LUMENDATA

Data Sheet

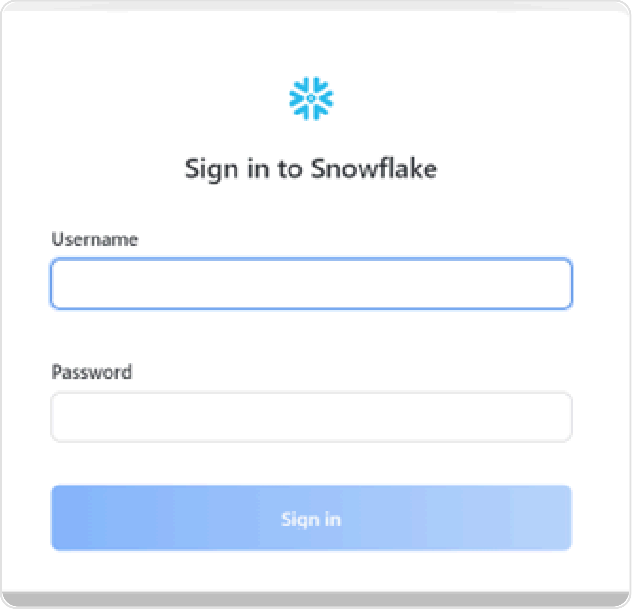
Microsoft Entra SSO Integration with Snowflake

Step-by-Step Guide

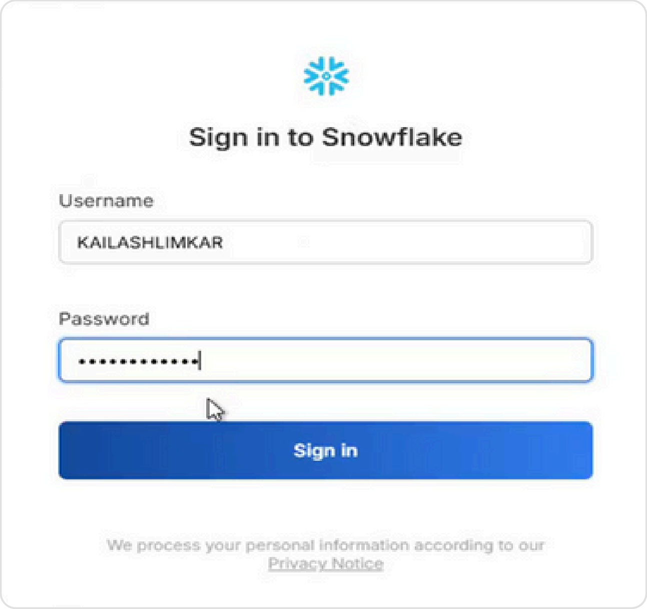
5201 GREAT AMERICAN PARKWAY, SUITE 320
SANTA CLARA, CA 95054
Tel: (855) 695-8636
E-mail: info@lumendata.com
Website: www.lumendata.com

Logging into Snowflake Before SSO:

1. Go to the Snowflake login page.

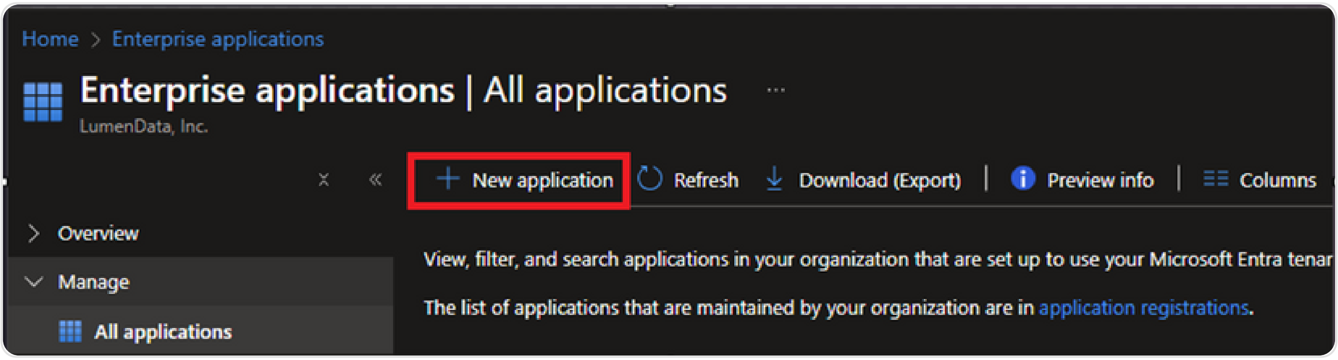


2. Enter Snowflake username & password to sign in.


Sign in to Snowflake
Username
KAILASHLIMKAR
Password
Sign in
We process your personal information according to our Privacy Notice

Configuring Azure AD SAML/SSO/Federated Authentication for Snowflake

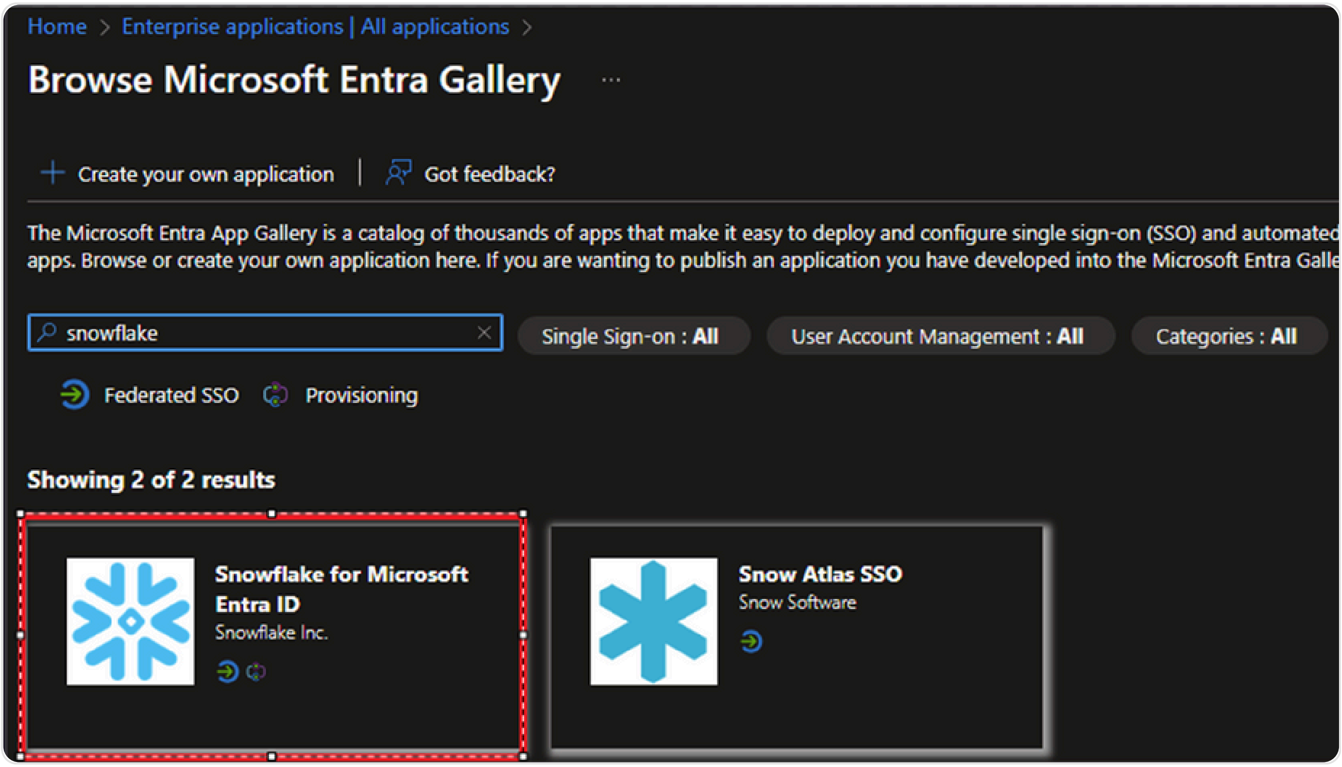
1. Login to Portal.Azure.com
2. Go to Microsoft Entra ID -> Enterprise Applications
3. Click New application



View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenar

The list of applications that are maintained by your organization are in application registrations.

4. In the Browse Azure AD Gallery search bar, search for Snowflake, and choose Snowflake for Microsoft Entra ID.



Home > Enterprise applications | All applications >

Browse Microsoft Entra Gallery ...

The Microsoft Entra App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated apps. Browse or create your own application here. If you are wanting to publish an application you have developed into the Microsoft Entra Galle

snowflake

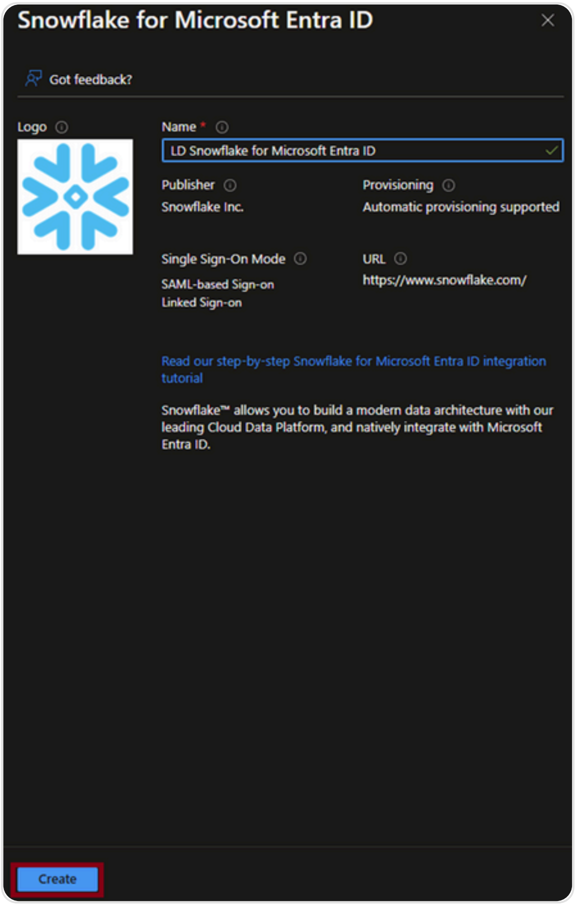
Single Sign-on : **All** | User Account Management : **All** | Categories : **All**

Showing 2 of 2 results

Snowflake for Microsoft Entra ID
Snowflake Inc.

