Credentials and subscriptions

BlueXP setup and administration

NetApp
August 21, 2025

Table of Contents

Credentials and subscriptions

AWS

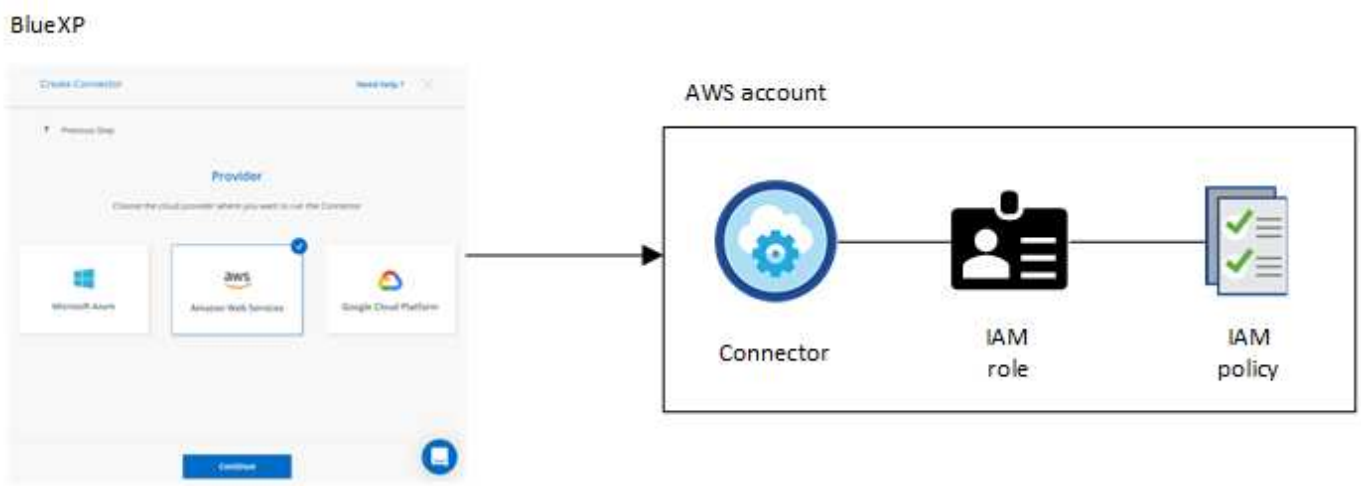
Learn about AWS credentials and permissions in BlueXP

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

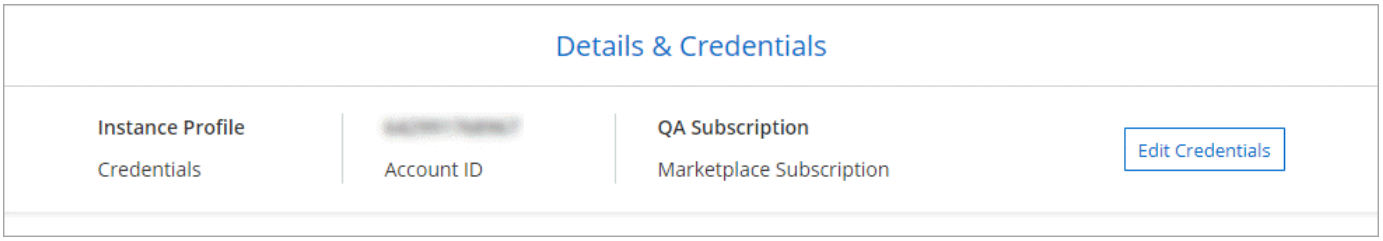
Initial AWS credentials

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

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



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



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

Additional AWS credentials

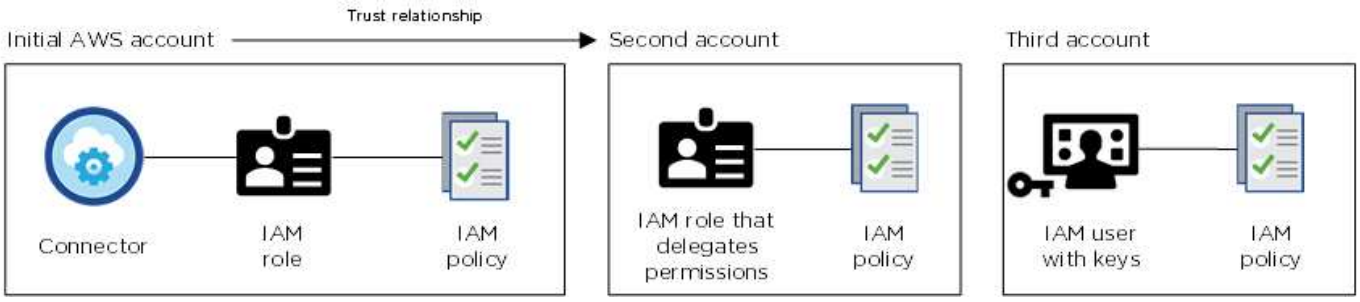
You might add additional AWS credentials to BlueXP in the following cases:

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

Review the sections below for more details.

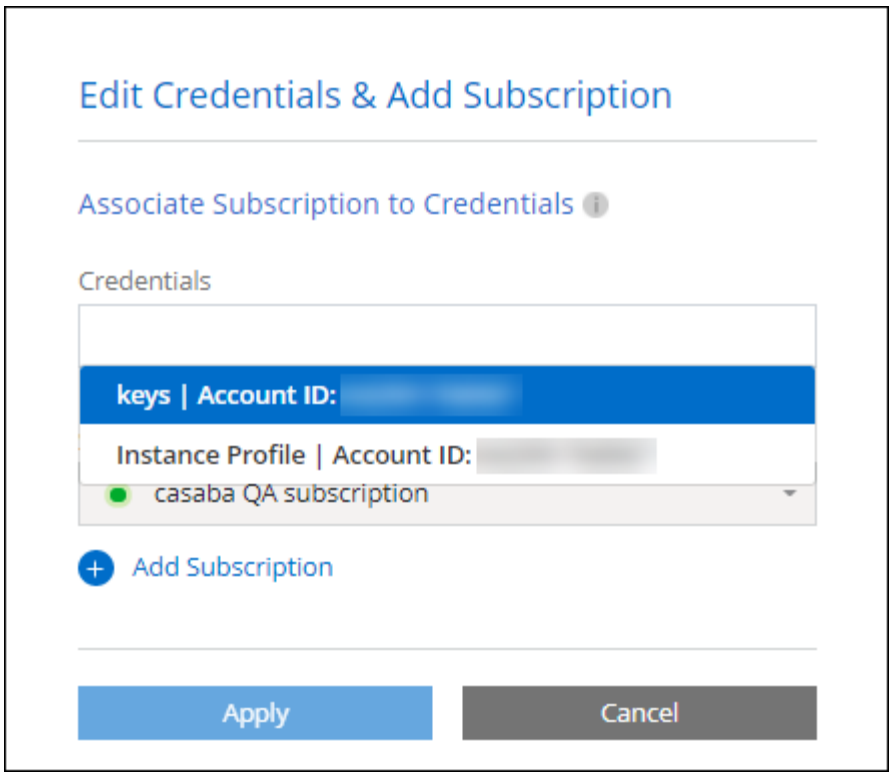
Add AWS credentials to use a Connector with another AWS account

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



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

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



Learn how to add AWS credentials to an existing Connector.

Add AWS credentials to create a Connector

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

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

Add AWS credentials for FSx for ONTAP

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

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

Credentials and marketplace subscriptions

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

Learn how to associate an AWS subscription.

Note the following about AWS credentials and marketplace subscriptions:

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

FAQ

The following questions are related to credentials and subscriptions.

How can I securely rotate my AWS credentials?

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

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

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

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

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

Learn how to associate an AWS subscription.

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

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

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

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

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

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

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

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

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

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

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

Manage AWS credentials and marketplace subscriptions for BlueXP

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

Overview

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

- Add additional AWS credentials to an existing Connector

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

- Add AWS credentials to BlueXP for creating a Connector

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

- Add AWS credentials to BlueXP for FSx for ONTAP

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

How to rotate credentials

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

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

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

Add additional credentials to a Connector

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

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

Grant permissions

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

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

Choices

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

Grant permissions by assuming an IAM role in another account

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

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

Steps

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

   Be sure to do the following:

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

Result

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

Grant permissions by providing AWS keys

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

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

Steps

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

   AWS Documentation: Creating IAM Policies

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

Result

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

Add the credentials

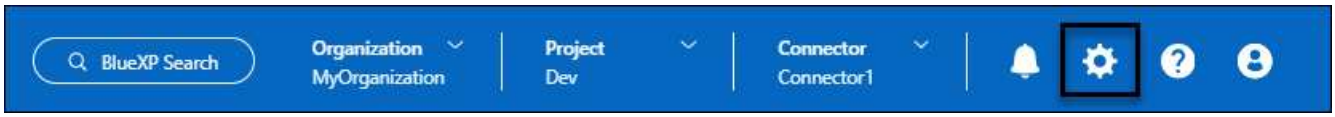
After you provide an AWS account with the required permissions, you can add the credentials for that account to an existing Connector. This enables you to launch Cloud Volumes ONTAP systems in that account using the same Connector.

Before you begin

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

Steps

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



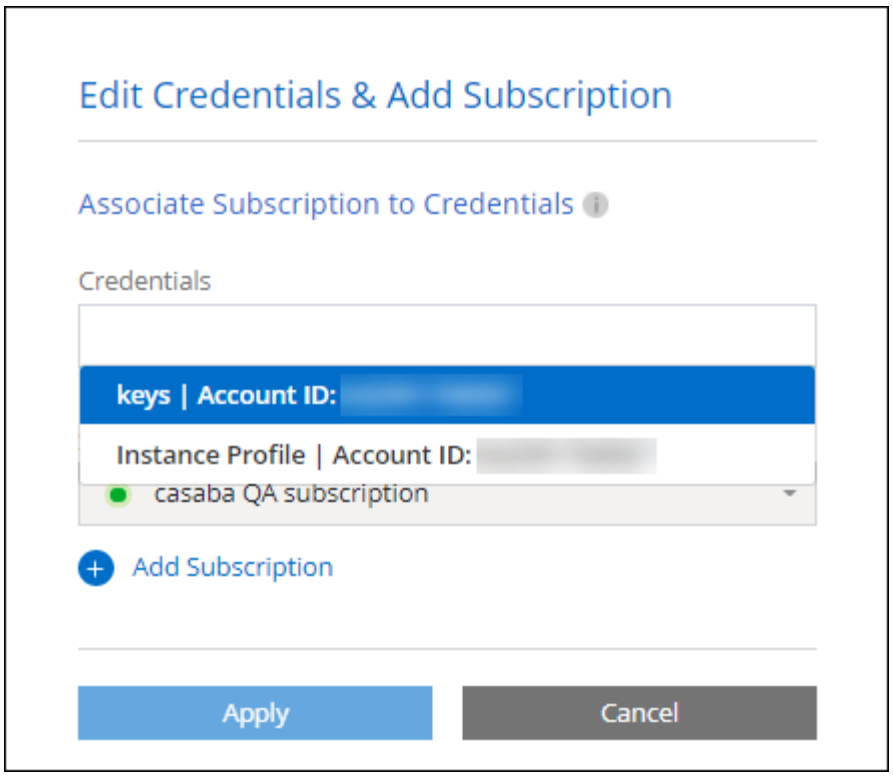
3. On the **Organization credentials** or **Account credentials** page, select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Amazon Web Services > Connector**.
   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of a trusted IAM role,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

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

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

Result

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



Add credentials to BlueXP for creating a Connector

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

Set up the IAM role

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

Steps

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

   Be sure to do the following:

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

     For example, the policy should look like this:

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

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

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

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

Result

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

Add the credentials

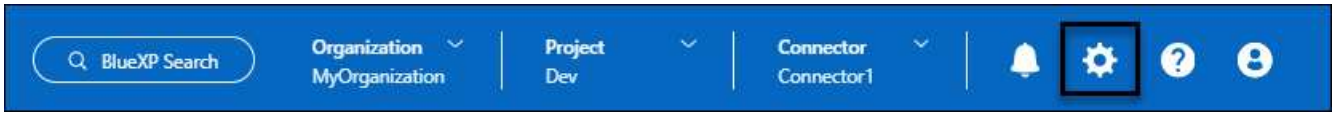
After you provide the IAM role with the required permissions, add the role ARN to BlueXP.

