

Prerequisites to create a Microsoft Azure Blob Storage V3 connection

Abstract

You can use Microsoft Azure Blob Storage V3 Connector to connect to Microsoft Azure Blob Storage from Cloud Data Integration. This article explains the prerequisite tasks that you must complete before you create a Microsoft Azure Blob Storage V3 connection.

Supported Versions

- Informatica Cloud® Data Integration Microsoft Azure Blob Storage V3 Connector

Table of Contents

Overview	2
Create a storage account to use with Microsoft Azure Blob Storage.	2
Create a blob container in the storage account.	5
Get credentials for shared key authentication.	7
Get credentials for shared access signature authentication.	7
Get SAS token for the storage account	8
Get SAS token for the container.	8

Overview

You can use Microsoft Azure Blob Storage V3 Connector to connect to Microsoft Azure Blob Storage using shared key authentication or shared access signature authentication.

Before you create a Microsoft Azure Blob Storage V3 connection, complete the following prerequisite tasks:

1. Create a storage account to use with Microsoft Azure Blob Storage.
2. Create a blob container in the storage account.
3. Get credentials for shared key authentication.
4. Get credentials for shared access signature authentication.

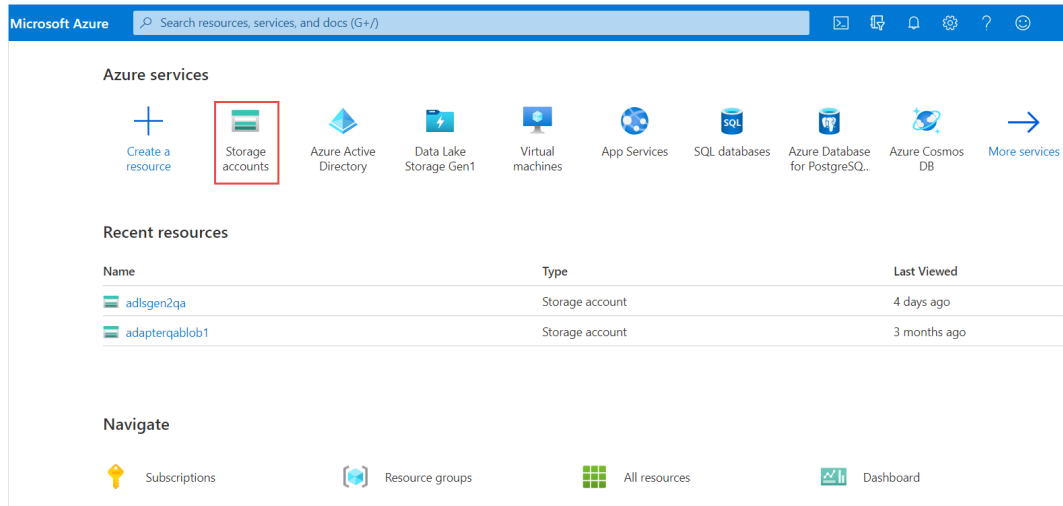
For information about configuring a Microsoft Azure Blob Storage V3 connection, see the Informatica Cloud® Data Integration Microsoft Azure Blob Storage V3 Connector documentation.

Create a storage account to use with Microsoft Azure Blob Storage

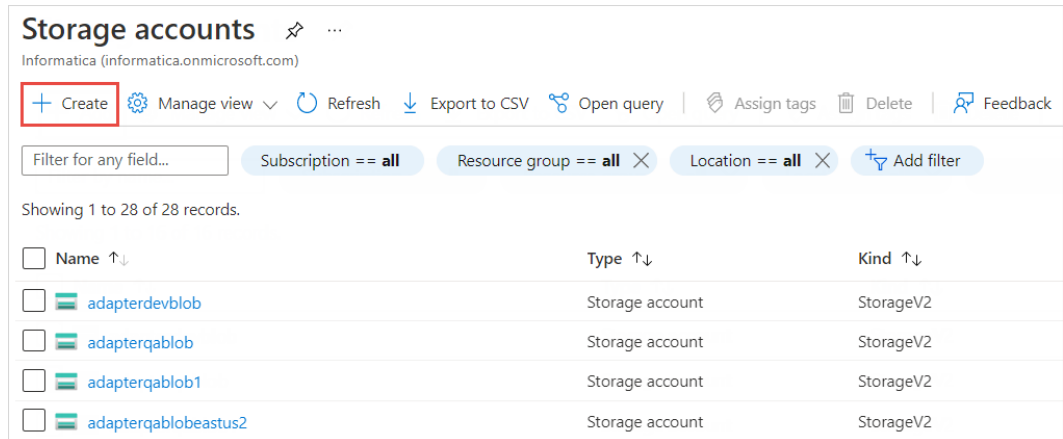
An Azure storage account contains all of your Azure Storage data objects, including blobs, file shares, queues, tables, and disks. Create a storage account and enable access to the storage account using the shared key or shared access signature.