Snow Atlas SSO
Snow Software

5. Give your Snowflake application a name, then click Create.



Snowflake for Microsoft Entra ID

Name * LD Snowflake for Microsoft Entra ID

Publisher
Snowflake Inc.

Provisioning
Automatic provisioning supported

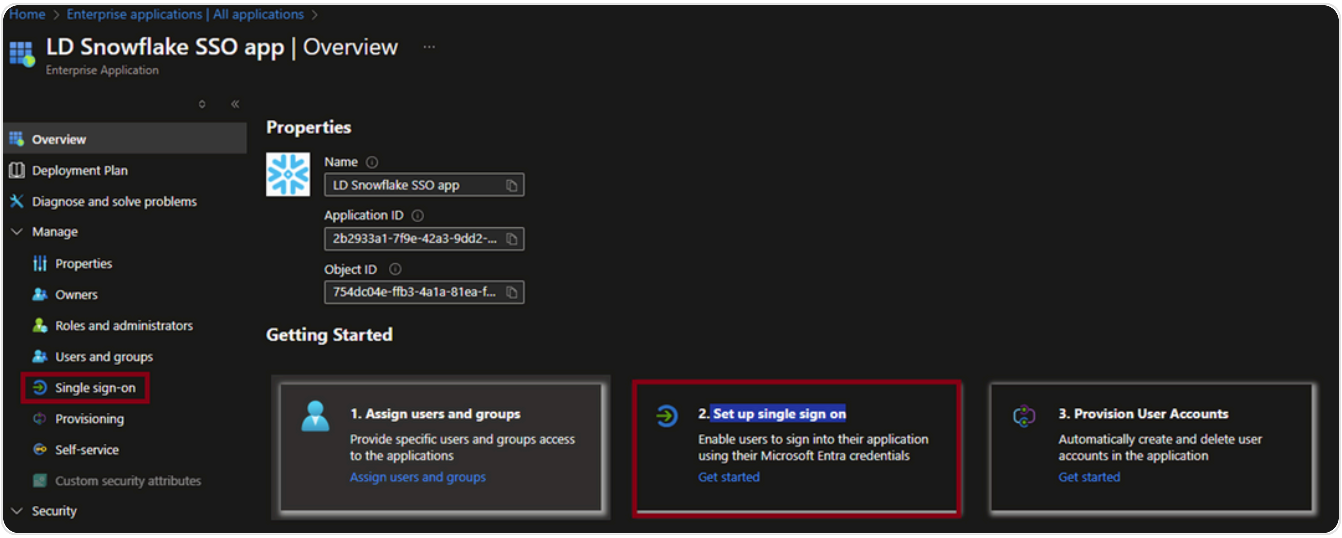
Single Sign-On Mode
SAML-based Sign-on
Linked Sign-on

URL
https://www.snowflake.com/

Read our step-by-step Snowflake for Microsoft Entra ID integration tutorial

Snowflake™ allows you to build a modern data architecture with our leading Cloud Data Platform, and natively integrate with Microsoft Entra ID.

6. Once the application is created, on the left side choose Single sign-on. Then select Set up single sign-on.



Home > Enterprise applications | All applications >

LD Snowflake SSO app | Overview ...

Enterprise Application

Properties

Name: LD Snowflake SSO app

Application ID: 2b2933a1-7f9e-42a3-9dd2-...

Object ID: 754dc04e-ffb3-4a1a-81ea-f...

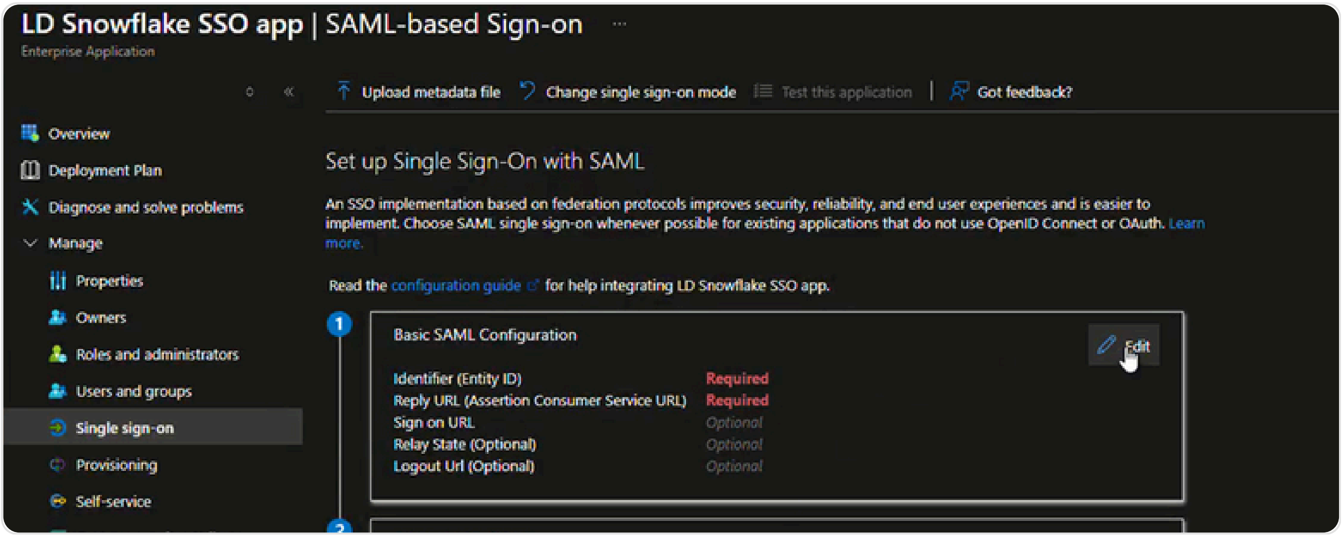
Getting Started

1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Microsoft Entra credentials
Get started

3. Provision User Accounts
Automatically create and delete user accounts in the application
Get started

7. Under the Basic SAML configuration section, click Edit.



LD Snowflake SSO app | SAML-based Sign-on ...

Enterprise Application

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating LD Snowflake SSO app.

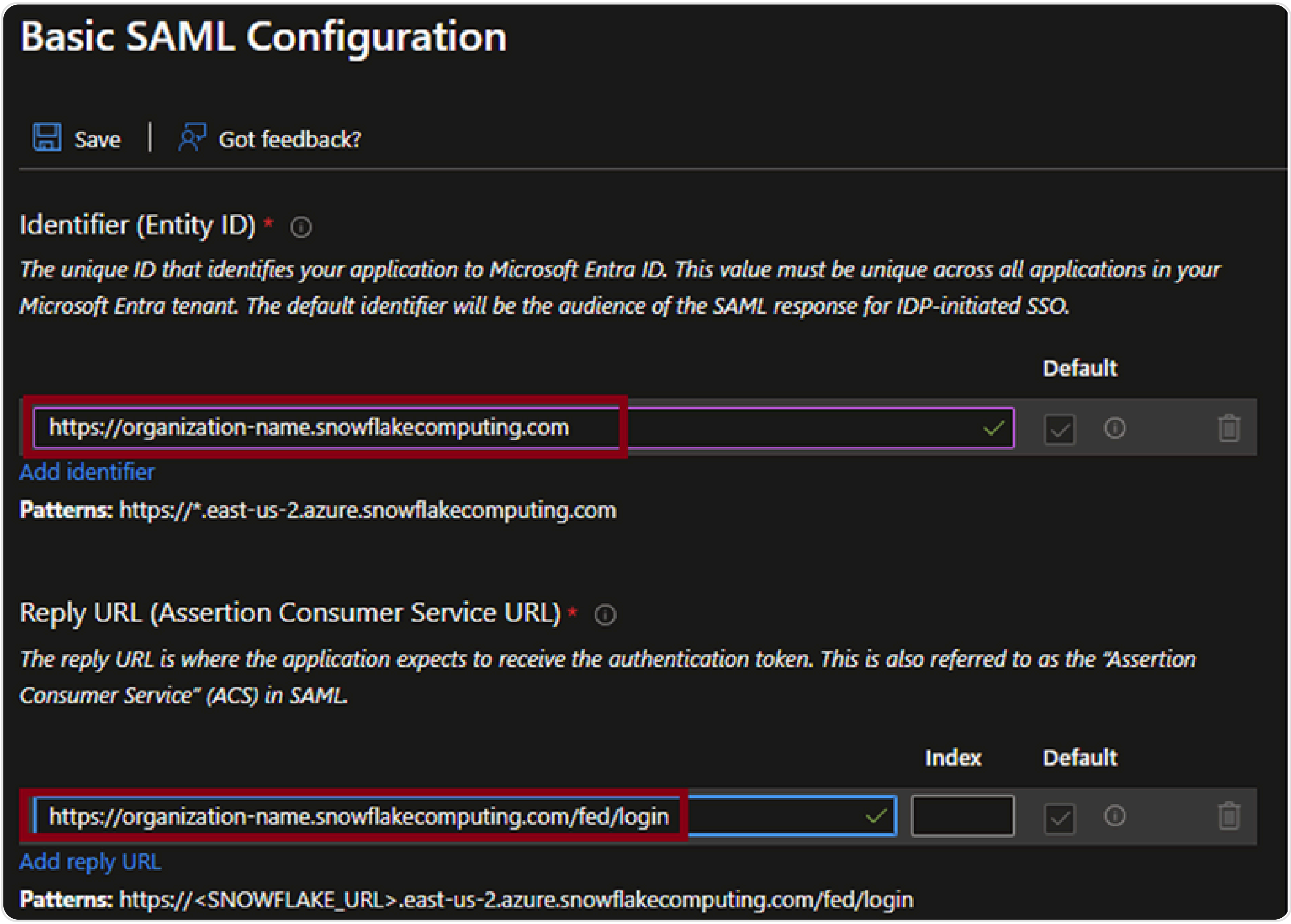
1 Basic SAML Configuration — Edit

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

8. In the Basic SAML Configuration section, perform the following steps, if you wish to configure the application in IDP initiated mode:

Here we will use the organization-name account format.

