



Administer BlueXP

Setup and administration

NetApp
July 19, 2023

This PDF was generated from <https://docs.netapp.com/us-en/bluexp-setup-admin/concept-federation.html> on July 19, 2023. Always check docs.netapp.com for the latest.

Table of Contents

- Administer BlueXP 1
 - Using identity federation with BlueXP 1
 - BlueXP accounts 6
 - Connectors 20
 - Credentials 32
 - Discovered cloud storage 69

Administer BlueXP

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 Azure Active Directory (AD)
- 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> 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.</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 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 Azure AD

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

Step	Completed by	Description
1	AD admin	<p>Configure Azure Active Directory to enable identity federation with BlueXP.</p> <p>View instructions for registering the application with Azure AD</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"> • Client ID • Client secret value • Microsoft Azure AD 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	Complete the configuration in Azure AD 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>

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.

BlueXP accounts

Manage your BlueXP account

When you create a BlueXP account, it only includes a single admin user and a workspace. You can manage the account to fit your organization's needs by adding users, creating service accounts for automation purposes, by adding workspaces, and more.

[Learn how BlueXP accounts work.](#)

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.

[View endpoints for the Tenancy API](#)

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.



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

Role

Associate User to Workspaces

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.

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.

5 Members					
Type	Name	Email	Role	Workspace	
	Ben		☆ Account Admin	All Workspaces	...
	Tom		☆ Account Admin	All Workspaces	...
	Ben		Workspace Admin	Newone	

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. And if you're using federation, you can create a token without generating a refresh token from the cloud.

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.

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.

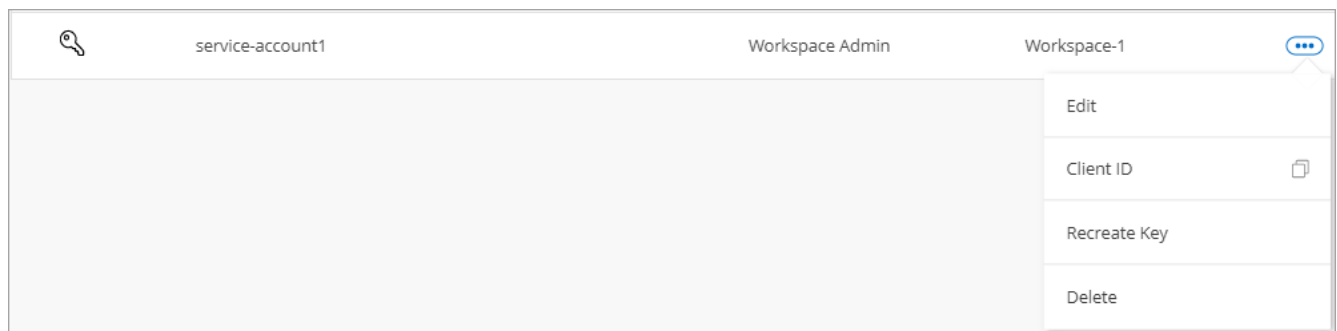
5. Select **Close**.

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.

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.

Monitor operations in your account


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 Notification Center, in the Timeline, or have notifications sent to your email.

The following table provides a comparison of the Notification Center and the Timeline 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 Account users and to others	No email capability

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 clicking 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 account, or to any other recipients who need to be aware of certain types of system activity. See how to [set email notification settings](#).

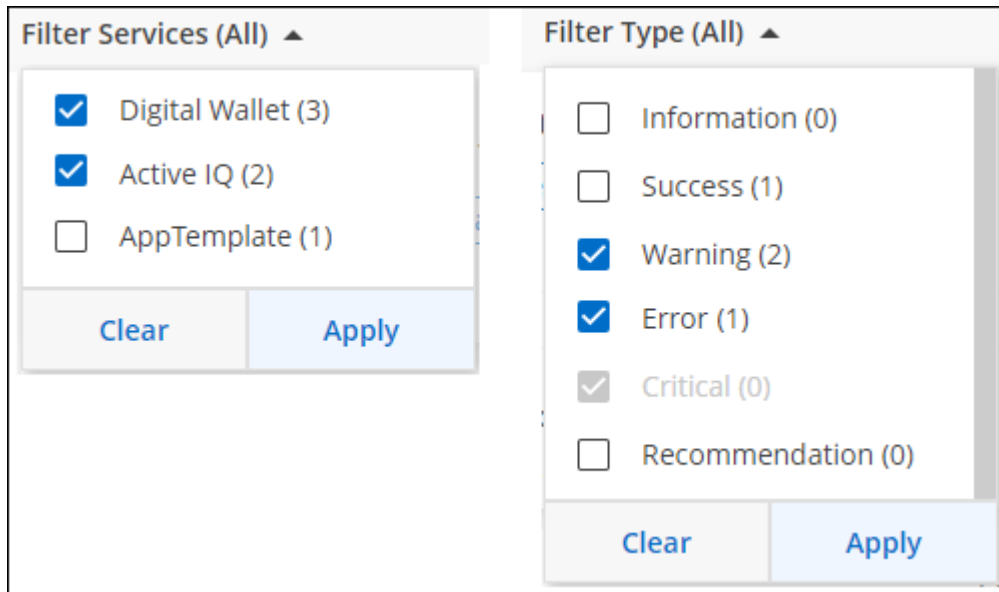
Notification types

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.
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".

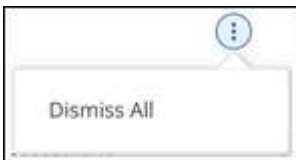


For example, if you want to see only "Error" and "Warning" notifications for BlueXP operations, select those entries and you'll see only those types of notifications.