1. Log in to the following Azure portal: <https://portal.azure.com/>

2. Under Azure Services, click **Storage accounts**.



3. On the **Storage accounts** page, click **Create** to create a new storage account.



4. On the **Basics** tab, enter the project and instance details.

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription *

Resource group * [Create new](#)

Instance details

If you need to create a legacy storage account type, please click [here](#).

Storage account name ⓘ *

Region ⓘ *

[Review + create](#) < Previous Next : Advanced >

- In the **Subscription** field, select the subscription for which you want to create the storage account.
- In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.
- In the **Storage account name** field, enter a name for your storage account.
Note: The name must be unique across Azure, between 3 and 24 characters in length, and can include only numbers and lowercase letters.
- In the **Region** field, select a location for your storage account, or use the default location.

5. On the **Advanced** tab, configure the security settings.

The screenshot shows the 'Create a storage account' wizard in the 'Advanced' tab. The 'Security' section is active, with the following settings:

- Require secure transfer for REST API operations**: (disabled)
- Enable blob public access**: (checked)
- Enable storage account key access**: (checked)
- Default to Azure Active Directory authorization in the Azure portal**: (disabled)
- Minimum TLS version**: Version 1.2 (dropdown menu)

Below the Security section is the 'Data Lake Storage Gen2' section, which is currently disabled. At the bottom of the wizard, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Networking >'.

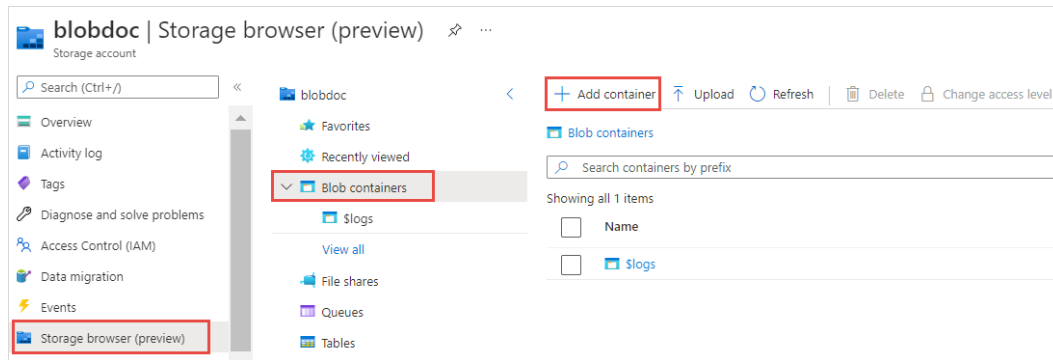
- a. Disable the **Require secure transfer for REST API operations** option.
 - b. Select **Enable blob public access** to allow anonymous access to blobs within the storage account.
 - c. Select **Enable storage account key access** to allow access to storage account using the shared key or shared access signature.
6. Click **Review + Create > Create**.

Create a blob container in the storage account

After you create the storage account, create a blob container and a virtual directory within the blob container.

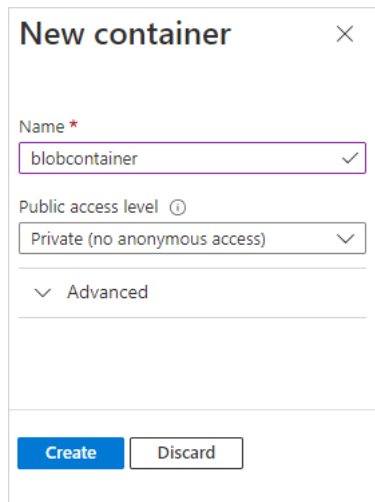
1. Open the storage account that you created.

