



Credentials

Setup and administration

NetApp
April 13, 2023

Table of Contents

- Credentials 1
 - Manage AWS credentials 1
 - Manage Azure credentials 10
 - Manage Google Cloud credentials 24
 - Manage NSS credentials associated with a BlueXP account 30
 - Manage credentials associated with your BlueXP login 36

Credentials

Manage AWS credentials

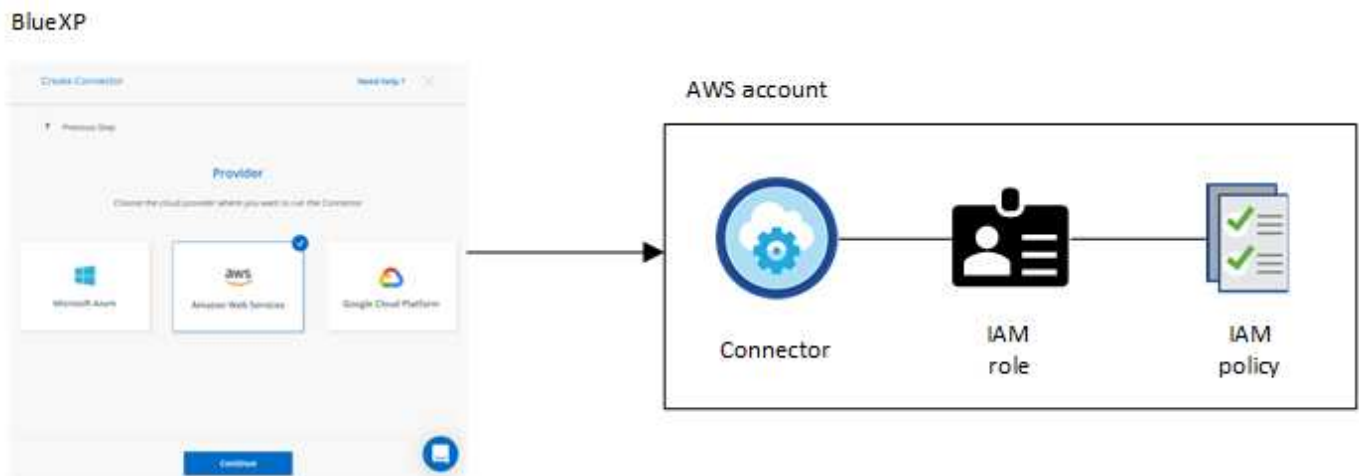
AWS credentials and permissions

You should understand how BlueXP uses AWS credentials and permissions so that you can manage credentials for one or more AWS accounts.

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](#).



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

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

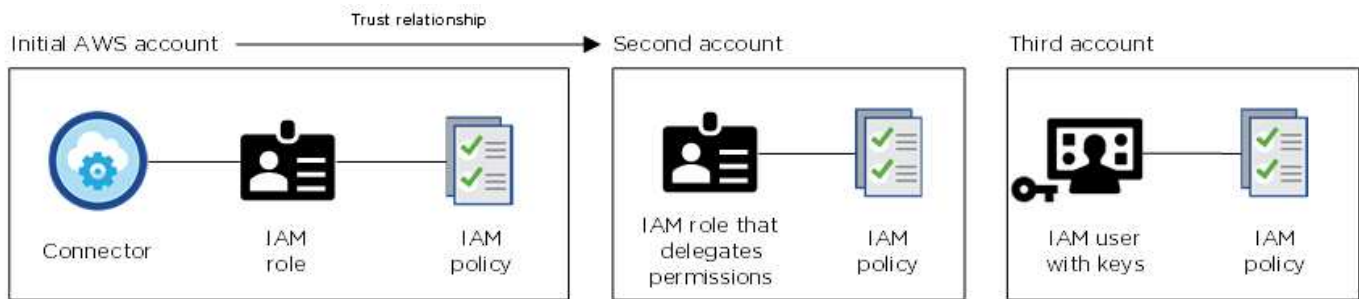
There are two ways to add additional AWS credentials:

- 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:

The screenshot shows the 'Edit Credentials & Add Subscription' dialog in BlueXP. It features a section titled 'Associate Subscription to Credentials' with an information icon. Below this is a 'Credentials' section containing a list of credentials. The first credential is 'keys | Account ID:' and the second is 'Instance Profile | Account ID:'. A dropdown menu is open, showing 'casaba QA subscription'. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

[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 get started

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 Cloud Volumes ONTAP at an hourly rate (PAYGO) or with an annual contract, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.
 - 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 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 get started

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.

