

## Prerequisites to create a Microsoft Azure Synapse SQL connection

# Abstract

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

# Supported Versions

- Informatica Cloud® Data Integration Microsoft Azure Synapse SQL Connector

# Table of Contents

Overview. . . . .	2
Configuring Azure Active Directory authentication. . . . .	2
Obtaining the JDBC URL. . . . .	3
Obtaining credentials for shared key authentication. . . . .	4
Obtaining credentials for service principal authentication. . . . .	4
Creating a Microsoft Azure Synapse SQL connection. . . . .	10

# Overview

You can use Azure Active Directory authentication or Microsoft SQL Server authentication to connect to Microsoft Azure Synapse SQL.

Before you create a Microsoft Azure Synapse SQL connection, complete the following prerequisite tasks:

1. Configure Azure Active Directory (AAD) authentication to connect to Microsoft Azure Synapse SQL.
2. Obtain the JDBC URL or connection string from Microsoft Azure Synapse SQL.
3. Obtain the credentials for shared key authentication and service principal authentication to connect to Azure storage to stage the files:
  - Shared key authentication - Obtain the account name and account key to connect to Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2.
  - Service principal authentication - Applicable to Microsoft Azure Data Lake Storage Gen2. Register an application in the Azure Active Directory, generate a client secret, and then assign the Storage Blob Contributor role to the application.

For more information about Microsoft Azure Synapse SQL Connector, see the *Informatica Cloud® Data Integration Microsoft Azure Synapse SQL Connector documentation*.

# Configuring Azure Active Directory authentication

To configure AAD authentication, perform the following tasks:

## Import the server certificate

If a trust store file is not configured for your organization and you want to use AAD authentication with Active Directory Federation Services in Azure, import the server certificate.

Import the server certificate to the following location:

<Secure Agent installation directory>\jdk\jre\lib\security\cacerts

Use the following command to import the certificate:

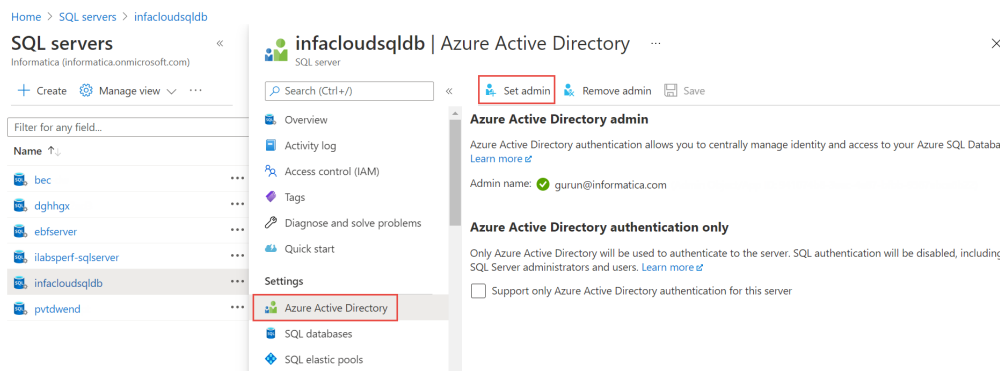
```
keytool -import -trustcacerts -alias <alias name of the certificate> -file <certificate file path> -keystore <Secure Agent installation directory>\jdk\jre\lib\security\cacerts -storepass <password for the truststore>
```

### Set the Azure Active Directory admin

To add new users or delete existing users from your Azure Active Directory, you must have the administrator role.

Perform the following steps to set Azure Active Directory administrator:

1. Log in to the Azure portal.
2. On the All Resources page, select the Microsoft SQL Server that hosts Microsoft Azure Synapse SQL.
3. Select the **Azure Active Directory** option under Settings.  
The image shows the Azure Active Directory settings:



4. Click **Set admin**.  
The Add admin page appears.
5. Enter the email ID that you want to use as admin, and click **Select**.
6. Click **Save**.