Before you begin

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

Steps

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



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

Add credentials to BlueXP for Amazon FSx for ONTAP

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

Configure an AWS subscription

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

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

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

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

Before you begin

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

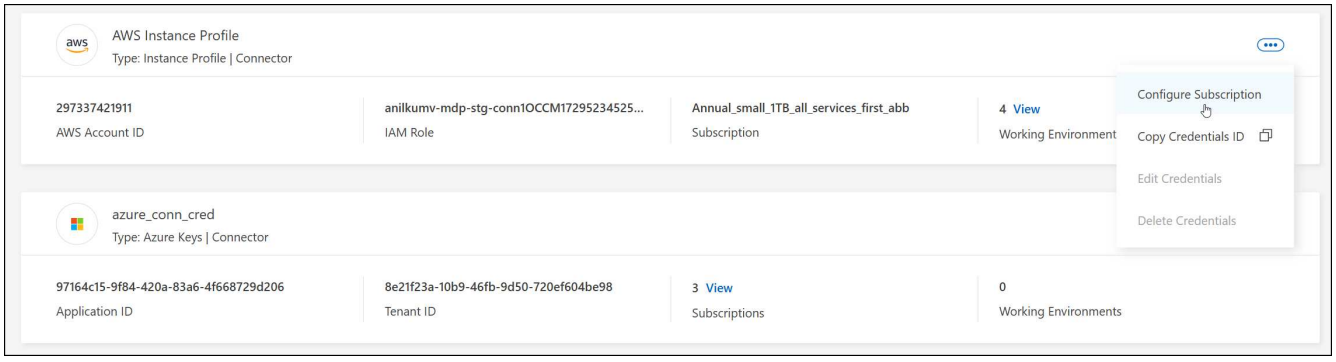
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

Subscribe to NetApp Intelligent Services from the AWS Marketplace

Steps

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

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



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

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

   You'll be redirected to the BlueXP website.

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

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

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

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

   - Select **Save**.

Associate an existing subscription with your organization or account

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

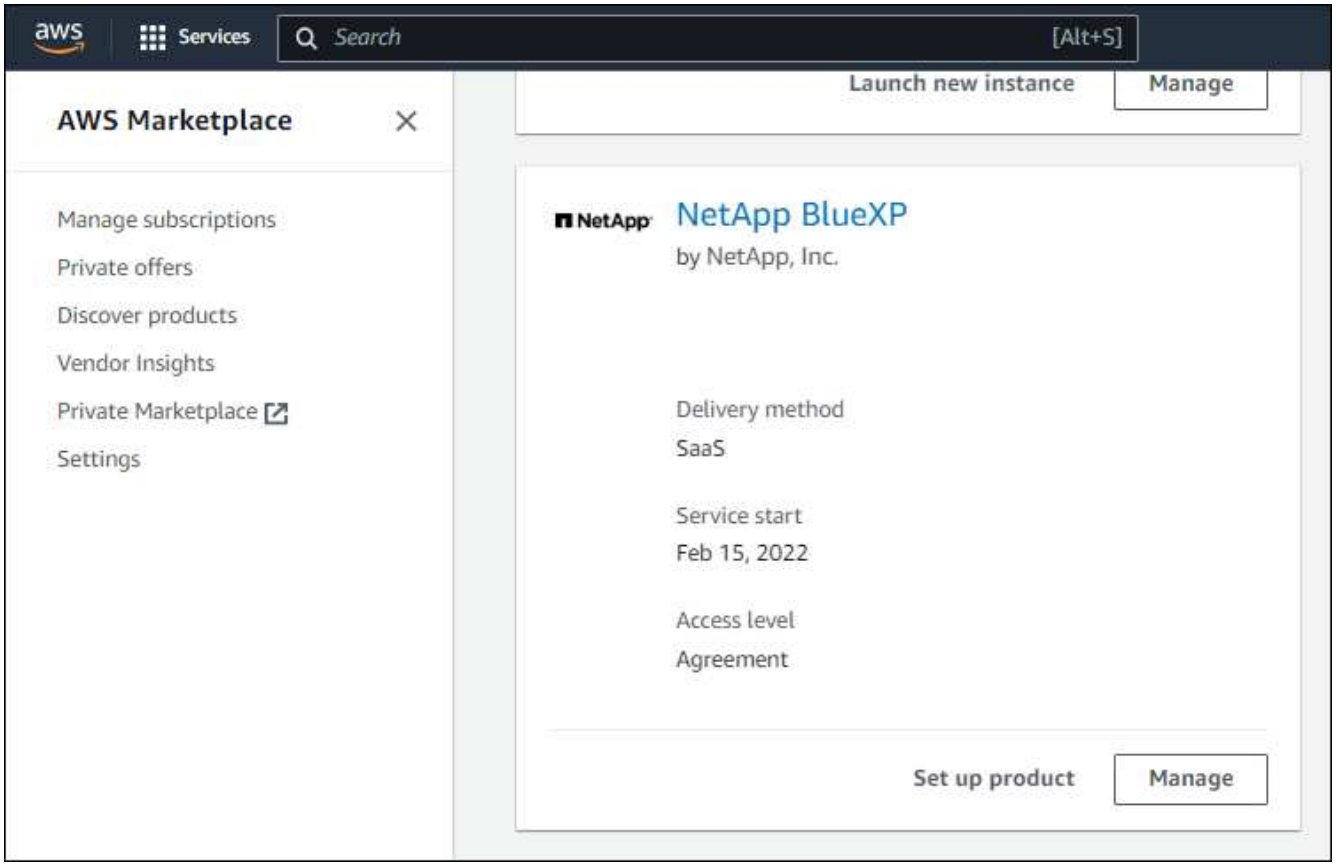
- Learn about BlueXP deployment modes
- Learn about BlueXP identity and access management

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

Steps

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

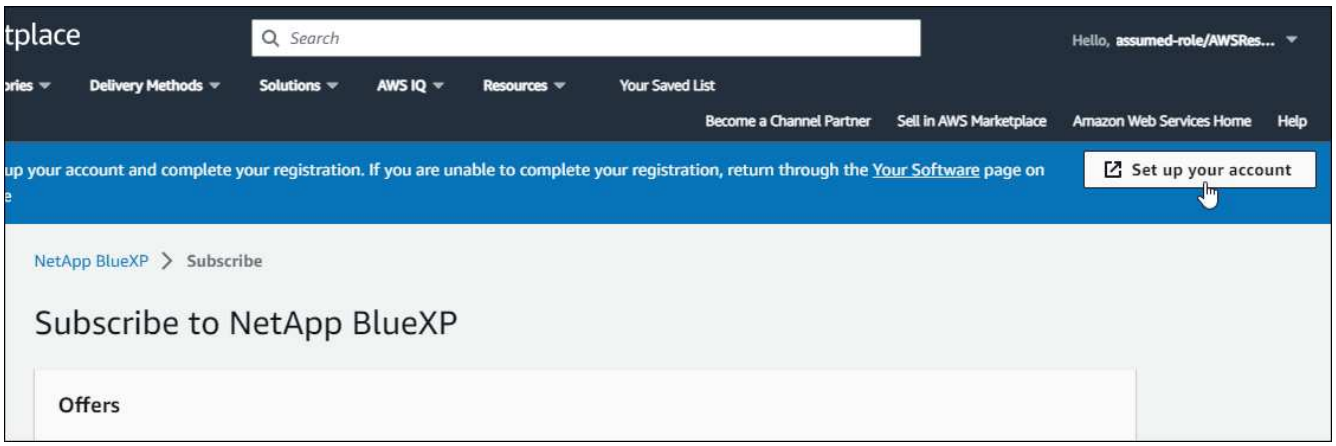
      You'll only see the subscriptions that are associated with the organization or account that you're currently viewing. If you don't see your subscription, proceed with the following steps.
2. Log in to the AWS Console and navigate to **AWS Marketplace Subscriptions**.
3. Find the NetApp Intelligent Data Services subscription.



4. Select **Set up product**.

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

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



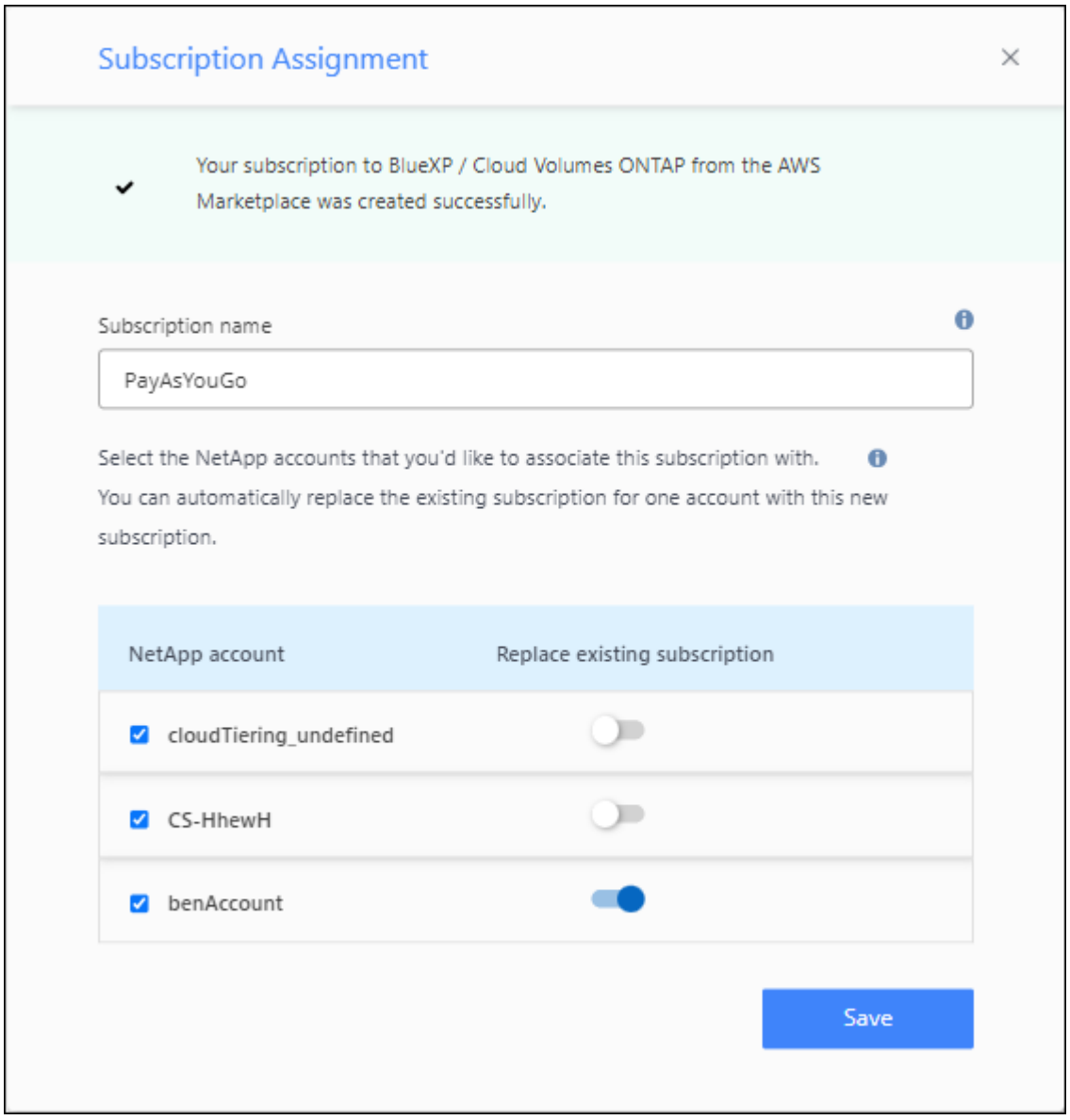
   The **Subscription Assignment** page on netapp.com should load in a new browser tab or window.

