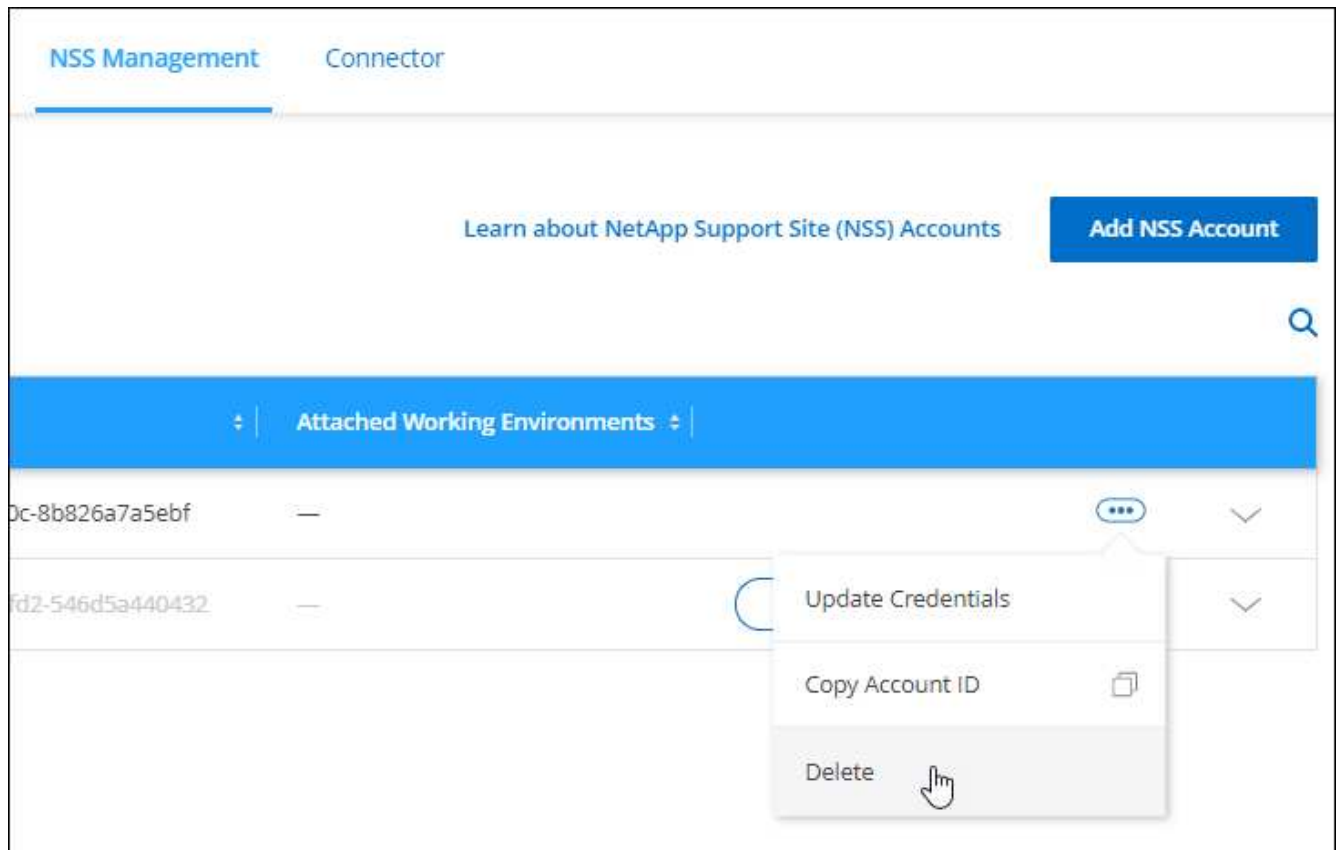
Remove an NSS account

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

Note that 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

When you directly discover an on-premises ONTAP cluster without using a Connector, you're prompted to enter ONTAP credentials for the cluster. These credentials are managed at the user level, which means they aren't viewable by other users who log in.