### Create a new user

Perform the following steps to create a user:

1. Connect to Microsoft Azure Synapse SQL using the Azure Active Directory admin created in the previous steps.  
You can use Microsoft SQL Server Management Studio to connect to the Microsoft Azure Synapse SQL.
2. Run the following command:  

```
create user [user@foobar.com] from external provider;
```

  
For more information, see the Microsoft Azure documentation.
3. Assign the required privileges to the user.

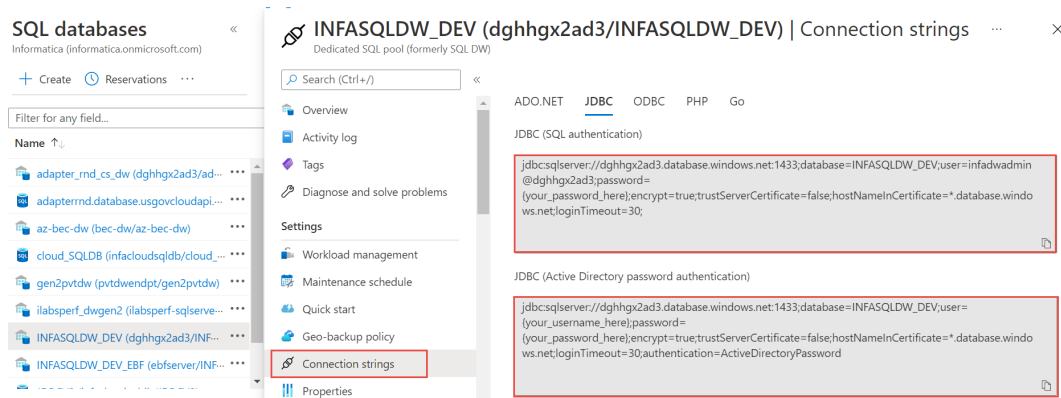
## Obtaining the JDBC URL

The JDBC URL contains the credentials to authenticate access to Microsoft Azure Synapse SQL.

To obtain the JDBC URL, perform the following steps:

1. Log in to the Azure portal.
2. Open your Microsoft Azure Synapse SQL account.
3. Under **Settings**, click **Connection strings**.

- Click the **JDBC** tab and note the connection string based on the type of authentication you want to use to connect to Microsoft Azure Synapse SQL.  
The following image shows the JDBC URL for Microsoft SQL Server authentication and Azure Active Directory authentication:

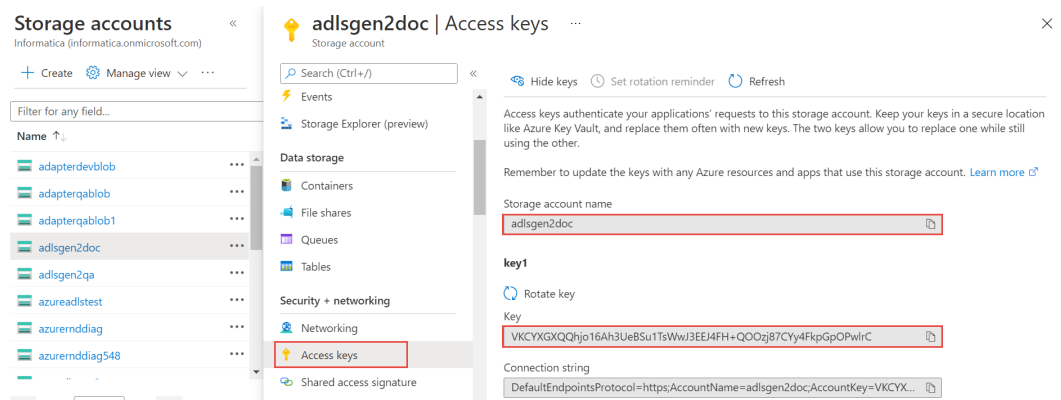


## Obtaining credentials for shared key authentication

You can use shared key authentication to connect to Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2 to stage files using the account name and account key.

To obtain the account name and account key, perform the following steps:

- Log in to the Azure portal.
- Open the storage account.
- Under **Security + Networking**, click **Access keys**.
- Click **Show keys** and note the storage account name and account key.



## Obtaining credentials for service principal authentication


You can use service principal authentication to connect to Microsoft Azure Data Lake Storage Gen2 to stage files.