What you'll need

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. On the **Account credentials** page, select the action menu for a set of credentials and then select **Associate Subscription**.



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

You'll be redirected to the BlueXP website.

- d. From the **Subscription Assignment** page:
 - Select the BlueXP 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.

- Select **Save**.

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

► https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video_subscribing_aws.mp4

(video)

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

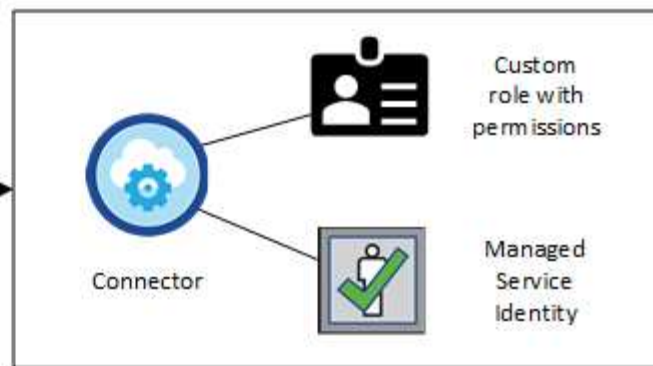
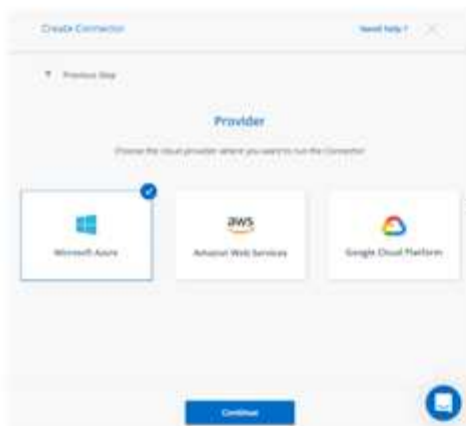
Azure credentials and permissions

You should understand how BlueXP uses Azure credentials and permissions so that you can manage credentials for one or more Azure subscriptions.

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](#).



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

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.

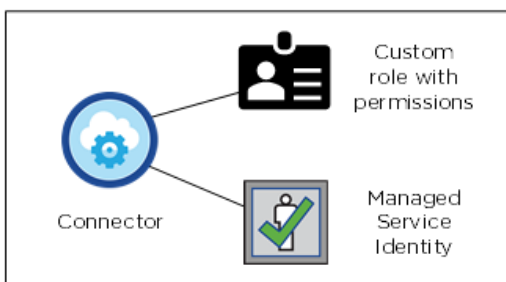
Additional Azure subscriptions for a managed identity

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](#).

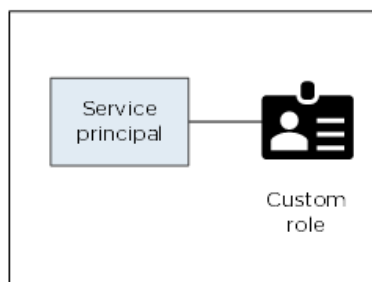
Additional Azure credentials

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:

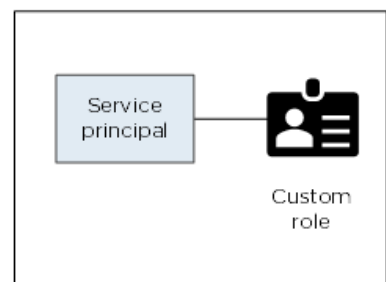
Initial Azure account



Second account

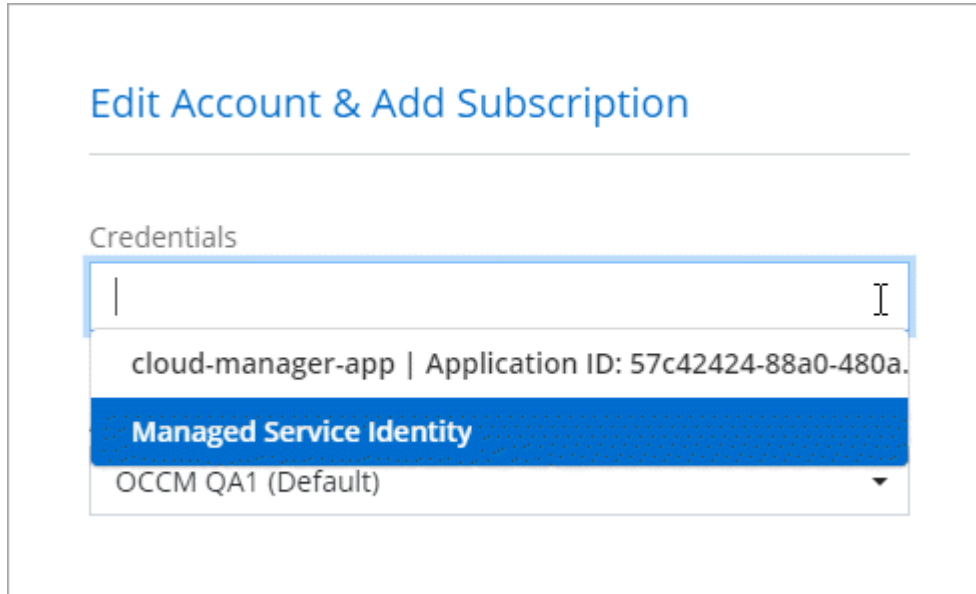


Third account



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.

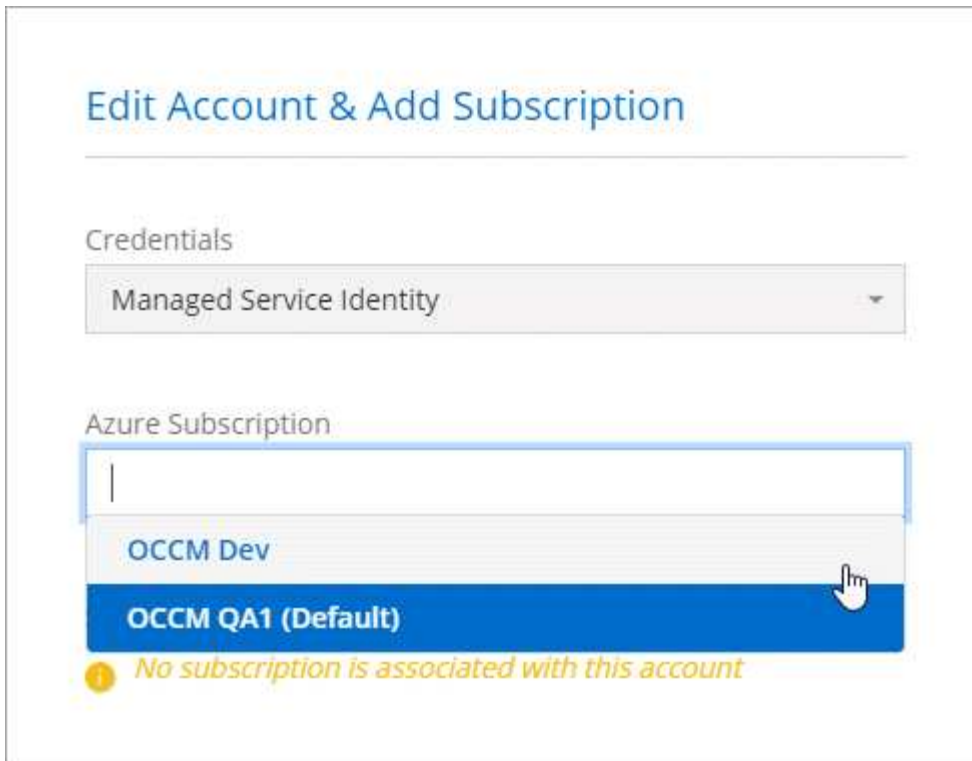


BlueXP Operator is the default name provided in the Connector policy. If you chose a different name for the role, then select that name instead.

