LUMENDATA

Data Sheet

OAUTH Setup with Informatica to Snowflake

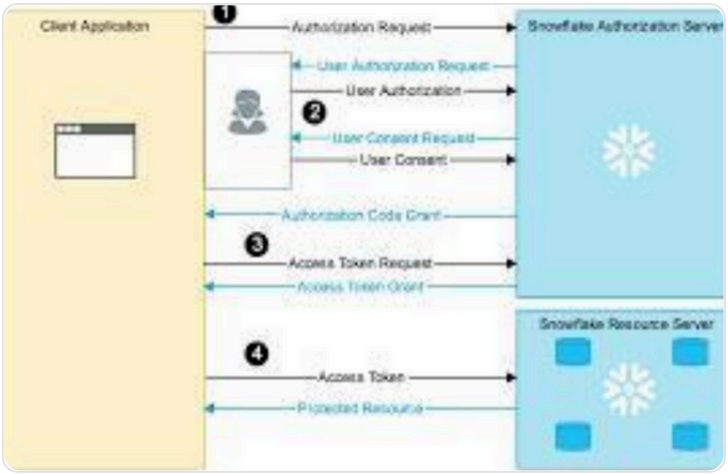
Step-by-Step Guide

5201 GREAT AMERICAN PARKWAY, SUITE 320
SANTA CLARA, CA 95054
Tel: (855) 695-8636
E-mail: info@lumendata.com
Website: www.lumendata.com

The OAuth (Open Authorization) protocol provides a secure and industry-standard framework for accessing resources between applications without sharing sensitive credentials.

When integrating **Snowflake** with **Informatica**, using OAuth ensures secure, token-based authentication to enable seamless data exchange.

This document outlines the steps to configure OAuth authentication between Snowflake & Informatica, ensuring secure and efficient data integration processes.



Key Benefits of Using OAuth for Snowflake and Informatica:

- **Enhanced Security:** OAuth eliminates the need to share and manage passwords, using access tokens instead.
- **Granular Permissions:** Provides fine-grained control over access, allowing tokens to be scoped for specific operations.
- **Compliance:** Aligns with modern security and compliance standards, ensuring best practices for data integration.
- **Simplified Access Management:** Streamlines authentication workflows by leveraging centralized identity providers (IDPs) or Snowflake's OAuth capabilities.

Pre-Requisites:

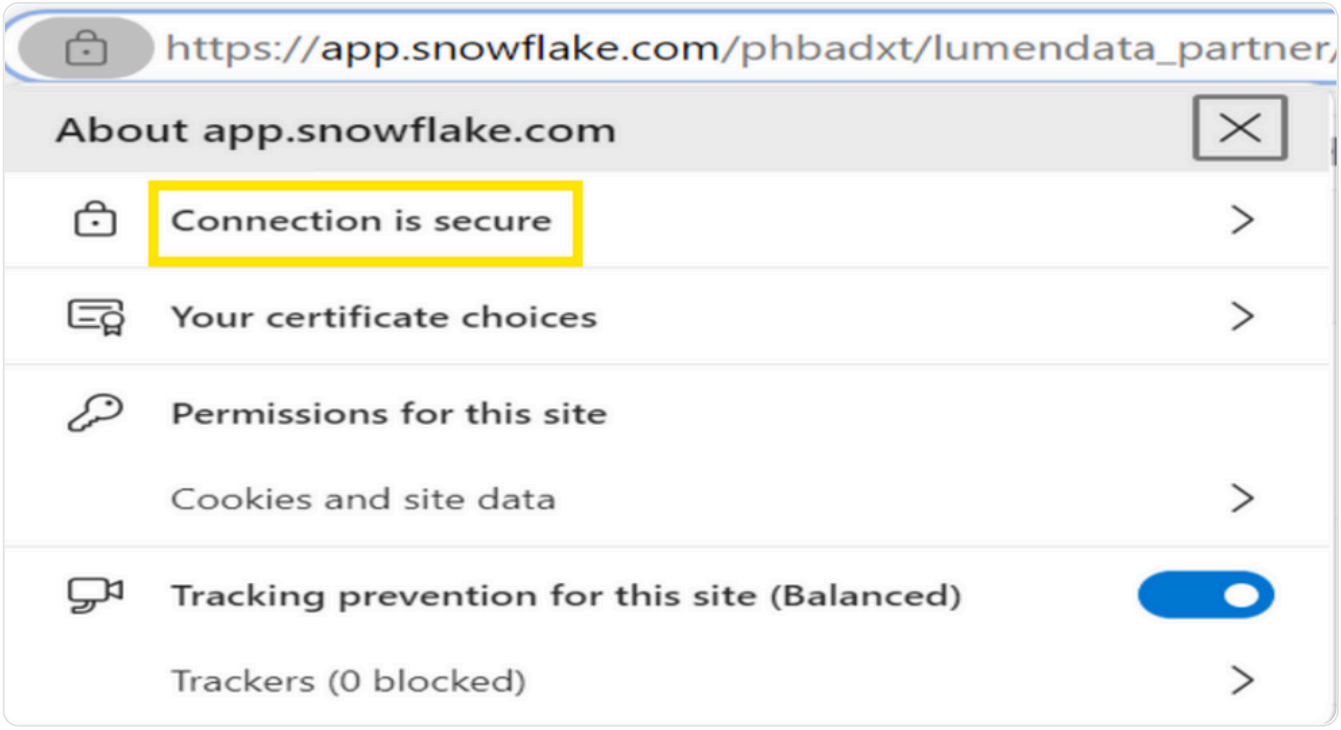
- Active Snowflake account with OAuth enabled.
- Informatica environment with the necessary permissions to configure OAuth.