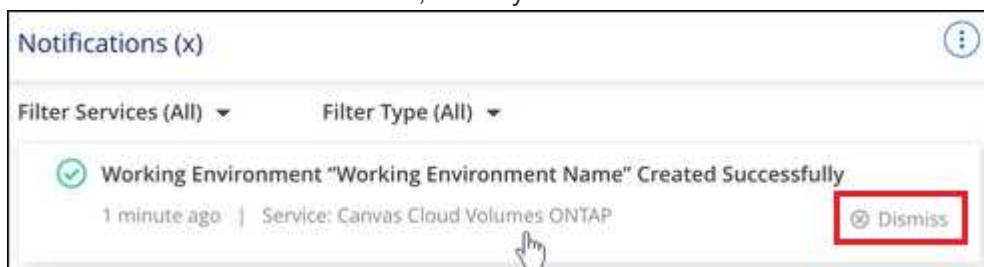
Dismiss notifications

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 account, or to any other recipients who need to be aware of certain types of system activity.



- At this time, notifications are sent by email for the following BlueXP features and services: Connector, BlueXP copy and sync, BlueXP backup and recovery, BlueXP digital wallet, and BlueXP ransomware protection. Additional services will be added in future releases.
- Sending email notifications is not supported when the Connector is installed in a site without internet access.

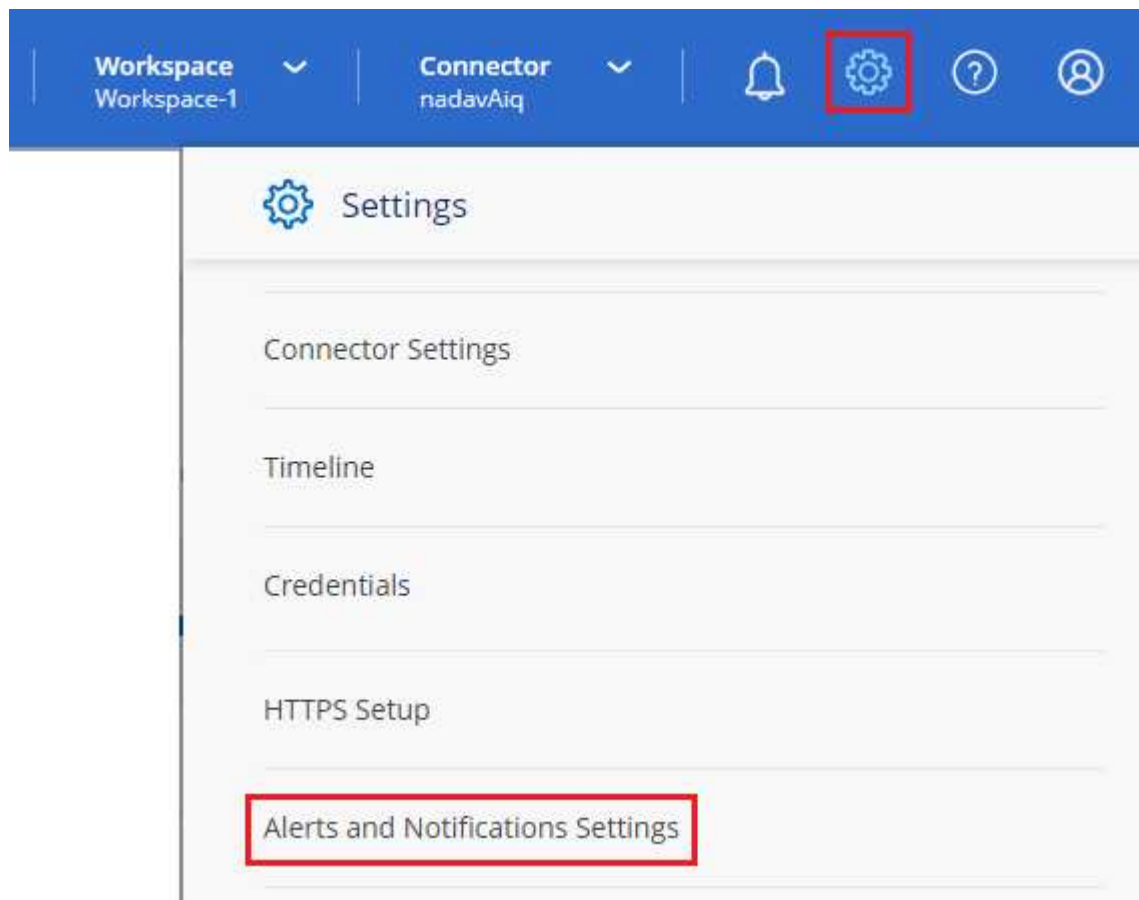
The filters you set in the Notification Center do not determine the types of notifications you'll receive by email. By default, BlueXP Account Admins will receive emails for all "Critical" and "Recommendation" notifications. These notifications are across all services - you can't choose to receive notifications 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 an Account 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 *Account Users* tab or the *Additional Recipients* tab, and choose the type of notifications to be sent:
 - To make changes for a single user, select the menu in the Notifications column for that user, check the types of Notifications to be sent, and select **Apply**.
 - To make changes for multiple users, check the box for each user, select **Manage Email Notifications**, check the types of Notifications to be sent, and select **Apply**.

Email	Name	Role
<input type="checkbox"/> Sabar@netapp.com	Sabar V	Account Admin
<input checked="" type="checkbox"/> activeiq@netapp-st.com	nadav	Account Admin
<input checked="" type="checkbox"/> nand@netapp.com	AnanK	Account Admin
<input type="checkbox"/> apra@netapp.com	Aradev	Workspace Admin
<input type="checkbox"/> ash@netapp.com	AshG	Account Admin

Notification Types: ☒ Critical, ☐ Recommendation, ☐ Info, ☐ Warning, ☒ Error

Buttons: Clear, Apply

Add additional email recipients

The users who appear in the *Account Users* tab are populated automatically from the users in your BlueXP account (from the [Manage Account page](#)). You can add email addresses in the *Additional Recipients* tab for other people, or groups, who do not have access to BlueXP, but who need to be notified about certain types of alerts and notifications.