- In the Identifier text box, type a URL using the following pattern: https://<organization-name.snowflakecomputing.com
- In the Reply URL text box, type a URL using the following pattern: https://SNOWFLAKE-URL.snowflakecomputing.com/fed/login



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

https://organization-name.snowflakecomputing.com ✓ ☑

Add identifier

Patterns: https://*.east-us-2.azure.snowflakecomputing.com

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

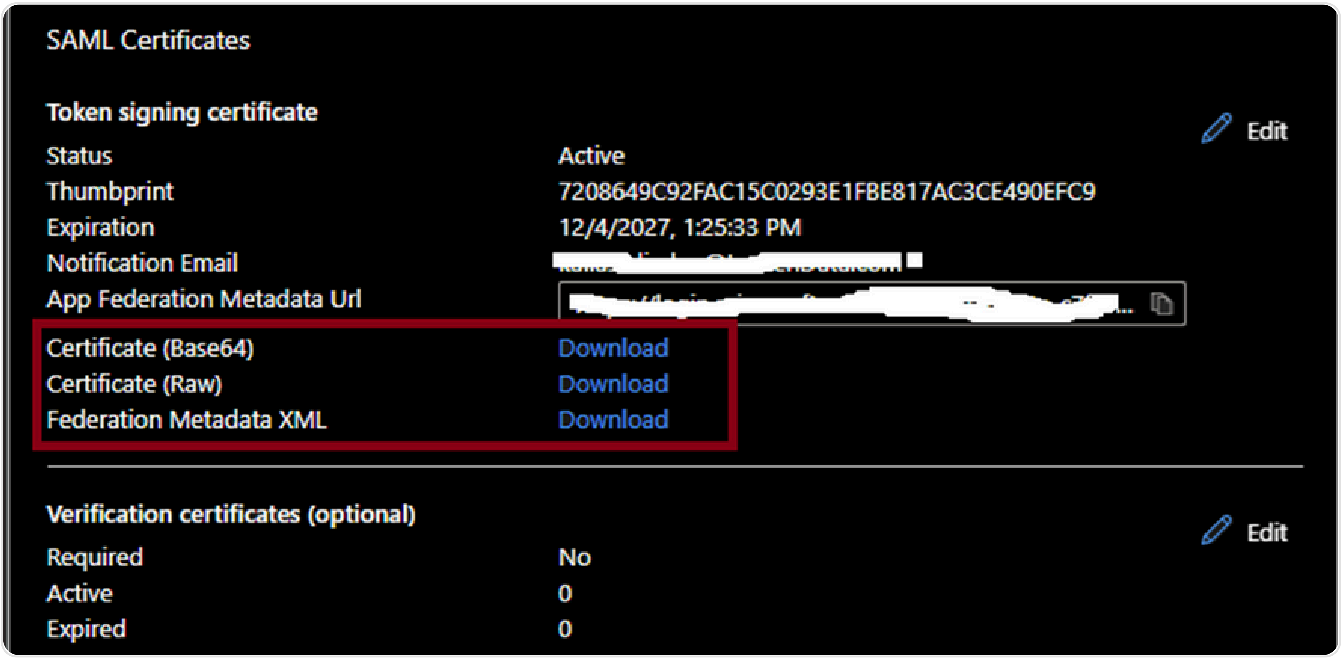
Index Default

https://organization-name.snowflakecomputing.com/fed/login ✓ ☑

Add reply URL

Patterns: https://<SNOWFLAKE_URL>.east-us-2.azure.snowflakecomputing.com/fed/login

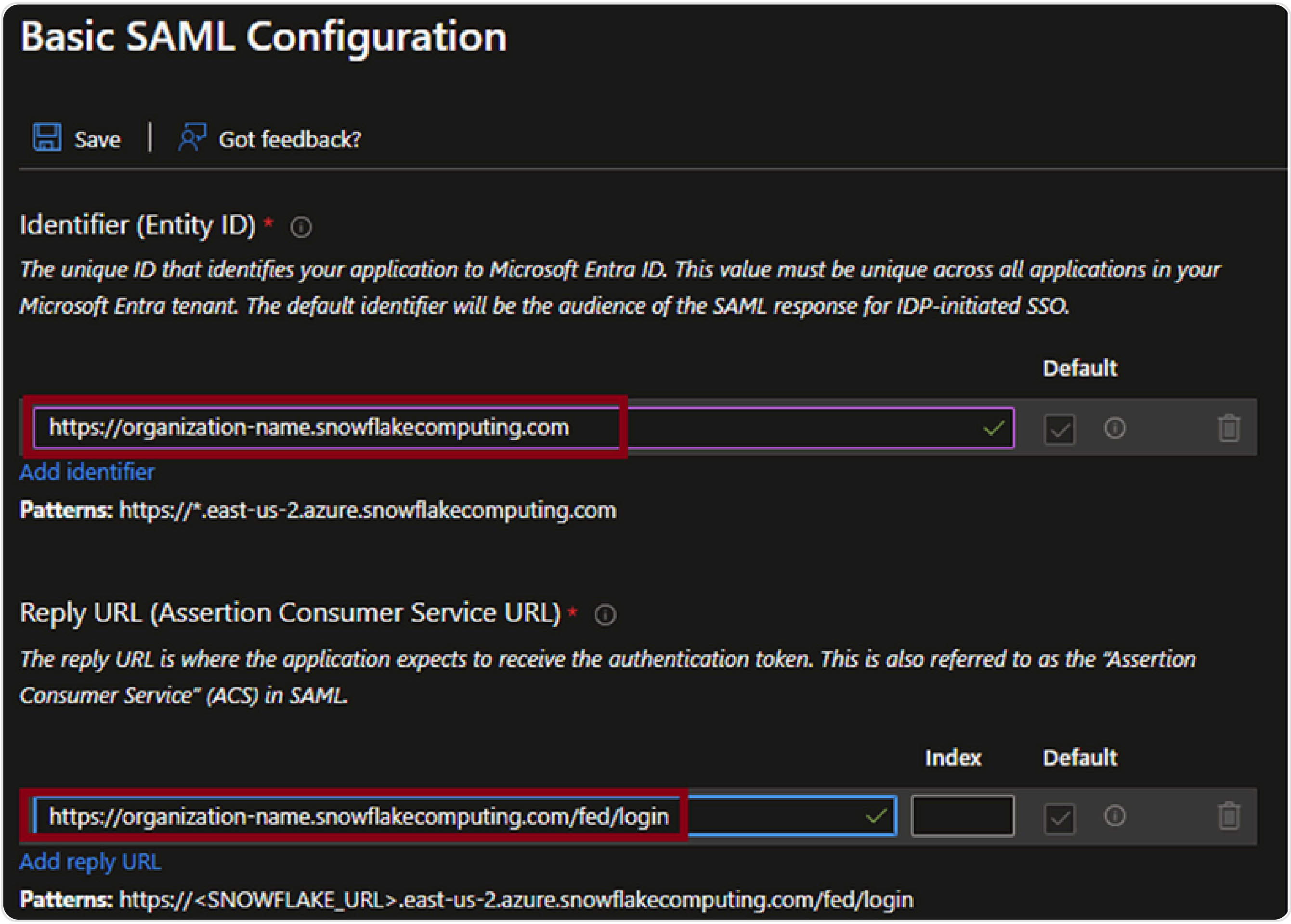
9. On the Set up Single Sign-On with SAML page, in the SAML Certificate section, click Download to download the Certificate (Base64) from the given options as per your requirement and save it on your Local Drive.



SAML Certificates

Token signing certificate	
Status	Active
Thumbprint	7208649C92FAC15C0293E1FBE817AC3CE490EFC9
Expiration	12/4/2027, 1:25:33 PM
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)	
Required	No
Active	0
Expired	0



Basic SAML Configuration

Identifier (Entity ID) *

The unique ID that identifies your application to Microsoft Entra ID. This value must be unique across all applications in your Microsoft Entra tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

	Default
https://organization-name.snowflakecomputing.com ✓	☑

Patterns: https://*.east-us-2.azure.snowflakecomputing.com

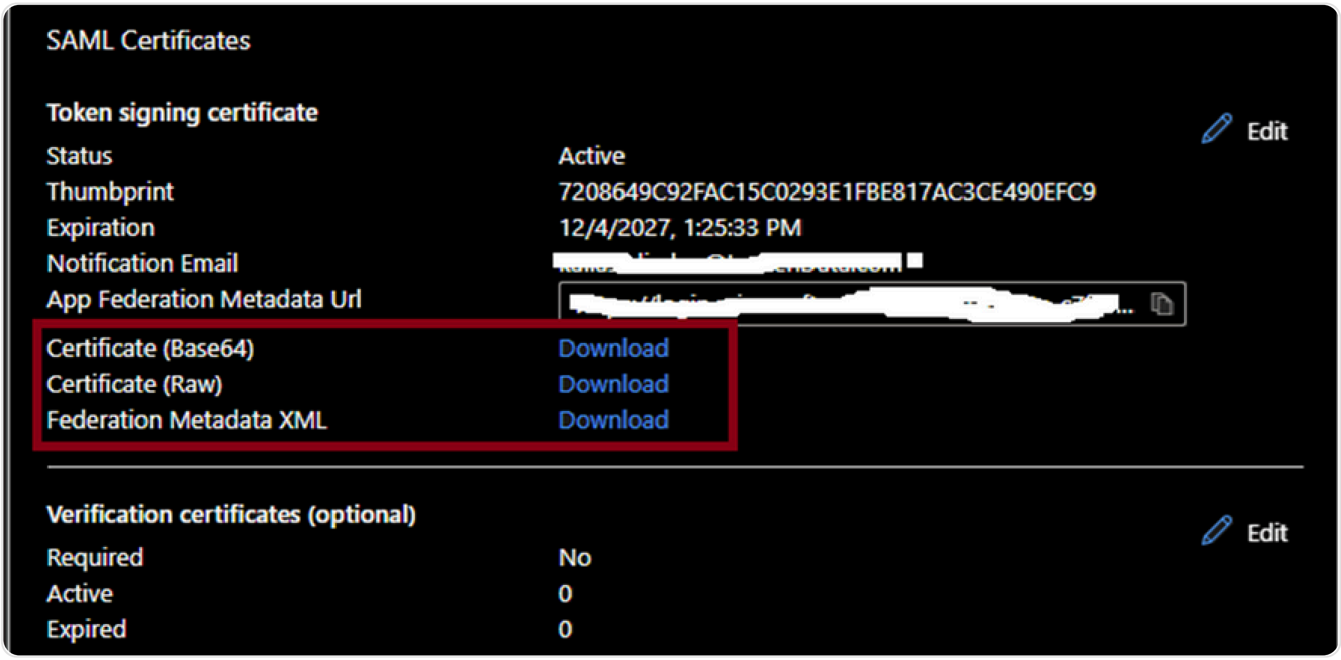
Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://organization-name.snowflakecomputing.com/fed/login ✓		☑

Patterns: https://<SNOWFLAKE_URL>.east-us-2.azure.snowflakecomputing.com/fed/login

9. On the Set up Single Sign-On with SAML page, in the SAML Certificate section, click Download to download the Certificate (Base64) from the given options as per your requirement and save it on your Local Drive.



