Azure Blob

Last Modified on 03/25/2024 3:43 am EDT

Azure Blob

Azure Blob Connector Docs

On this page:

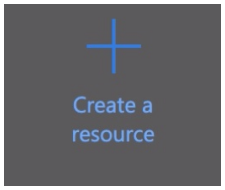
Authentication Prerequisites

The Azure Blob connector uses two custom authentication types - **Shared Access Signature** (**SAS**) and **Shared Key**. Before you can authenticate an instance of the Azure Blob connector, you must do the following:

1. Have an active subscription with Microsoft Azure platform
2. Have a storage account within the Azure portal
3. Generate required authentication credentials

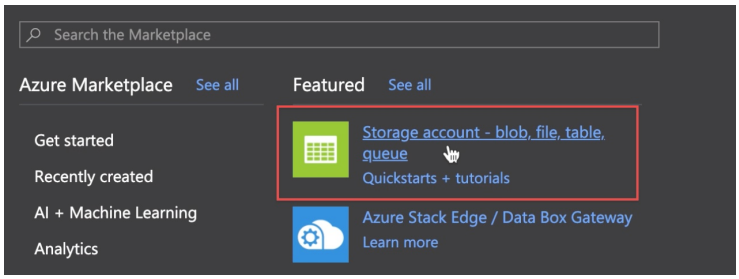
Create Storage Account

1. Login via portal.azure.com/#home
2. Click on **Create a resource**.



3. On the Navigation Panel on the left, click Storage.

4. Click on the Storage account.

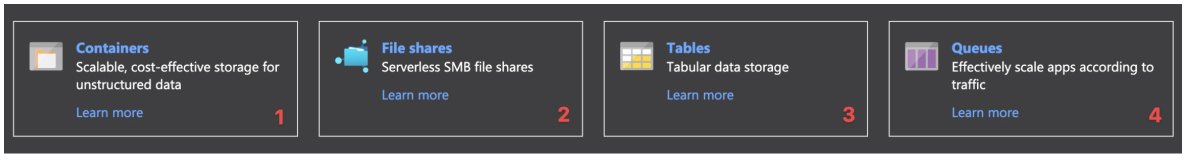


You have now created a new Storage account.

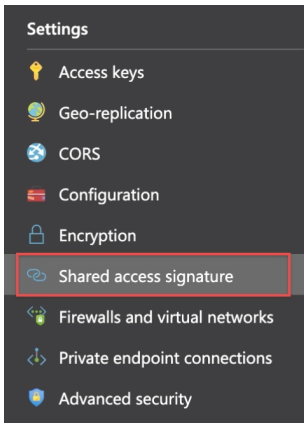
Locate Credentials for SAS Authentication

1. Login via portal.azure.com/#home.
2. Go to your storage account.

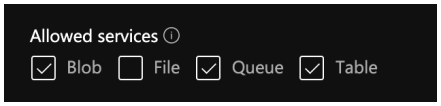
3. There are different types of Storage available on Azure for your account -



4. Click **Shared Access Signature** (SAS) on the navigation panel.

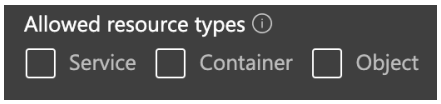


5. On the console that opens, select the allowed services.



Depending on the services you allow the value of the allowed services field will change; it can be any combination of **b**lob, **f**ile, **q**ueue, **t**able (bfqt).

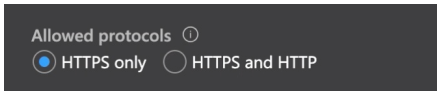
6. Now, select the allowed resource types.



The value for the allowed resource types depends on the resource types you select. That is, it could be 'sco' for all three resource types being available or any combination of the three, where 's' stands for 'service', 'c' for container, and O for 'object'.

- If you enter either 'co' or 'o', then value for the field '**Container Name**' (or sas.container) is also required to validate and create an instance. You must enter the name of the container, that you have created already, in the field `Container Name`.
- If you enter 'o', then the container must have a file or object or directory in it and must be passed in the field `Container Name` as `{containerName}/{object or file name}`.
  It is not required if all three are selected (sco). The value entered in the field 'Container Name' depends on the allowed services selected in the previous step (bfqt).