Steps

1. From the Alerts and Notifications Settings page, select **Add New Recipients**.

Add New Recipient

Email: saul.jenkin@gmail.com

Name: Saul Jenkin

Notification Type: Critical, Recommendation, Error

Buttons: Add New Recipient, Cancel

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

Audit user activity in your account

The Timeline in BlueXP shows the actions that users completed to manage your account. This includes management actions such as associating users, creating workspaces, 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. From the BlueXP menu bar, select **Settings > Timeline**.
2. Under the Filters, select **Service**, enable **Tenancy**, and select **Apply**.

Result

The Timeline updates to show you account management actions.

Create another BlueXP account

When you sign up to BlueXP, you're prompted to create an account for your organization. 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.

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 links

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

Roles

The Account Admin, Workspace Admin, Compliance Viewer, and SnapCenter Admin roles provide specific permissions to users. You can assign one of these roles when you associate a new user with your BlueXP account.

The Compliance Viewer role is for read-only BlueXP classification access.

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
Manage working environments	Yes	Yes	No	No
Enable services on working environments	Yes	Yes	No	No

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
View data replication status	Yes	Yes	No	No
View the timeline	Yes	Yes	No	No
Switch between workspaces	Yes	Yes	Yes	No
View BlueXP classification scan results	Yes	Yes	Yes	No
Delete working environments	Yes	No	No	No
Connect Kubernetes clusters to working environments	Yes	No	No	No
Receive the Cloud Volumes ONTAP report	Yes	No	No	No
Create Connectors	Yes	No	No	No
Manage BlueXP accounts	Yes	No	No	No
Manage credentials	Yes	No	No	No
Modify BlueXP settings	Yes	No	No	No
View and manage the Support Dashboard	Yes	No	No	No
Remove working environments from BlueXP	Yes	No	No	No
Install an HTTPS certificate	Yes	No	No	No

Related links

- [Setting up workspaces and users in the BlueXP account](#)
- [Managing workspaces and users in the BlueXP account](#)

Connectors

Find the system ID for a Connector

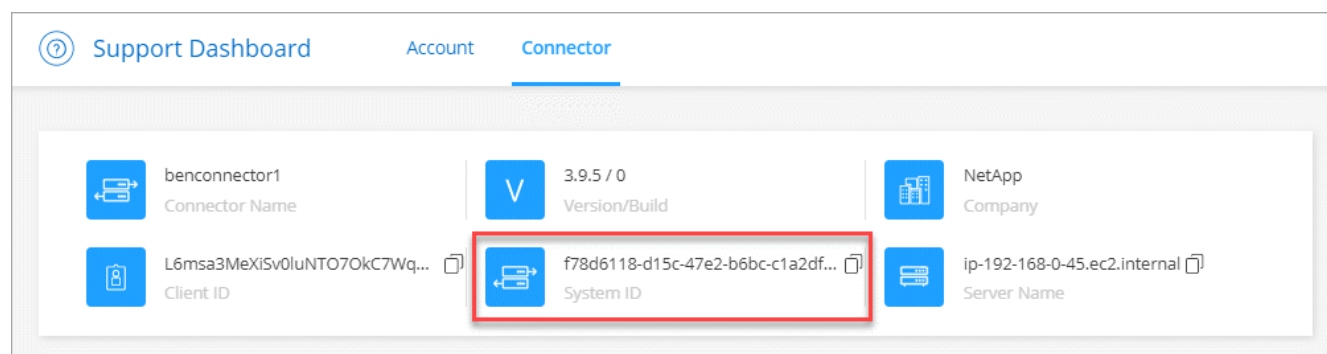
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

Steps

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

The system ID appears at the top.

Example



Manage existing Connectors

After you create a Connector, you might need to manage it every now and then. For example, you might want to switch between Connectors if you have more than one. Or you might need to manually upgrade the Connector when using BlueXP in private mode.

[Learn how Connectors work.](#)

Operating system and VM maintenance

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.

Note that you don't need to stop any services on the Connector host when running an OS update.

If you need to stop and then start the Connector VM, 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.](#)

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.

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.



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.

[AWS Docs: Connect to your Linux instance](#)

Azure

When you created the Connector VM in Azure, you 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](#)

Upgrade the 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.

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



On hosts that have internet access, the Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update.

Steps

1. Download the Connector software from the [NetApp Support Site](#).
2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

```
chmod +x /path/cloud-manager-connector-offline-<version>
```

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

4. Run the installation script:

```
sudo /path/cloud-manager-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**.

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.
 - a. Run the following command from the Cloud Volumes ONTAP CLI to remove the current backup target:

```
system configuration backup settings modify -destination ""
```

- b. Go to BlueXP and open the working environment.
- c. Select the menu and select **Advanced > Configuration Backups**.
- d. Select **Set Backup Target**.

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**.

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](#)

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.

Uninstall the Connector software

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 whether you installed the Connector on a host that has internet access or a host in a restricted network that doesn't have internet access.

Uninstall from a host with internet access

The online Connector includes an uninstallation script that you can use to uninstall the software.

Step

1. From the Linux host, run the uninstallation script:

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

silent runs the script without prompting you for confirmation.

Uninstall from a host without internet access

Use these commands if you downloaded the Connector software from the NetApp Support Site and installed it in a restricted network that doesn't have internet access.

Step

1. From the Linux host, run the following commands:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

Install an HTTPS certificate for secure access

By default, BlueXP uses a self-signed certificate for HTTPS access to the web console. 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.

Before you begin

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

Install an HTTPS certificate

Install a certificate signed by a CA for secure access.

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 BlueXP account 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.

BlueXP supports HTTP and HTTPS. The proxy server can be in the cloud or in your network.

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.

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



2. Under **General**, 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

The user must be a local user. Domain users are not supported.

- d. Select **Save**.



BlueXP doesn't support passwords that include the @ character.

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



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

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.xlarge.
- The operating system for the image is Ubuntu 22.04.

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

- The user name for the EC2 Linux instance is 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 DS3 v2.
- The operating system for the image is Ubuntu 22.04.

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

- 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-4.
- The operating system for the image is Ubuntu 22.04.

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

- 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 and docker images.

- `/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

Manage AWS credentials

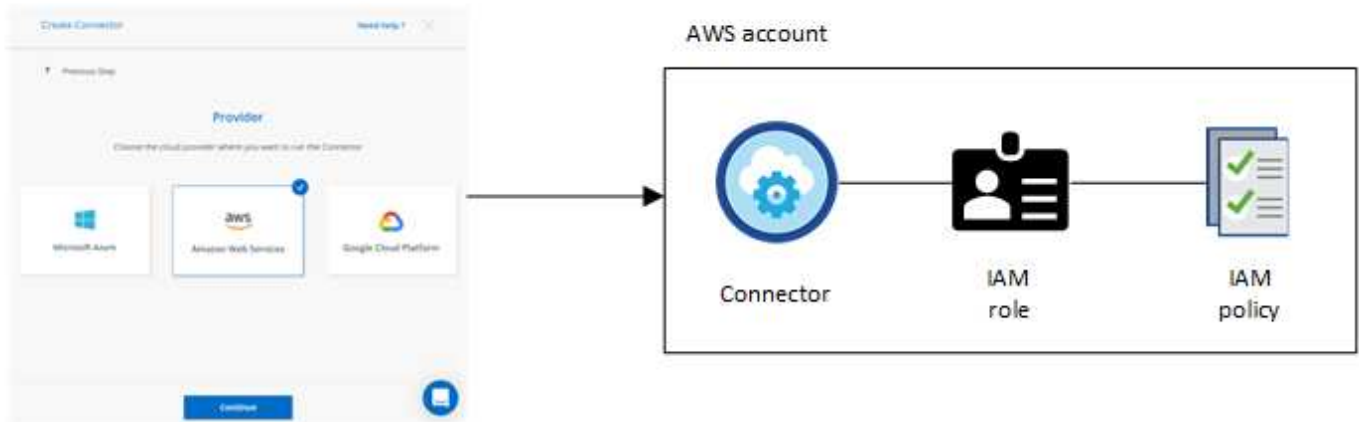
AWS credentials and permissions

Learn how BlueXP uses AWS credentials and permissions to perform actions on your behalf. 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

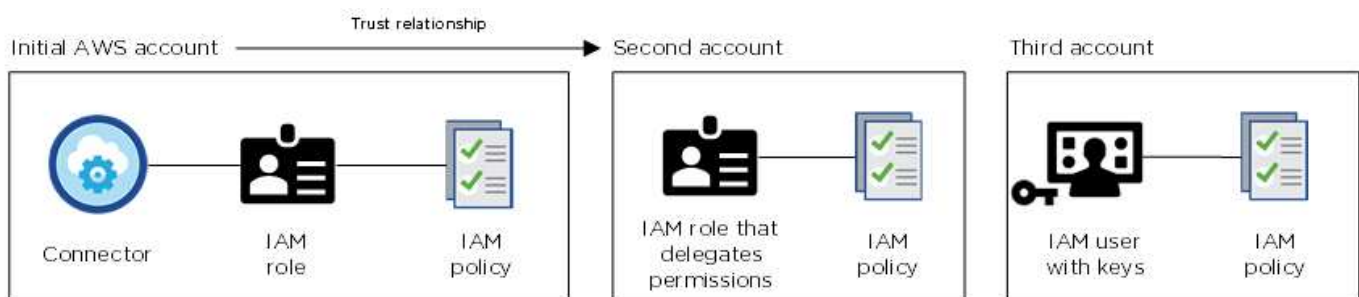
There are two ways to add additional AWS credentials:

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

Review the sections below for more details.

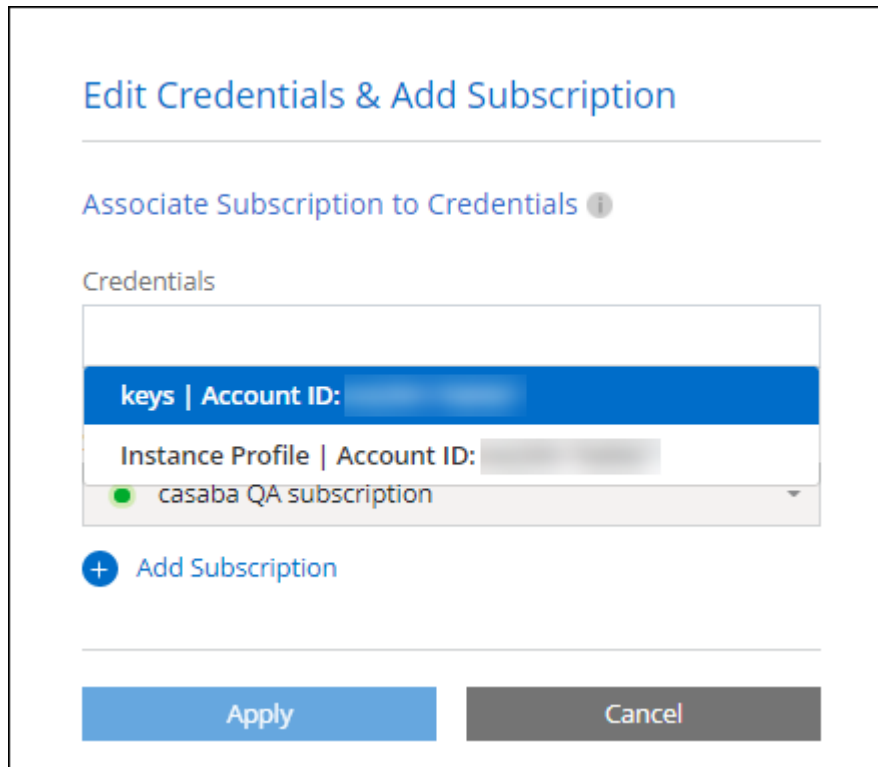
Add AWS credentials to an existing Connector

If you want to launch Cloud Volumes ONTAP in different 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.

After you add another set of credentials, you can switch to them when creating a new working environment:



[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](#)

What about 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 AWS permissions](#)