SAML Certificates

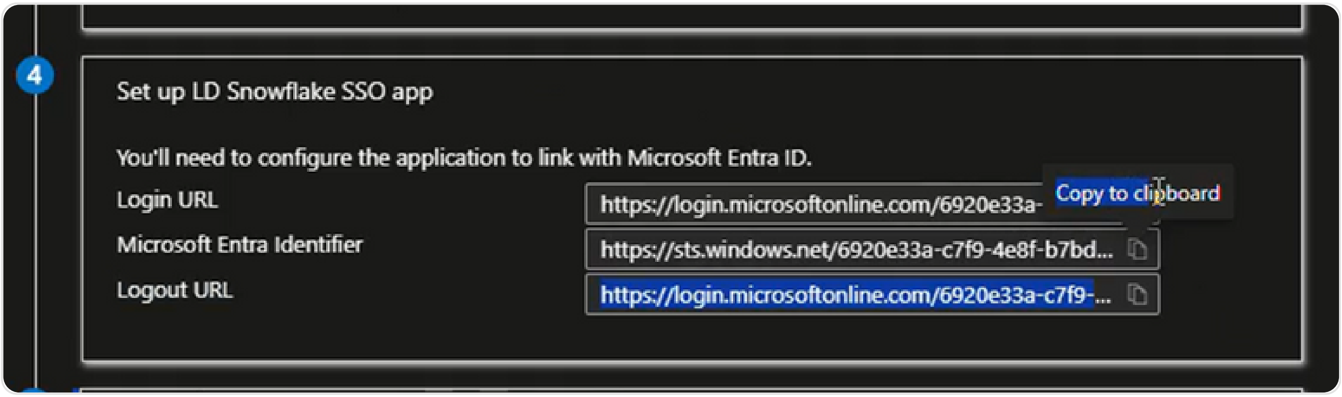
Token signing certificate

Status	Active
Thumbprint	7208649C92FAC15C0293E1FBE817AC3CE490EFC9
Expiration	12/4/2027, 1:25:33 PM
Notification Email	[redacted]
App Federation Metadata Url	[redacted]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Required	No
Active	0
Expired	0

10. On the **Set up Snowflake** section, copy the appropriate URL(s) as per your requirement.



4

Set up LD Snowflake SSO app

You'll need to configure the application to link with Microsoft Entra ID.

Login URL https://login.microsoftonline.com/6920e33a-

Microsoft Entra Identifier https://sts.windows.net/6920e33a-c7f9-4e8f-b7bd...

Logout URL https://login.microsoftonline.com/6920e33a-c7f9-...

Step 2: Configuring Snowflake for SAML/SSO/Federated Authentication using Azure AD

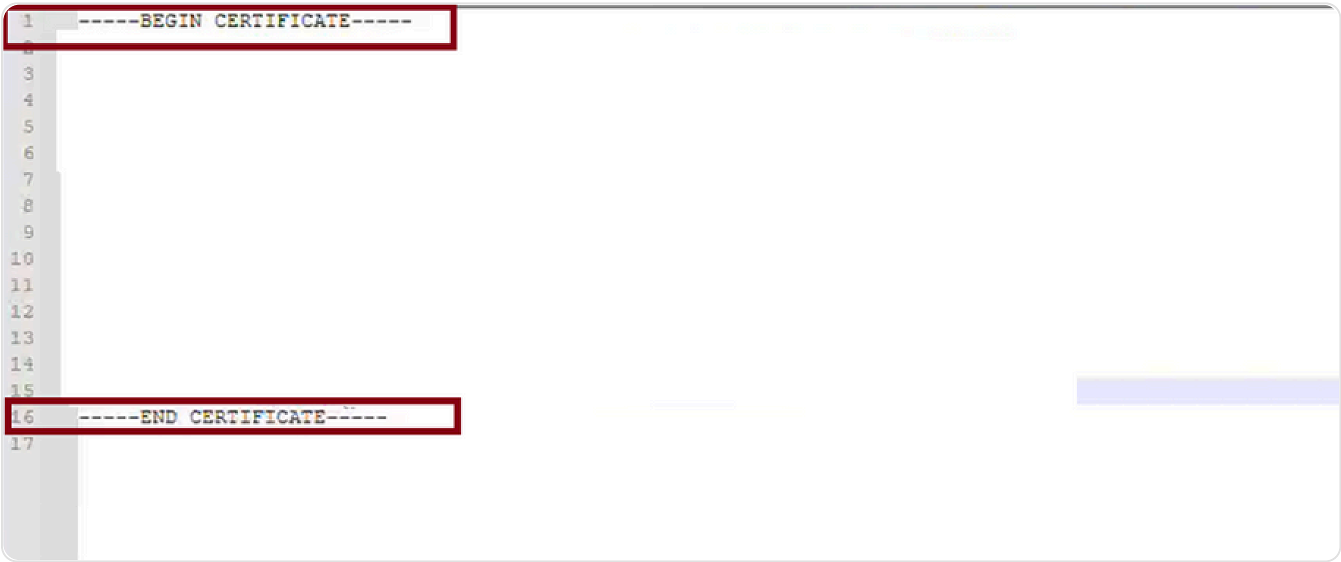
To create a SAML2 integration with Azure AD in Snowflake, you should have previously collected the following information from the Azure AD Snowflake for AAD application:

- Certificate (Base64)
- Azure Issuer (Entity ID)
  - SAML2_ISSUER = '<EntityID/Issuer value which you have copied>'
- LOGIN URL
  - SAML2_SSO_URL = '<Login URL value which you have copied>'

The above values can all be found in the XML Federation Metadata file, where:

- X509Certificate
- entityID in format https://sts.windows.net/[...]/ (include the trailing forward slash).
- Location in format https://login.microsoftonline.com/[...]/saml2

1. In a different web browser window, log in to Snowflake as a Security Administrator.
2. Switch Role to ACCOUNTADMIN, by clicking on profile on the top right side of page.
3. Open the downloaded certificate in notepad editor. Copy the value between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" and paste this content into the SAML2_X509_CERT.

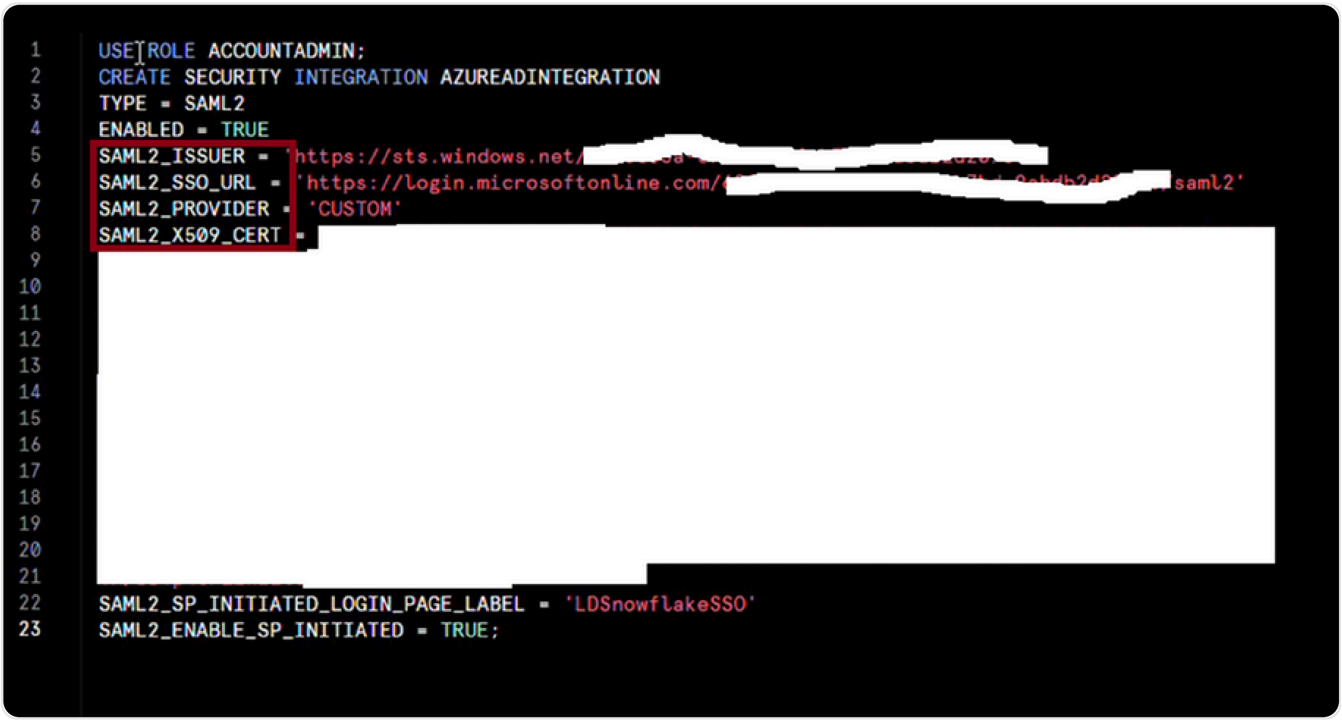


```
-----BEGIN CERTIFICATE-----
[redacted]
-----END CERTIFICATE-----
```