Steps to be followed:

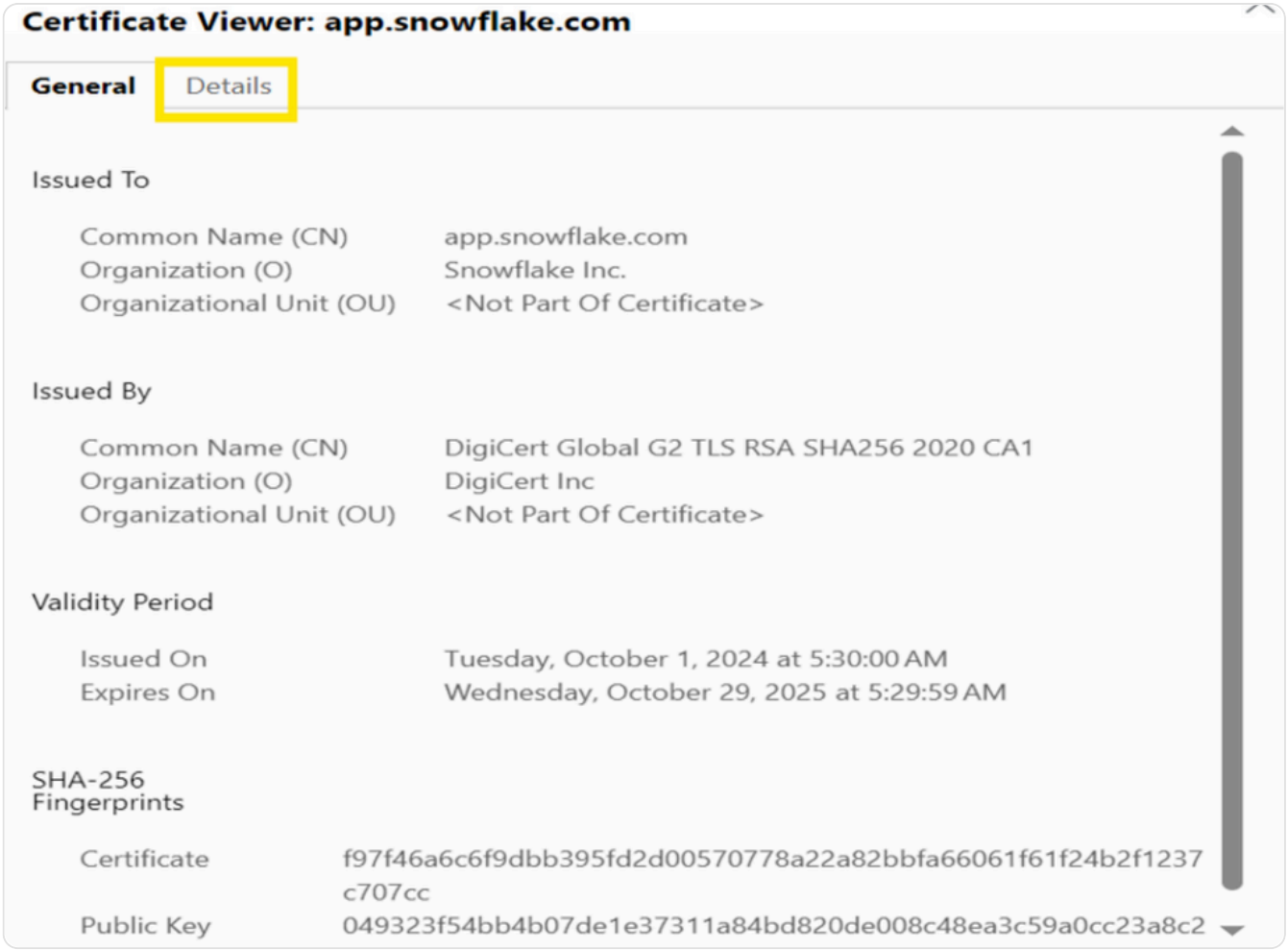
Step 1: Export Certificate Authorities (CAs) Using Chrome Browser