- [Set up cloud permissions for on-prem deployments](#)
- [Set up cloud permissions for restricted mode](#)
- [Set up cloud permissions for private mode](#)

How can I securely rotate my AWS credentials?

As described 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.

Manage AWS credentials and 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 **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 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 **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 replace an existing AWS Marketplace subscription with a new subscription.

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, click the Settings icon, and select **Credentials**.
2. Click 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 click **Associate**.
4. To associate the credentials with a new subscription, click **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
 - a. Click **View purchase options**.
 - b. Click **Subscribe**.
 - c. Click **Set up your account**.

You'll be redirected to the BlueXP website.

- d. From the **Subscription Assignment** page:
 - Select the BlueXP 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 account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the 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 accounts, you'll need to manually associate the subscription by repeating these steps.

- Click **Save**.

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

► <https://docs.netapp.com/us-en/bluexp-setup-admin/tmp/d20230719-6274->

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 **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 **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Manage Azure credentials

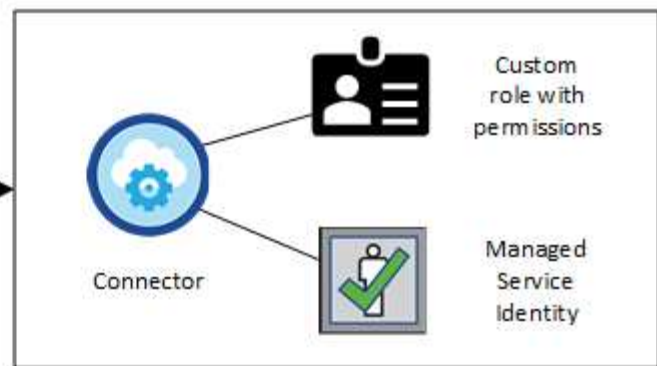
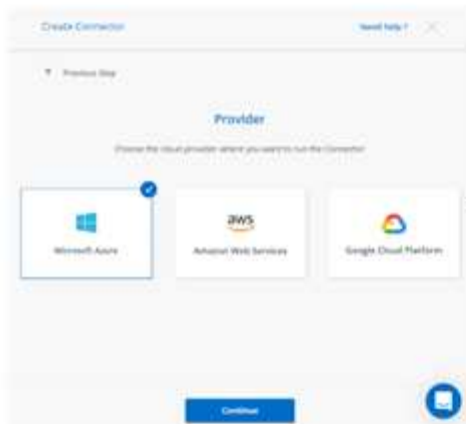
Azure credentials and permissions

Learn how BlueXP uses Azure credentials and permissions to perform actions on your behalf. 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.

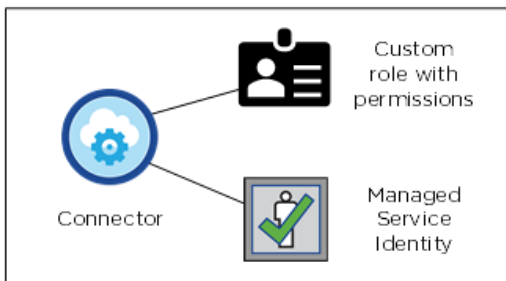
Additional Azure subscriptions for a managed identity

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](#).

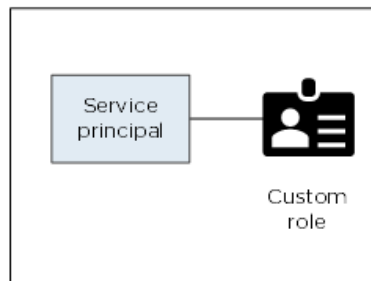
Additional Azure credentials

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 Azure Active Directory](#) for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:

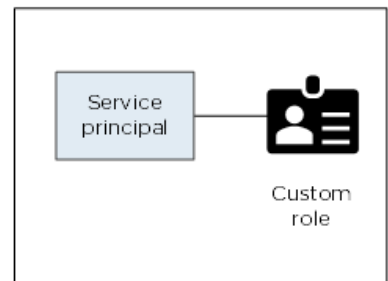
Initial Azure account



Second account



Third account



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:



What about 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 Azure AD 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 Azure permissions](#)
 - [Set up cloud permissions for on-prem deployments](#)
- [Set up cloud permissions for restricted mode](#)
- [Set up cloud permissions for private mode](#)

Manage Azure credentials and 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 Azure Active Directory 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 Azure Active Directory 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 Azure Active Directory and is assigned to a custom role that allows the required permissions.



Steps

1. [Create an Azure Active Directory 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 an Azure Active Directory application

Create an Azure Active Directory (AD) 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 **Azure Active Directory** service.



3. In the menu, click **App registrations**.
4. Click **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. Click **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. Click **Access control (IAM) > Add > Add role assignment**.
- d. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.
- e. In the **Members** tab, complete the following steps:
 - Keep **User, group, or service principal** selected.
 - Click **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 click **Select**.