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 action registers the BlueXP 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 when you bring your own license (BYOL), register PAYGO systems, and upgrade Cloud Volumes ONTAP software.

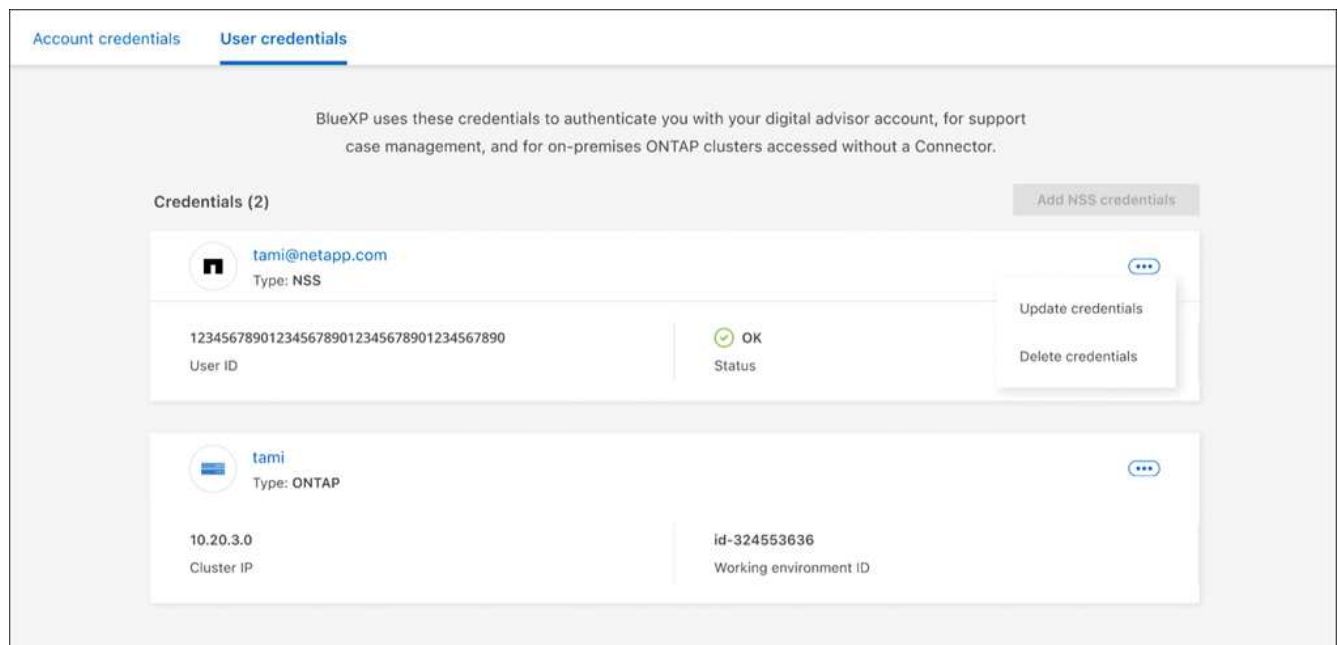
[Learn more about using NSS credentials with your BlueXP organization or account.](#)

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:
 - **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. The changes will be reflected when you access 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 following table provides a comparison of the Timeline and the Notification Center so you can understand what each has to offer.


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 won't 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 in BlueXP 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.

Checking the Timeline can be helpful if you need to identify who performed a specific action, or if you need to identify the status of an action.

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.

Result

The Timeline updates to show you completed management actions.

Monitor activities using the Notification Center

Notifications track the progress of operations that you've initiated in BlueXP so you can verify whether the operation was successful or not. 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.



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

Notifications are classified in 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.

Notification type	Description
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

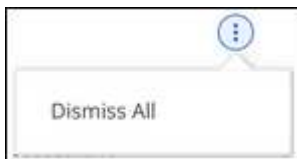
By default you'll see all active notifications in the Notification Center. You can filter the notifications that you see to show only those notifications that are important to you. You can filter by BlueXP "Service" and by notification "Type".

