

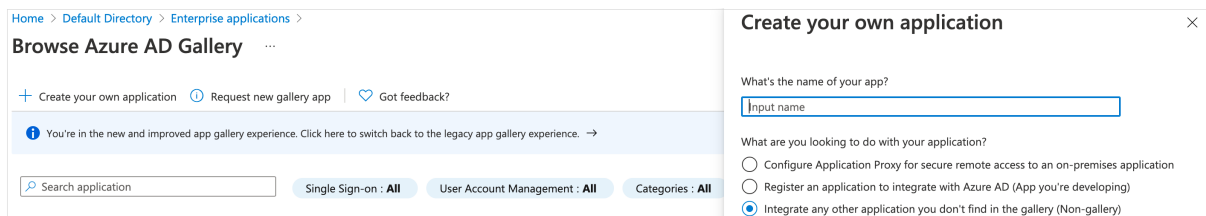
SKY SSO (Single Sign-On)

Last Modified on 09/24/2025 11:10 am CDT

For more information or to enable SSO, reach out to SSI Support.

Step 1: Add New Application in Azure AD

1. Log in to the Azure Portal.
2. In the *Azure Services* section, choose **Azure Active Directory**.
3. In the left sidebar, choose *Enterprise applications*.
4. Choose **New application**.
5. On the *Browse Azure AD Gallery* page, choose **Create your own application**.
6. Under *What's the name of your app?*, enter a name for the application and select *Integrate any other application you don't find in the gallery (Non-gallery)*, as shown in the image below.



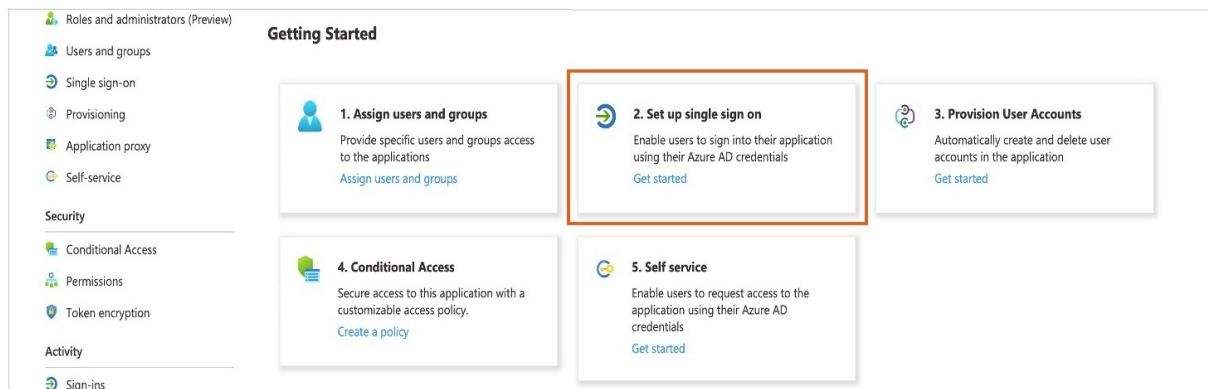
7. Choose **Create**.

It will take few seconds for the application to be created in Azure AD. The *Overview* page should then display for the newly added application.

Note: Occasionally, this step can result in a *Not Found* error even though Azure AD has successfully created a new application. If that happens, in Azure AD, navigate back to **Enterprise applications** and search for the application by name.

Step 2: Set Up Single Sign-On Using SAML

1. On the *Getting Started* page, choose **Get Started** on the *Set up single sign on* card.



2. On the next screen, select **SAML**.

3. In the middle pane under *Set up Single Sign-On with SAML*, choose the **Edit** icon in the *Basic SAML Configuration* section.
4. In the right pane under *Basic SAML Configuration*, enter the *Identifier ID (Entity ID)* and the *Reply URL* below.
 - **Entity ID:** `urn:amazon:cognito:sp:us-east-1_FOTVuspmid`
 - **Reply URL:** `https://skyusers-prod.auth.us-east-1.amazoncognito.com/saml2/idpresponse`

5. Choose **Save**.
6. In the middle pane under *Set up Single Sign-On with SAML*, choose **Edit** in the *User Attributes & Claims* section.
7. Choose **Add a group claim**.
8. On the *User Attributes & Claims* page, select *Groups assigned to the application* in the right pane under *Group Claims*. Leave *Source attribute* as *Group ID*.

9. Choose **Save**.

This adds the group claim so that Amazon Cognito can receive the group membership detail of the authenticated user as part of the SAML assertion.

1. In a text editor, note the *Claim names* under *Additional claims*, as shown in Step 8 above. These will be needed when creating attribute mapping in Amazon Cognito.
2. Close the *User Attributes & Claims* screen by choosing the **X** in the top right corner. The *Set up Single Sign-on with SAML* page will display.
3. Scroll down to the *SAML Signing Certificate* section, and copy the *App Federation Metadata Url* by choosing the

Copy to Clipboard icon. Keep this URL in a text editor, as it will be needed in the next step.

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating cognito-ap-southeast-2_3DEOUBXPw.

- #### Basic SAML Configuration

[Edit](#)

Identifier (Entity ID)	urn:amazon:cognito:sp:ap-southeast-2-██████████
Reply URL (Assertion Consumer Service URL)	https://██████████auth.ap-southeast-2.amazoncognito.com
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- #### User Attributes & Claims

[Edit](#)


givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
Group	user.groups
- #### SAML Signing Certificate


[Edit](#)

Status	Active
Thumbprint	E93DE30820C791A024D3E96C839160D181AB0A2D
Expiration	9/1/2023, 12:09:51 PM
Notification Email	██████████
App Federation Metadata Url	https://login.microsoftonline.com/69797cb4-71e1... Copy
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download


4. Add users to the app in Azure (Entra) with the same email as the SKY User to use in their company.


- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups**
 - Single sign-on
 - Provisioning
 - Application proxy
 - Self-service
 - Custom security attributes
- > Security
- > Activity
- > Troubleshooting + Support


 Add user/group

 Edit assignment

 Remove assignment


 Update credential


 Refresh

 Manage view

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this.

Assign users and groups to app-roles for your application here. To create new app-roles for this application, use the [application registrar](#)

 First 200 shown, search all users & groups

Display name		Object type
<input type="checkbox"/>	 S [redacted]	Group