- Click **Next**.

f. Click **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 **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **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.



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

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

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

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

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

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

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

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

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

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

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

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

4. Click **Access Azure Service Management as organization users** and then click **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 **Azure Active Directory** service, click **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 Azure AD.

Steps

1. Open the **Azure Active Directory** service.

2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Click **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 Azure AD.

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, click the Settings icon, and select **Credentials**.

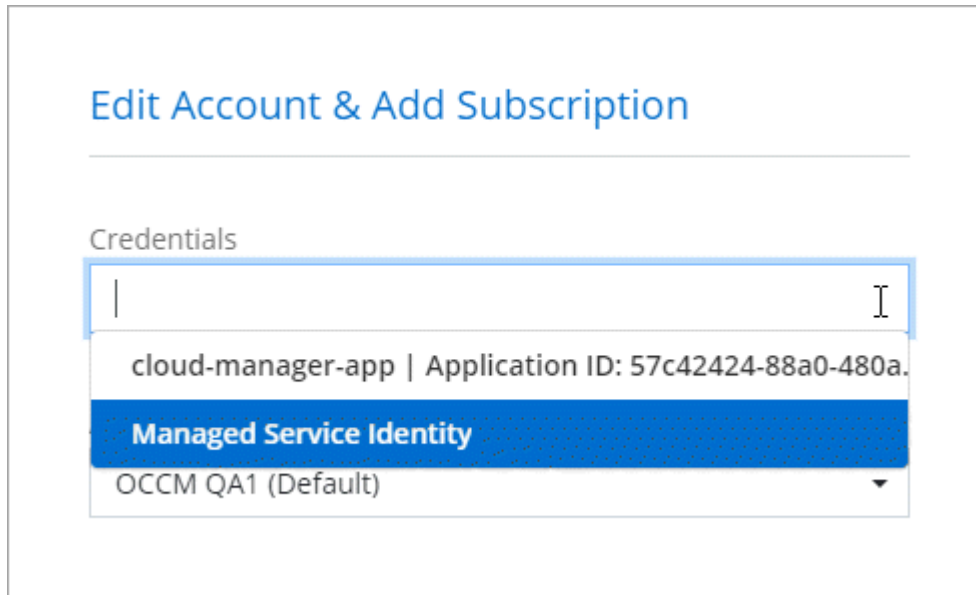


2. Click **Add Credentials** and follow the steps in the wizard.
 - a. **Credentials Location:** Select **Microsoft Azure > Connector**.
 - b. **Define Credentials:** Enter information about the Azure Active Directory service principal that grants the required permissions:
 - Application (client) ID

- 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 click **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 replace an existing Azure Marketplace subscription with a new subscription.

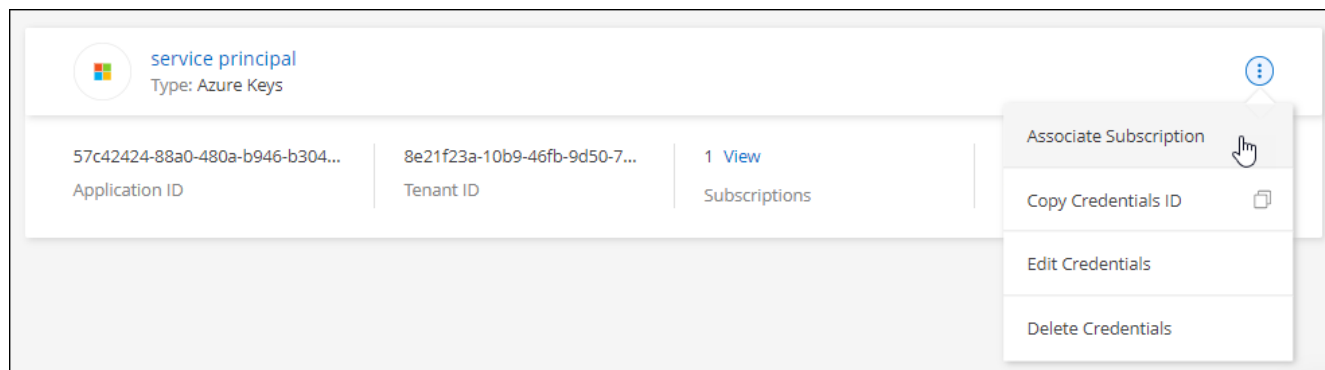
Before you begin

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

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click 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 click **Associate**.
4. To associate the credentials with a new subscription, click **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
 - a. If prompted, log in to your Azure account.
 - b. Click **Subscribe**.
 - c. Fill out the form and click **Subscribe**.
 - d. After the subscription process is complete, click **Configure account now**.

You'll be redirected to the BlueXP website.

- e. From the **Subscription Assignment** page:
 - Select the BlueXP 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 account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the 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 accounts, you'll need to manually associate the subscription by repeating these steps.

- Click **Save**.

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

► <https://docs.netapp.com/us-en/bluexp-setup-admin/tmp/d20230719-6274->

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 **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 **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Manage Google Cloud credentials

Google Cloud projects, permissions, and accounts

Learn how BlueXP uses Google Cloud credentials and permissions to perform actions on your behalf. 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.

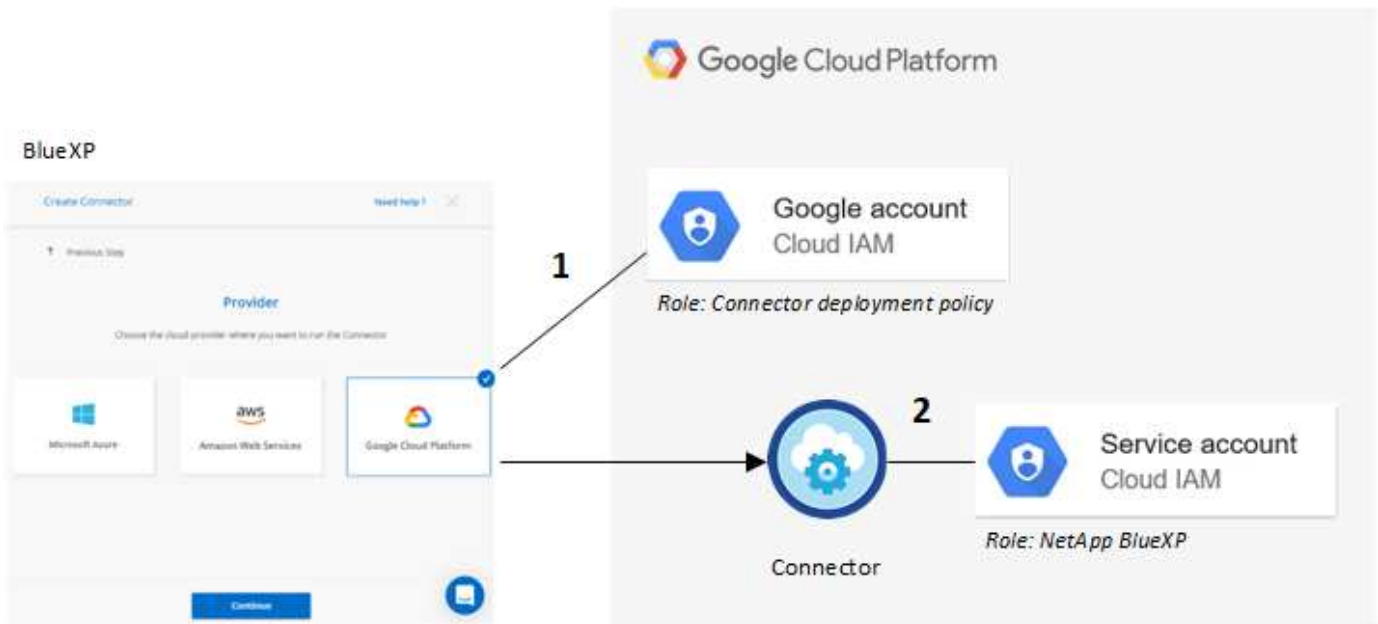
Project and permissions for BlueXP

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 cloud permissions for restricted mode](#)
- [Set up cloud permissions for private mode](#)

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 Marketplace subscription that's 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.

Steps

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