7. Select the protocol you would like to allow.

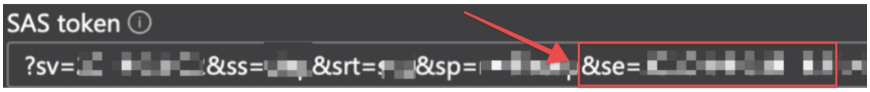


8. Click on the Generate SAS and connection string button.

9. This will generate a SAS token, as shown below. **You need to use this token to locate the credentials that you will need to authenticate.**

10. Below are the fields that help you locate the credentials:
    - **Azure Storage Account Name** is the name of your storage account.
    - **Azure Storage Allowed Services**

    - **End Date**



    - **Azure Storage Permissions**

    - **Communication Protocol** is the protocol you selected in step 4.

    - **Resource Type**

- Signature

- Start Date

- Version

Enter the above credentials to authenticate using the SAS method.

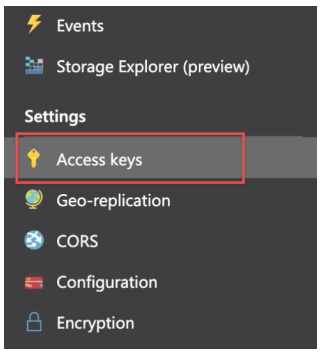
> **Note:** The SAS token is generated for a given period of time, as shown below.
>
> 
>
>
> Once the given period expires you will need to generate a new SAS token.
> If the SAS token is re-generated before the given time period, you will need to provision a new instance.

Locate Credentials for Shared Key Authentication

1. Login via portal.azure.com/#home
2. Go to your storage account.

3. There are different types of Storage available on Azure for your account -

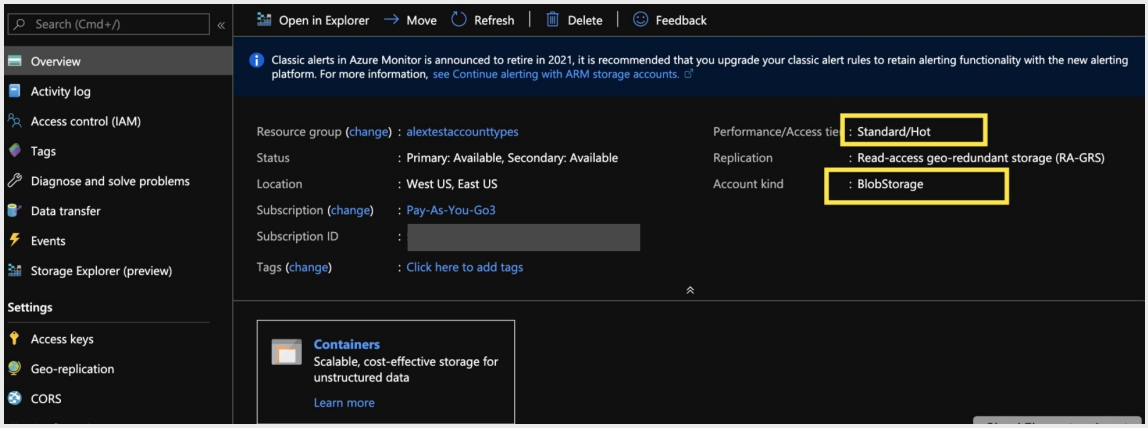
4. Click on **Access Keys** on the navigation panel.



5. On the console that appears, copy the key under **key1. Alternatively,** you can also use the entire connection string below it.

Excerpt from Azure documentation - You can use either key to access Azure Storage, but in general it's a good practice to use the first key and reserve the use of the second key for when you are rotating keys.

Enter the shared key, your Storage account name, and an instance name to authenticate with the Azure Blob connector.