Register an application in the Azure Active Directory, generate a client secret, and then assign the Storage Blob Contributor role to the application.


- Log in to the Azure portal.


## 2. Click **Azure Active Directory**.


**Azure services**


 Create a resource


 Storage accounts


 Azure Active Directory


 Data Lake Storage Gen1


 Virtual machines

 App Services

 SQL databases

 Azure Database for PostgreSQL...


 Azure Cosmos DB


 More services


**Recent resources**


Name	Type	Last Viewed
adlsgen2doc	Storage account	an hour ago
adlsgen2qa	Storage account	3 weeks ago
adapterqablob1	Storage account	4 months ago

**Navigate**

 Subscriptions

 Resource groups

 All resources

 Dashboard

## 3. In the **Manage** section, click **App registrations**.

Home > Informatica | App registrations

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Download](#) [Preview features](#) [Got feedback?](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

**Manage**

- Overview
- Getting started
- Preview hub
- Diagnose and solve problems
- App registrations**
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names

**Owned applications**

Start typing a name or Application ID to filter these results

Display name	Application (client) ID	Created on	Certificates & secrets
AADappdoc		7/23/2020	Current
adlsgen2doc2		8/5/2020	Current

## 4. Click **New registration** to create a new Azure Active Directory application.

5. On the **Register an application** page, enter the details for the new application.

[Home](#) > [Informatica](#) >

## Register an application

\* Name

The user-facing display name for this application (this can be changed later).

### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Informatica only - Single tenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- ☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

▼



e.g. https://myapp.com/auth


By proceeding, you agree to the [Microsoft Platform Policies](#) 

**Register**

- a. In the **Name** field, enter the application name.
- b. In the **Redirect URI** section, select **Web** as the type of the application and enter the URL of the application.
- c. Click **Register**.

The details of the newly created Azure Active Directory application page are displayed.

 Delete  Endpoints

 Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [→](#)

Display name <a href="#">Some_Application_demo</a>	Supported account types <a href="#">My organization only</a>
Application (client) ID <a href="#">7f45516a-a02c-4139-86f0-c5075b993240</a>	Redirect URIs <a href="#">1 web, 0 public client</a>
Directory (tenant) ID <a href="#">2638f43e-f77d-4fc7-ab92-7b753b7876fd</a>	Managed application in local directory <a href="#">Some_Application_demo</a>
Object ID 5d8d63de-5247-4b24-800e-9a4e420de3af	

6. In the Manage section, click **Certificates & secrets** section.

7. Click **New client secret**.

Home > Informatica > AADappdoc

**AADappdoc | Certificates & secrets**

Search (Ctrl+/) Got feedback?

**Add a client secret**

Description

Expires

☒ In 1 year  
☐ In 2 years  
☐ Never

Add Cancel

**Certificates & secrets**

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

8. In the **Add a client secret** page, perform the following steps:

- Enter a name for the client secret in the **Description** field.
- In the **Expires** field, you can select the duration of the key as **Never**(Recommended).
- Click **Add**.
- The value of the key is generated and displayed in the **Value** field.

Client secrets

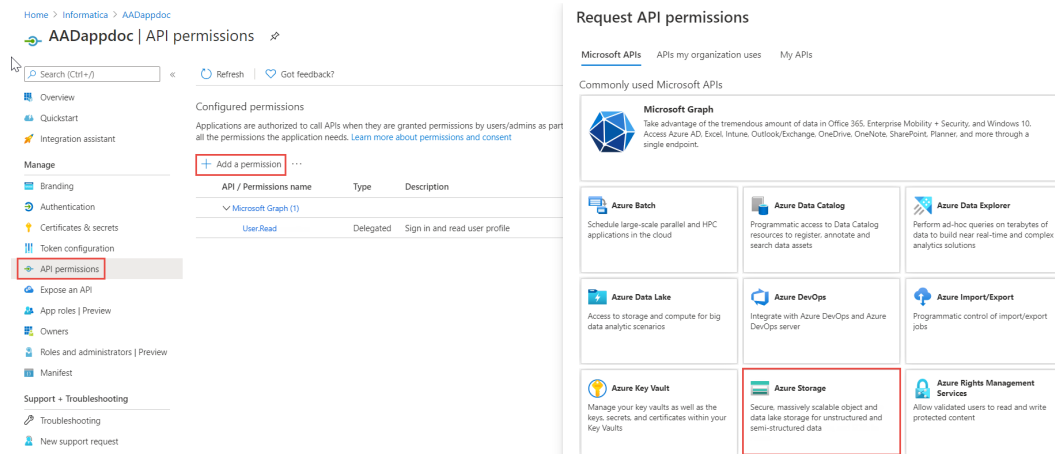
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	ID
AADapp_doc	12/31/2299	Lgw*****	f6a97b93-703c-4d8c-a632-4ac9