 A screenshot of the 'Associate Subscription' form in the Google Cloud console. It features two dropdown menus. The first is labeled 'Google Cloud Project' and has 'OCCM-Dev' selected. The second is labeled 'Subscription' and has 'GCP subscription for staging' selected, which is preceded by a green dot icon. Below these dropdowns is a horizontal line, and at the bottom left is a blue button with a plus icon and the text 'Add Subscription'.

4. If you don't already have a subscription, click **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.

The screenshot shows the 'Product details' page for NetApp BlueXP on the Google Cloud platform. At the top, there's a navigation bar with the Google Cloud logo and a dropdown menu showing 'netapp.com'. Below this, a back arrow and the text 'Product details' are visible. The main content area features the NetApp logo, the product name 'NetApp BlueXP', and a link to 'NetApp, Inc.'. A description states: 'BlueXP lets you build, protect, and govern your hybrid multicloud data estate.' A prominent blue 'SUBSCRIBE' button is centered. Below the button is a horizontal menu with four tabs: 'OVERVIEW' (which is selected and underlined), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'Overview' section contains two paragraphs of text describing BlueXP as a hybrid multicloud storage and data services experience. To the right of the overview, under the heading 'Additional details', there is information about the product type ('SaaS & APIs'), the last update date ('12/19/22'), and a category list ('Analytics, Developer tools, Storage').

- b. Click **Subscribe**.
- c. Select the appropriate billing account and agree to the terms and conditions.
- d. Click **Subscribe**.

This step sends your transfer request to NetApp.

- e. On the pop-up dialog box, click **Register with NetApp, Inc.**

This step must be completed to link the Google Cloud subscription to your BlueXP 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 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 account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the 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 accounts, you'll need to manually associate the subscription by repeating these steps.

- Click **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

► <https://docs.netapp.com/us-en/bluexp-setup-admin/tmp/d20230719-6274->

- 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	
<div></div>	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 account

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



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

Overview

Associating NetApp Support Site credentials with your specific BlueXP account ID 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 ID. Users who belong to the BlueXP 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 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 Azure Active Directory 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.

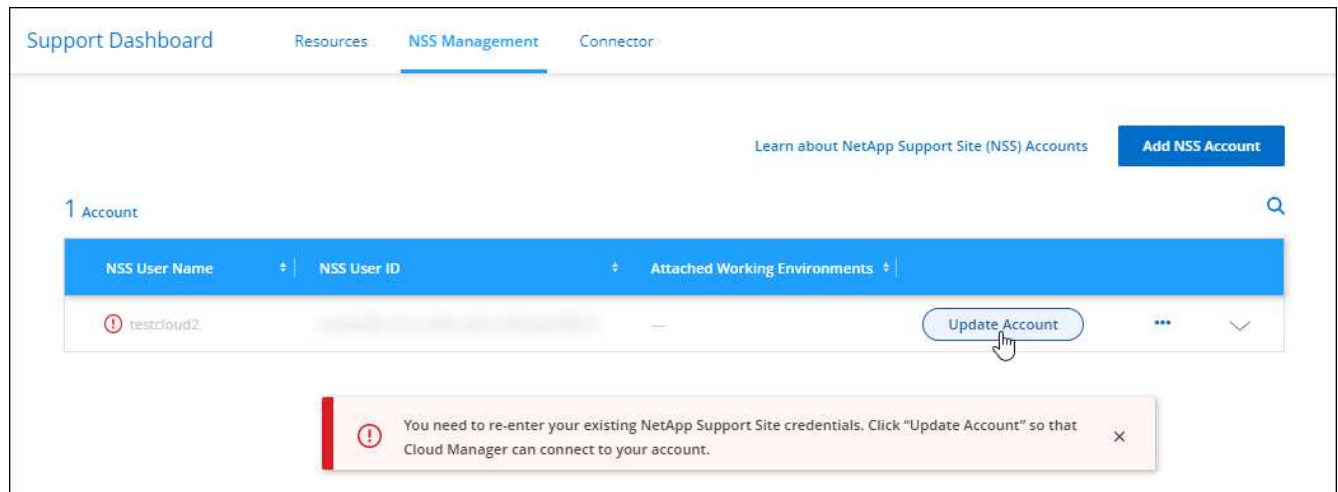
- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Launching Cloud Volumes ONTAP in Google Cloud](#)
- [Registering pay-as-you-go systems](#)

Update an NSS account for the new authentication method

Starting in November 2021, NetApp now uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing. As a result of this update, BlueXP will prompt you to update the credentials for any existing accounts that you previously added.

Steps

1. If you haven't already done so, [create a Microsoft Azure Active Directory B2C account that will be linked to your current BlueXP account](#).
2. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
3. Select **NSS Management**.
4. For the NSS account that you want to update, select **Update Account**.



5. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

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

