Databricks authentication

Overview

The Alchemer Databricks integration uses **OAuth 2.0 (Client Credentials)** to authenticate with the Databricks API. This authentication method uses a **Databricks service principal** with a Client ID and Client Secret.

Databricks API Credentials

What You Need
- A Databricks workspace
- A Databricks service principal
- A Databricks workspace URL
- Client ID
- Client Secret

How to Get Your Databricks API Credentials

1. Create a Service Principal in Databricks

Log in to your Databricks workspace as an administrator and follow these steps:
- Open the **Admin Console**
- Navigate to **Identity and Access → Service Principals**
- Select **Add Service Principal**
- Provide a name and create the service principal

2. Generate a Client ID and Client Secret

Once the service principal is created:
- Open the service principal details
- Locate the **OAuth secrets** or **Client secrets** section
- Generate a new secret
- Copy and securely store the **Client ID** and **Client Secret**

Important: The client secret is only shown once. Make sure to store it securely.

3. Grant Permissions to the Service Principal

Ensure the service principal has access to the Databricks resources it needs:
- Assign workspace permissions
- Grant access to clusters, SQL warehouses, schemas, or jobs as required

Authenticate Databricks in Alchemer

After obtaining your Databricks Client ID and Client Secret, add them to the Alchemer Databricks integration. Credentials are securely stored in Alchemer and can be reused across workflows.

How to Authenticate

1. Start a New Authentication

- Inside any Databricks integration action, select **New Authentication**.

2. Enter Your Databricks Credentials

Provide the following values:

- Client ID
- Client Secret
- Databricks Workspace URL

3. Save Your Authentication

- Select **Create**.
- Once created:
    - The authentication is saved and reused for all Databricks actions
    - You only need to update it if your credentials change or expire

Related Articles