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.

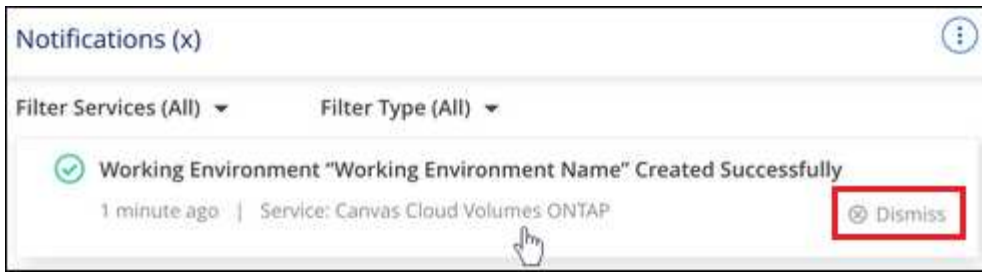
Dismiss notifications

You can remove notifications from the page if you no longer need to see them. You can dismiss all notifications at once, or you can dismiss individual notifications.

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**.



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.



- Notifications are sent by email for the following BlueXP features and services: the Connector, BlueXP digital wallet, BlueXP copy and sync, and BlueXP 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 be a BlueXP admin 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**.

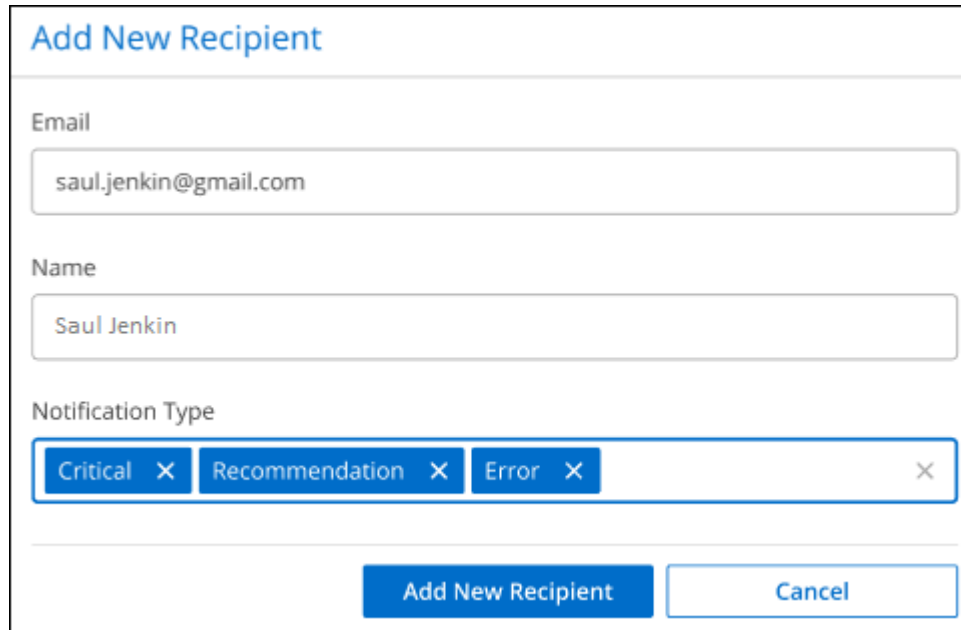


Add additional email recipients

The users who appear in the *Users* tab are populated automatically from the users in your BlueXP 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**.



The screenshot shows a web form titled "Add New Recipient" in blue text. The form has three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown containing "Critical", "Recommendation", and "Error". Each item in the dropdown has a small "x" icon to its right. At the bottom of the form, there are two buttons: a blue "Add New Recipient" button and a white "Cancel" button with a blue border.

2. Enter the name, email address, and select the types of Notifications that recipient will receive, and select **Add New Recipient**.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.