After the process is complete, the account that you updated should now be listed as a *new* account in the table. The *older* version of the account is still listed in the table, along with any existing working environment associations.

7. If existing Cloud Volumes ONTAP working environments are attached to the older version of the account, follow the steps below to [attach those working environments to a different NSS account](#).
8. Go to the older version of the NSS account, select **...** and then select **Delete**.

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 Azure Active Directory 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 Azure AD 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 Azure Active Directory for authentication services, the NSS user name that displays in BlueXP is typically an identifier generated by Azure AD. 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.

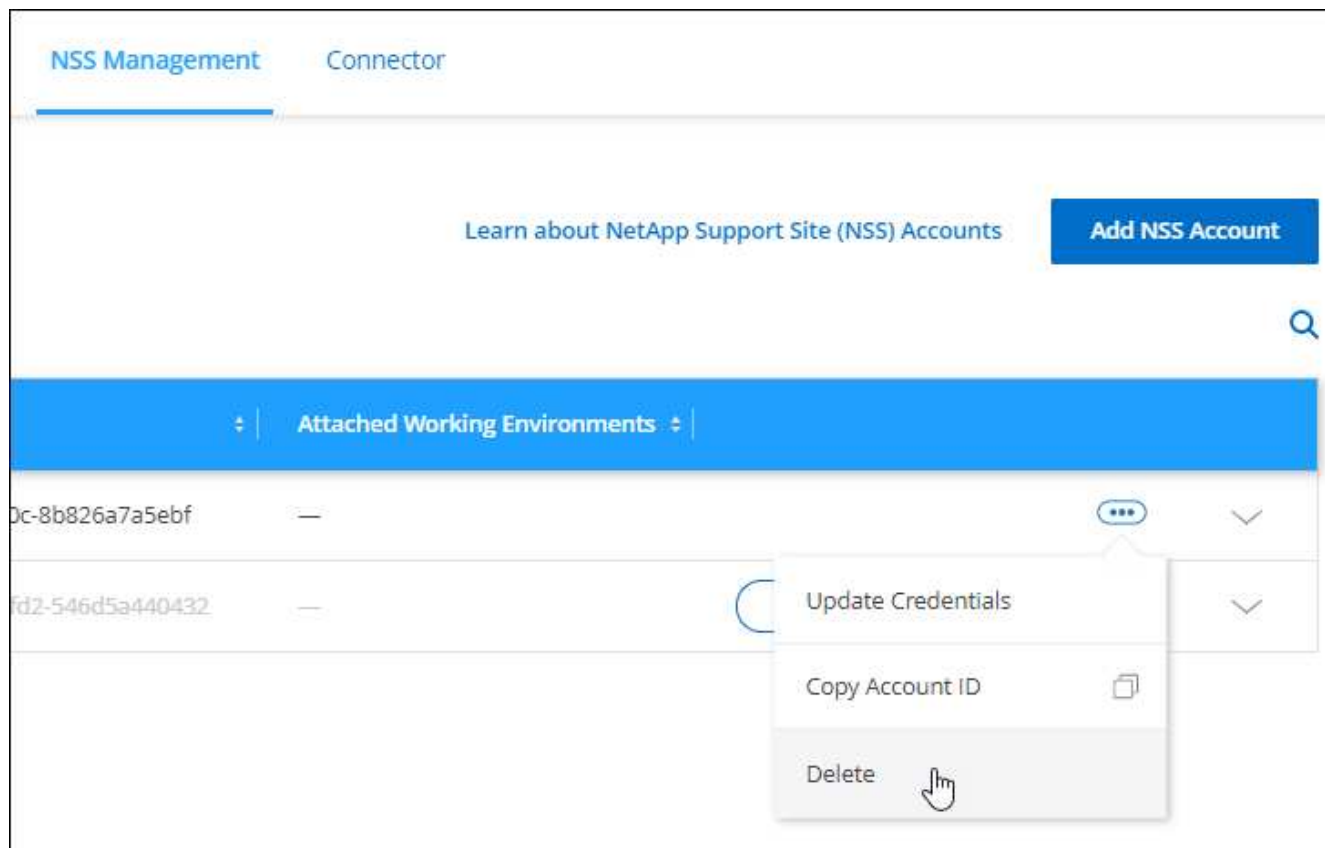
Remove an NSS account

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 account for support and activates support entitlement. Only one user in your BlueXP 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 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 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, click the Settings icon, and select **Credentials**.
2. Click **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.

Discovered cloud storage

Manage your Amazon S3 buckets

After you install a Connector in AWS, BlueXP can automatically discover information about the Amazon S3 buckets that reside in the AWS account where the Connector is installed. An Amazon S3 working environment is added to the Canvas so you can view this information.



You can view details about your S3 buckets, including the region, access policy, account, total and used capacity, and more. These buckets can be used as destinations for BlueXP backup and recovery, BlueXP tiering, or BlueXP copy and sync operations. Additionally, you can use BlueXP classification to scan these buckets.

A newly added feature now enables you to create and edit S3 buckets. [Go here to see how you can view, create, and manage your S3 buckets using BlueXP.](#)

Manage your Azure Blob accounts

After you install a Connector in Azure, BlueXP can automatically discover information about the Azure storage accounts that reside in the Azure Subscriptions where the Connector is installed. An Azure Blob working environment is added to the Canvas so you can view this information.



You can see details about your Azure storage accounts, including the location, resource group, total and used capacity, and more. These accounts can be used as destinations for BlueXP backup and recovery, BlueXP tiering, or BlueXP copy and sync operations.

A newly added feature now enables you to create and edit Azure storage accounts. [Go here to see how you can view, create, and manage your Azure storage accounts using BlueXP.](#)

View your Google Cloud Storage buckets

After you install a Connector in Google Cloud, BlueXP can automatically discover information about the Google Cloud Storage buckets that reside in the Google account where the Connector is installed. A Google Cloud Storage working environment is added to the Canvas so you can view this information.



You can see details about your Google Cloud Storage buckets, including the location, access status, storage class, total and used capacity, and more. These buckets can be used as destinations for BlueXP backup and recovery, BlueXP tiering, or BlueXP copy and sync operations.

A newly added feature now enables you to create and edit Google Cloud Storage buckets. [Go here to see how you can view, create, and manage your Cloud Storage buckets using BlueXP.](#)

Copyright information

Copyright © 2023 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.