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

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

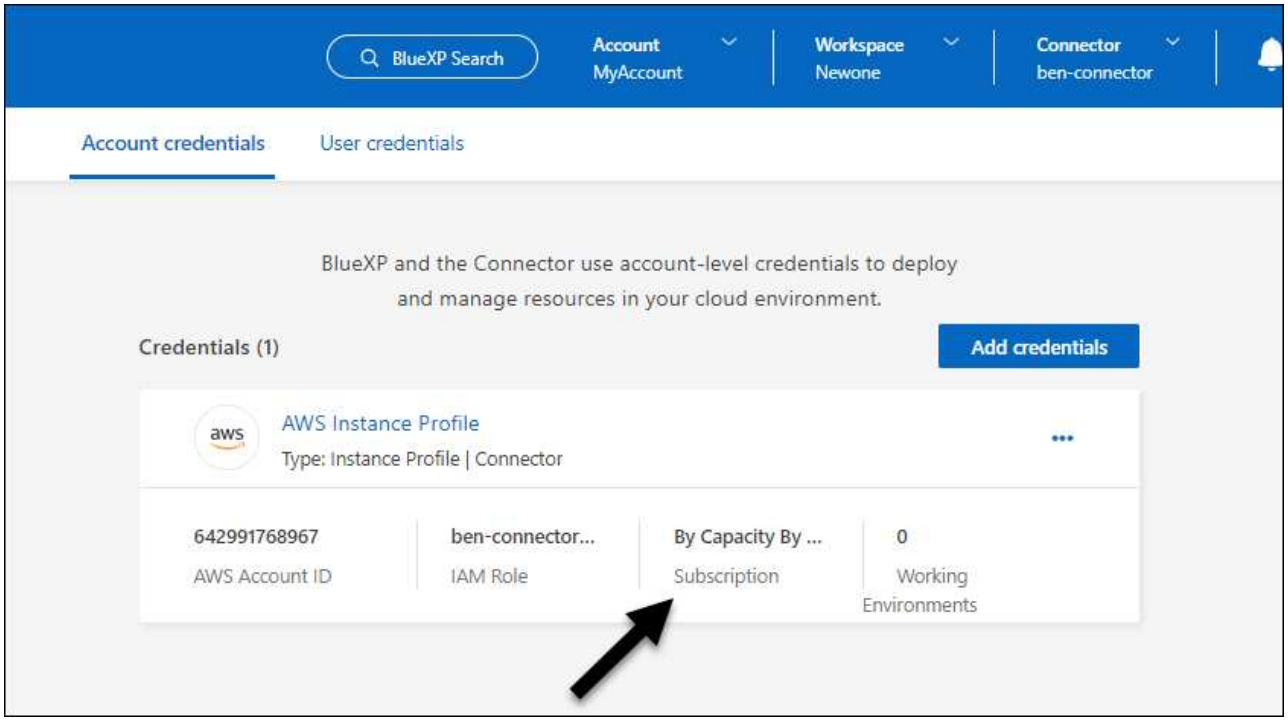
BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

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



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

Here's an example.



Edit credentials

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

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

Steps

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

Delete credentials

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

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

Steps

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

3. Select **Delete** to confirm.

Azure

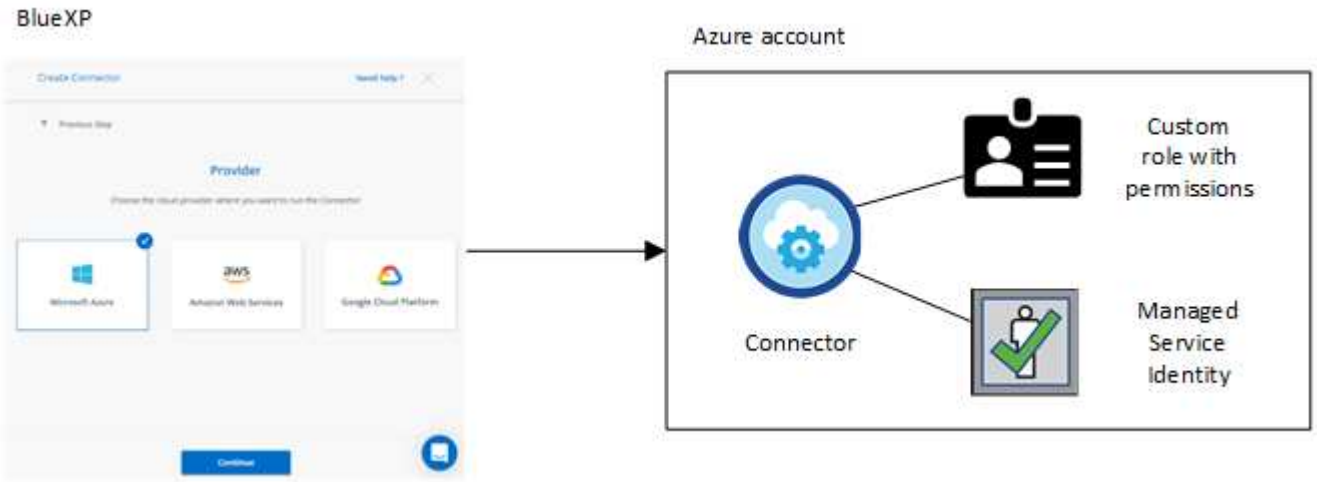
Learn about Azure credentials and permissions in BlueXP

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

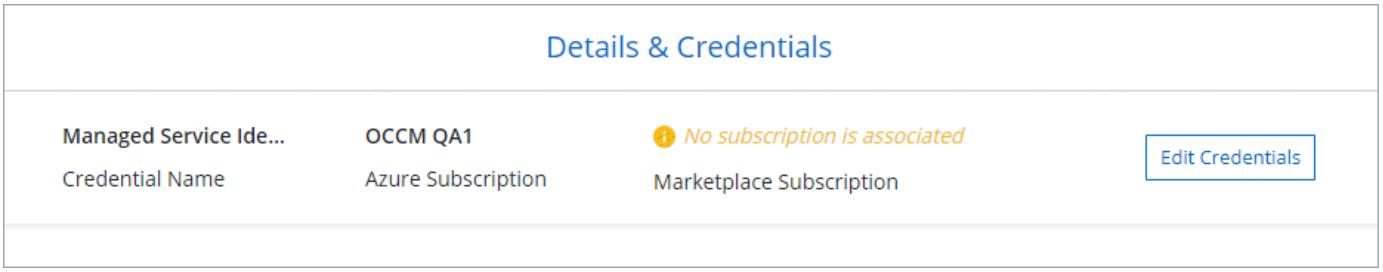
Initial Azure credentials

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

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



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



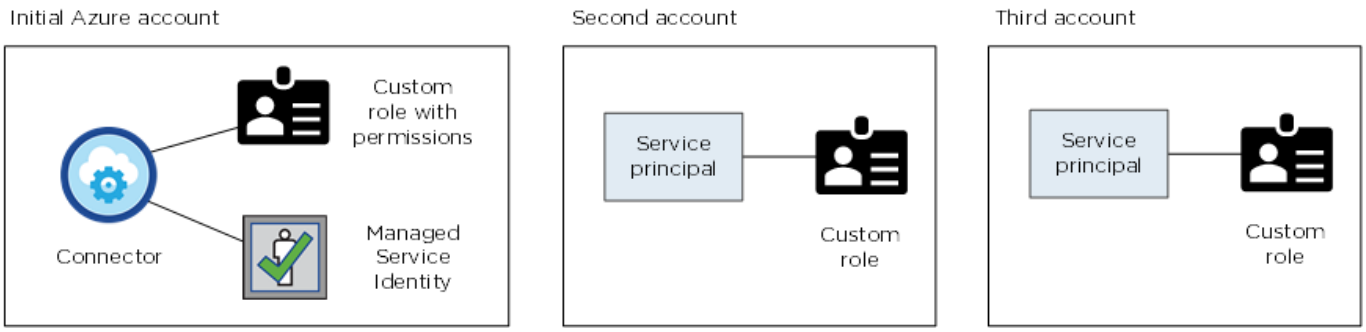
You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

Additional Azure subscriptions for a managed identity

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

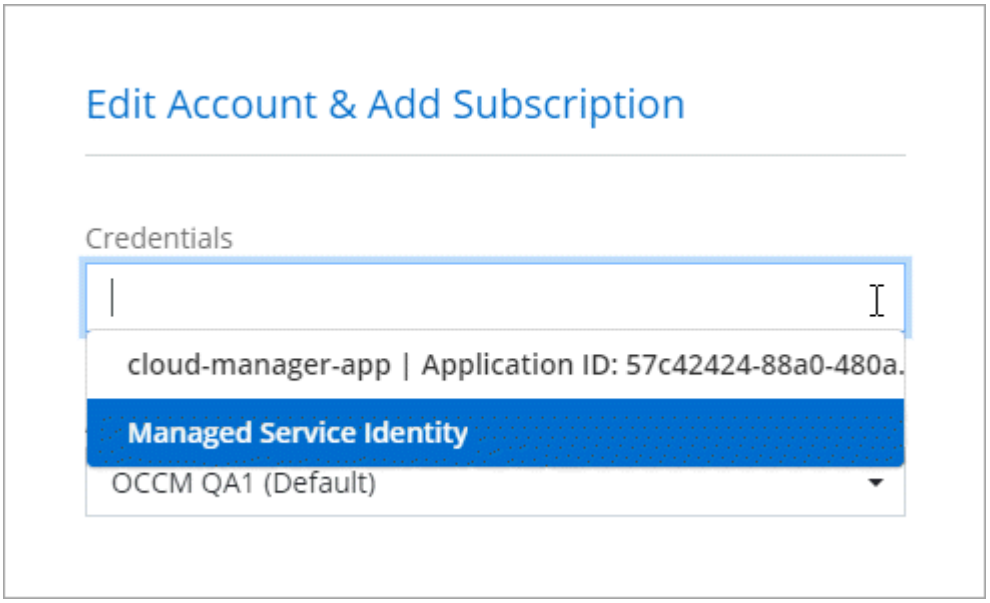
Additional Azure credentials

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



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

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



Credentials and marketplace subscriptions

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

Learn how to associate an Azure subscription.

