AAD Snowflake Single Sign-on Integrations

Saturday, December 12, 2020 4:33 PM

Why use AAD with Snowflake?

- Control in Azure AD who has access to Snowflake
- Enable users to be automatically signed-in to Snowflake (Single Sign-On) with their Azure AD accounts
- Manage user accounts in one central location - the Azure portal.

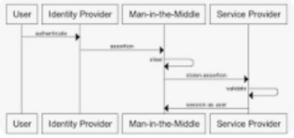
To configure Azure AD integration with Snowflake, you need the following items:

- An Azure AD subscription
- Snowflake single sign-on enabled subscription

FYI: Snowflake supports:

- SP and IDP initiated SSO

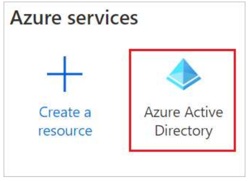
  SP (Service Provider) initiated **SSO** involves the **SP** creating a SAML request, forwarding the user and the request to the IdP (Identity Provider), and then, once the user has authenticated, receiving a SAML response & assertion from the IdP. This flow would typically be initiated by a login button within the **SP**.

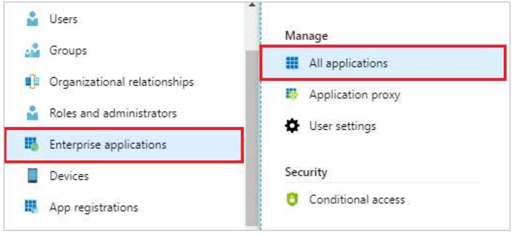
- Automated user provisioning and deprovisioning (recommended)

Add Snowflake from the gallery:

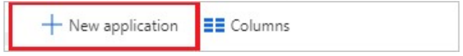
1. In the Azure portal, on the left navigation panel, click Azure Active Directory icon.

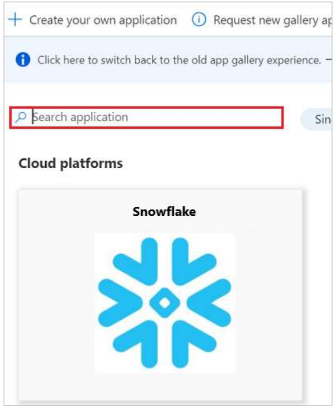
2. Navigate to Enterprise Applications and select All Applications option.

3. To add new application, click New application button on the top of page.

4. In the search box, type Snowflake, select Snowflake from result panel then click Add button to add the application.

   
   Create your own application
Request new gallery ap
Click here to switch back to the old app gallery experience. →
Search application
Sin
Cloud platforms
Snowflake

Configure and test Azure AD single sign-on

To configure and test Azure AD single sign-on with Snowflake, complete the following building blocks:

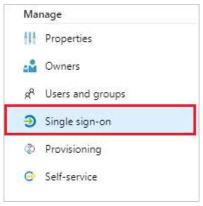
1. Configure Azure AD Single Sign-On - to enable your users to use this feature.
2. Configure Snowflake Single Sign-On - to configure the Single Sign-On settings on application side.
3. Create an Azure AD test user - to test Azure AD single sign-on with Britta Simon.
4. Assign the Azure AD test user - to enable Britta Simon to use Azure AD single sign-on.
5. Create Snowflake test user - to have a counterpart of Britta Simon in Snowflake that is linked to the Azure AD representation of user.
6. Test single sign-on - to verify whether the configuration works.

Configure Azure AD single sign-on

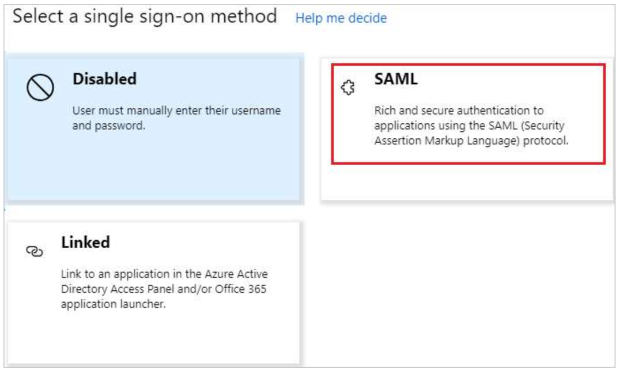
Enable Azure AD single sign-on in the Azure portal.