**Note:** You must copy the key value as you cannot retrieve the value after you leave the page. Ensure that the client secret does not contain special characters.

- In the Manage section, click **Owners**.
- Click **Add owner**.
- In the **Search** field, search for the owner name or email address that you used to log in to the Azure portal.
- Select the owner name or email address, and click **Select**.
- In the Manage section, click **API permissions**.  
The configured permissions are displayed.



14. Click **Add a permission**.  
The **Request API permissions** page appears.
15. In the **Microsoft APIs** section, click **Azure Storage**.
16. Select **Delegated permissions** as the type of permissions.
17. Select **Access Azure Storage** from the listed permissions.

## Request API permissions ✕

[← All APIs](#)

 Azure Storage  
<https://storage.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

🔍 Start typing a reply url to filter these results

Permission	Admin consent required
<div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <span style="font-size: 0.8em;">▼</span> Permissions </div> </div>	
<div style="display: flex; align-items: center;"> <input style="margin-right: 10px;" type="checkbox"/> <div> <b>user_impersonation</b> ⓘ  Access Azure Storage </div> </div>	-

Add permissions

Discard

18. Click **Add permissions**.
19. In the **Configured permissions**, select **Azure Active directory** and ensure that the **Sign in and read user profile** option is enabled in the **Delegated permissions** section.





If **Azure Active directory** is not listed under the **Configured permissions**, perform the following steps:


- Click **Add a permission**.  
The **Request API permissions** page appears.
- In the Microsoft APIs section, click **Azure Active Directory Graph**.

## Request API permissions


### More Microsoft APIs

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

**Speech**  
Create powerful speech-enabled features using speech to text and text to speech conversion

**Universal Print**  
Programmatic access to create and manage printer and print job resources

### Supported legacy APIs

**Azure Active Directory Graph**  
Programmatic access to directory data and objects

- Select **Delegated permissions** as the type of permissions.
- Select **Sign in and read user profile** from the listed permissions.

## Request API permissions

[All APIs](#)

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](#)

Permission		Admin consent required
User (1)		
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	-
<input type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	-
Group		
<input type="checkbox"/>	Group.Read.All ⓘ Read all groups	Yes

Add permissions

Discard

20. Go to the home page and in the Storage Account section, select the storage account that you created.
21. Click **Access control (IAM) > Add**.
22. In the **Add role assignment** page, provide the **Storage Blob Data Contributor** to the application.

## Creating a Microsoft Azure Synapse SQL connection

You can use Microsoft SQL Server authentication or Azure Active Directory authentication to connect to Microsoft Azure Synapse SQL. Based on the authentication type, you must provide the JDBC URL.

Configure the following connection properties to create a Microsoft Azure Synapse SQL connection:

Connection property	Description
Runtime Environment	The name of the runtime environment where you want to run the tasks. Specify a Secure Agent, Hosted Agent, or serverless runtime environment.
Azure DW JDBC URL	<p>Microsoft Azure Synapse SQL JDBC connection string.</p> <p>Example for Microsoft SQL Server authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433;database=&lt;Database&gt;</pre> <p>Example for Azure Active Directory (AAD) authentication:</p> <pre>jdbc:sqlserver://&lt;Server&gt;.database.windows.net:1433; database=&lt;Database&gt;;encrypt=true;trustServerCertificate=false; hostNameInCertificate=*.database.windows.net;loginTimeout=30; Authentication=ActiveDirectoryPassword;</pre> <p>The default authentication is Microsoft SQL Server authentication.</p>
Azure DW JDBC Username	User name to connect to the Microsoft Azure Synapse SQL account. Provide the AAD user name for AAD authentication.
Azure DW JDBC Password	Password to connect to the Microsoft Azure Synapse SQL account.
Azure DW Schema Name	Name of the schema in Microsoft Azure Synapse SQL.
Azure Storage Type	<p>Type of Azure storage to stage the files.</p> <p>You can select any of the following storage type:</p> <ul style="list-style-type: none"> <li>- Azure Blob. Default. To use Microsoft Azure Blob Storage to stage the files.</li> <li>- ADLS Gen2. To use Microsoft Azure Data Lake Storage Gen2 as storage to stage the files.</li> </ul>
Authentication Type	<p>Authentication type to connect to Azure storage to stage the files.</p> <p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>- <b>Shared Key Authentication</b>. Select to use the account name and account key to connect to Microsoft Azure Blob Storage or Microsoft Azure Data Lake Storage Gen2.</li> <li>- <b>Service Principal Authentication</b>. Applicable to Microsoft Azure Data Lake Storage Gen2. To use Service Principal authentication, you must register an application in the Azure Active Directory, generate a client secret, and then assign the Storage Blob Contributor role to the application.</li> </ul>
Azure Blob Account Name	<p>Applicable to shared key authentication for Microsoft Azure Blob Storage.</p> <p>Name of the Microsoft Azure Blob Storage account to stage the files.</p>
Azure Blob Account Key	<p>Applicable to shared key authentication for Microsoft Azure Blob Storage.</p> <p>Microsoft Azure Blob Storage access key to stage the files.</p>

Connection property	Description
ADLS Gen2 Storage Account Name	Applicable to shared key authentication and service principal authentication for Microsoft Azure Data Lake Storage Gen2. Name of the Microsoft Azure Data Lake Storage Gen2 account to stage the files.
ADLS Gen2 Account Key	Applicable to shared key authentication for Microsoft Azure Data Lake Storage Gen2. Microsoft Azure Data Lake Storage Gen2 access key to stage the files.
Client ID	Applicable to service principal authentication for Microsoft Azure Data Lake Storage Gen2. The application ID or client ID for your application registered in the Azure Active Directory.
Client Secret	Applicable to service principal authentication for Microsoft Azure Data Lake Storage Gen2. The client secret for your application.
Tenant ID	Applicable to service principal authentication for Microsoft Azure Data Lake Storage Gen2. The directory ID or tenant ID for your application.
Blob End-point	Type of Microsoft Azure endpoints. You can select any of the following endpoints: - core.windows.net. Default. - core.usgovcloudapi.net. To select the Azure Government endpoints.
VNet Rule	Connects to a Microsoft Azure Synapse SQL endpoint residing in a virtual network (VNet). When you use a serverless runtime environment, you cannot connect to a Microsoft Azure Synapse SQL endpoint residing in a virtual network.

#### Guidelines to use a Microsoft Azure Synapse SQL connection

Consider the following guidelines when you use a Microsoft Azure Synapse SQL connection in a mapping:

- Verify that either the `db_owner` privilege or the following more granular privileges are granted to the user to connect to Microsoft Azure Synapse SQL and perform read and write operations successfully:
  - `EXEC sp_addrolemember 'db_datareader', '<user>';` // Alternately assign permission to individual table
  - `EXEC sp_addrolemember 'db_datawriter', '<user>';` // Alternately assign permission to individual table
  - `GRANT ALTER ANY EXTERNAL DATA SOURCE TO <user>;`
  - `GRANT ALTER ANY EXTERNAL FILE FORMAT TO <user>;`
  - `GRANT CONTROL TO <user>;`
  - `GRANT CREATE TABLE TO <user>;`
  - Assign required privileges for tasks performed through Pre-SQL and Post-SQL commands.
- Ensure that a default schema is present at the account level or user or group level in Microsoft Azure Synapse SQL.

## Author

Adrija Pandya

## Acknowledgements

The author would like to acknowledge V Nirosha for her technical assistance with this article.