To proceed with downloading the certificate:

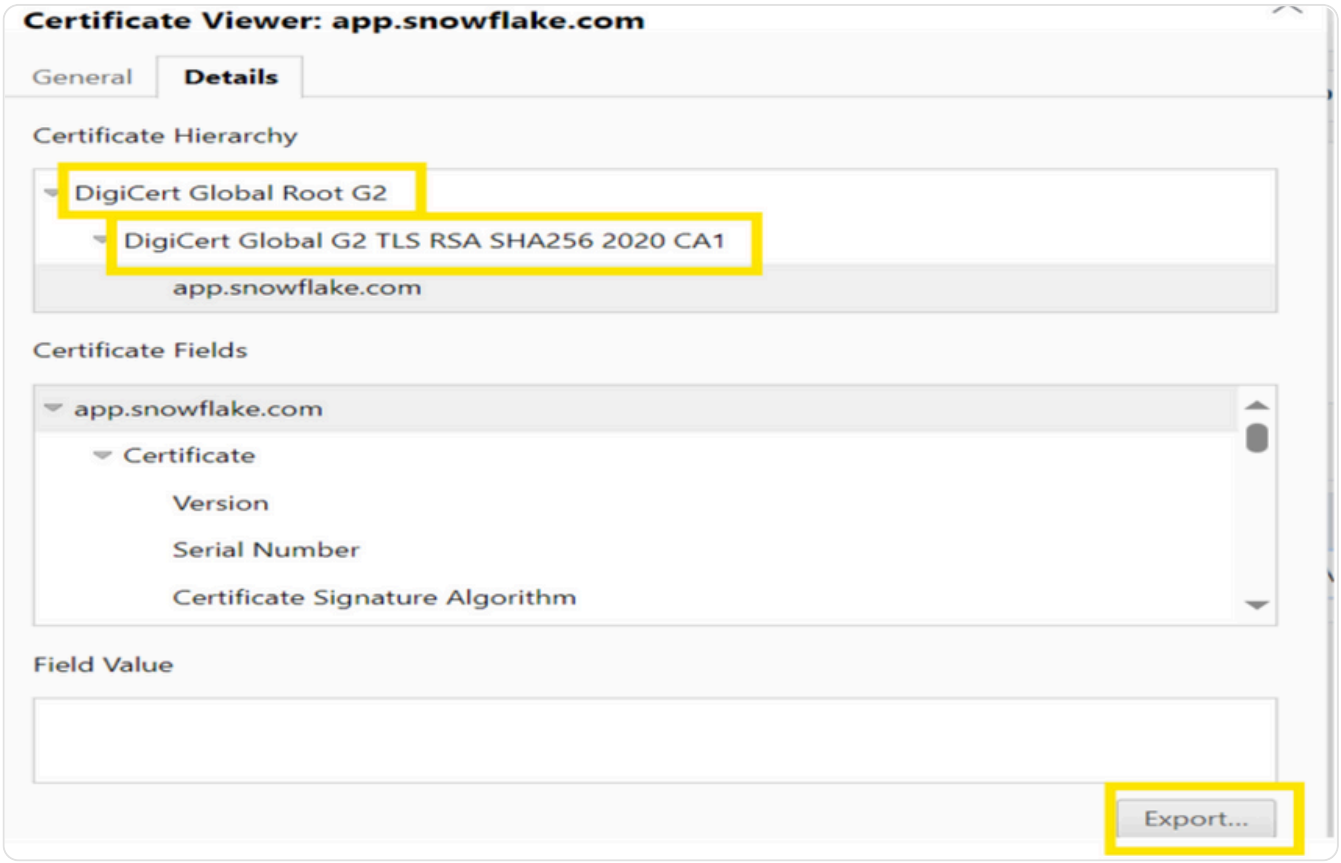
1. **Access Certificate Options:** Click on "Your certificate choices" (or a similar option visible in your browser).