Note the following about Azure credentials and marketplace subscriptions:

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

FAQ

The following question is related to credentials and subscriptions.

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

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

Learn how to associate an Azure subscription.

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

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

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

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

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

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

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

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

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

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

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

Manage Azure credentials and marketplace subscriptions for BlueXP

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

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

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

Overview

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

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

Associate additional Azure subscriptions with a managed identity

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

About this task

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

Steps

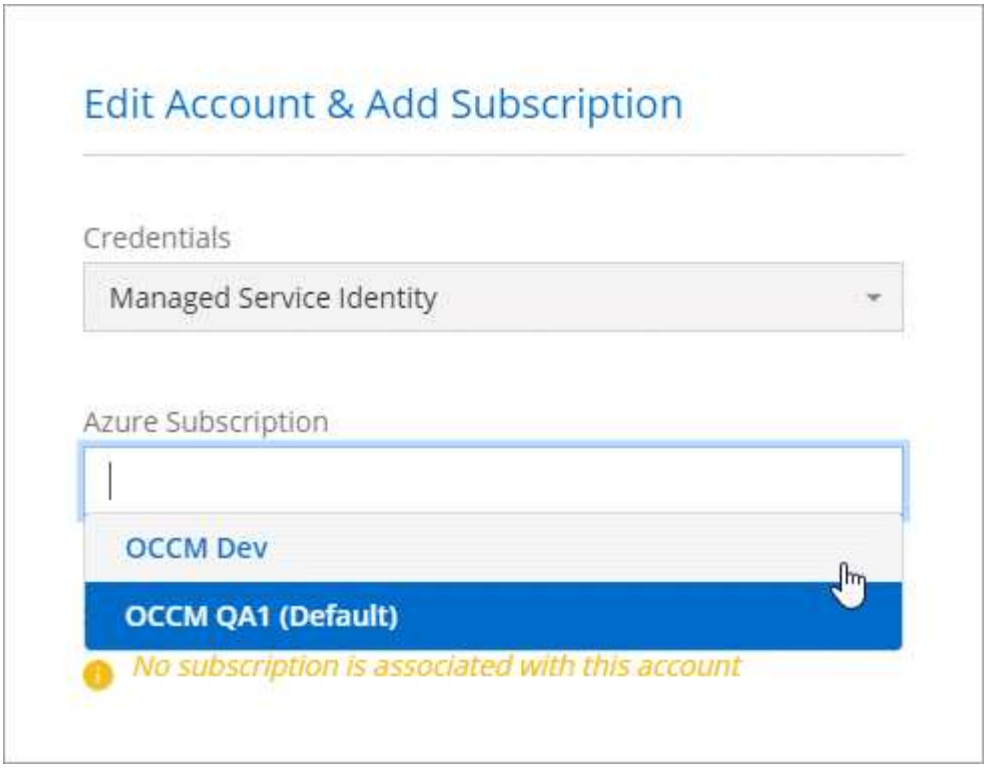
1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Select **Access control (IAM)**.
   a. Select **Add** > **Add role assignment** and then add the permissions:
      - Select the **BlueXP Operator**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

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

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

Result

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



Add additional Azure credentials to BlueXP

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

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

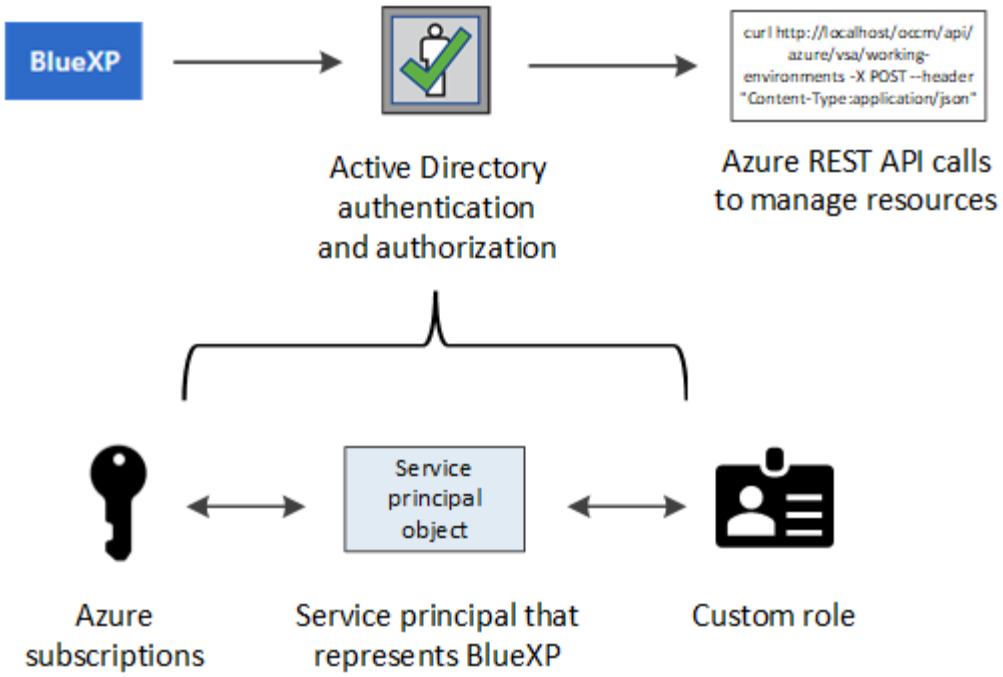
If you want to deploy Cloud Volumes ONTAP using *different* Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Microsoft Entra ID for each Azure account. You can then add the new credentials to BlueXP.

Grant Azure permissions using a service principal

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

About this task

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



Steps

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

Create a Microsoft Entra application

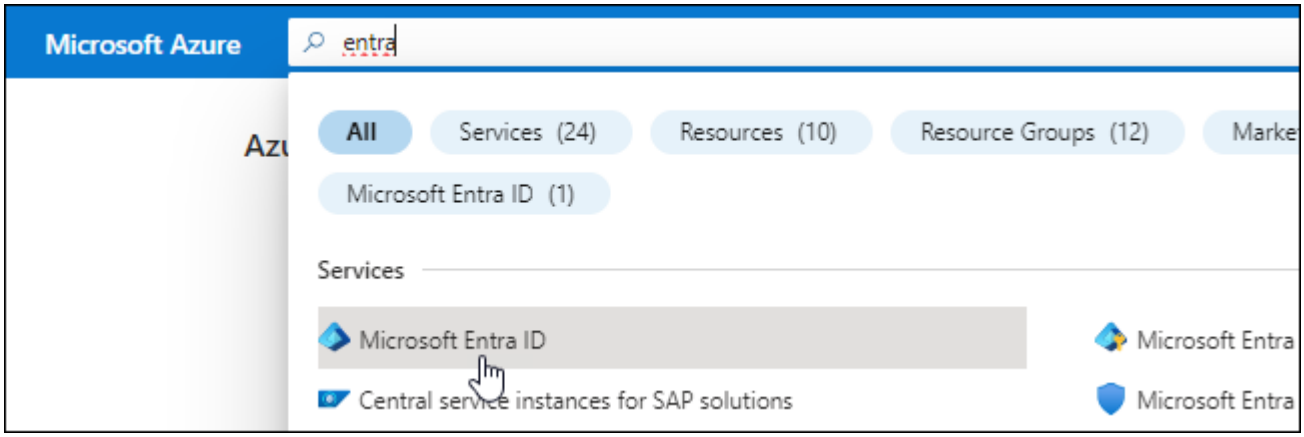
Create a Microsoft Entra application and service principal that BlueXP can use for role-based access control.

Steps

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

   For details, refer to Microsoft Azure Documentation: Required permissions

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



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

   You've created the AD application and service principal.

Result

You've created the AD application and service principal.

Assign the application to a role

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

Steps

1. Create a custom role:

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

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

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

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

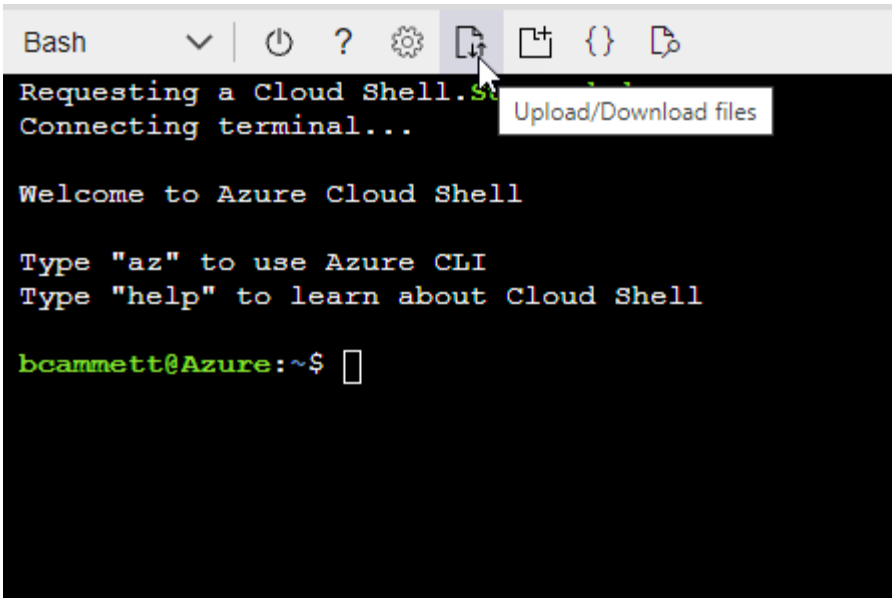
      Example

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

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

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

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

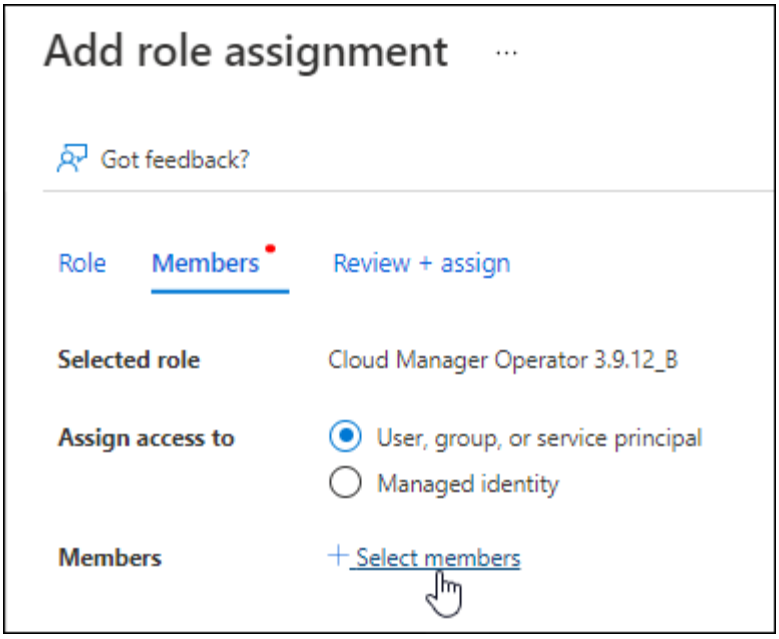


- Use the Azure CLI to create the custom role:

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

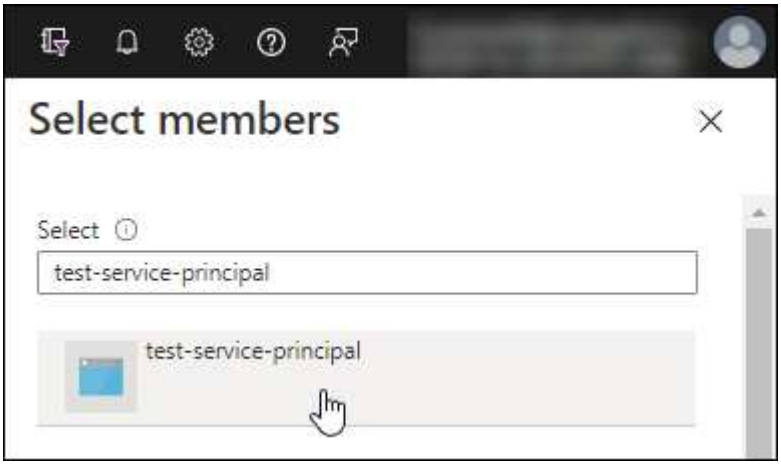
You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

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



- Search for the name of the application.

