



# Rydoo Single-Sign-On

SUPPORT

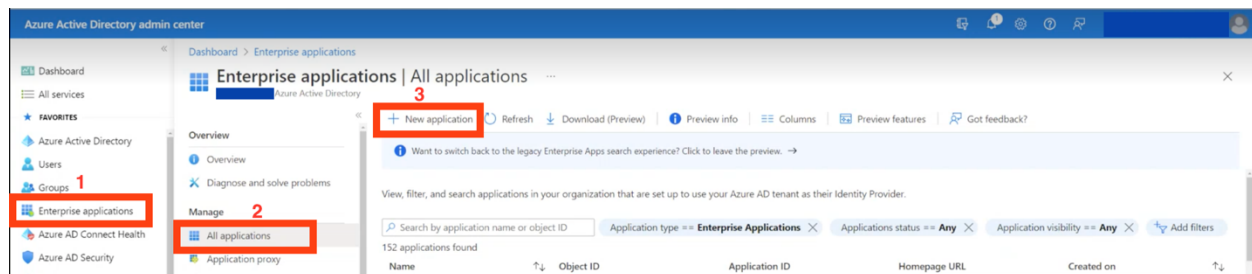


# Configure Rydoo Single Sign-On using Azure Active Directory

## Step 1:

Sign in to the Azure portal using your Azure Active Directory administrator account.

Browse to the **Active Directory > Enterprise Applications > All Applications >** and select **New application**



## Step 2:

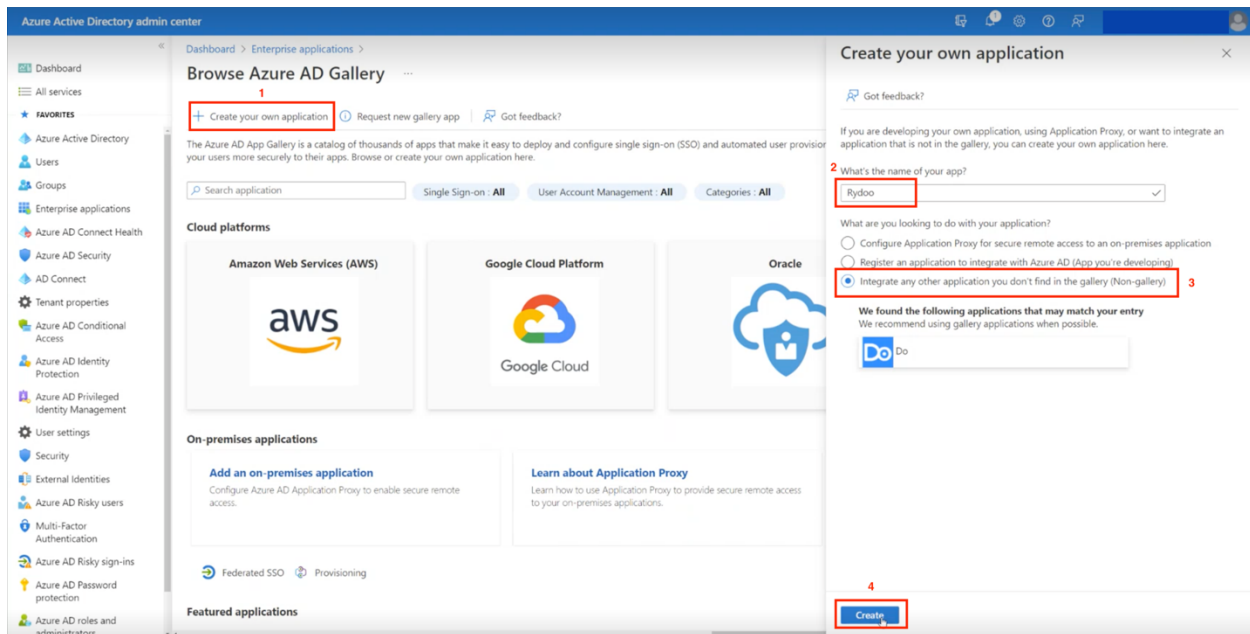
When the New application has been selected, you will be redirected to the Azure AD Gallery.

Select > **Create your own application** option

On the right a window will pop up where you can specify your own application details.

