OSSO - ADFS Setup Guide

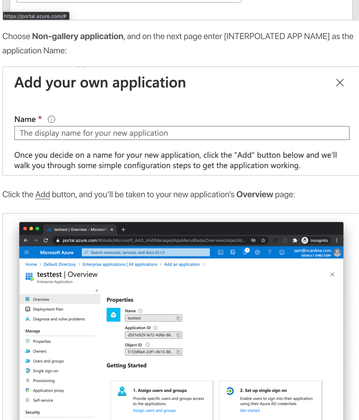
To configure SSO to log in to our application, you will need to create a **Non-gallery Enterprise Application** inside your Azure ADFS portal. This is typically performed by someone in IT or InfoSec who has administrative privileges to the Azure ADFS portal.

Once you configure the application in your portal, you will need to return to us the **Federation Metadata XML** so that we can finalize configuration on our end.

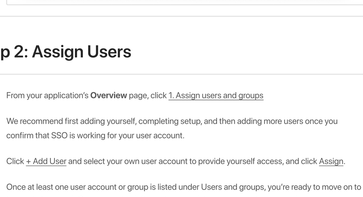
Follow the steps below to create an application with information we've generated for your account, and be sure to return the Federation Metadata XML to us so your team can begin signing in with SSO.

Step 1: Create new application

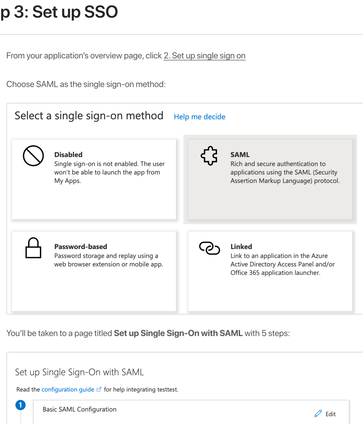
1. Log in to your Azure portal at portal.azure.com - you will need an account with at least the Application administrator role, though we recommend that a Global administrator completes this process.
2. Access your **Azure Active Directory**, and in the left-hand menu click Enterprise Applications. Then click + New Application in the top nav. You should land on a page like this:



3. Choose **Non-gallery application**, and on the next page enter [INTERPOLATED APP NAME] as the application Name:



4. Click the Add button, and you'll be taken to your new application's **Overview** page:

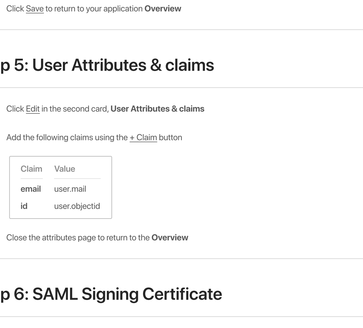


Step 2: Assign Users

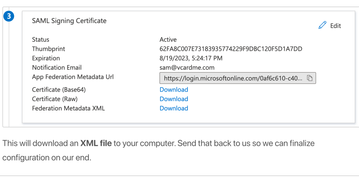
1. From your application's **Overview** page, click 1. Assign users and groups
2. We recommend first adding yourself, completing setup, and then adding more users once you confirm that SSO is working for your user account.
3. Click + Add User and select your own user account to provide yourself access, and click Assign.
4. Once at least one user account or group is listed under Users and groups, you're ready to move on to the next step - click Overview in the left-nav to go back to your application's overview

Step 3: Set up SSO

1. From your application's overview page, click 2. Set up single sign on
2. Choose SAML as the single sign-on method:



3. You'll be taken to a page titled **Set up Single Sign-On with SAML** with 5 steps:



Step 4: Basic SAML Configuration

1. Click Edit in the first card, **Basic SAML Configuration**
2. A form will open - enter the following information into the relevant form fields:

Field	Value
Identifier (Entity ID)	[Interpolated]
Reply URL (Assertion Consumer Service URL)	[Interpolated]

3. Click Save to return to your application **Overview**

Step 5: User Attributes & claims

1. Click Edit in the second card, **User Attributes & claims**
2. Add the following claims using the + Claim button

Claim	Value
email	user.mail
id	user.objectid

3. Close the attributes page to return to the **Overview**

Step 6: SAML Signing Certificate

1. You've now completed configuration, but you won't be able to sign in until we complete configuration on our end.
2. In the third card, click the Download link next to **Federation Metadata XML**:

3. This will download an **XML file** to your computer. Send that back to us so we can finalize configuration on our end.