Click on "**Connection is secure**" from options.



Click on **Details**.



Click on **Digicert Global Root G2** and **DigiCert Global G2 TLS RSA SHA256 2020 CA1** and click on export.

Step 2:

Import downloaded certificates from local machine to secure agent folder using below mentioned steps:

- Make sure you have installed Java and set the java home and path environment variables.

Open cmd (run as admin)/shell

1. Go to location *{Secure Agent Root Dir}\apps\jdk {LatestVersion}\jre\lib\security*
   - If this the above path does not exist, Go to location *{Secure Agent Root Dir}\jdk\jre\lib\security*

2. Run the following cmd in command prompt to view all imported certificates details:
   - *keytool -list -keystore cacerts*

3. Refer to the following steps to import certificates into cacerts:
   - Go to location *{Secure Agent Root Dir}\apps\jdk\{LatestVersion}\jre\bin.* If this the above path does not exist, Go to location *{Secure Agent Root Dir}\jdk\jre\lib\security*
   - Run the following cmd in the command prompt: *keytool -import -keystore cacerts -alias <Alias_Name> -file <certificate file location>*

4. Then there would be a password prompt for the keystore password.
   - Enter *changeit* and then enter yes to import the certificate.

5. Repeat the above command for all the CAs exported with different alias:
   - Example: *keytool -import -alias rootCA -file C:\Root.cer -keystore ../lib/security/cacerts -trustcacerts.*

Step 3:

Open Snowflake and login with Account Admin Role and create new security integration with the code below:

```
CREATE  or replace SECURITY INTEGRATION oauth_kp_int
  TYPE = OAUTH
  ENABLED = TRUE
  OAUTH_CLIENT = CUSTOM
  OAUTH_CLIENT_TYPE = 'CONFIDENTIAL'
  OAUTH_REDIRECT_URI = 'https://dm-us.informaticacloud.com/ma/proxy/oauthcallback'
  OAUTH_ISSUE_REFRESH_TOKENS = TRUE
  OAUTH_REFRESH_TOKEN_VALIDITY = 86400;
```

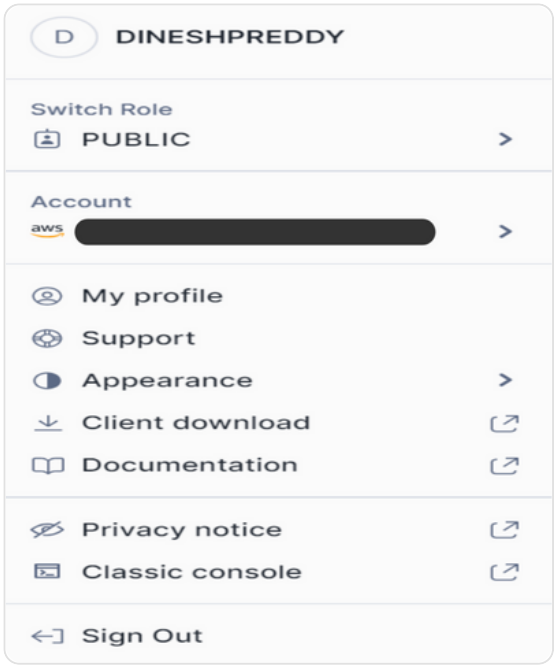
Step 4:

Use the command to get description of Integration: *desc integration oauth_kp_int;*

Results | Chart

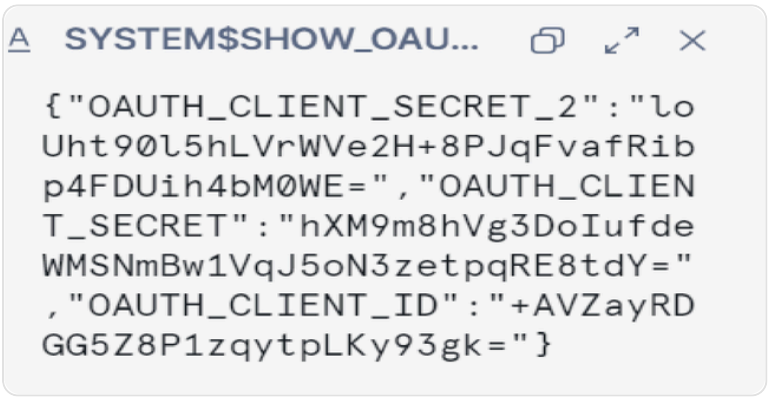
	property	property_type	property_value	property_default
1	ENABLED	Boolean	true	false
2	OAUTH_REDIRECT_URI	String	https://dm-us.informaticacloud.com/ma/proxy/oa	
3	OAUTH_CLIENT_TYPE	String	CONFIDENTIAL	CONFIDENTIAL
4	OAUTH_ISSUE_REFRESH_TOKENS	Boolean	true	true
5	OAUTH_REFRESH_TOKEN_VALIDITY	Integer	86400	7776000
6	OAUTH_ENFORCE_PKCE	Boolean	false	false
7	OAUTH_USE_SECONDARY_ROLES	String	NONE	NONE
8	OAUTH_CLIENT_ID	String	[redacted]	
9	OAUTH_AUTHORIZATION_ENDPOINT	String	[redacted]	
10	OAUTH_TOKEN_ENDPOINT	String	[redacted]	
11	OAUTH_ALLOWED_AUTHORIZATION_ENDPOINTS	List	[redacted]	[]
12	OAUTH_ALLOWED_TOKEN_ENDPOINTS	List	[redacted]	[]
13	PRE_AUTHORIZED_ROLES_LIST	List		[]
14	BLOCKED_ROLES_LIST	List	ACCOUNTADMIN,ORGADMIN,SECURITYADMIN	[]
15	OAUTH_ALLOW_NON_TLS_REDIRECT_URI	Boolean	false	false
16	OAUTH_CLIENT_RSA_PUBLIC_KEY_FP	String		

Make sure role should be set to any role apart from AccountAdmin,OrgAdmin,SecurityAdmin in Snowflake.



Step 5:

Use below Statement to get client secret for integration created in snowflake.
select system$show_oauth_client_secrets('OAUTH_KP_INT');

