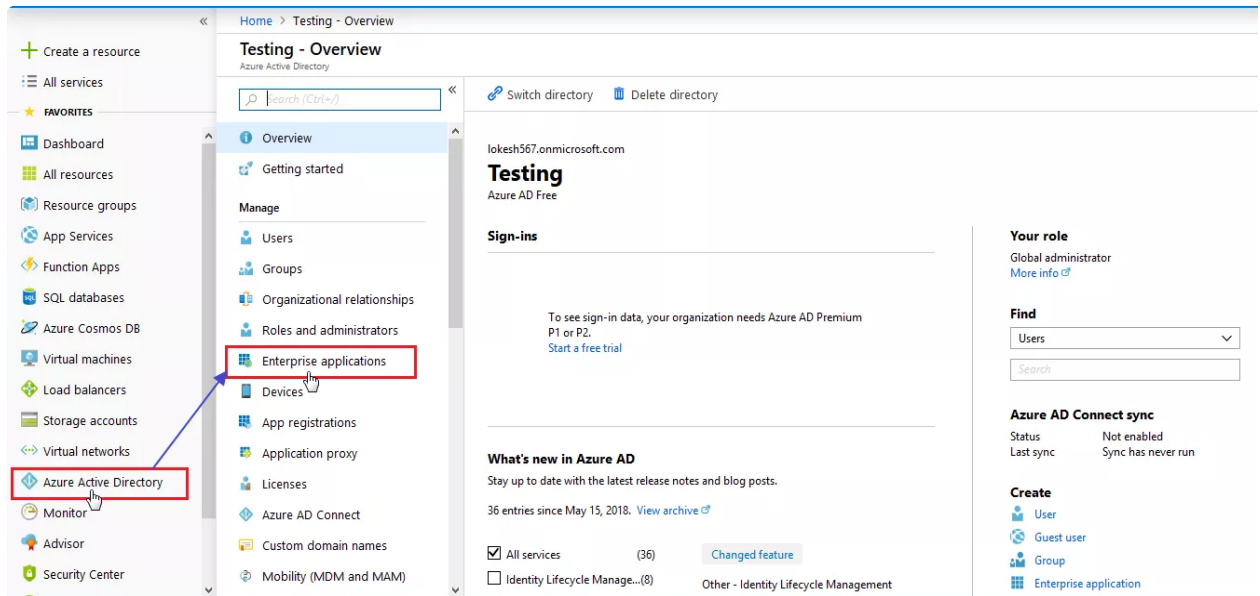


Single Sign-On (SSO) For Shopify Using Azure AD

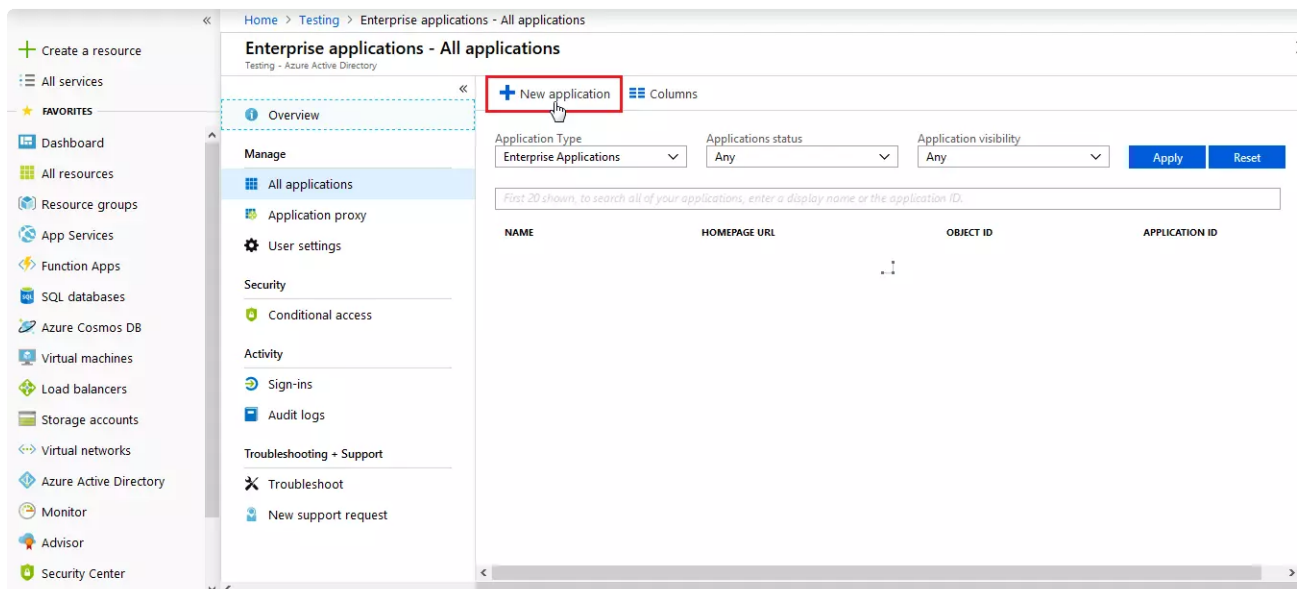
Azure AD Single Sign-On (SSO) for Shopify Store, miniOrange provides a ready to use solution. This solution ensures that you are ready to roll out secure access to Shopify Store using Azure AD within minutes.