  Here's an example:



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

f. Select **Review + assign**.

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

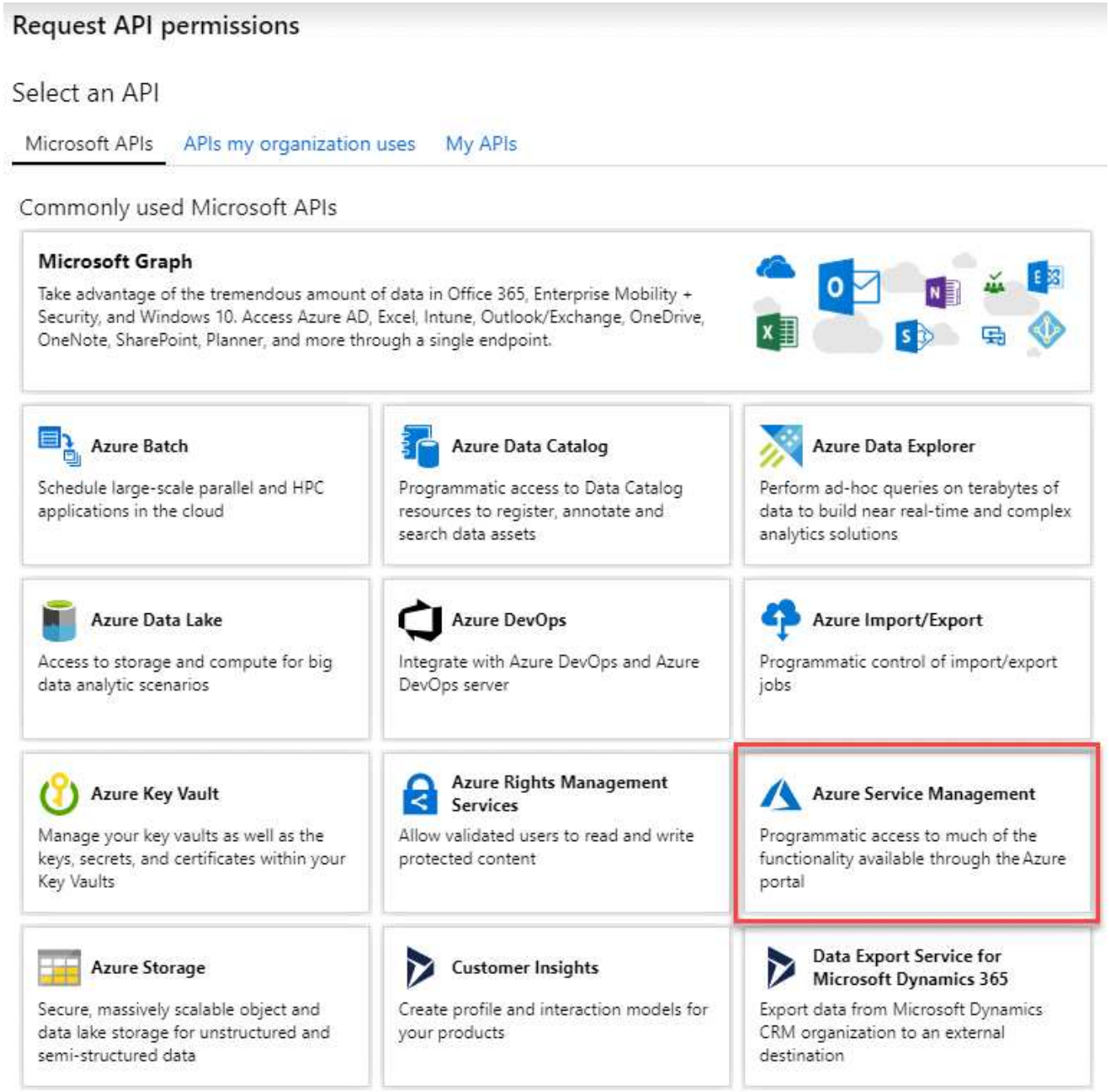
   If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

Add Windows Azure Service Management API permissions

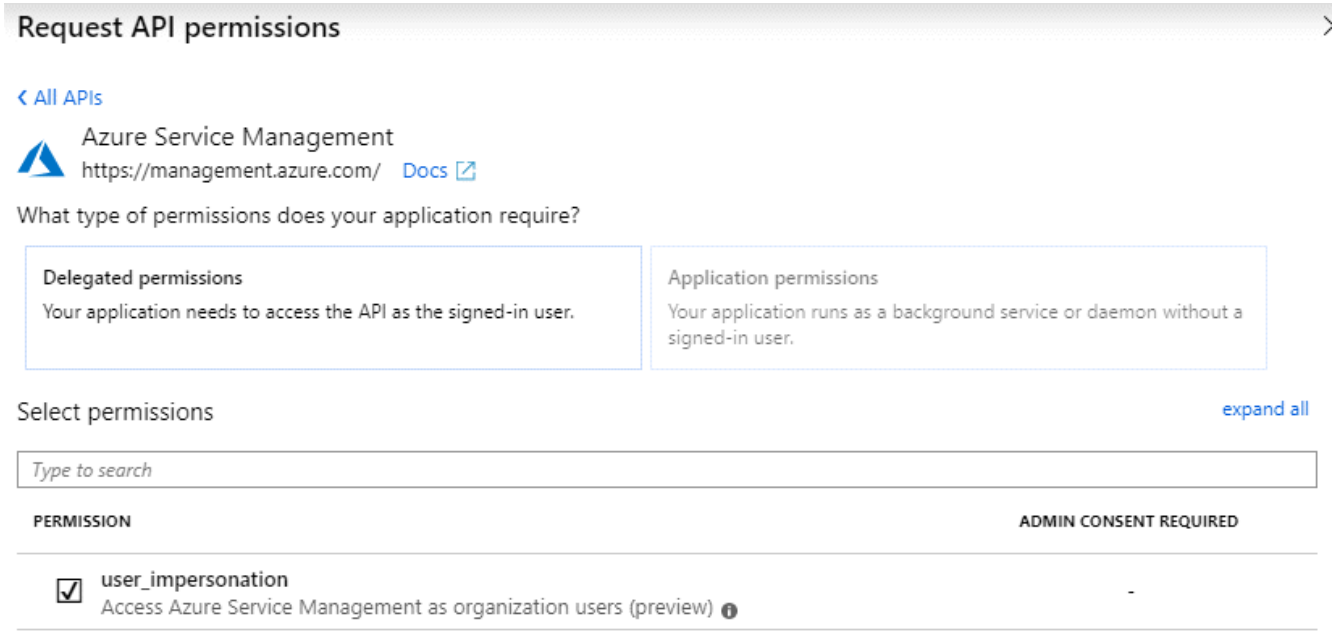
The service principal must have "Windows Azure Service Management API" permissions.

Steps

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



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

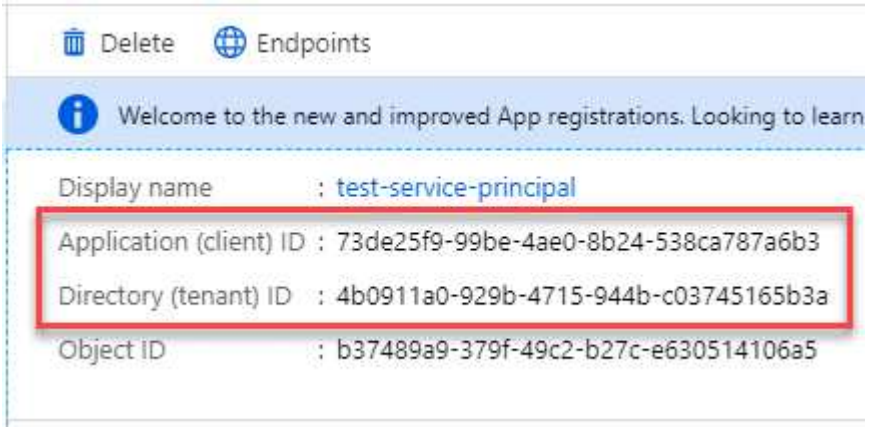


Get the application ID and directory ID

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

Steps

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



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

Create a client secret

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

Steps

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

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

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

Result

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

Add the credentials to BlueXP

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

Before you begin

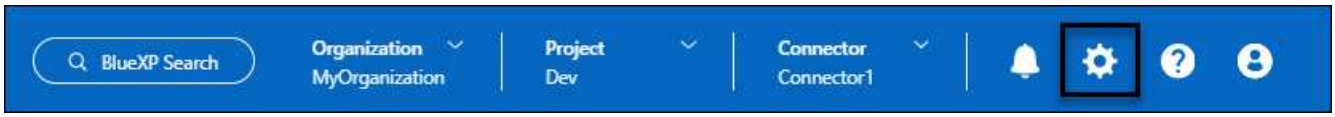
If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

Before you begin

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

Steps

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



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

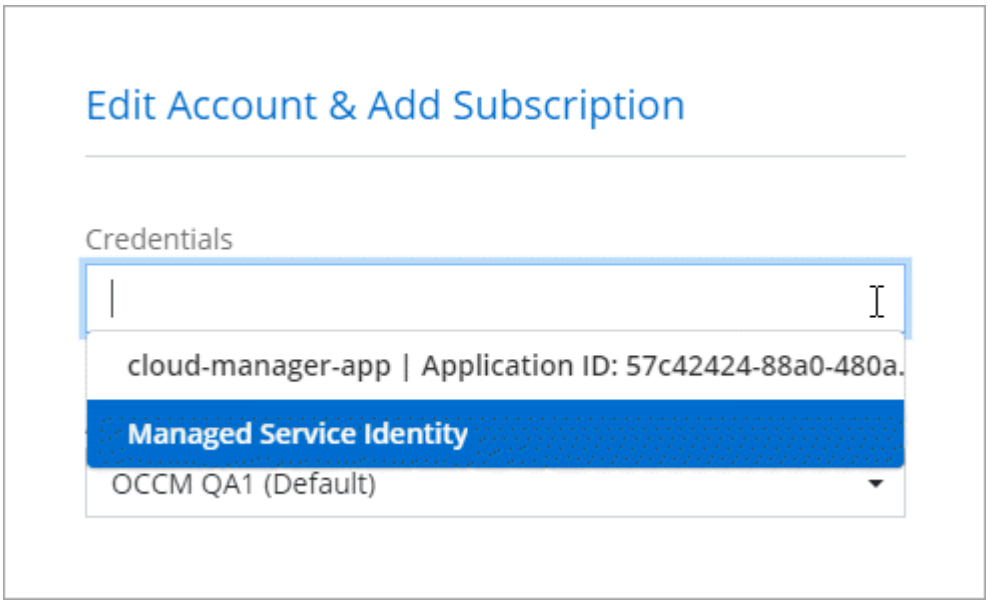
- Client Secret

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

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

Result

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



Manage existing credentials

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

Associate an Azure Marketplace subscription to credentials

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

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

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

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

Before you begin

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

Steps

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

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

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

      You'll be redirected to BlueXP.