4. In the SAML2_ISSUER, paste Identifier value, which you copied previously.

5. In the SAML2_SSO_URL, paste Login URL value, which you copied previously.

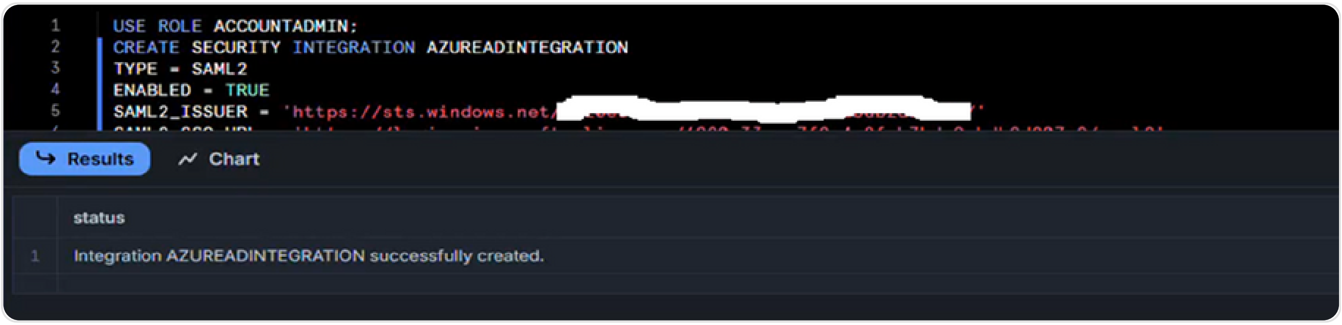
6. In the SAML2_PROVIDER, give the value like CUSTOM.



```
USE ROLE ACCOUNTADMIN;
CREATE SECURITY INTEGRATION AZUREADINTEGRATION
TYPE = SAML2
ENABLED = TRUE
SAML2_ISSUER = 'https://sts.windows.net/[redacted]
SAML2_SSO_URL = 'https://login.microsoftonline.com/[redacted]saml2'
SAML2_PROVIDER = 'CUSTOM'
SAML2_X509_CERT = [redacted]
SAML2_SP_INITIATED_LOGIN_PAGE_LABEL = 'LDSnowflakeSSO'
SAML2_ENABLE_SP_INITIATED = TRUE;
```

CREATE [OR REPLACE] SECURITY INTEGRATION [IF NOT EXISTS]
TYPE = SAML2
ENABLED = TRUE | FALSE
SAML2_ISSUER = '<EntityID/Issuer value which you have copied>'
SAML2_SSO_URL = '<Login URL value which you have copied>'
SAML2_PROVIDER = 'CUSTOM'
SAML2_X509_CERT = '<Paste the content of downloaded certificate from Azure portal>'
SAML2_SP_INITIATED_LOGIN_PAGE_LABEL = '<string_literal>'
SAML2_ENABLE_SP_INITIATED = TRUE | FALSE

7. Select the All Queries and click Run.



```
USE ROLE ACCOUNTADMIN;
CREATE SECURITY INTEGRATION AZUREADINTEGRATION
TYPE = SAML2
ENABLED = TRUE
SAML2_ISSUER = 'https://sts.windows.net/[redacted]'
```

	status
1	Integration AZUREADINTEGRATION successfully created.

11. Configure Snowflake to support provisioning with Microsoft Entra ID

Before you configure Snowflake for automatic user provisioning with Microsoft Entra ID, you need to enable System for Cross-domain Identity Management (SCIM) provisioning on Snowflake.

1. Sign in to Snowflake as an administrator and execute the following.

use role accountadmin;

create role if not exists AzureConnection;

grant create user on account to role AzureConnection;

grant create role on account to role AzureConnection;

grant role AzureConnection to role accountadmin;

create or replace security integration AzureConnection

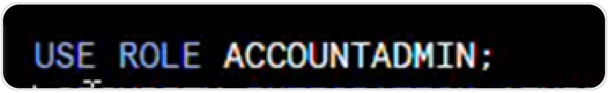
type = scim

scim_client = 'azure'

run_as_role = ' AzureConnection ';

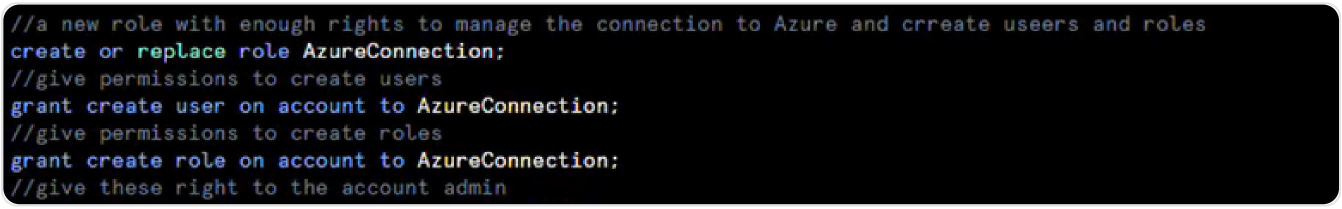
select system$generate_scim_access_token(' AzureConnection ');

2. Use the ACCOUNTADMIN role.



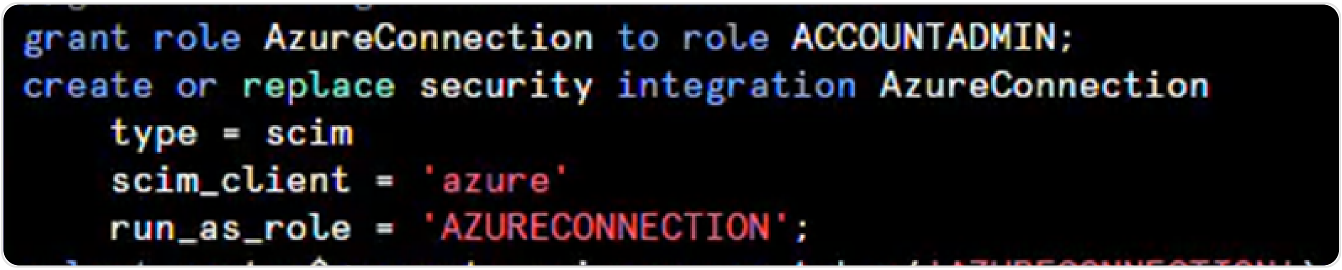
```
USE ROLE ACCOUNTADMIN;
```

3. Create the custom role AzureConnection. All users and roles in Snowflake created by Microsoft Entra ID will be owned by the scoped down AzureConnection role.



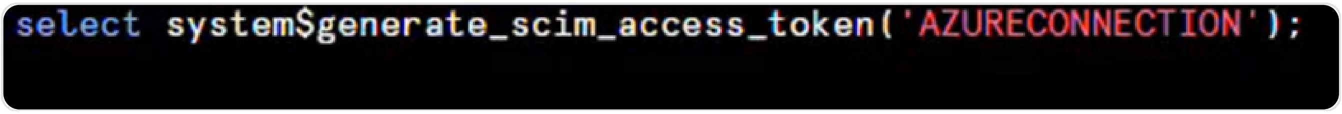
```
//a new role with enough rights to manage the connection to Azure and crreate useers and roles
create or replace role AzureConnection;
//give permissions to create users
grant create user on account to AzureConnection;
//give permissions to create roles
grant create role on account to AzureConnection;
//give these right to the account admin
```

4. Let the ACCOUNTADMIN role create the security integration using the AzureConnection custom role.



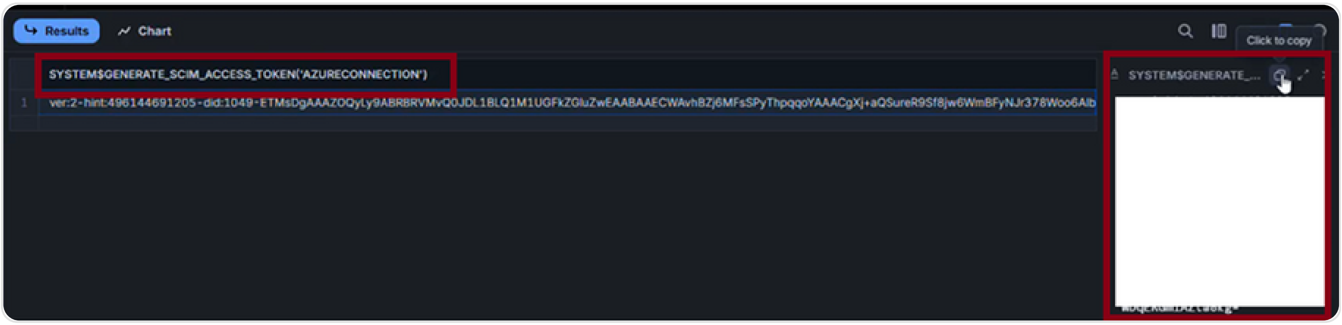
```
grant role AzureConnection to role ACCOUNTADMIN;
create or replace security integration AzureConnection
    type = scim
    scim_client = 'azure'
    run_as_role = 'AZURECONNECTION';
```

5. Create authorization token by running the select statement as below:



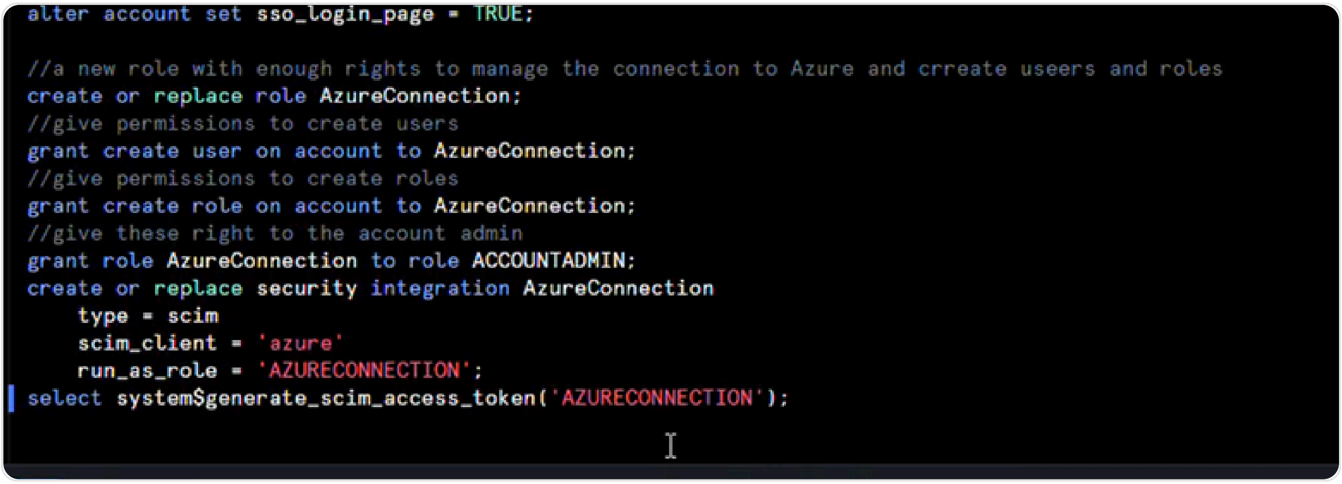
```
select system$generate_scim_access_token('AZURECONNECTION');
```

Copy the token and store securely for later use.