To configure Azure AD single sign-on with Snowflake, perform the following steps:

1. In the Azure portal, on the Snowflake application integration page, select Single sign-on.



2. On the Select a Single sign-on method dialog, select **SAML**/WS-Fed mode to enable single sign-on.

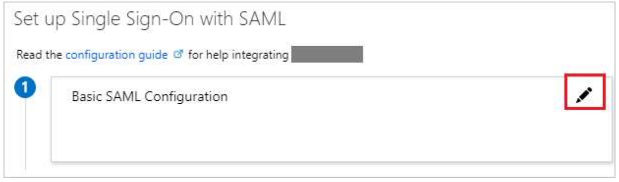


User must manually enter their username and password.

Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

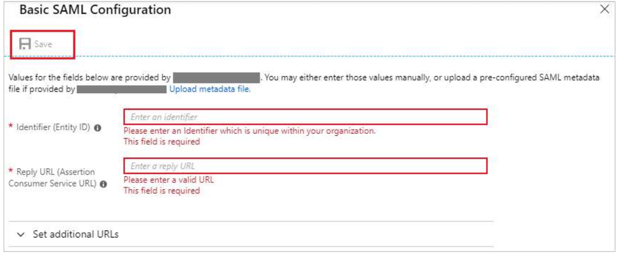
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

3. On the Set up Single Sign-On with SAML page, click Edit icon to open Basic SAML Configuration dialog.



Read the configuration guide for help integrating [redacted]

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

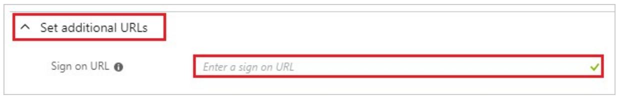


Values for the fields below are provided by [redacted]. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by [redacted] Upload metadata file.

* Identifier (Entity ID): Enter an identifier
Please enter an identifier which is unique within your organization.
This field is required

* Reply URL (Assertion Consumer Service URL): Enter a reply URL
Please enter a valid URL
This field is required

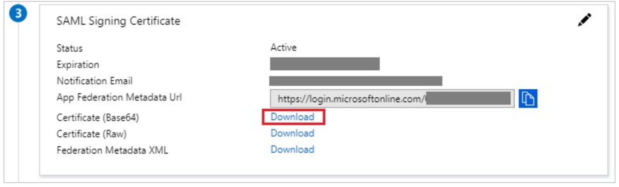
a. In the Identifier text box, type a URL using the following pattern: https://*<SNOWFLAKE-URL>*.snowflakecomputing.com
b. In the Reply URL text box, type a URL using the following pattern: https://*<SNOWFLAKE-URL>*.snowflakecomputing.com/fed/login
c. Click Set additional URLs and perform the following step if you wish to configure the application in SP initiated mode:



Sign on URL: Enter a sign on URL

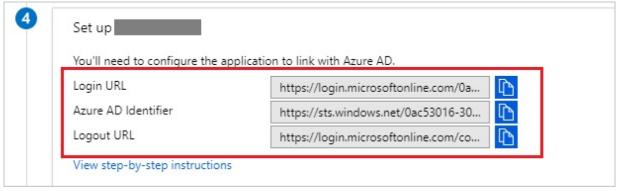
In the Sign-on URL text box, type a URL using the following pattern: https://*<SNOWFLAKE-URL>*.snowflakecomputing.com
In the Logout URL text box, type a URL using the following pattern: https://*<SNOWFLAKE-URL>*.snowflakecomputing.com/fed/logout

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



Status: Active
Expiration: [redacted]
Notification Email: [redacted]
App Federation Metadata Url: https://login.microsoftonline.com/[redacted]
Certificate (Base64): Download
Certificate (Raw): Download
Federation Metadata XML: Download

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



You'll need to configure the application to link with Azure AD.