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

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

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

      - Select **Save**.

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

        Subscribe to NetApp Intelligent Services from the Azure Marketplace

Edit credentials

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

Steps

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

Delete credentials

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

Steps

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

Google Cloud

Learn about Google Cloud projects and permissions

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

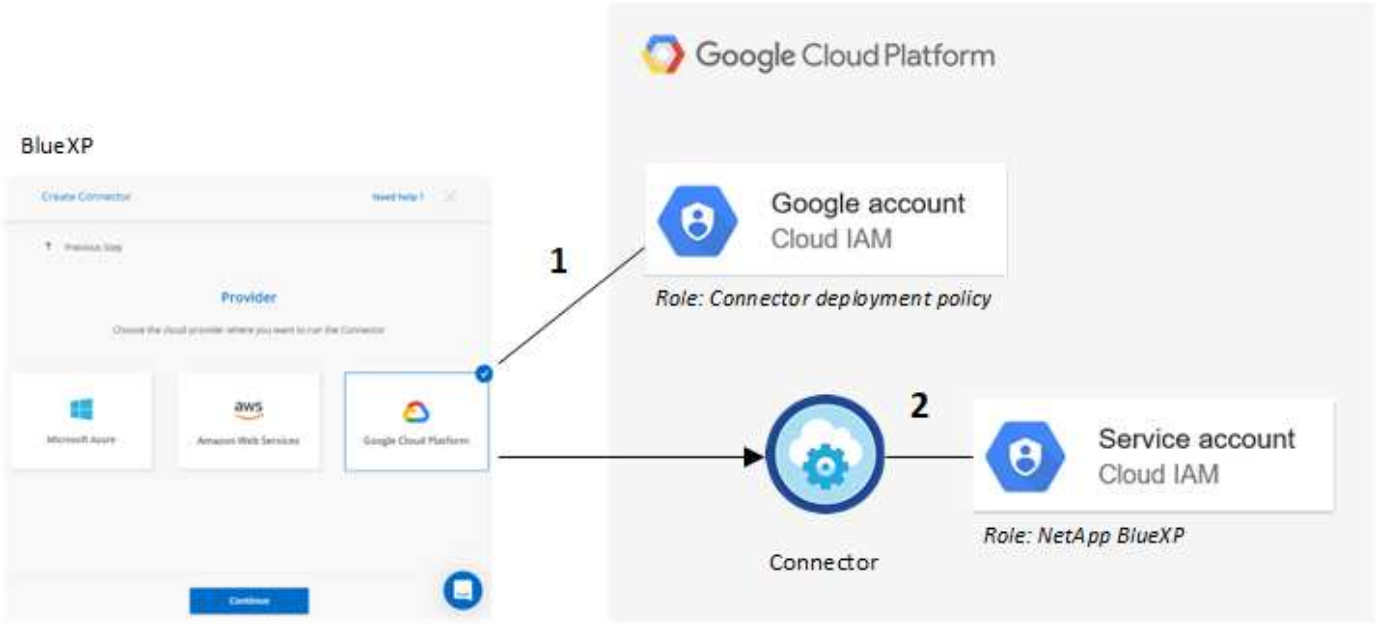
Project and permissions for BlueXP

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

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

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

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



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

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

Credentials and marketplace subscriptions

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

Learn how to associate a Google Cloud Marketplace subscription.

Note the following about Google Cloud credentials and marketplace subscriptions:

- Only one set of Google Cloud credentials can be associated with a Connector
- You can associate only one Google Cloud Marketplace subscription with the credentials
- You can replace an existing marketplace subscription with a new subscription

Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as the Connector, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Connector service account and role to that project.

- Learn how to set up the service account
- Learn how to deploy Cloud Volumes ONTAP in Google Cloud and select a project

Manage Google Cloud credentials and subscriptions for BlueXP

You can manage the Google Cloud credentials that are associated with the Connector

VM instance by associating a marketplace subscription and by troubleshooting the subscription process. Both of these tasks ensure that you can use your marketplace subscription to pay for data services.

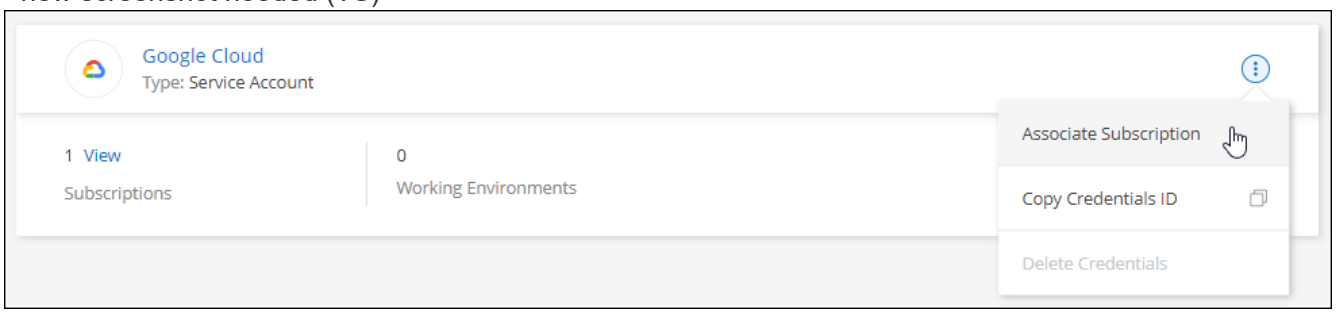
Associate a Marketplace subscription with Google Cloud credentials

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials that are associated with the Connector VM instance. At any time, you can change the Google Cloud Marketplace subscription that is associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other data services.

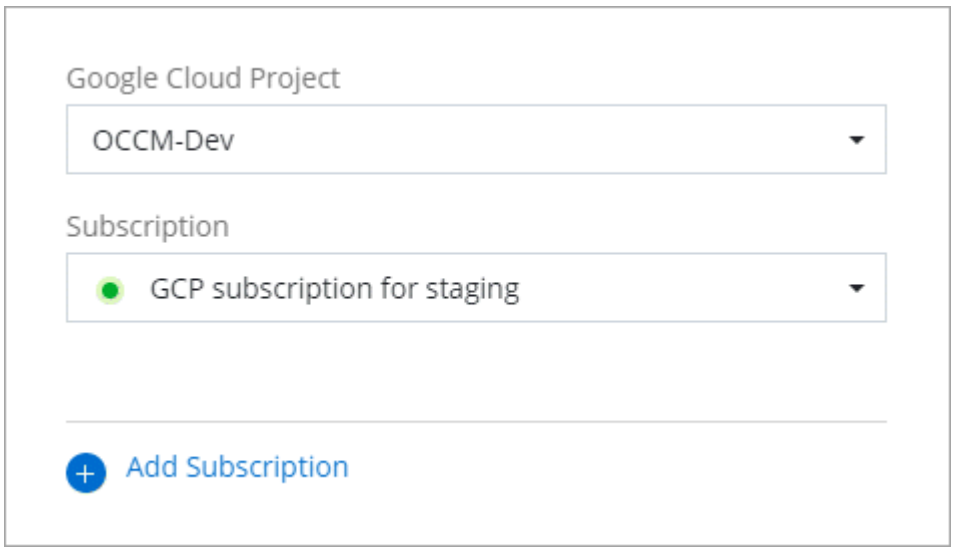
Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

Steps

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.
   +new screenshot needed (TS)



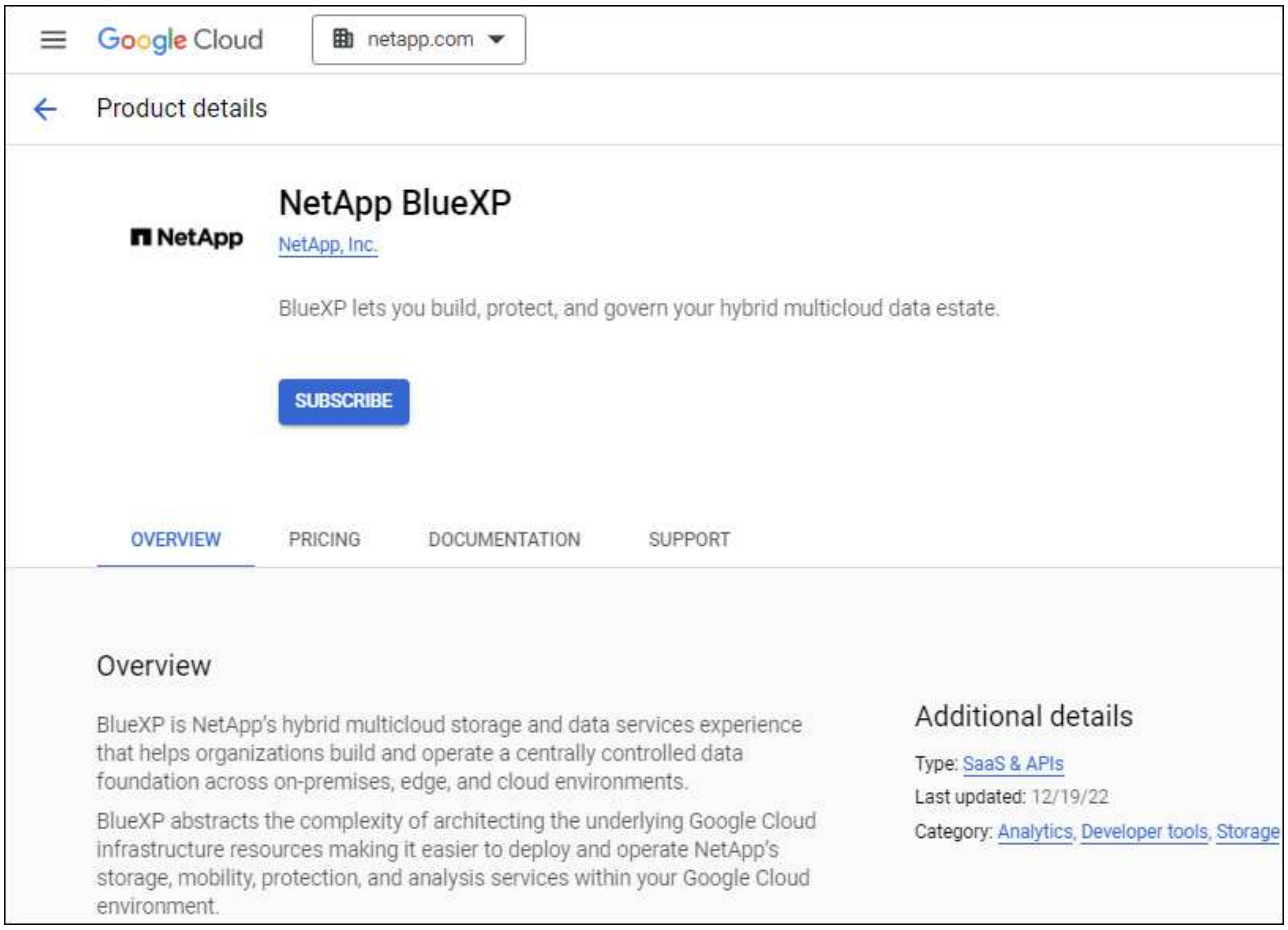
3. To configure an existing subscription with the selected credentials, select a Google Cloud project and subscription from the drop-down list, and then select **Configure**.