2. Click **Storage browsers > Blob containers**.



3. Click **Add container**.

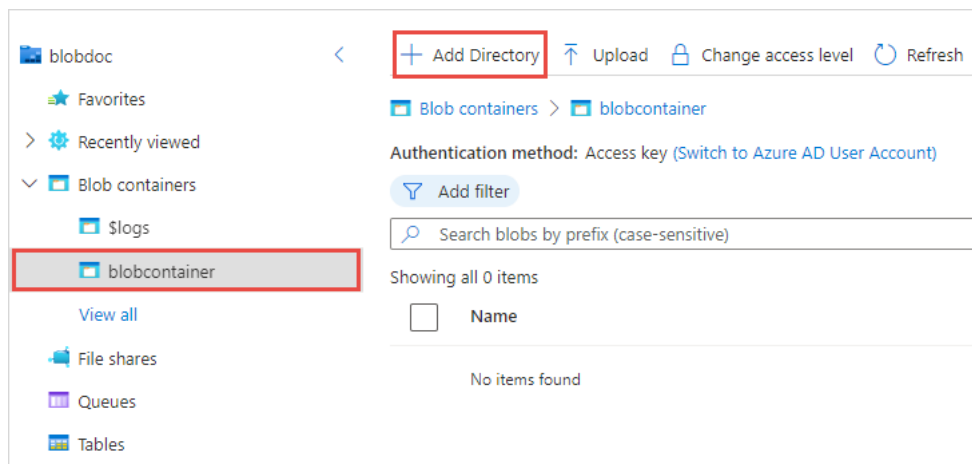
4. Enter a name for the new container.



5. Click **Create**.

6. Click the container that you created.

7. Click **Add Directory** to create a new directory within the container.



8. Enter a name for the directory.

Add virtual directory

This will create a virtual directory. A virtual directory does not actually exist in Azure until you paste or upload blobs into it.

Name

9. Click **Ok**.

Get credentials for shared key authentication

You can use the shared key authentication to connect to Microsoft Azure Blob Storage using the account name and account key. Obtain the account name and account key.

1. Open the storage account.
2. Under **Security + Networking**, click **Access keys**.
3. Click **Show keys**.

The screenshot shows the 'Access keys' page for a storage account named 'blobdoc'. The left-hand navigation pane is open, with 'Access keys' selected under the 'Security + networking' section. The main content area displays the 'Show keys' button, which is highlighted with a red box. Below this, there are two keys listed: 'key1' and 'key2'. Each key entry shows the last rotation date as '4/19/2022 (0 days ago)' and includes a 'Rotate key' button. The 'Key' and 'Connection string' fields for each key are masked with dots. The 'Storage account name' field is also visible, containing the value 'blobdoc'.

4. Make a note of the storage account name and account key. You can use key1 or key2.

Get credentials for shared access signature authentication

The shared access signature authentication uses the SAS token to connect to Microsoft Azure Blob Storage.

Get the SAS token to grant access to the resources in the storage account or container for a specific time range without sharing the account key.

Get SAS token for the storage account

You can get the SAS token for the storage account from the Azure portal.

1. Navigate to the storage account.
2. Under **Security + Networking**, click **Shared access signature**.

The screenshot shows the 'Shared access signature' configuration page in the Azure portal. The left sidebar is expanded to 'Security + Networking' > 'Shared access signature'. The main content area is titled 'blobdoc | Shared access signature' and contains the following configuration options:

- Allowed services:** Blob, File, Queue, Table
- Allowed resource types:** Service, Container, Object
- Allowed permissions:** Read, Write, Delete, List, Add, Create, Update, Process, Immutability storage
- Blob versioning permissions:** Enables deletion of versions
- Allowed blob index permissions:** Read/Write, Filter
- Start and expiry date/time:** Start: 04/19/2022 6:12:58 PM, End: 04/20/2022 2:12:58 AM
- Allowed IP addresses:** For example, 168.1.5.65 or 168.1.5.65-168.1.5.70
- Allowed protocols:** HTTPS only, HTTPS and HTTP
- Preferred routing tier:** Basic (default), Microsoft network routing, Internet routing
- Signing key:** key1

A blue button at the bottom reads 'Generate SAS and connection string'.

3. In the **Allowed services** field, select **Blob**.
4. In the **Allowed resource types** field, select **Container** and **Object**.
5. In the **Allowed permissions** field, select **Read, Write, Delete, List, and Create**.
6. Set the start and expiry date during which the SAS token is valid.
7. In the **Allowed IP addresses** field, specify a public IP address or a range of public IP addresses.
Note: When you read Avro or Parquet files, do not specify the IP address.
8. In the **Preferred routing tier** field, select **Basic**.
9. Select the **Signing key**.
10. Click **Generate SAS and connection string** and make a note of the SAS token.