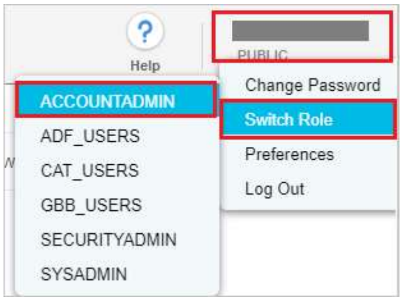
Login URL: https://login.microsoftonline.com/0a...
Azure AD Identifier: https://sts.windows.net/0ac53016-30...
Logout URL: https://login.microsoftonline.com/co...

a. Login URL
b. Azure Ad Identifier
c. Logout URL

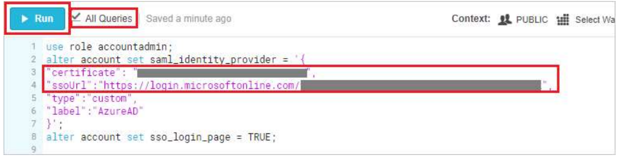
Configure Snowflake Single Sign-On

1. In a different web browser window, login to Snowflake as a Security Administrator.
2. Switch Role to ACCOUNTADMIN, by clicking on profile on the top right side of page.

   P.S. This is separate from the context you have selected in the top-right corner under your User Name



3. Open the downloaded Base 64 certificate in notepad. Copy the value between “-----BEGIN CERTIFICATE-----” and “-----END CERTIFICATE-----" and paste this into the quotation marks next to certificate below. In the ssoUrl, paste Login URL value which you have copied from the Azure portal. Select the All Queries and click Run.

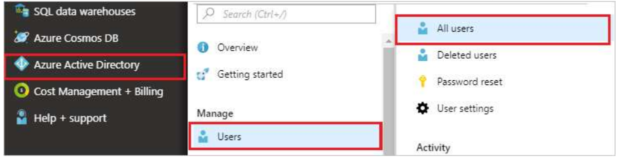


```
use role accountadmin;
alter account set saml_identity_provider = '{
"certificate": "[redacted]",
"ssoUrl":"https://login.microsoftonline.com/[redacted]",
"type":"custom",
"label":"AzureAD"
}';
alter account set sso_login_page = TRUE;
```

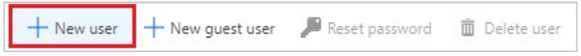
Create an Azure AD test user

Create a test user in the Azure portal named Britta Simon.

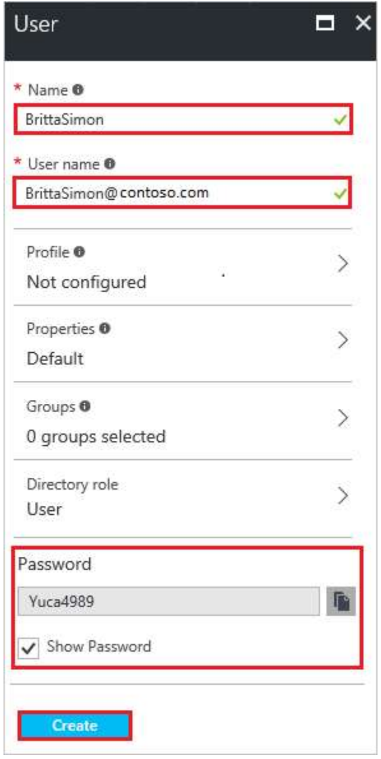
1. In the Azure portal, in the left pane, select Azure Active Directory, select Users, and then select All users.



2. Select New user at the top of the screen.



3. In the User properties, perform the following steps.



* Name

BrittaSimon

* User name

BrittaSimon@contoso.com

Profile

Not configured

Properties

Default

Groups

0 groups selected

Directory role

User

Password

Yuca4989

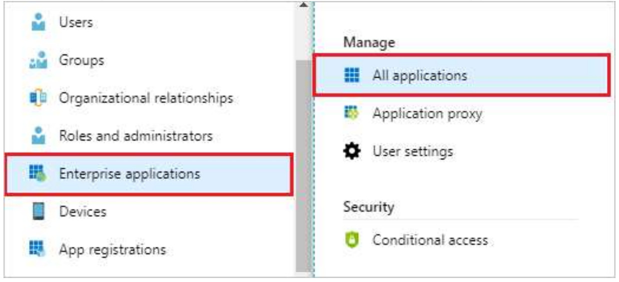
☑ Show Password

   a. In the Name field enter BrittaSimon.
   b. In the User name field type brittasimon@yourcompanydomain.extension
   For example, BrittaSimon@contoso.com
   c. Select Show password check box, and then write down the value that's displayed in the Password box.
   d. Click Create.