	SYSTEM$GENERATE_SCIM_ACCESS_TOKEN('AZURECONNECTION')
1	ver:2-hint:496144691205-did:1049-ETMsDgAAAZOQyLy9ABRBRVMvQ0JDL1BLQ1M1UGFkZGluZwEAABAAECWAvhBZj6MFsSPyThpqqoYAAACgXj+aQSureR9Sf8jw6WmBFyNJr378Woo6Alb

<span>Note:</span> The access token expires after six months, and a new access token can be generated with this statement.

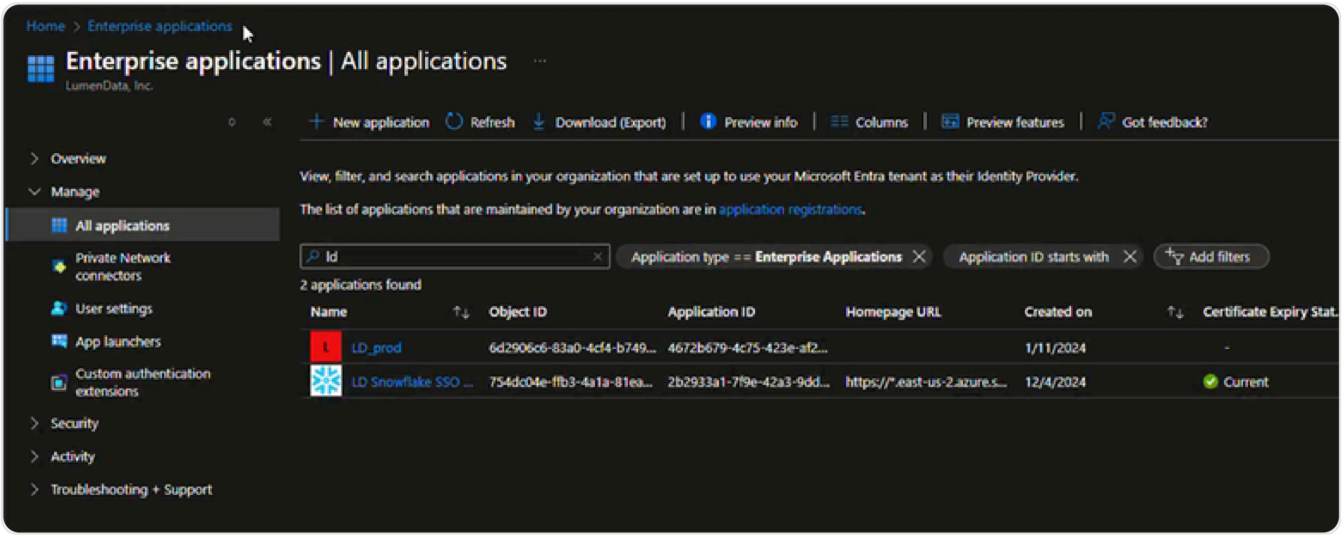


```
alter account set sso_login_page = TRUE;

//a new role with enough rights to manage the connection to Azure and crreate useers and roles
create or replace role AzureConnection;
//give permissions to create users
grant create user on account to AzureConnection;
//give permissions to create roles
grant create role on account to AzureConnection;
//give these right to the account admin
grant role AzureConnection to role ACCOUNTADMIN;
create or replace security integration AzureConnection
    type = scim
    scim_client = 'azure'
    run_as_role = 'AZURECONNECTION';
select system$generate_scim_access_token('AZURECONNECTION');
```

12. To configure automatic user provisioning for Snowflake in Microsoft Entra ID:

- Sign in to the Microsoft Entra admin center as a Admin.
- Browse to Identity > Applications > Enterprise applications.



View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

The list of applications that are maintained by your organization are in application registrations.

ld

Application type == Enterprise Applications

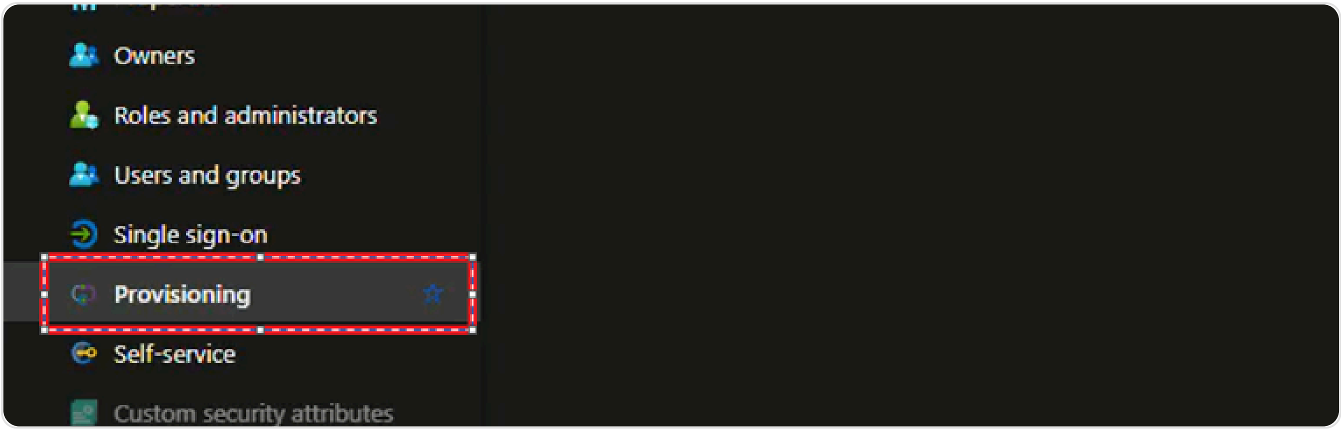
Application ID starts with

Add filters

2 applications found

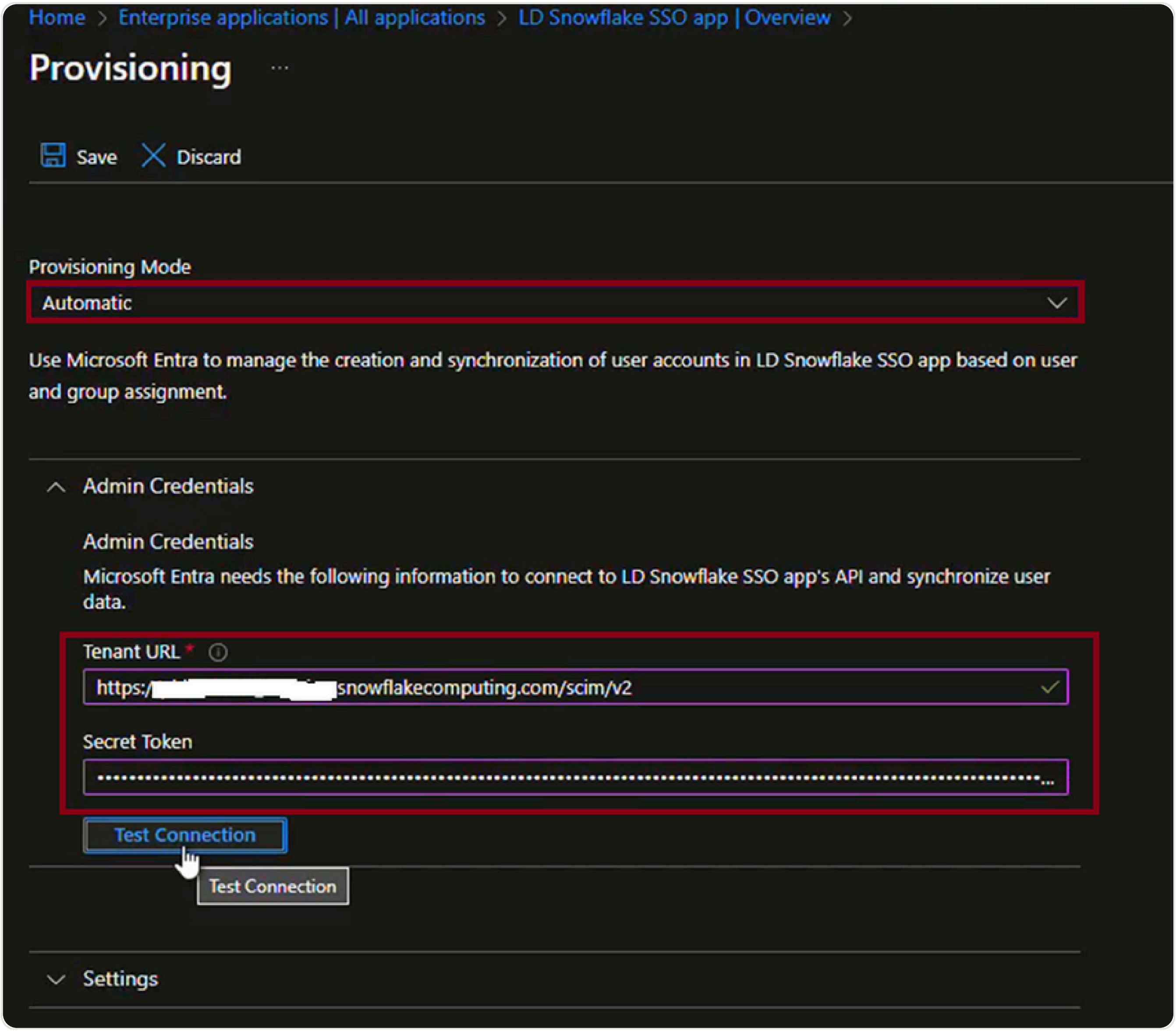
Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Stat.
LD_prod	6d2906c6-83a0-4cf4-b749...	4672b679-4c75-423e-af2...		1/11/2024	-
LD Snowflake SSO ...	754dc04e-ffb3-4a1a-81ea...	2b2933a1-7f9e-42a3-9dd...	https://*.east-us-2.azure.s...	12/4/2024	Current

- In the list of applications, select LDSnowflakeSSO that you created earlier.
- Select the Provisioning tab.



- Set Provisioning Mode to Automatic.

In the Admin Credentials section, enter the SCIM 2.0 base URL and authentication token that you retrieved earlier in the Tenant URL and Secret Token boxes, respectively.



Home > Enterprise applications | All applications > LD Snowflake SSO app | Overview >

Provisioning

Provisioning Mode

Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in LD Snowflake SSO app based on user and group assignment.

