Azure AD SSO Integration with Snowflake

Part 1: Setting Up Snowflake Trial Account

Step 1: Create Snowflake Trial Account

1. **Go to Snowflake Website**
   - Visit https://signup.snowflake.com/
2. **Fill Out Registration Form**
   - Enter your email address
   - Choose a username and password
   - Select your organization name
   - Choose cloud provider (Azure recommended for Azure AD integration)
   - Select region closest to you
3. **Choose Edition**
   - Select "Enterprise" for full SSO capabilities
4. **Verify Email**
   - Check your email for verification link
   - Click to activate your account
5. **Initial Login**
   - Log into your Snowflake account at https://app.snowflake.com

Part 2: Azure AD Configuration

Step 2: Set Up Azure AD Enterprise Application

1. **Access Azure Portal**
   - Go to https://portal.azure.com
   - Sign in with your Azure AD admin account
2. **Create Enterprise Application**
   - Navigate to **Azure Active Directory**
   - Go to **Enterprise Applications**
   - Click **+ New application**
   - Click **+ Create your own application**
   - Enter name: "Snowflake SSO"

  - Select **Integrate any other application you don't find in the gallery**
  - Click **Create**

Step 3: Configure SAML SSO

1. **Set Up Single Sign-On**
   - In your new Snowflake application, click **Single sign-on**
   - Select **SAML** as method
2. **Basic SAML Configuration**
   - Click **Edit** in Basic SAML Configuration
   - Add these identifiers:
     - **Identifier (Entity ID)**: https://<your_snowflake_account>.snowflakecomputing.com
     - **Reply URL**: https://<your_snowflake_account>.snowflakecomputing.com/fed/login

Replace <your_snowflake_account> with your actual Snowflake account identifier (e.g., abc12345)

3. **Attributes & Claims**
   - Click **Edit** for Claims
   - Add these claims:
     - **Name**: email
       - Value: user.mail
     - **Name**: login_name
       - Value: user.userprincipalname
     - **Name**: first_name
       - Value: user.givenname
     - **Name**: last_name
       - Value: user.surname

Step 4: Download Federation Metadata

1. **Get Azure AD Metadata**

- In the SAML SSO configuration, go to **SAML Signing Certificate** section
- Download the **Federation Metadata XML**
- Save this file securely

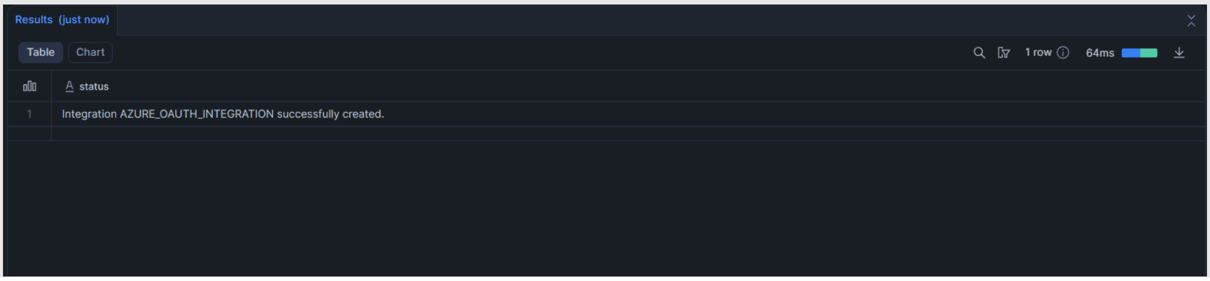
Part 3: Snowflake Configuration

Step 5: Configure Security Integration in Snowflake

1. **Login to Snowflake**
    - Use your ACCOUNTADMIN role
2. **Create Security Integration**

sql

```
CREATE SECURITY INTEGRATION azure_ad_sso
TYPE = SAML2
ENABLED = TRUE
SAML2_ISSUER = 'https://sts.windows.net/<your-azure-ad-tenant-id>/'
SAML2_SSO_URL = 'https://login.microsoftonline.com/<your-azure-ad-tenant-id>/saml2'
SAML2_PROVIDER = 'AZURE'
SAML2_X509_CERT = '<Azure-AD-certificate>'
SAML2_SP_INITIATED_LOGIN_PAGE = TRUE
SAML2_ENABLE_SP_INITIATED = TRUE;
```



	status
1	Integration AZURE_OAUTH_INTEGRATION successfully created.

To get the required values:

- **Tenant ID**: Found in Azure AD > Properties > Directory ID
- **Certificate**: From the Federation Metadata XML file, copy the contents of the <X509Certificate> tag

Step 6: Configure Snowflake in Azure AD

1. **Get Snowflake URLs**
    - In Snowflake, run:

sql

```
DESCRIBE SECURITY INTEGRATION azure_ad_sso;
```

- Note the saml2_snowflake_acs_url and saml2_snowflake_issuer_url

2. **Update Azure AD Configuration**
   - Go back to Azure AD Enterprise Application
   - Update these values in Basic SAML Configuration:
     - **Identifier**: Use the saml2_snowflake_issuer_url
     - **Reply URL**: Use the saml2_snowflake_acs_url

Part 4: User Assignment and Testing

Step 7: Assign Users in Azure AD

1. **User Assignment**
   - In your Snowflake Enterprise App, go to **Users and groups**
   - Click **+ Add user/group**
   - Select users who need Snowflake access
   - Click **Assign**

Step 8: Test SSO Configuration

1. **Test SSO Login**
   - Go to your Snowflake login URL: https://<your_account>.snowflakecomputing.com
   - Click "Sign in with SSO"
   - Enter your organization name (Azure AD tenant name)
   - You should be redirected to Azure AD login
   - After successful authentication, you'll be redirected to Snowflake

Step 9: Configure User Mapping (Optional)

1. **Set Up User Mapping in Snowflake**

sql

```
ALTER SECURITY INTEGRATION azure_ad_sso

SET SAML2_USER_MAPPING_ATTRIBUTE = 'login_name';
```

Part 5: Troubleshooting and Verification

Step 10: Verify Configuration

1. **Check SAML Response**

  - Use browser developer tools to inspect SAML responses
  - Verify all required attributes are being passed

2. **Common Issues to Check**
   - Clock synchronization between systems
   - Certificate validity
   - Correct URLs and identifiers
   - Proper attribute mapping

Step 11: Enable SP-Initiated SSO

1. **For Direct SSO Access**
   - Users can access Snowflake directly via: https://<your_account>.snowflakecomputing.com
   - Click "Sign in with SSO"
   - Enter your Azure AD domain

Important Notes

Security Considerations

- Keep certificates secure
- Regularly rotate certificates
- Monitor login attempts
- Set up proper user provisioning

Required Permissions

- Azure AD Global Administrator or Application Administrator
- Snowflake ACCOUNTADMIN role

Support Information

- Snowflake documentation: Snowflake SSO
- Azure AD documentation: Azure AD SAML