> **Note**: Find your account type from the overview section:
>
> 
>
>
> - In case of only Blobstorage, modify the OnProvision-auth to point to .blob.core.windows.net/ instead of .queue.core.windows.net/

Required Authentication Parameters

You can authenticate a connector instance using the UI or via API calls. For detailed information on how to authenticate an instance, see our related documentation:

- Authenticate a Connector Instance (UI)
- Authenticate a Connector Instance (API)

To authenticate an instance of the Azure Blob connector with **SAS** as the authentication type, you will need the following parameters:

Parameter Name/UI Value	API Value	Description	Source
Account Name	accountname	Created by user before authentication	Create Storage Account
Allowed Services	sas.allowedservices	Generated before authentication	Locate Credentials for SAS Authentication
End Date	as.enddate	Generated before authentication	Locate Credentials for SAS Authentication

Parameter Name/UI Value	API Value	Description	Source
Permissions	sas.permissions	Generated before authentication	Locate Credentials for SAS Authentication
Communication Protocol	sas.protocol	Generated before authentication	Locate Credentials for SAS Authentication
Resource Type	sas.resourcetype	Generated before authentication	Locate Credentials for SAS Authentication
Signature	sas.signature	Generated before authentication	Locate Credentials for SAS Authentication
Start Date	sas.startdate	Generated before authentication	Locate Credentials for SAS Authentication
Version	sas.version	Generated before authentication	Locate Credentials for SAS Authentication
OAuth Callback URL	oauth.callback.url	Default value is https://auth.cloudelements.io/oauth	Authenticate a Connector Instance (API)

To authenticate an instance of the Azure Blob connector with **Shared Key** as the authentication type, you will need the following parameters:

Parameter Name/UI Value	API Value	Description	Source
Account Name	accountname	Created by user before authentication	Create Storage Account
Shared Key	sharedkey.key	Generated before authentication	Locate Credentials for Shared Key Authentication
OAuth Callback URL	oauth.callback.url	Default value is https://auth.cloudelements.io/oauth	Authenticate a Connector Instance (API)

Sample Configuration JSON

SAS as the authentication type

```
"configuration": {
   "authentication.type": "sas",
   "accountname": "[myAccountName]",
   "sas.allowedservices": "[myAllowedServices]",
   "sas.enddate": "[myEndDate]",
   "sas.permissions": "[myPermissions]",
   "sas.protocol": "[myCommunicationProtocol]",
   "sas.resourcetype": "[myResourceType]",
   "sas.signature": "[mySignature]",
   "sas.startdate": "[myStartDate]",
   "sas.version": "[myVersion]",
   "oauth.callback.url": "https://auth.cloudelements.io/oauth"
  }
```

Shared Key as the Authentication type

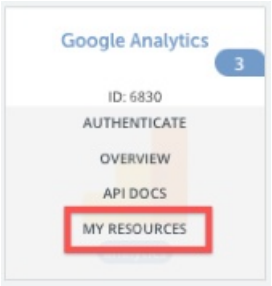
```
"configuration": {
   "authentication.type": "sharedkey",
   "accountname": "[myAccountName]",
   "sharedkey.key": "[mySharedKey",
   "oauth.callback.url": "https://auth.cloudelements.io/oauth"
  }
```

Connector Fact Sheet and Reference

Authentication and Configuration Parameters

To see all authentication parameters for the Azure Blob connector, follow these steps:

1. Sign in to SAP Open Connectors and navigate to Connectors.
2. Hover over the card for a connector, and then click My Resources.



3. In the top navigation toolbar, click Setup.
4. From the Setup page, you can view a complete list of the connector's authentication and configuration parameters.

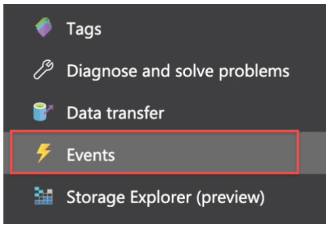
Events and Supported Resources

The Azure Blob connector supports events via webhooks. For detailed information about our Events framework and how to configure a connector instance with events, see our documentation:

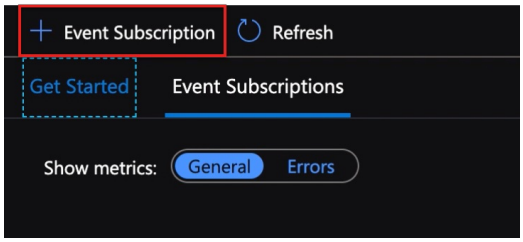
- Authenticate a Connector Instance with Events (UI)
- Authenticate a Connector Instance with Events (API)

To set up Events for Azure Blob:

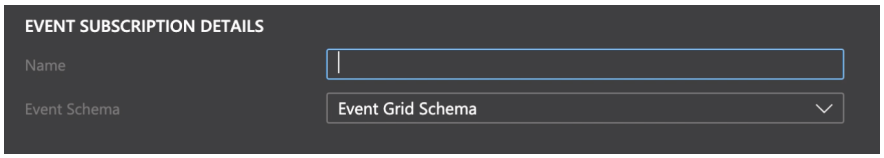
1. Login via portal.azure.com/#home.
2. On the navigation panel on the left, click **Events**.