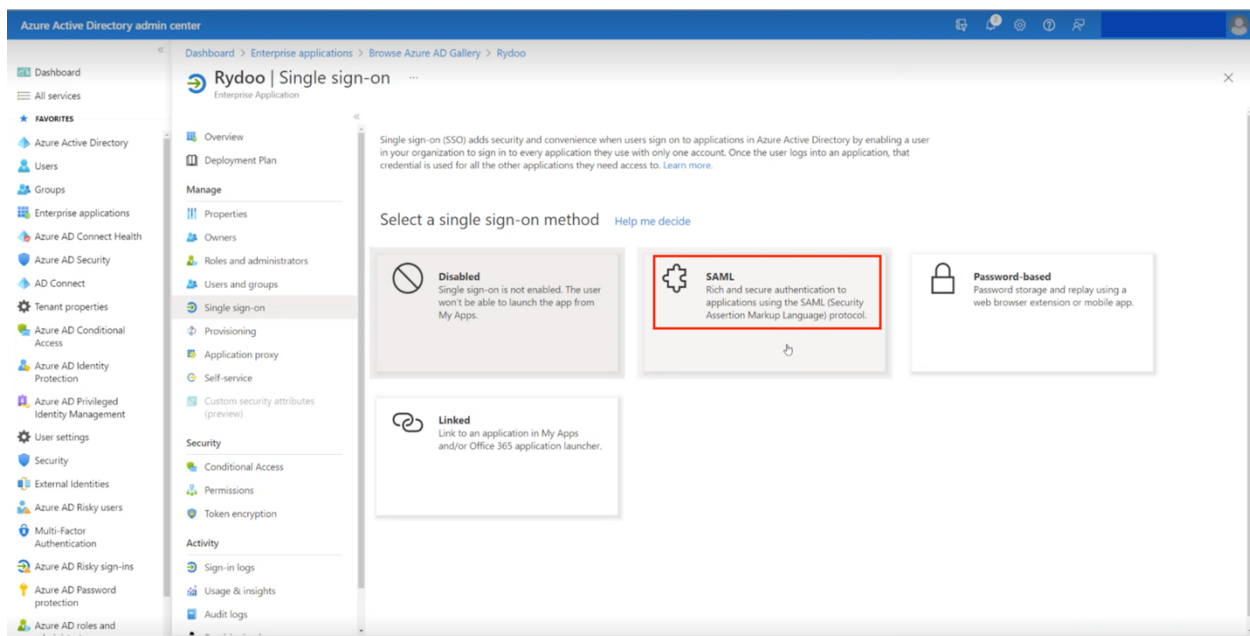
Two questions will appear as follows:

1. What's the name of the app? → Enter Rydoo
2. What are you looking to do with your application? Click on > Integrate any other applications you don't find in the gallery (Non-gallery) > Create



### Step 3:

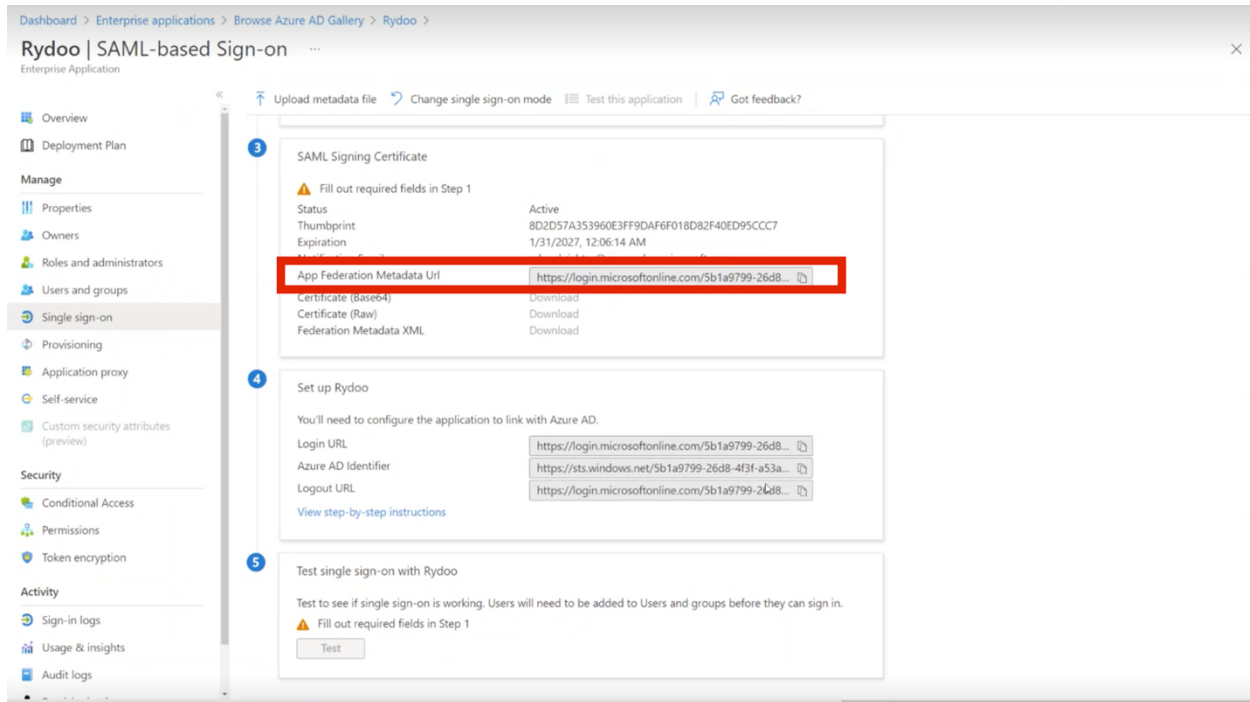
Please head to **Dashboard > Enterprise Applications > Browse Azure AD Gallery > Rydoo** to **Single Sign On** where you can find the option **SAML** to select.