Step 1: Configuring miniOrange as Service Provider (SP) in Azure AD

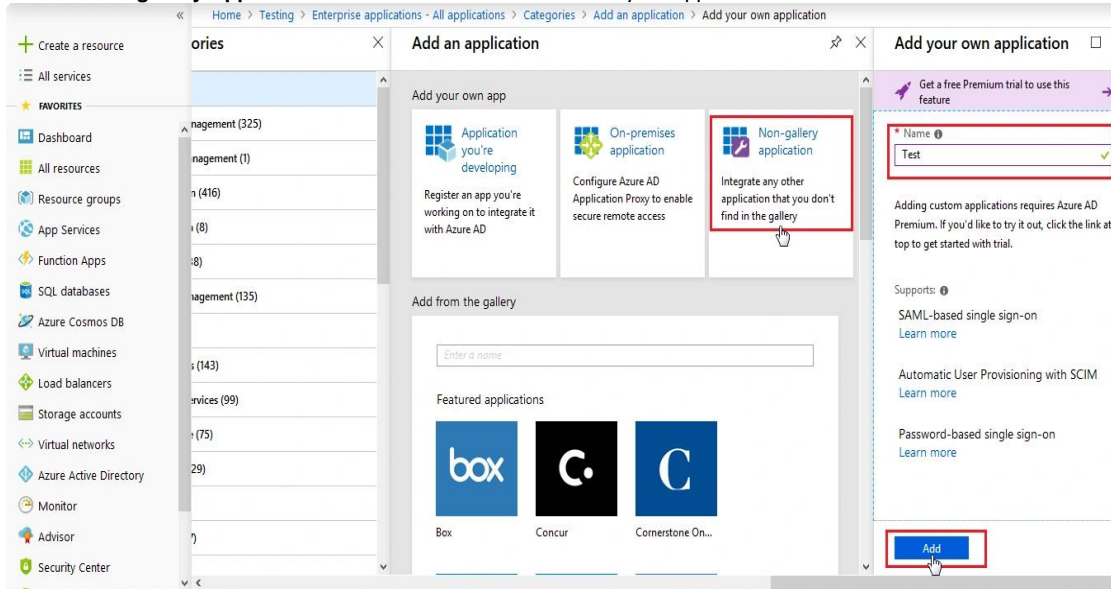
- Log in to [Azure AD Portal](#)
- Select **Azure Active Directory** ⇒ **Enterprise Applications**.