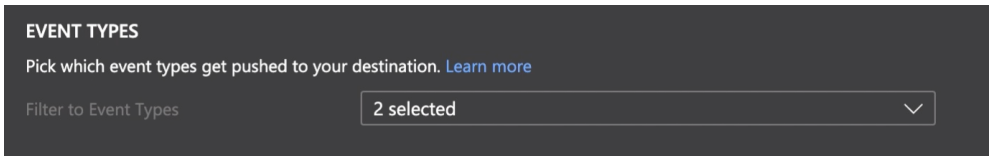
3. The Events console appears. Click **Event Subscription.**



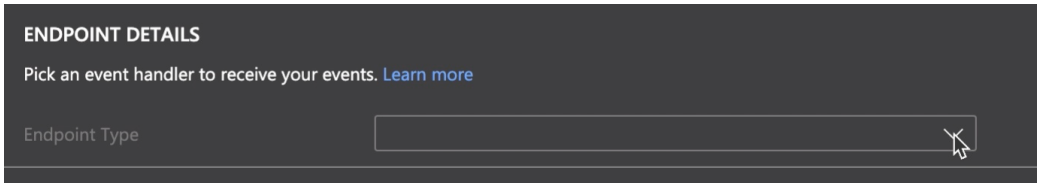
4. Provide a name for your event.



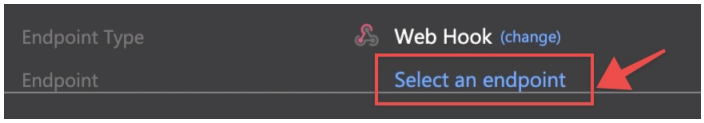
5. Select an Event Type.



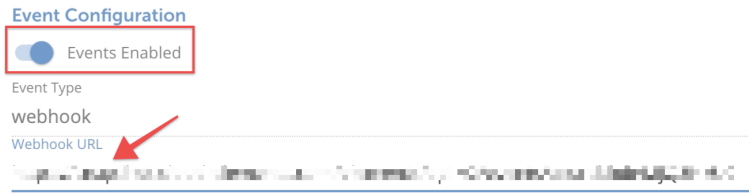
6. Select '**Web Hook**' as your Endpoint Type from the drop down.



7. Once you select Web Hook as your endpoint type, click **Select an endpoint.**



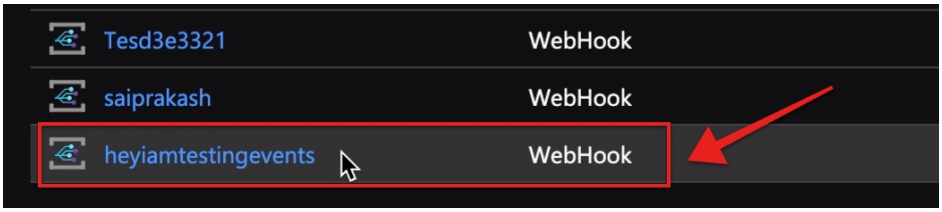
8. Head to the SAP Open Connectors Instance Creation page, create an instance and then toggle the Events button **On**.
9. Once Events is enabled, copy the Webhook URL.



10. Go back to the Azure Portal once again and paste this Webhook URL in the **Subscriber Endpoint** field.

11. Click **Create** to create an event.

You have set up events for your instance via webhooks and will be able to see the new event you created on the Events console.



Queryable Endpoints

You can use OCNQL to query the following endpoints of the Azure Blob connector:

- GET /files
- GET /message-queues
- GET /message-queues/{id}/messages
- GET /{objectName}
- GET /{objectName}/{objectId}/{childObjectName}
- GET /share-drives
- GET /share-drives/folders
- GET /share-drives/folders/files
- GET /tables
- GET/tables/{id}/records

Connector API Documentation

The base URL for all API requests is `https://api.openconnectors.us2.ext.hana.ondemand.com/elements/api-v2` .

Azure Blob API Documentation

API Documentation