Scroll down to point 3 in Azure → here you can find App Federation Metadata URL

Send this URL to your assigned Rydoo CSM or to connect@rydoo.com to set up the single sign-on.

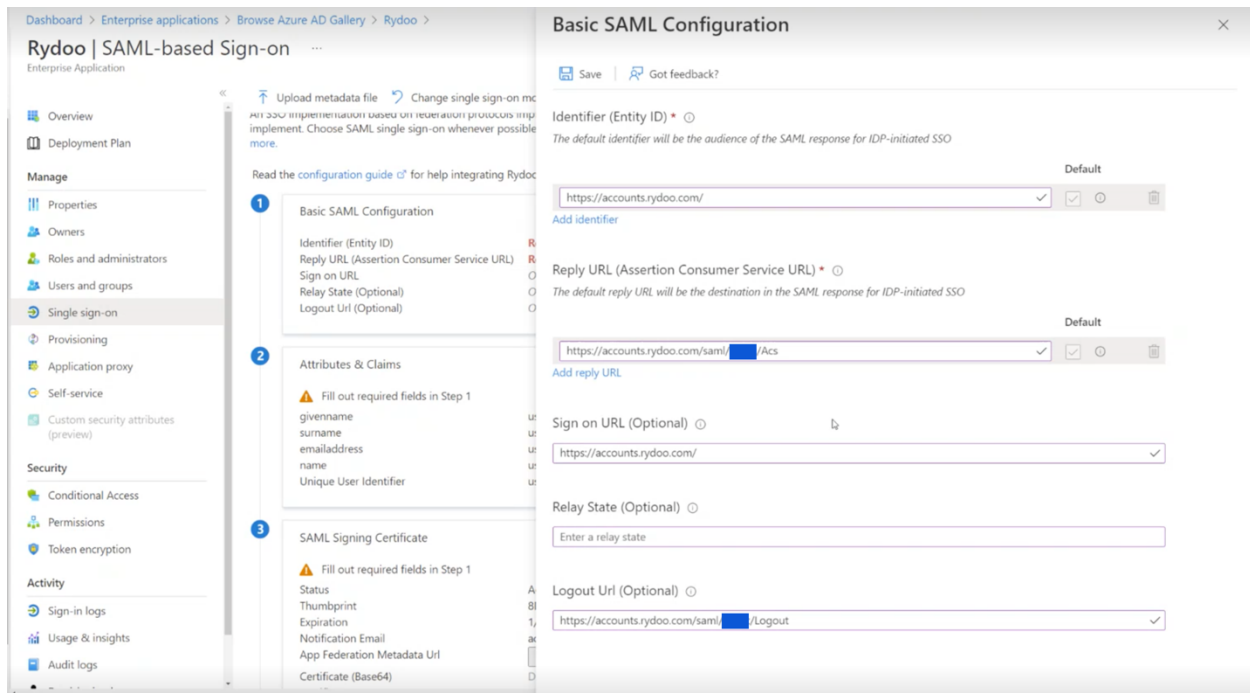
Rydoo will send you a confirmation as soon as it's set up on our and we will provide the URLs you would need to finalize configurations.



#### Step 4:

Configure URLs provided by Rydoo

Go to to **Dashboard > Enterprise Applications > Browse Azure AD Gallery > Rydoo to Single Sign On > SAML >** and edit Basic SAML configuration (point 1). Fill it out with the links that Rydoo has sent to you as you can see in the screenshot below.