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

Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a BlueXP login.

a. After you're redirected to the NetApp Intelligent Services page on the Google Cloud Marketplace, ensure that the correct project is selected at the top navigation menu.



b. Select **Subscribe**.

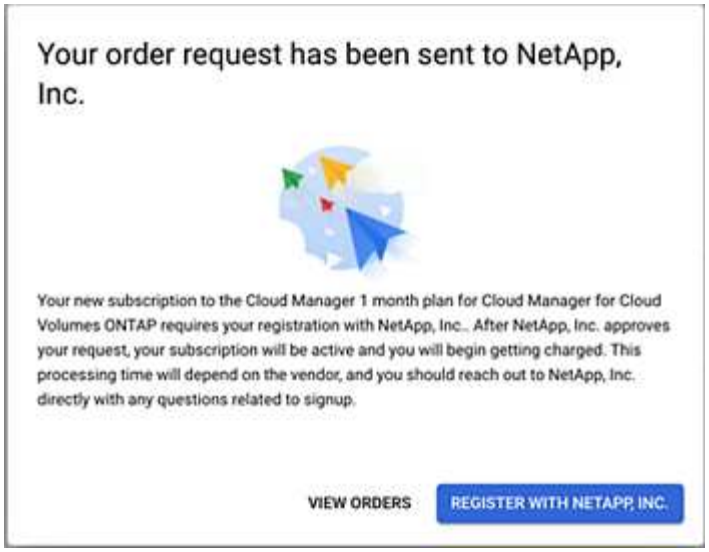
c. Select the appropriate billing account and agree to the terms and conditions.

d. Select **Subscribe**.

This step sends your transfer request to NetApp.

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

This step must be completed to link the Google Cloud subscription with your BlueXP organization or account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.



f. Complete the steps on the **Subscription Assignment** page:

> If someone from your organization has already subscribed to the NetApp BlueXP subscription from your billing account, then you will be redirected to the Cloud Volumes ONTAP page on the BlueXP website instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

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

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

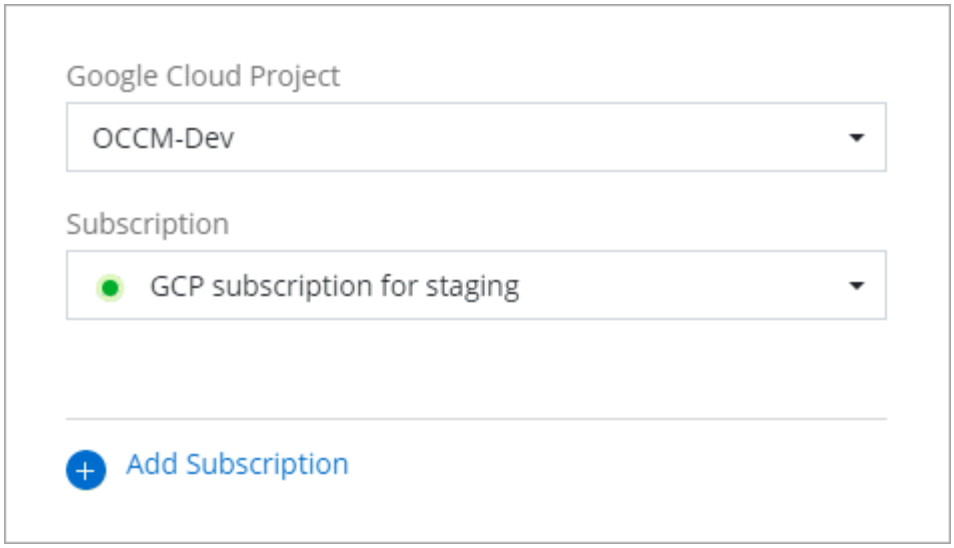
  For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

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

  Subscribe to BlueXP from the Google Cloud Marketplace

g. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.

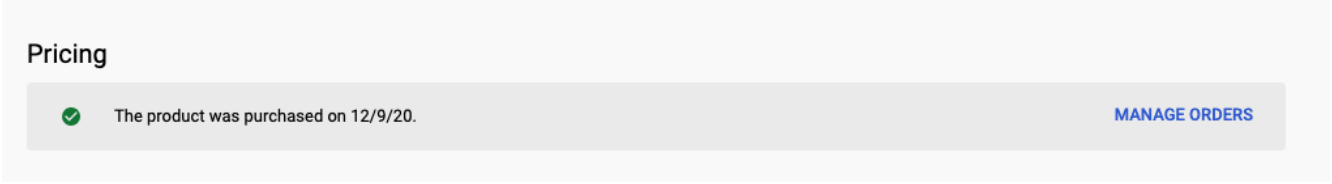


Troubleshoot the Marketplace subscription process

Sometimes subscribing to NetApp Intelligent Services through the Google Cloud Marketplace can become fragmented due to incorrect permissions or accidentally not following the redirection to the BlueXP website. If this happens, use the following steps to complete the subscription process.

Steps

1. Navigate to the NetApp BlueXP page on the Google Cloud Marketplace to check on the state of the order. If the page states **Manage on Provider**, scroll down and select **Manage Orders**.



   - 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.

   - 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.

Manage NSS credentials associated with BlueXP

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

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

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

Overview

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

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

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

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

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

- Upgrading Cloud Volumes ONTAP software to the latest release

These credentials are associated with your specific BlueXP account serial number. Users who belong to the BlueXP organization or account can access these credentials from **Support > NSS Management**.

Add an NSS account

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

When you have added your NSS account, BlueXP can use this information for things like license downloads, software upgrade verification, and future support registrations.

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

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

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management > Add NSS Account**.
3. Select **Continue** to be redirected to a Microsoft login page.
4. At the login page, provide your NetApp Support Site registered email address and password.

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

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

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

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

What's next?

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

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

Update NSS credentials

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

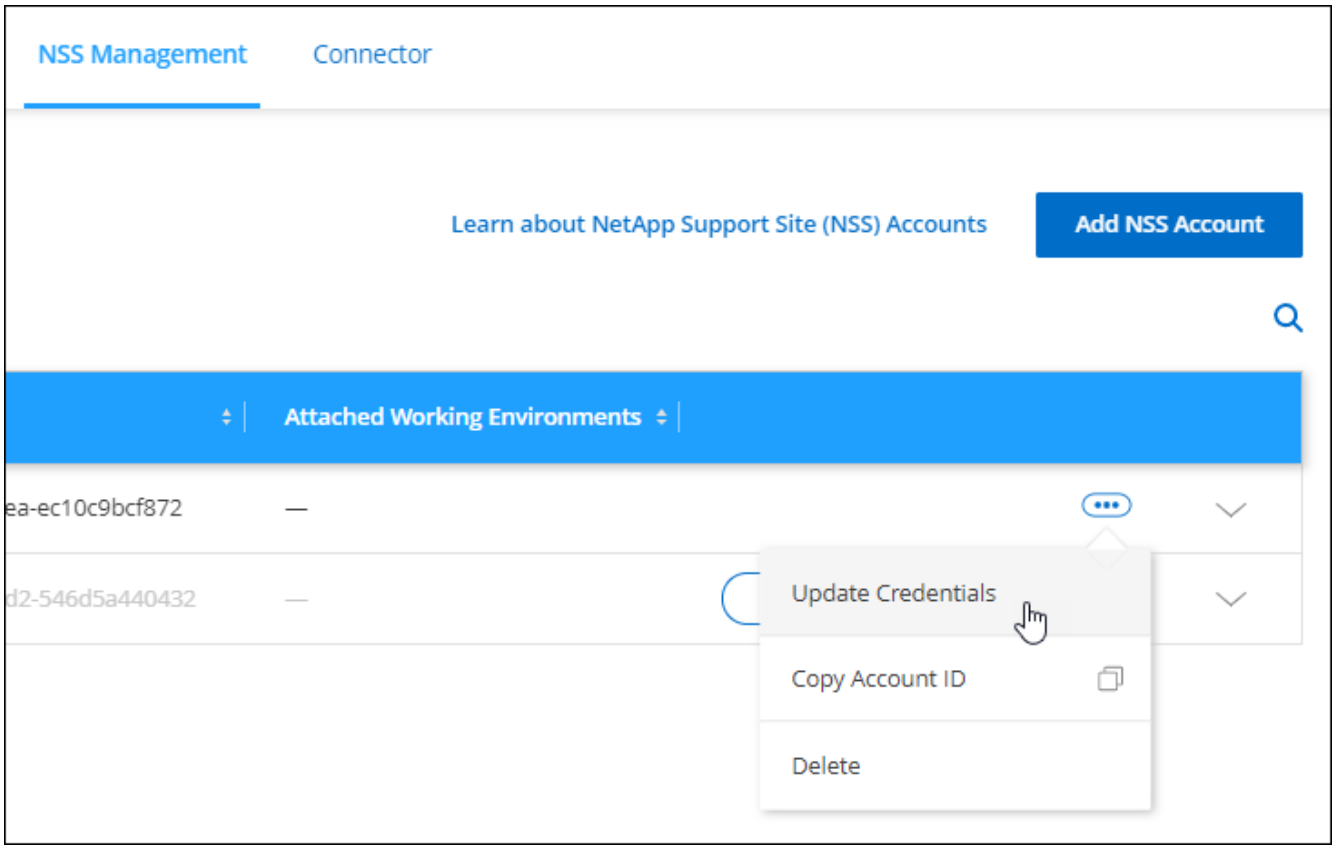
Expired credentials can disrupt the following, but are not limited to:

- License updates in digital wallet, which means you won't be able to take advantage of newly purchased capacity.
- Ability to submit and track support cases.

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

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ••• and then select **Update Credentials**.



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

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

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

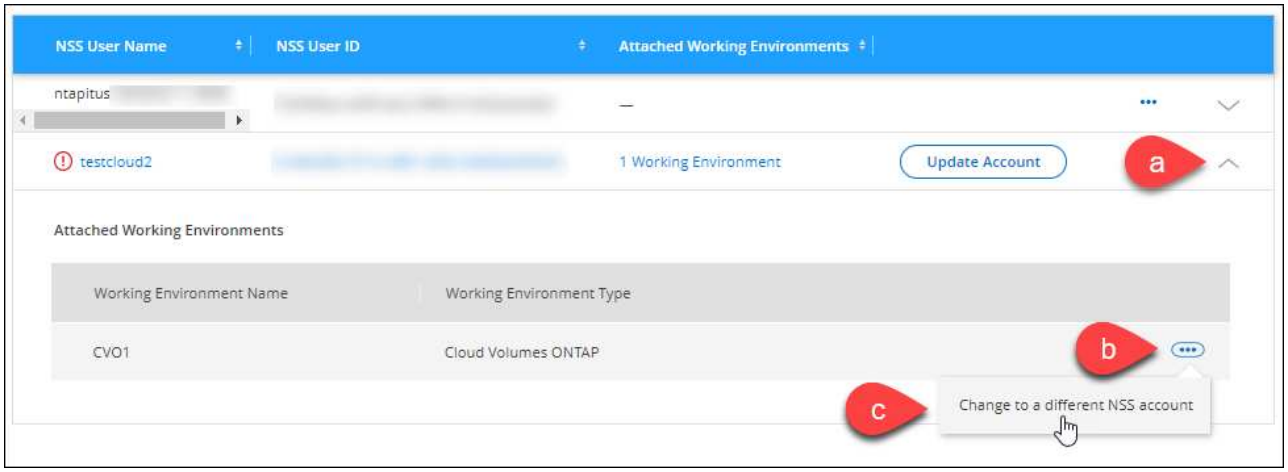
Attach a working environment to a different NSS account

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

You must first have associated the account with BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. Complete the following steps to change the NSS account:
   a. Expand the row for the NetApp Support Site account that the working environment is currently associated with.
   b. For the working environment that you want to change the association for, select •••
   c. Select **Change to a different NSS account**.