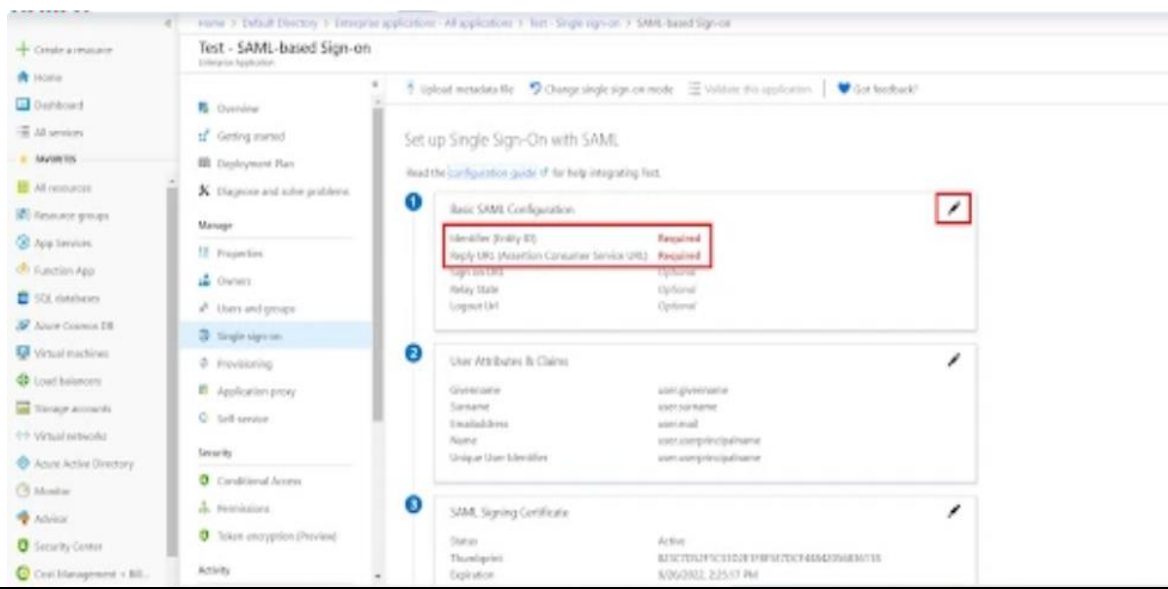
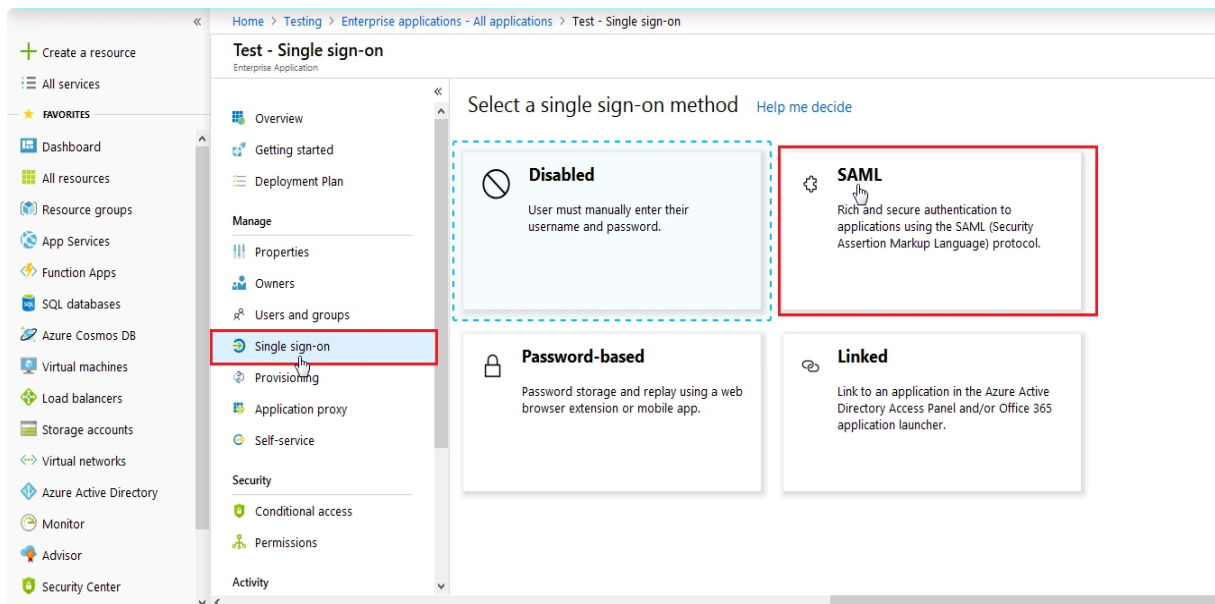
- Click on **New Application**.