- 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

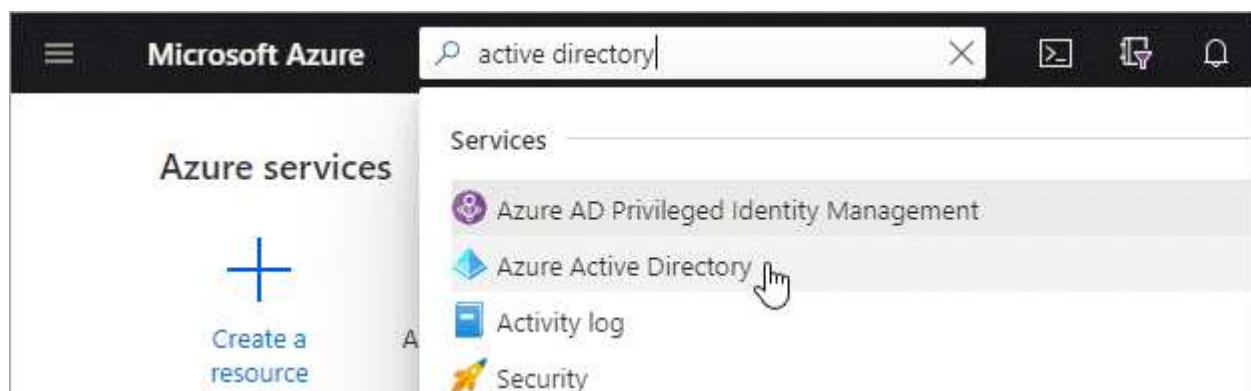
Create an Azure Active Directory (AD) application and service principal that BlueXP can use for role-based access control.

Before you begin

You must have the right 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](#).

Steps

1. From the Azure portal, open the **Azure Active Directory** service.



2. In the menu, select **App registrations**.
3. Select **New registration**.
4. 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.
5. Select **Register**.

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:
 - a. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
 - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

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

Example

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

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

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

- Start [Azure Cloud Shell](#) and choose the Bash environment.
- Upload the JSON file.



- Use the Azure CLI to create the custom role:

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

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

2. Assign the application to the role:

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

Add role assignment ...

[Got feedback?](#)

Role **Members** [Review + assign](#)

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Search for the name of the application.

Here's an example:

Select members ×

Select ⓘ

test-service-principal

test-service-principal

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

f. Select **Review + assign**.

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

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

Add Windows Azure Service Management API permissions

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

Steps

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

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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

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

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

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<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, select **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



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. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.

4. Provide a description of the secret and a duration.
5. Select **Add**.
6. Copy the value of the client secret.

Client secrets

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

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

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 get started

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.

What you'll need

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

Steps

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



2. On the **Account credentials** page, select **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: See [Get the application ID and directory ID](#).
 - Directory (tenant) ID: See [Get the application ID and directory ID](#).
 - Client Secret: See [Create a client secret](#).
 - c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO), these Azure credentials must be associated with a subscription from the Azure Marketplace.

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

What you'll need

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

Steps

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



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

You'll be redirected to the BlueXP website.

- e. From the **Subscription Assignment** page:
 - Select the BlueXP 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.

- Select **Save**.

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

► <https://docs.netapp.com/us-en/cloud-manager-setup->

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

You should understand how BlueXP uses Google Cloud credentials and permissions so that you can manage credentials for one or more Google Cloud projects.

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 on your behalf. 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 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.

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, 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 **Associate Subscription**.



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

 A screenshot of the Google Cloud console configuration page. It shows 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 circle icon. Below these dropdowns is a blue button with a plus sign and the text 'Add Subscription'.

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



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

- a. After you're redirected to the [NetApp BlueXP page on the Google Cloud Marketplace](#), ensure that the correct project is selected at the top navigation menu.

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, there are four tabs: 'OVERVIEW' (which is selected and underlined), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'Overview' section contains two paragraphs: 'BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.' and 'BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment.' To the right of the overview text, under the heading 'Additional details', there is information about the product type ('SaaS & APIs'), the last update date ('12/19/22'), and categories ('Analytics', 'Developer tools', 'Storage').

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

This step sends your transfer request to NetApp.

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

This step must be completed to link the Google Cloud subscription 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.

- Select **Save**.