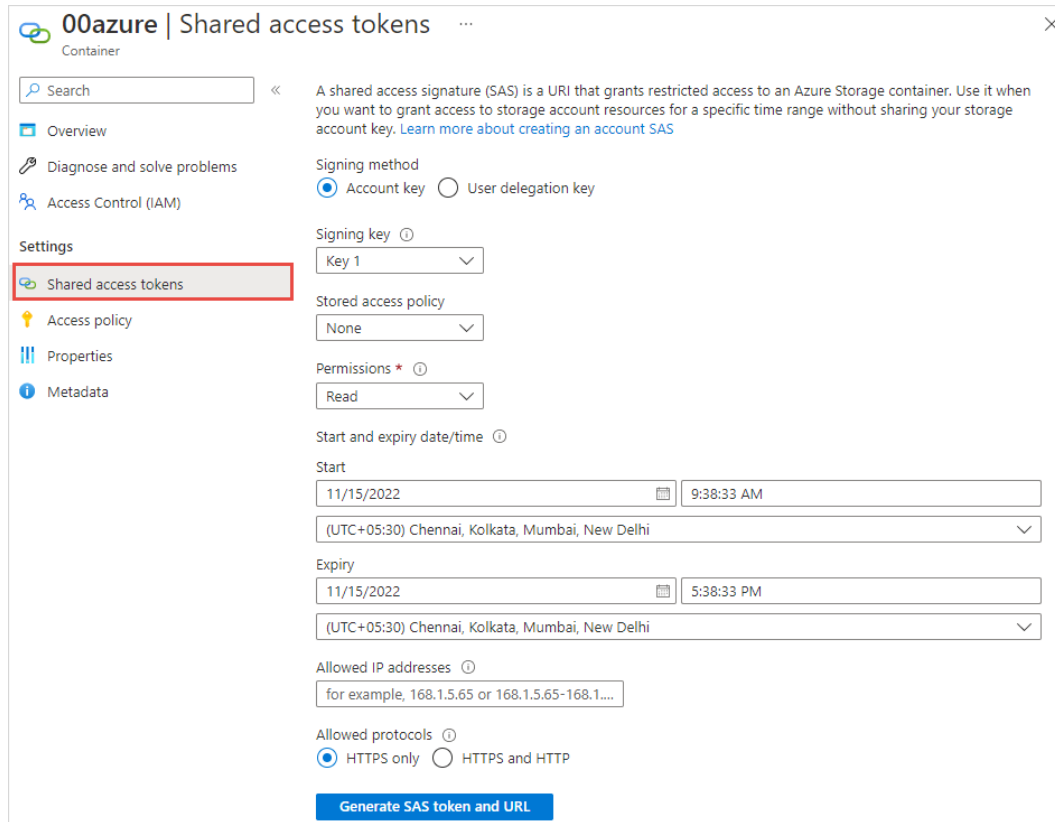
Get SAS token for the container

You can get the SAS token for the container from the Azure Portal or Microsoft Azure Storage Explorer.

Get SAS token from the Azure Portal

Perform the following steps to get the SAS token for the container from the Azure portal:

1. Navigate to the blob container.
2. Under **Settings**, click **Shared access tokens**.



3. In the **Signing method** field, select **Account key** or **User delegation key**.
Note: If you use the User delegation key signing method, ensure that you have the Storage Blob Data Owner role for the container or the storage account.
4. If you select the Account key signing method, select the **Signing key**.
5. In the **Permissions** field, select **Read, Write, Delete, List, and Create**.
6. Set the start and expiry date during which the SAS token is valid.
7. In the **Allowed IP addresses** field, specify a public IP address or a range of public IP addresses.
Note: When you read Avro or Parquet files, do not specify the IP address.
8. Click **Generate SAS token and URL** and make a note of the SAS token.

Get SAS token from Microsoft Azure Storage Explorer

Perform the following steps to get the SAS token for the container from Microsoft Azure Storage Explorer:

1. Log in to your Microsoft Azure Storage Explorer account.
2. On the Explorer, right-click on the container name and select **Get Shared Access Signature**. The Shared Access Signature window appears.

Shared Access Signature

Access policy: none

Start time: 31-10-2022 18:32

Expiry time: 01-11-2022 18:32

Time zone:
 Local
 UTC

Permissions:
 Read
 Add
 Create
 Write
 Delete

Signing key: key1

[Learn more about permissions.](#)

Create Cancel

3. In the Access policy field, select **none**.
4. Set the start and expiry date during which the SAS token is valid.
5. Select the time zone.
6. In the **Permissions** field, select **Read, Create, Write, Delete, and List**.
7. Select the **Signing key**.
8. Click **Create** to generate the SAS token and make a note of the SAS token.

Author

Adrija Pandya

Acknowledgements

The author would like to acknowledge K.R. Kiran for his technical assistance with this article.