### Identifier:

Should uniquely identify the application for which single sign-on is being configured. You can find this value as the Issuer element in the AuthRequest (SAML request) sent by the application. This value also appears as the **Entity ID** in any SAML metadata provided by the application. Check the application's SAML documentation for details on what its Entity ID or Audience value is. <https://accounts.rydoo.com/>

### Reply URL:

The reply URL is where the application expects to receive the SAML token. This is also referred to as the Assertion Consumer Service (ACS) URL. Check the application's SAML documentation for details on what its SAML token reply URL or ACS URL is. <https://accounts.rydoo.com/saml/CompanyName/Acs> should be configured.

### Sign On URL (SP-initiated only) :

Where the user goes to sign-in to this application. If the application is configured to perform service provider-initiated single sign-on, then when a user navigates to this URL, the service provider will do the necessary redirection to Azure AD to authenticate and log on the user in. <https://accounts.rydoo.com/> should be configured as the service provider.

**NOTE:** Company name to be changed accordingly based on information provided by Rydoo.

## Step 5:


Please head to the **Dashboard > Enterprise Applications > Browse Azure AD Gallery > Rydoo to Single Sign On > SAML >** and edit **Attributes & Claims** (point 2)

Make sure the Unique User Identifier (ID) is correctly set up.

**NameIDPolicy – EmailAddress** should be configured. Additional attributes like first name and last name may also be configured. Review or customize the claims.

User Attributes [Learn more](#)

Edit the user information sent in the SAML token when user sign in to Litware.

User Identifier 

user.mail

☒ View and edit all other user attributes

SAML Token Attributes

NAME	VALUE	NAMESPACE	
givenname	user.givenname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	...
surname	user.surname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	...
emailaddress	user.mail	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	...
name	user.userprincipalname	http://schemas.xmlsoap.org/ws/2005/05/identity/claims	...

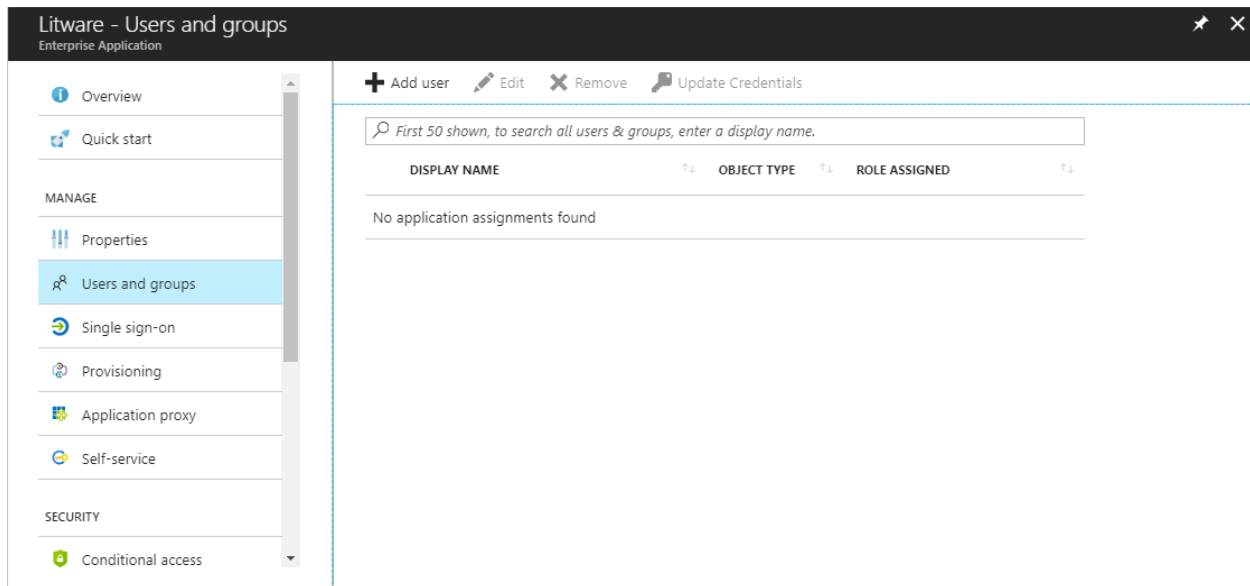
Add attribute

## Step 8:

Assign users and groups to your SAML application

To assign a user or group to your application, click the **Assign Users** button.

Select the user or group you wish to assign, and then select the Assign button. Assigning a user will allow Azure AD to issue a token for the user. It also causes a tile for this application to appear in the user's Access Panel. An application tile will also appear in the Office 365 application launcher if the user is using Office 365.



**NOTE:** You can upload a tile logo for the application using the Upload Logo button on the Configure tab for the application.

### Step 9:

Test the SAML application: Rydoo can enable the SSO for the key users initially, and upon successful testing, the SSO can then be enabled for the whole account.