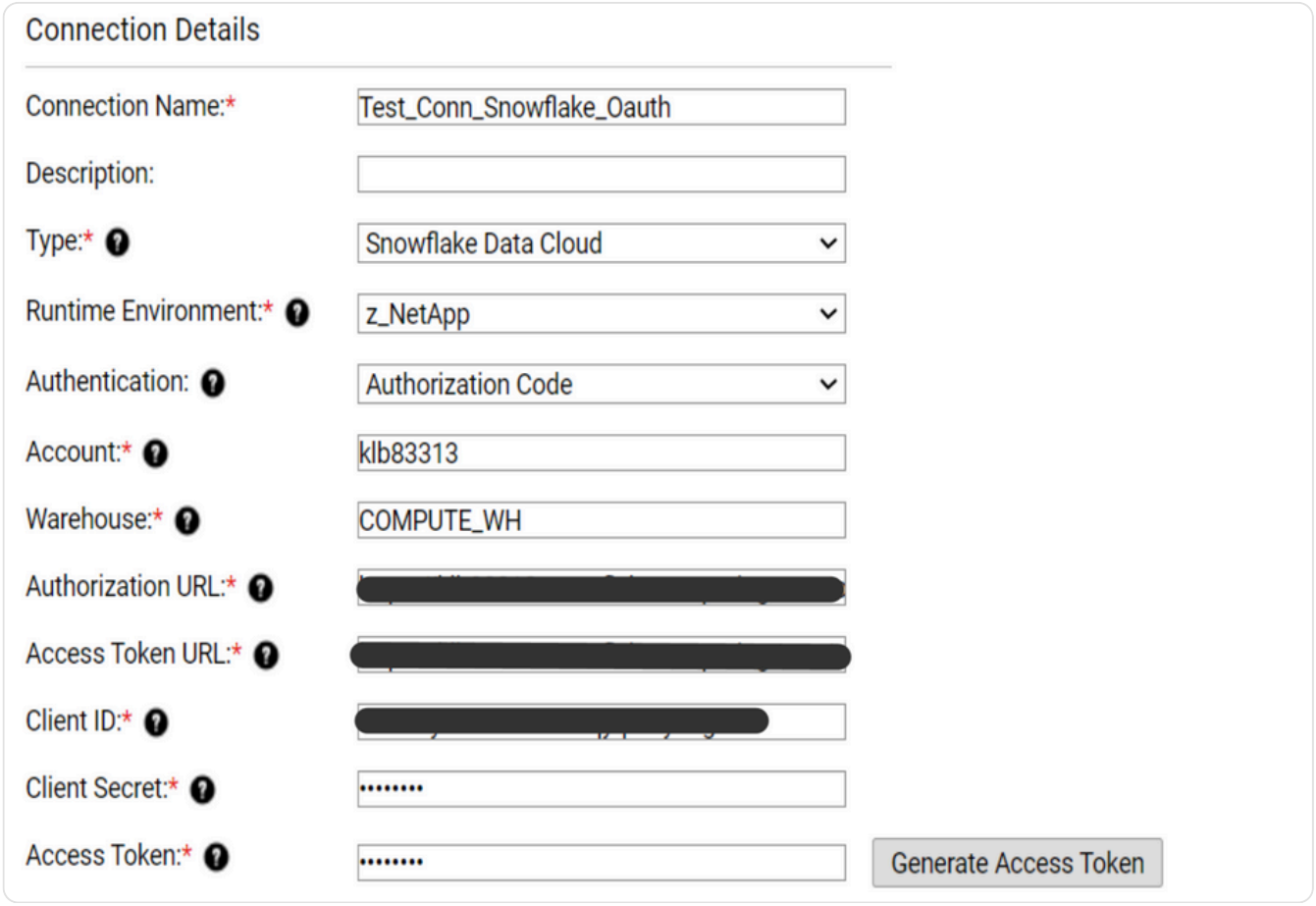


Step 6:

Open Informatica's Administrator service and navigate to connections click on new connection.