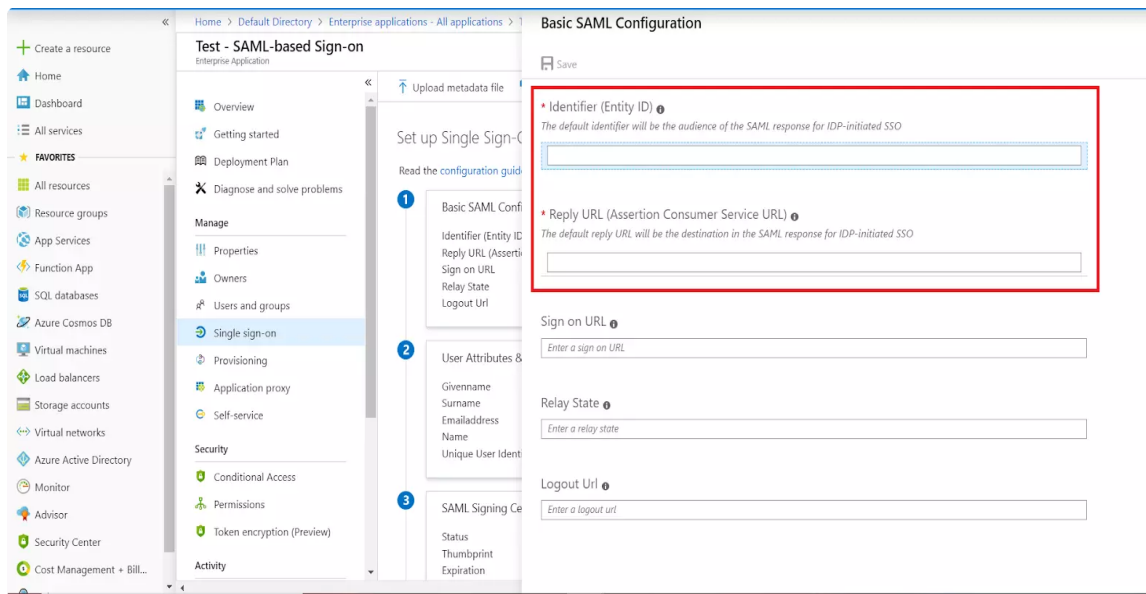


- Click on **Non-gallery application** section and enter the name for your app and click on **Add** button

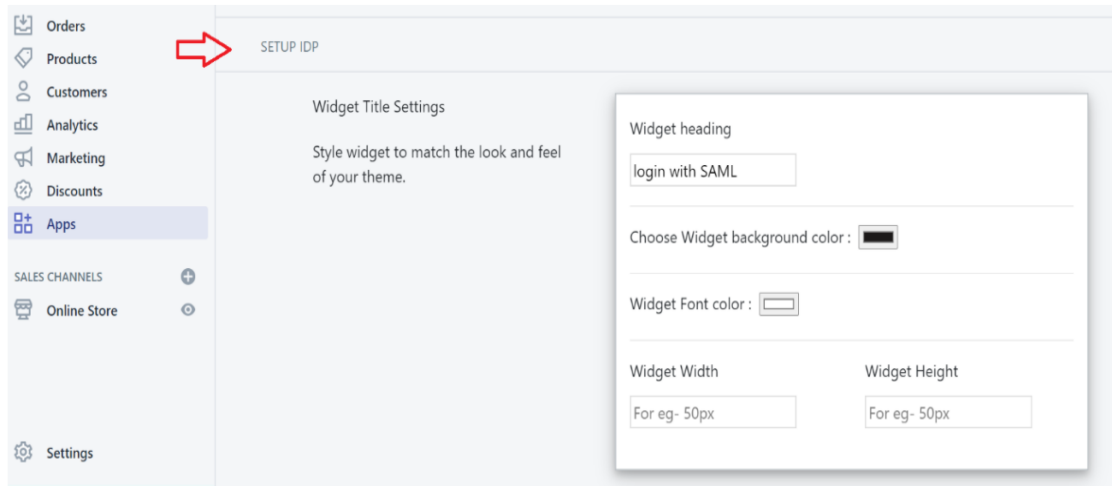


- Click on **Single sign-on** from the application's left-hand navigation menu. The next screen presents the options for configuring singlesign-on. Click on **SAML**.

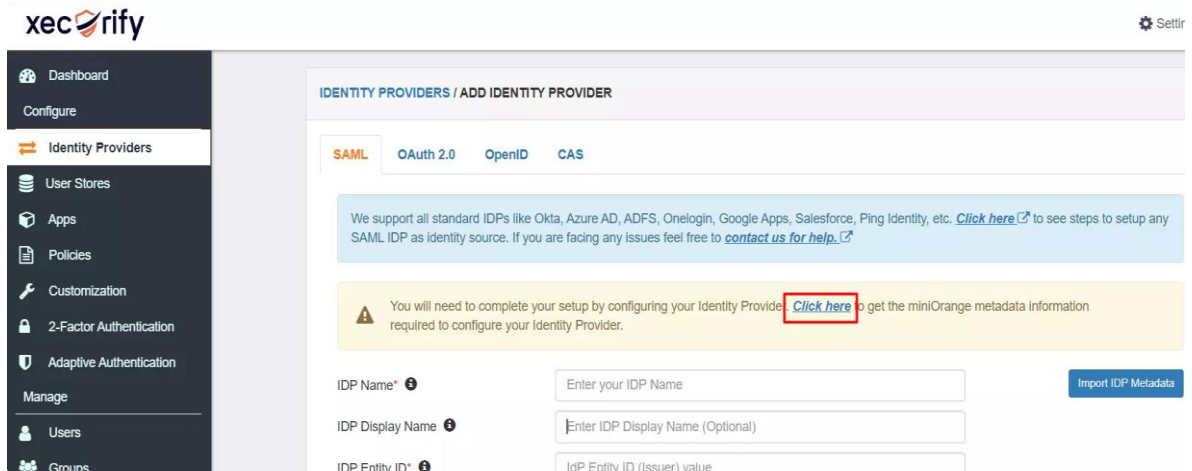




- For **Basic SAML configuration** you need to get the **Entity ID and ACS URL** from **miniOrange**
- Now go to your **Shopify store** and click on **Setup IDP** button in the top left in navigation bar.