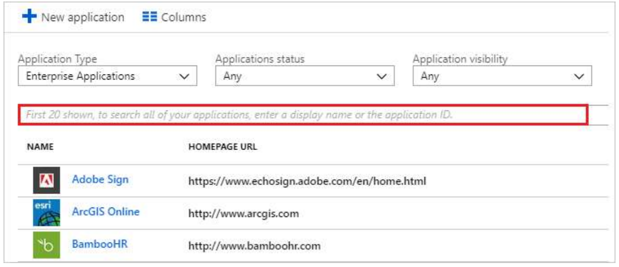
Assign the Azure AD test user

Enable Britta Simon to use Azure single sign-on by granting access to Snowflake.

1. In the Azure portal, select Enterprise Applications, select All applications, then select Snowflake.



2. In the applications list, type and select Snowflake.

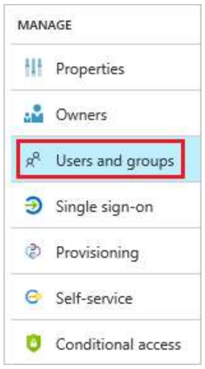


Application Type	Applications status	Application visibility
Enterprise Applications	Any	Any

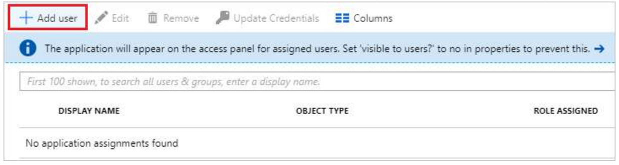
First 20 shown, to search all of your applications, enter a display name or the application ID.

NAME	HOMEPAGE URL
Adobe Sign	https://www.echosign.adobe.com/en/home.html
ArcGIS Online	http://www.arcgis.com
BambooHR	http://www.bamboohr.com

3. In the menu on the left, select Users and groups.



4. Click the Add user button, then select Users and groups in the Add Assignment dialog.



The application will appear on the access panel for assigned users. Set 'visible to users?' to no in properties to prevent this.

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE	ROLE ASSIGNED
No application assignments found		

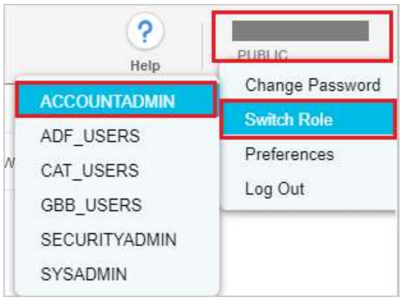
5. In the Users and groups dialog select Britta Simon in the Users list, then click the Select button at the bottom of the screen.
6. If you are expecting any role value in the SAML assertion then in the Select Role dialog select the appropriate role for the user from the list, then click the Select button at the bottom of the screen.
7. In the Add Assignment dialog click the Assign button.

Create Snowflake test user

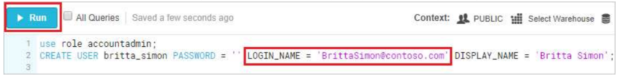
To enable Azure AD users to log in to Snowflake, they must be provisioned into Snowflake. In Snowflake, provisioning is a manual task.

To provision a user account, perform the following steps:

1. 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. Create the user by running the below SQL query, ensuring "Login name" is set to the Azure AD username on the worksheet as shown below.



```
use role accountadmin;
CREATE USER britta_simon PASSWORD = '' LOGIN_NAME = 'BrittaSimon@contoso.com' DISPLAY_NAME = 'Britta Simon';
```

Test single sign-on

Test your Azure AD single sign-on configuration using the Access Panel.

When you click the Snowflake tile in the Access Panel, you should be automatically signed in to the Snowflake for which you set up SSO.