Admin Credentials

Admin Credentials

Microsoft Entra needs the following information to connect to LD Snowflake SSO app's API and synchronize user data.

Tenant URL *

https:/[redacted]snowflakecomputing.com/scim/v2

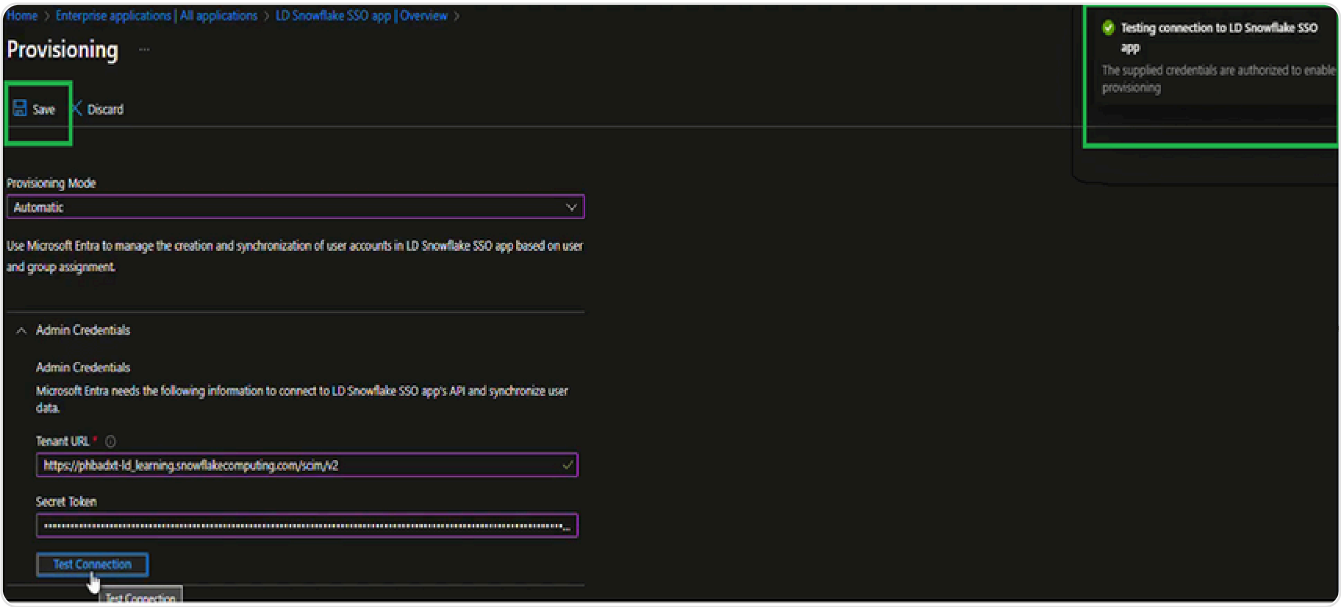
Secret Token

••...

- Note: The Snowflake SCIM endpoint consists of the Snowflake account URL appended with /scim/v2/.

the Tenant URL value is https://.snowflakecomputing.com/scim/v2.
Select Test Connection to ensure that Microsoft Entra ID can connect to Snowflake. If the connection fails, ensure that your Snowflake account has admin permissions and try again.

- Test the connection and if the connection is successful. Save the connection.



Home > Enterprise applications | All applications > LD Snowflake SSO app | Overview >

Provisioning

Testing connection to LD Snowflake SSO app

The supplied credentials are authorized to enable provisioning

Provisioning Mode: Automatic

Use Microsoft Entra to manage the creation and synchronization of user accounts in LD Snowflake SSO app based on user and group assignment.

Admin Credentials

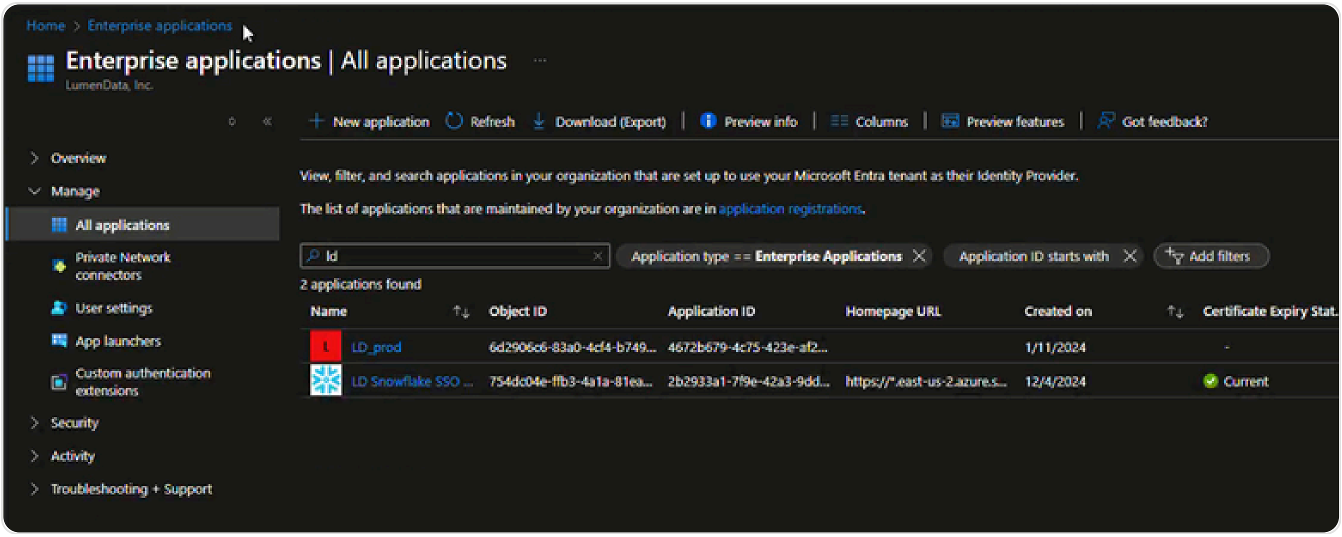
Admin Credentials

Microsoft Entra needs the following information to connect to LD Snowflake SSO app's API and synchronize user data.

Tenant URL *: https://phbadxt-ld_learning.snowflakecomputing.com/scim/v2

Secret Token: ••

13. Adding/configuring the provision user/group
    - Sign in to the Microsoft Entra admin center as a Admin.
    - Browse to Identity > Applications > Enterprise applications.



Enterprise applications | All applications

LumenData, Inc.

View, filter, and search applications in your organization that are set up to use your Microsoft Entra tenant as their Identity Provider.

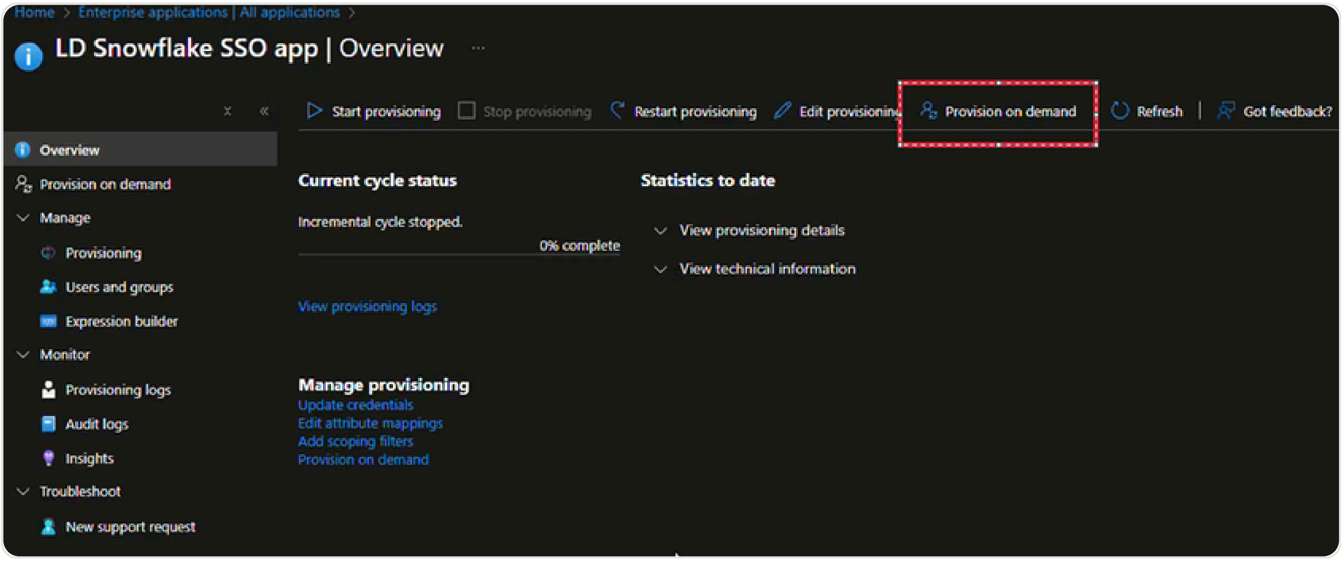
The list of applications that are maintained by your organization are in application registrations.

Search: ld | Application type == Enterprise Applications | Application ID starts with | Add filters

2 applications found

Name	Object ID	Application ID	Homepage URL	Created on	Certificate Expiry Stat.
LD_prod	6d2906c6-83a0-4cf4-b749...	4672b679-4c75-423e-af2...		1/11/2024	-
LD Snowflake SSO ...	754dc04e-ffb3-4a1a-81ea...	2b2933a1-7f9e-42a3-9dd...	https://*.east-us-2.azure.s...	12/4/2024	Current

- select LDSnowflakeSSO that you created earlier.
- Select Provision on demand
- Select the required user or group and click on provision at the bottom.



Home > Enterprise applications | All applications >

LD Snowflake SSO app | Overview ···

Current cycle status

Incremental cycle stopped.