- Now click on the **Click here** link to get miniorange metadata as shown in Screen below.



- For SP -INITIATED SSO section Select Show Metadata Details

FOR SP - INITIATED SSO



SP-Initiated SSO means that users would initiate the SSO process from the App that you configure with miniOrange

Show Metadata Details

Metadata URL

Download Certificate

Download Metadata

ACS URL (For SP-Initiated SSO):

Single Logout URL:

X.509 Certificate:

Entity ID or Issuer:

SSO Login URL (Use this url to auto-redirect to IDP):

- Enter the values in basic SAML configuration as shown in below screen

| | |
|---|---------------------------|
| Identifier (Entity ID) | Entity ID or Issuer |
| Reply URL (Assertion Consumer Service URL) | ACS URL |
| Sign on URL (optional required during IDP-initiated SSO) | Show SSO Link from Step 4 |

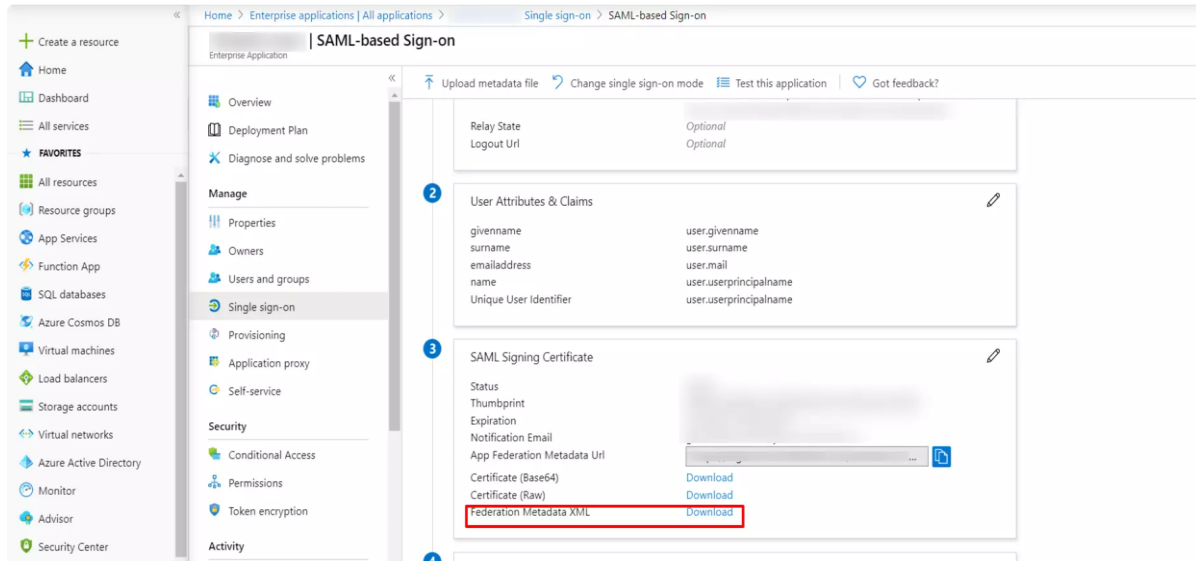
- By default, the following **Attributes** will be sent in the SAML token. You can view or edit the claims sent in the SAML token to the application under the **Attributes** tab.

The screenshot shows the Azure portal interface for configuring a SAML-based sign-on. The main content area is titled "Set up Single Sign-On with SAML" and includes a "Basic SAML Configuration" section with fields for Identifier (Entity ID), Reply URL (Assertion Consumer Service URL), Sign on URL, Relay State, and Logout Uri. The "User Attributes & Claims" section is highlighted with a red box, showing a table of attributes and their corresponding values:

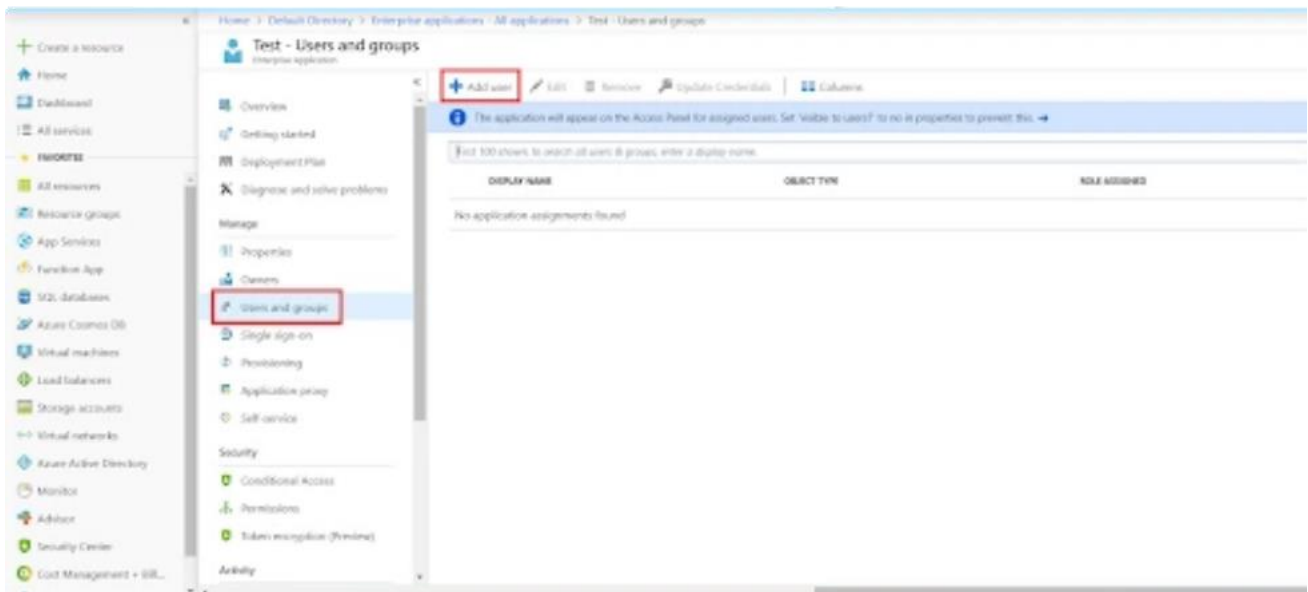
| Attribute | Value |
|------------------------|------------------------|
| Givenname | user.givenname |
| Surname | user.surname |
| Emailaddress | user.mail |
| Name | user.userprincipalname |
| Unique User Identifier | user.userprincipalname |

Below this, the "SAML Signing Certificate" section shows the status as "Active" and provides the thumbprint and expiration date (9/26/2022, 2:25:17 PM).

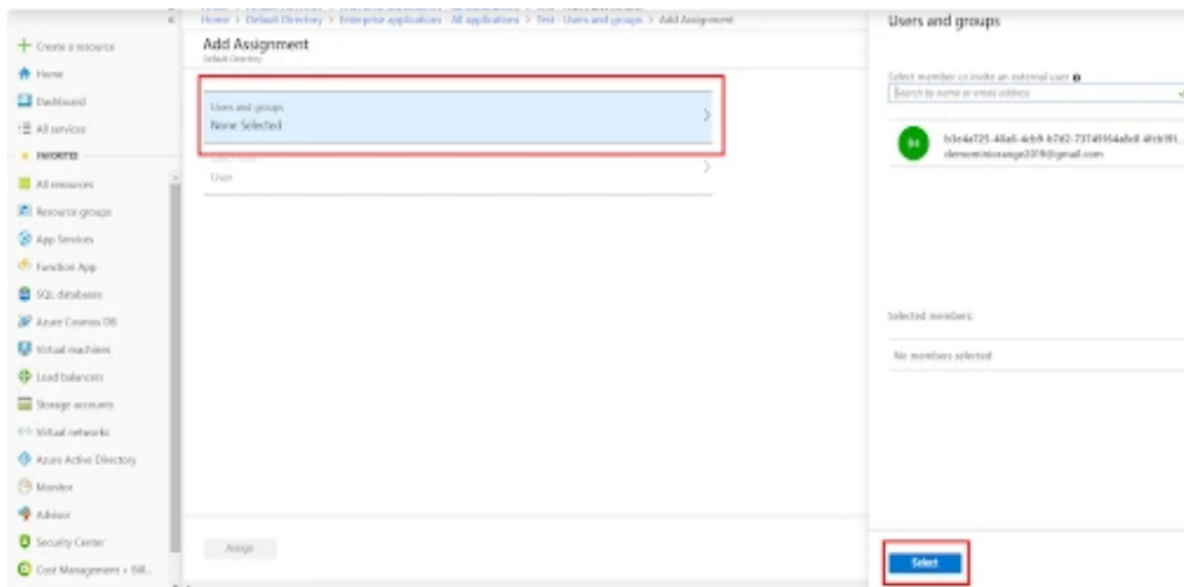
- Download **Federation Metadata xml**. This will be used while configuring the Azure AD as IDP in Step 2.