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

► <https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video-subscribing-google->

[cloud.mp4](#) (video)

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

Google Cloud Project

OCCM-Dev

Subscription



GCP subscription for staging

 Add Subscription

Troubleshoot the Marketplace subscription process

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

Steps

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




Pricing



The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- If the order shows a green check mark and this is unexpected, somebody else from the organization using the same billing account might already be subscribed. If this is unexpected or you require the details of this subscription, contact your NetApp sales team.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc... 	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	

- If the order shows a clock and **Pending** status, go back to the marketplace page and choose **Manage on Provider** to complete the process as documented above.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
⌚	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

Manage NSS credentials associated with a BlueXP account

Provide the credentials for your NetApp Support Site (NSS) accounts to register for support, enable key workflows for Cloud Volumes ONTAP, and more. 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:

- Registering for support
- Creating support cases
- 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, when registering existing Cloud Volumes ONTAP systems, and when registering for support.

- [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 enables access to Digital Advisor and case management capabilities.

- When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials.
- 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 manage the support cases associated with your NSS account and with your company.

Note the following about the NSS account:

- The account is managed at the user level, which means it isn't viewable by other users who log in.
- The account can't be used with any other BlueXP feature: not with Cloud Volumes ONTAP creation, licensing, or support case creation.
- There can be only one NSS account associated with Digital Advisor and case management, per user.

NetApp Support Site credentials are also associated with the BlueXP account that you are a member of. NSS account-level credentials enable you to register for support, deploy Cloud Volumes ONTAP when you bring your own license (BYOL), and more.

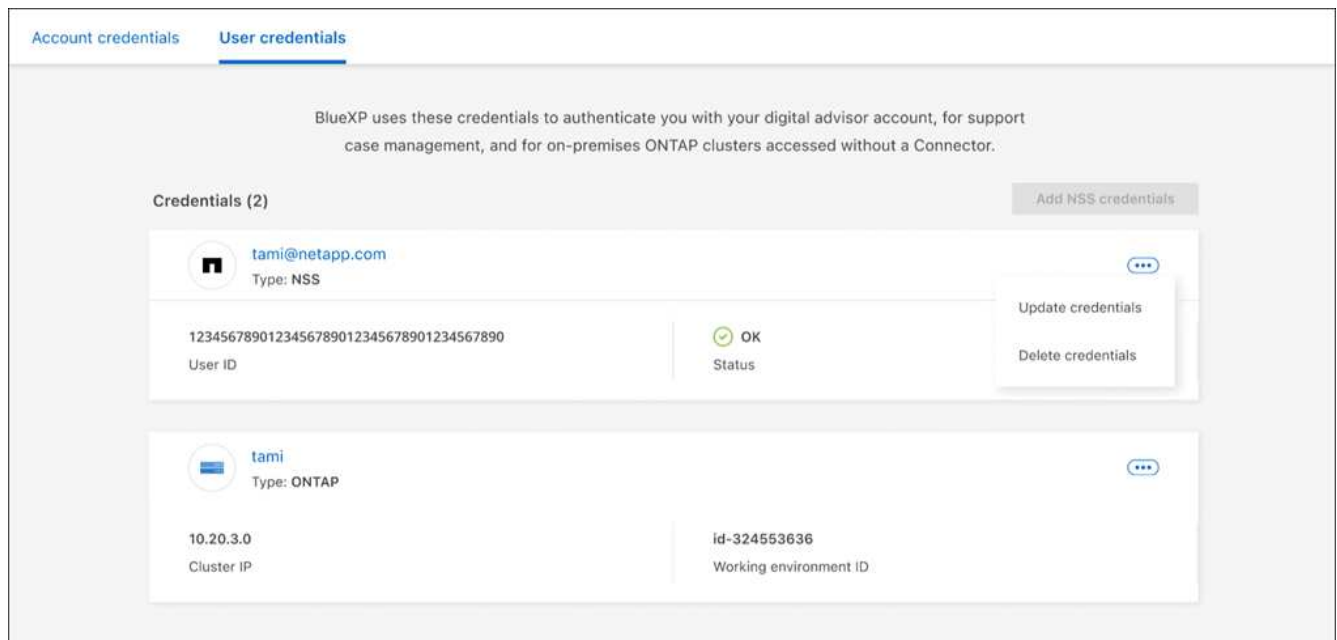
[Learn more about using NSS credentials with your BlueXP account.](#)

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.

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.