0% complete

View provisioning logs

Statistics to date

View provisioning details

View technical information

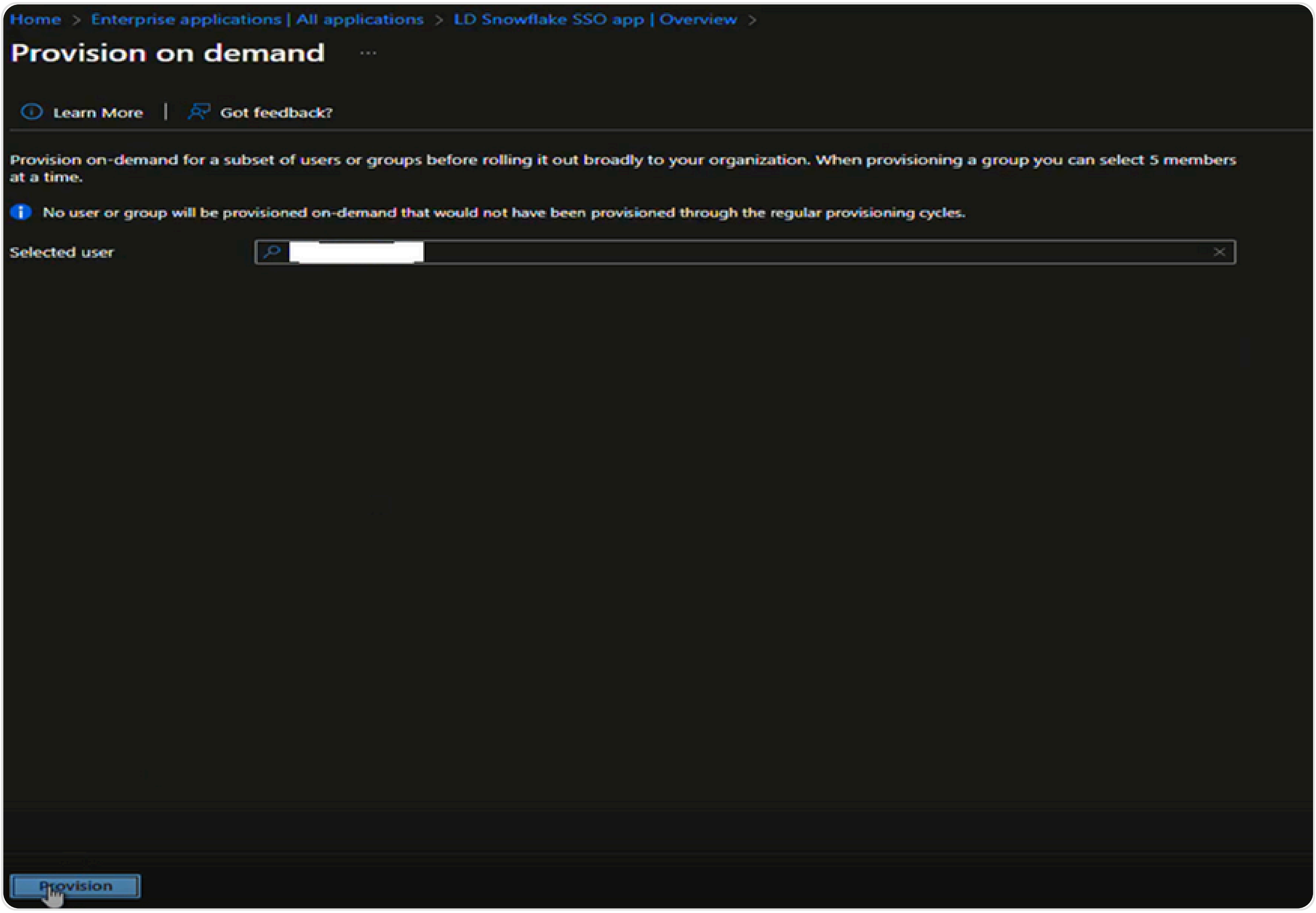
Manage provisioning

Update credentials

Edit attribute mappings

Add scoping filters

Provision on demand



Home > Enterprise applications | All applications > LD Snowflake SSO app | Overview >

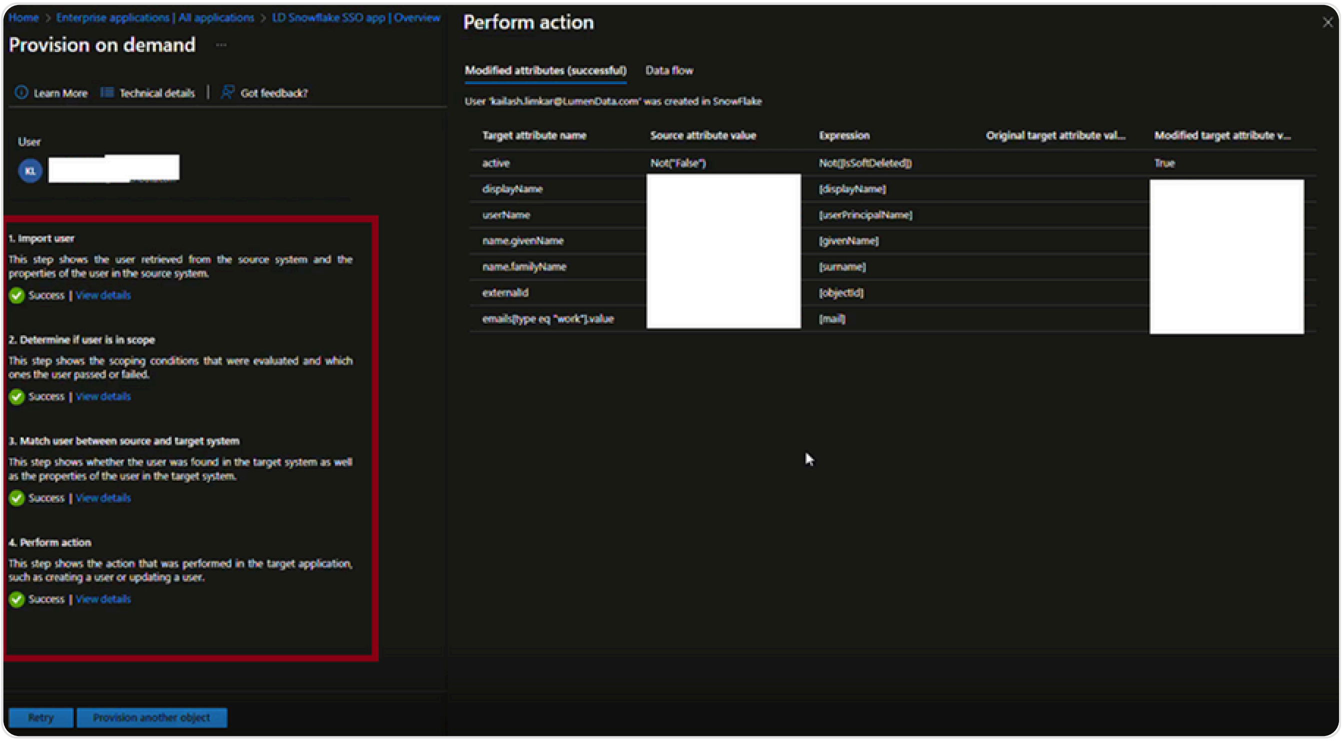
Provision on demand ···

Provision on-demand for a subset of users or groups before rolling it out broadly to your organization. When provisioning a group you can select 5 members at a time.

No user or group will be provisioned on-demand that would not have been provisioned through the regular provisioning cycles.

Selected user [redacted]

- Please validate the user/group.



Home > Enterprise applications | All applications > LD Snowflake SSO app | Overview

Provision on demand

Learn More
Technical details
Got feedback?

User

KL [redacted]

1. Import user

This step shows the user retrieved from the source system and the properties of the user in the source system.

✓ Success | View details

2. Determine if user is in scope

This step shows the scoping conditions that were evaluated and which ones the user passed or failed.

✓ Success | View details

3. Match user between source and target system

This step shows whether the user was found in the target system as well as the properties of the user in the target system.

✓ Success | View details

4. Perform action

This step shows the action that was performed in the target application, such as creating a user or updating a user.

✓ Success | View details

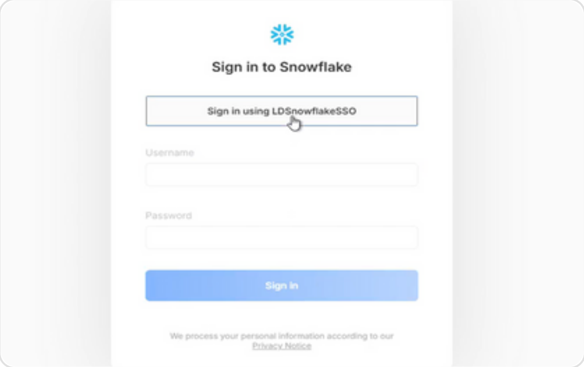
Perform action

User 'kailash.limkar@LumenData.com' was created in SnowFlake

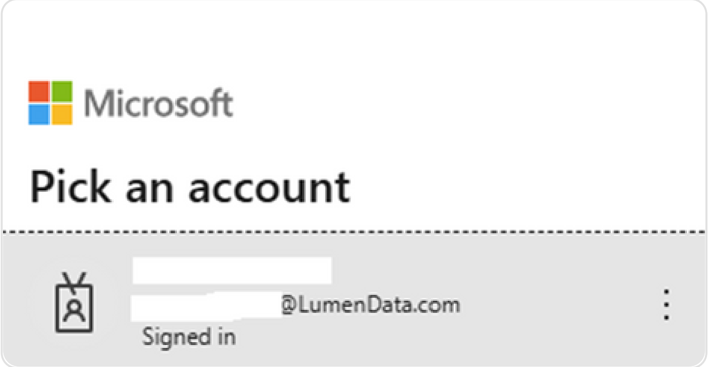
Target attribute name	Source attribute value	Expression	Original target attribute val...	Modified target attribute v...
active	Not("False")	Not([IsSoftDeleted])		True
displayName	[redacted]	[displayName]		[redacted]
userName	[redacted]	[userPrincipalName]		[redacted]
name.givenName	[redacted]	[givenName]		[redacted]
name.familyName	[redacted]	[surname]		[redacted]
externalId	[redacted]	[objectId]		[redacted]
emails[type eq "work"].value	[redacted]	[mail]		[redacted]

Logging in into snowflake with SSO

- Select Sign in using LDSnowflakeSSO instead of entering credentials.
- Select the required account.



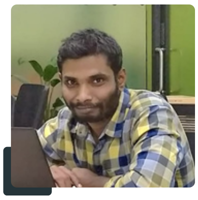
Sign in to Snowflake
Sign in using LDSnowflakeSSO
Username
Password
Sign in
We process your personal information according to our Privacy Notice



Pick an account

[redacted]
[redacted]@LumenData.com
Signed in

Authors



Kailash Limkar
System Administrator

Nandini K
Consultant - Level 1

Sai Bharadwaja
Senior Consultant

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.