- Assign users and groups to your SAML application.
- As a security control, Azure AD will not issue a token allowing a user to sign in to the application unless Azure AD has granted access to the user. Users may be granted access directly, or through group membership.
- Click on **Users and groups** from the applications left-hand navigation menu. The next screen presents the options for assigning the users/groups to the application.



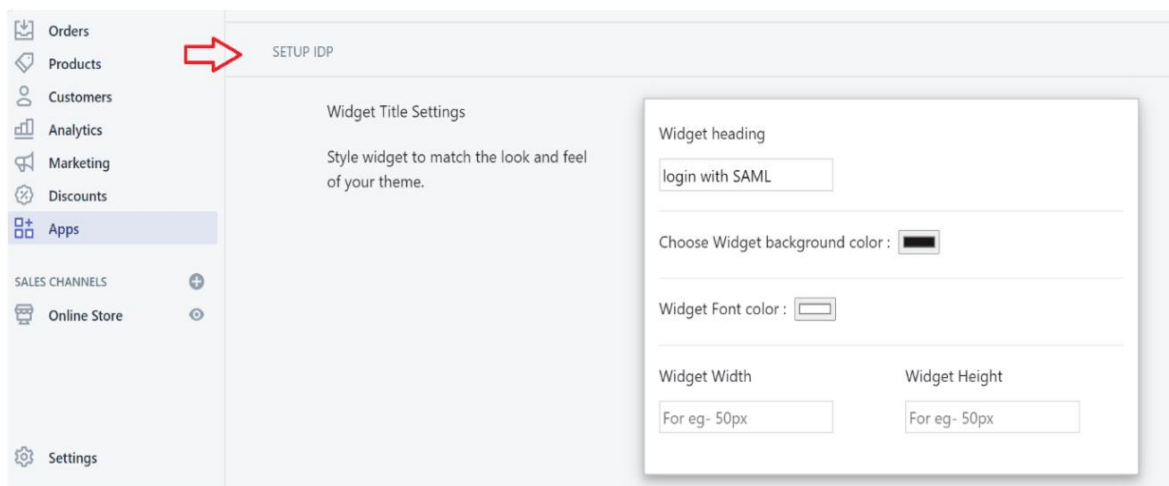
- After clicking on **Add user**, Select **Users and groups** in the **Add Assignment** screen.
- The next screen presents the option for selecting user or invite an external user. Select the appropriate user and click on the **Select** button.



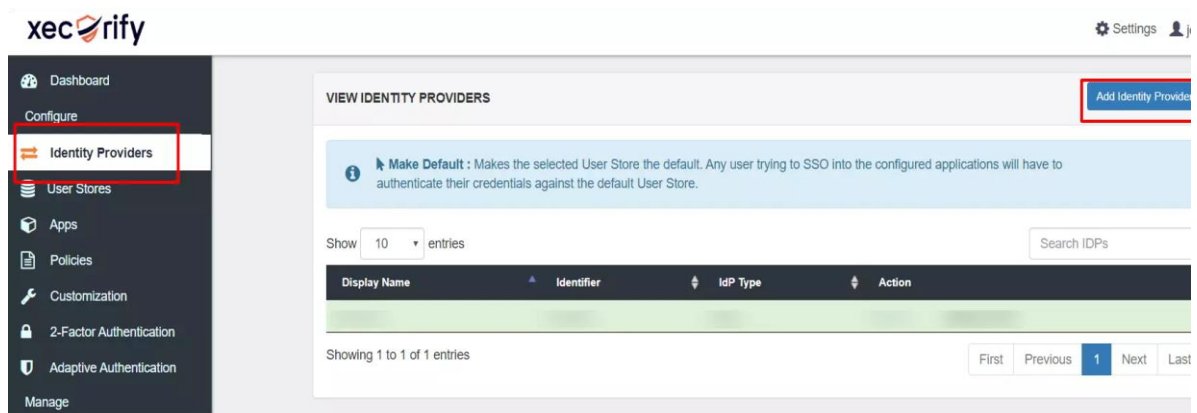
- Here, you can also assign a role to this user under **Select Role** section. Finally, click on **Assign** button to assign that user or group to SAML application.

Step 2: Configure Azure AD as Identity Provider (IDP) in miniOrange

- Now go to your **Shopify store** and click on **Setup IDP** button in the top left in navigation bar.



- From the left navigation bar select **Identity Provider**




- Select SAML. Click on Import IDP metadata


IDENTITY PROVIDERS / ADD IDENTITY PROVIDER


SAML OAuth 2.0 OpenID CAS


We support all standard IDPs like Okta, Azure AD, ADFS, Onelogin, Google Apps, Salesforce, Ping Identity, etc. [Click here](#) to see steps to setup any saml idp as identity source. If you are facing any issues feel free to [contact us for help](#).