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

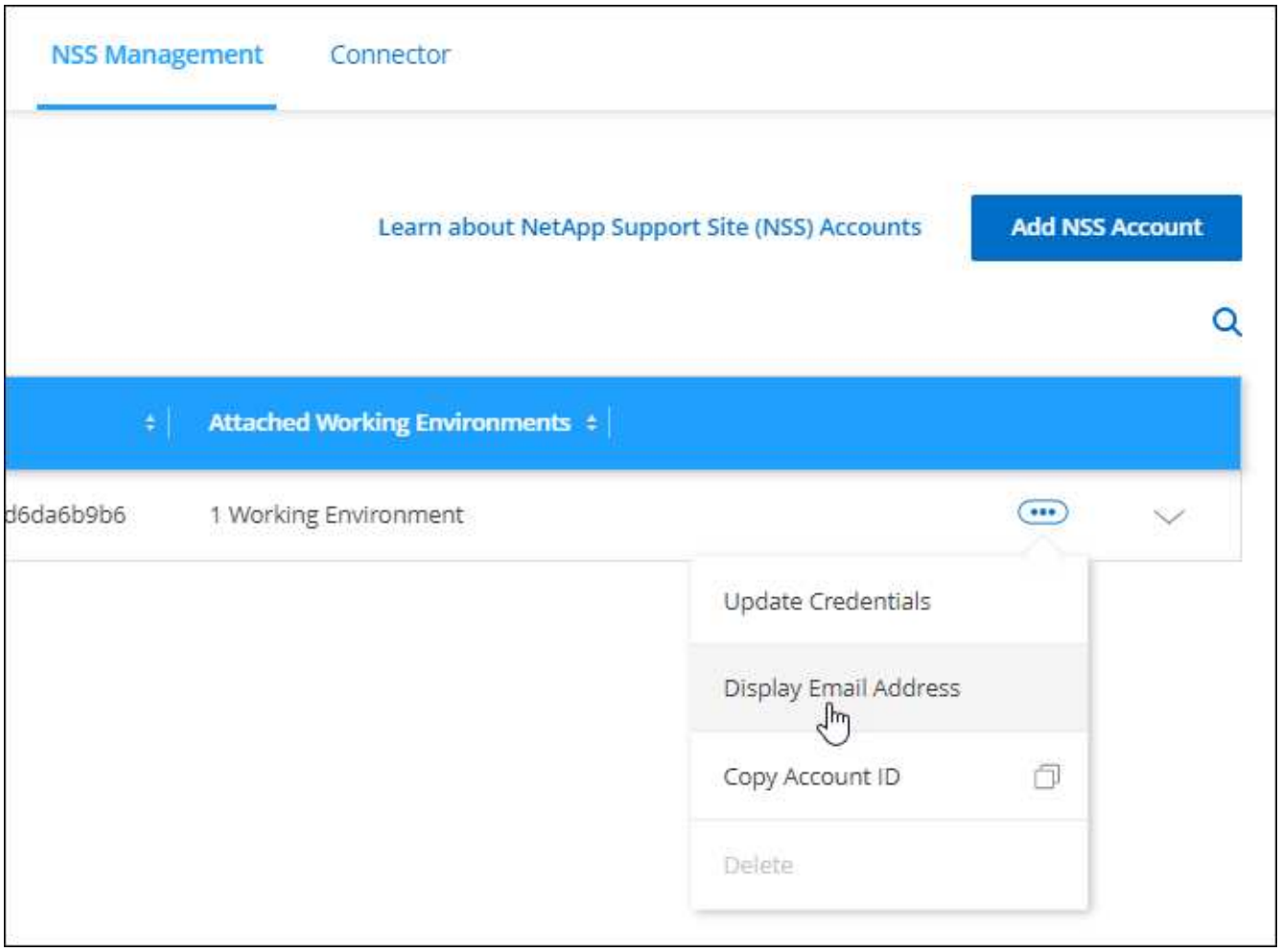
Display the email address for an NSS account

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

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

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ••• and then select **Display Email Address**. You can use the copy button to copy the email address.



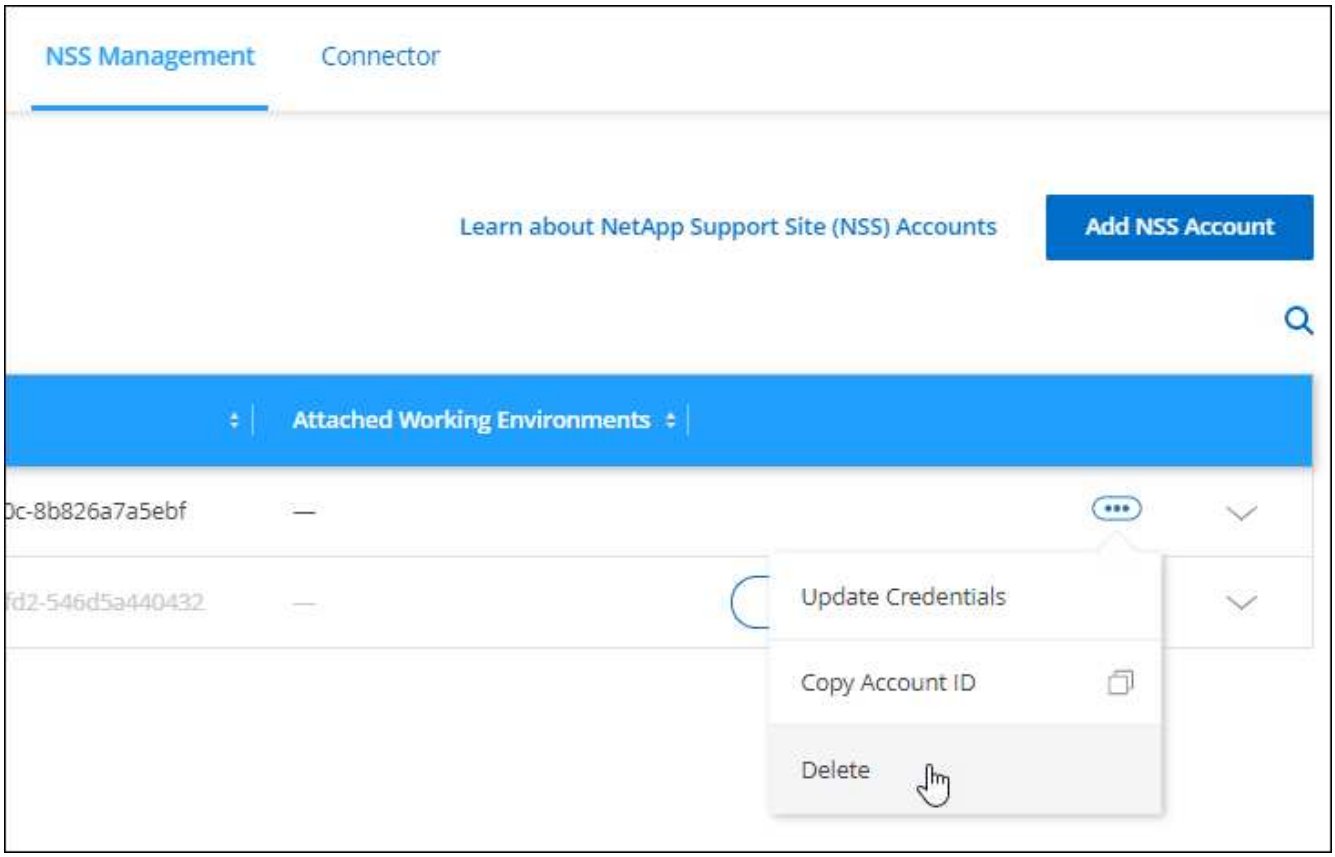
Remove an NSS account

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

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

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to delete, select ••• and then select **Delete**.



4. Select **Delete** to confirm.

Manage credentials associated with your BlueXP login

Depending on the actions that you've taken in BlueXP, you might have associated ONTAP credentials and NetApp Support Site (NSS) credentials with your BlueXP user login. You can view and manage those credentials in BlueXP after you've associated them. For example, if you change the password for these credentials, then you'll need to update the password in BlueXP.

ONTAP credentials

Users need ONTAP admin credentials to discover ONTAP clusters in BlueXP. However, ONTAP System Manager access depends on whether or not you are using a Connector.

Without a Connector

Users are prompted to enter their ONTAP credentials to access ONTAP System Manager for the cluster. Users can choose to save these credentials in BlueXP which means they won't be prompted to enter them each time. User credentials are only visible to the respective user and can be managed from the User credentials page.

With a Connector

By default, users are not prompted to enter their ONTAP credentials to access ONTAP System Manager. However, a BlueXP administrator (with the Organization admin role) can configure BlueXP to prompt users to enter their ONTAP credentials. When this setting is enabled, users need enter their ONTAP credentials each time.

Learn more.

NSS credentials

The NSS credentials associated with your BlueXP login enable support registration, case management, and access to Digital Advisor.

- When you access **Support > Resources** and register for support, you're prompted to associate NSS credentials with your BlueXP login.

  This registers your organization or account for support and activates support entitlement. Only one user in your BlueXP organization or account must associate a NetApp Support Site account with their BlueXP login to register for support and activate support entitlement. After this is completed, the **Resources** page shows that your account is registered for support.

  Learn how to register for support

- When you access **Support > Case Management**, you're prompted to enter your NSS credentials, if you haven't already done so. This page enables you to create and manage the support cases associated with your NSS account and with your company.
- When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials.

Note the following about the NSS account associated with your BlueXP login:

- The account is managed at the user level, which means it isn't viewable by other users who log in.
- There can be only one NSS account associated with Digital Advisor and support case management, per user.
- If you're trying to associate a NetApp Support Site account with a Cloud Volumes ONTAP working environment, you can only choose from the NSS accounts that were added to the BlueXP organization or account that you are a member of.

  NSS account-level credentials are different than the NSS account that's associated with your BlueXP login. NSS account-level credentials enable you to deploy Cloud Volumes ONTAP with BYOL, register PAYGO systems, and upgrade its software.

  Learn more about using NSS credentials with your BlueXP organization or account.

Manage your user credentials

Manage your user credentials by updating the user name and password or by deleting the credentials.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.
3. If you don't have any user credentials yet, you can select **Add NSS credentials** to add your NetApp Support Site account.
4. Manage existing credentials by choosing the following options from the Actions menu:
   - **Update credentials**: Update the user name and password for the account.
   - **Delete credentials**: Remove the account associated with your BlueXP user account.

Result

BlueXP updates your credentials, and you see the changes when accessing the ONTAP cluster, digital advisor, or the Case Management page.

Copyright information

Trademark information