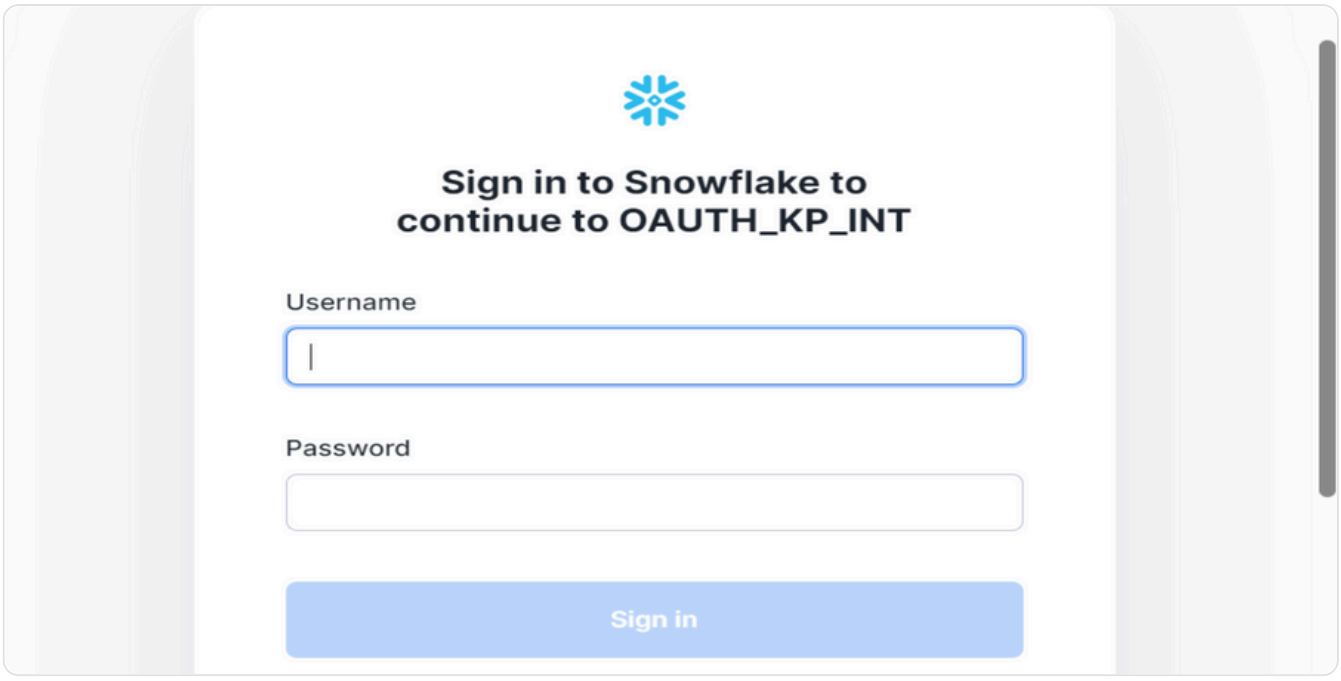
Select connection type is snowflake data cloud and set authentication as snowflake datacloud.

Give necessary information as shown in picture below:



Step 7:

Generate Tokens from access tokens and new snowflake authentication prompt will popup.



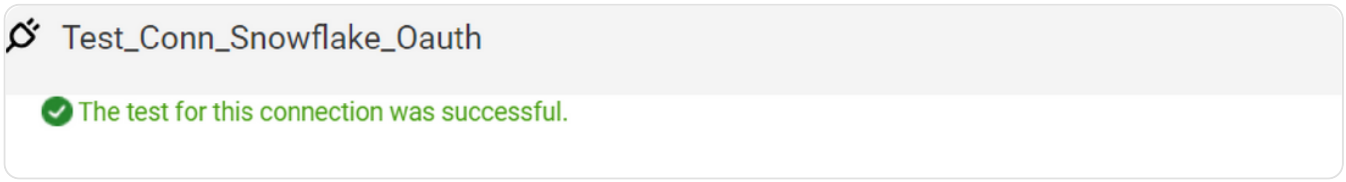
Login snowflake with credentials to generate tokens.

Step 8:

Add Database and schema names in additional JDBC URL Parameters to make sure the connection point outs to particular Database and schema.

Step 9:

Test the connections once necessary details are filled.



Authors

Abhishek Gaur
Technical Lead - Level 1

P Dinesh Reddy
Junior Data Analyst

About LumenData

LumenData is a leading provider of **Enterprise Data Management, Cloud & Analytics** solutions. We help businesses navigate their data visualization and analytics anxieties and enable them to accelerate their innovation journeys.

Founded in 2008, with locations in multiple countries, LumenData is privileged to serve over 100 leading companies. LumenData is **SOC2 certified** and has instituted extensive controls to protect client data, including adherence to GDPR and CCPA regulations.

LUMENDATA

Get in touch with us:
info@lumendata.com

Let us know what you need:
lumendata.com/contact-us