⚠ You will need to complete your setup by configuring your Identity Provider. [Click here](#) to get the miniOrange metadata information required to configure your Identity Provider.

IDP Name*  **Import IDP Metadata**

IDP Display Name 

IDP Entity ID* 

SAML SSO Login URL* 

- Choose appropriate IDP name. Browse for the file downloaded in **step 1**.
- Click on **Import**.

Import IDP Metadata ✕

*IDP Name:

*IDP Metadata: URL Text File

- As shown in the below screen the **IDP Entity ID**, **SAML SSO Login URL** and **x.509 Certificate** will be filled from the file imported.

The screenshot shows the 'IDENTITY PROVIDERS / ADD IDENTITY PROVIDER' configuration page in the miniOrange dashboard. The 'SAML' tab is selected. The page includes a sidebar with navigation options like Dashboard, Configure, Identity Providers, User Stores, Apps, Policies, Customization, 2-Factor Authentication, Adaptive Authentication, Manage, Users, Groups, Reports, and License. The main content area has a header with 'Settings' and a user profile icon. Below the header, there are tabs for 'SAML', 'OAuth 2.0', 'OpenID', and 'CAS'. A blue information box states: 'We support all standard IDPs like Okta, Azure AD, ADFS, OneLogin, Google Apps, Salesforce, Ping Identity, etc. [Click here](#) to see steps to setup any SAML IDP as identity source. If you are facing any issues feel free to [contact us for help](#).' A yellow warning box says: 'You will need to complete your setup by configuring your Identity Provider. [Click here](#) to get the miniOrange metadata information required to configure your Identity Provider.' The configuration fields are: IDP Name* (Azure AD), IDP Display Name* (Azure AD), IDP Entity ID* (empty), SAML SSO Login URL* (empty), Single Logout URL* (IdP SAML logout URL), X.509 Certificate* (empty), Enable for EndUser Login* (toggle off), Override Return URL* (toggle off), Default Return URL* (Return URL), Sign SAML request* (toggle off), SSO Binding* (HTTP-Redirect), Domain Mapping* (Comma separated domain names), Show IdP to Users* (toggle off), Prompt for User Registration* (toggle off), and Send Configured Attributes* (toggle off). At the bottom, there are 'Save' and 'Cancel' buttons, with 'Save' highlighted by a red box.

- Click on **Save**.

Step 3: Test Connection


- Go to **Identity Providers** tab.
- Click on **Select>>Test Connection** option against the Identity Provider you configured.

The screenshot shows the xecorify dashboard interface. On the left is a dark sidebar with navigation options: Dashboard, Configure, Identity Providers (highlighted), User Stores, Apps, Policies, Customization, 2-Factor Authentication, Adaptive Authentication, Manage, Users, and Groups. The main content area is titled 'VIEW IDENTITY PROVIDERS' and includes an 'Add Identity Provider' button. A blue information banner reads: 'Make Default : Makes the selected User Store the default. Any user trying to SSO into the configured applications will have to authenticate their credentials against the default User Store.' Below this, there's a 'Show 10 entries' dropdown and a 'Search IDPs' search box. A table with columns 'Display Name', 'Identifier', 'IdP Type', and 'Action' contains one entry: 'Azure AD' with identifier 'AzureAD' and type 'SAML'. The 'Action' column for 'Azure AD' has a 'Select' dropdown menu open, showing options: Edit, Metadata, Test Connection (highlighted), Make Default, Show SSO Link, and Delete. The table footer indicates 'Showing 1 to 2 of 2 entries' and includes 'First' and 'Last' navigation buttons.

The screenshot shows a Microsoft sign-in page. At the top left is the Microsoft logo. Below it is the heading 'Sign in'. Underneath is a text input field with the placeholder text 'Email, phone, or Skype'. Below the input field is a link that says 'Can't access your account?'. At the bottom right of the page is a blue button with the text 'Next'.

- On entering valid Azure Ad credentials, you will see a pop-up window which as shown in below screen.

TEST SUCCESSFUL



Hello,

ATTRIBUTES RECEIVED:

| ATTRIBUTES | ATTRIBUTES VALUE |
|---|------------------|
| http://schemas.microsoft.com/identity/claims/displayname | |
| http://schemas.microsoft.com/identity/claims/tenantid | |
| http://schemas.microsoft.com/identity/claims/identityprovider | |
| NameID | |
| http://schemas.microsoft.com/identity/claims/objectidentifier | |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname | |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name | |
| http://schemas.microsoft.com/claims/authnmethodsreferences | |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname | |

[Close](#)

- Hence your configuration of Azure AD as IDP in miniOrange is successfully completed.