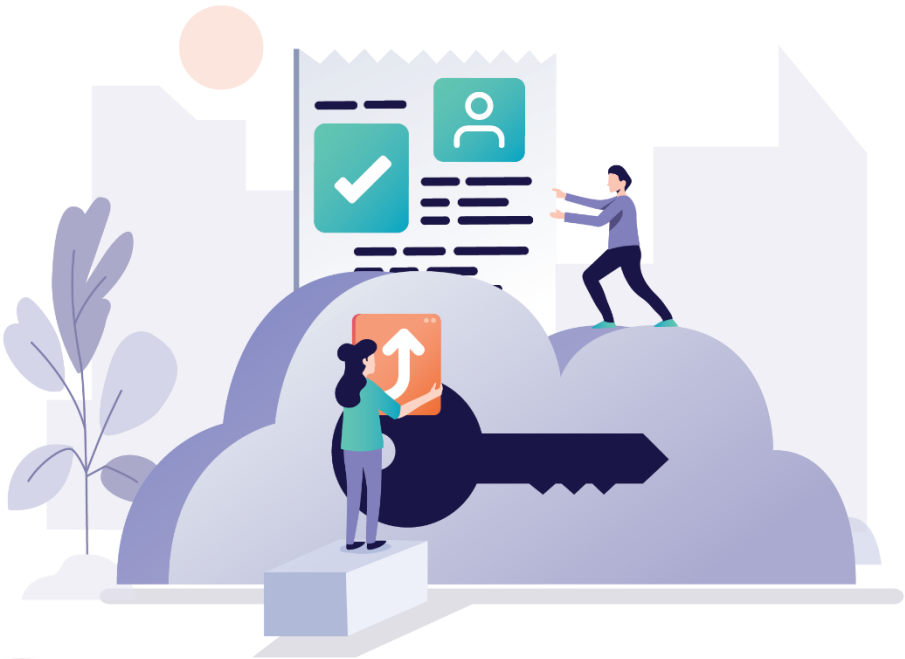
rydoo

Rydoo Single-Sign-On

Support



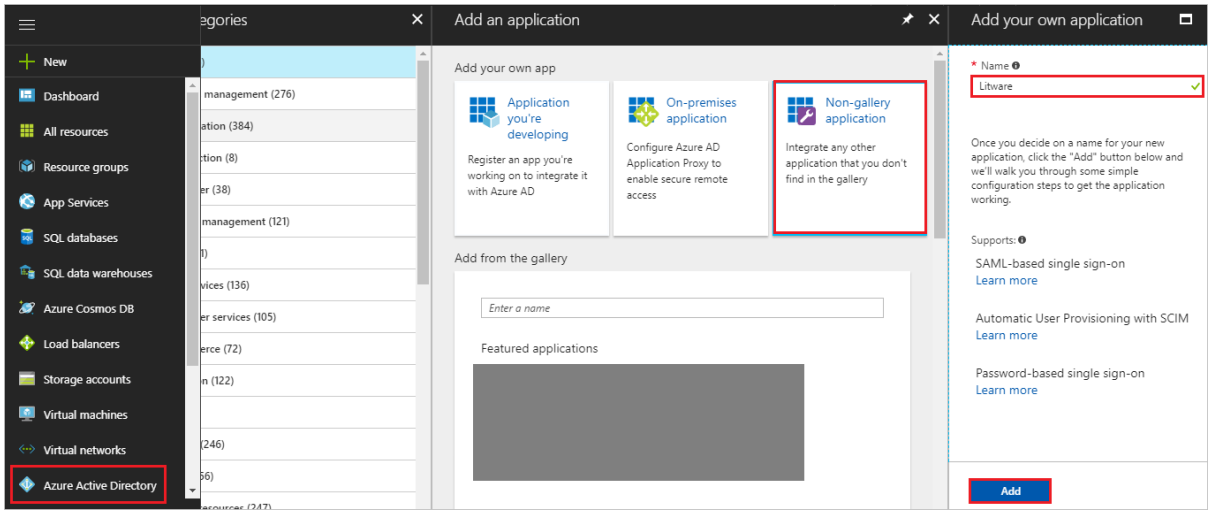
Configure Rydoo single sign-on using Azure Active Directory

Step 1:

Adding Rydoo application: To connect an application using an app integration template, sign in to the Azure portal using your Azure Active Directory administrator account.

Step 2:

Browse to the **Active Directory > Enterprise Applications > New application > Non-gallery application** section, select **Add**. After entering a Rydoo name, you can configure the single sign-on options and behavior.



Step 3:

Review certificate expiration data, status, and email notification

When you create a Non-Gallery application, Azure AD will create an application-specific certificate with an expiration date of 3 years from the date of creation. You need this certificate to set up the trust between Azure AD and Rydoo. From Azure AD, you can download the application metadata XML file or by using the App federation metadata URL.

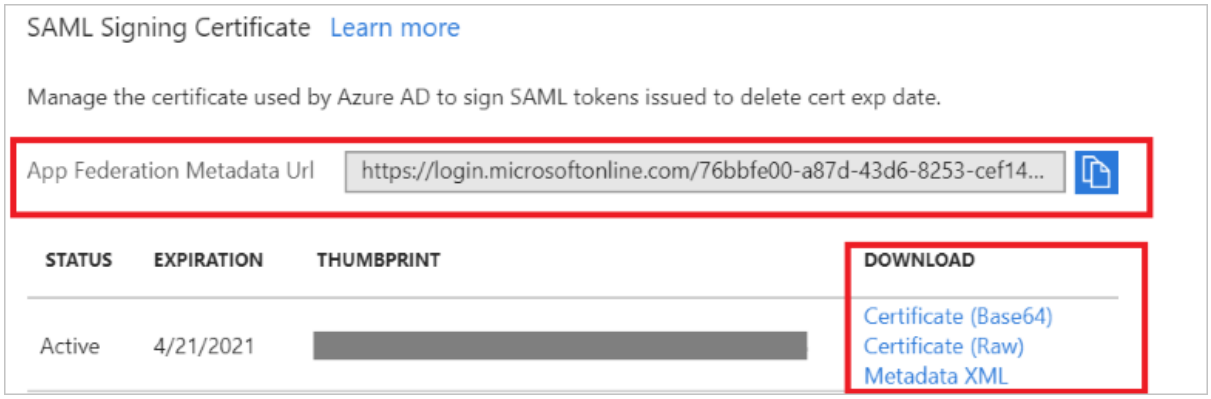
Example of a metadataURL:

Azure AD publishes federation metadata at `https://login.microsoftonline.com/<TenantDomainName>/FederationMetadata/2007-06/FederationMetadata.xml?appid=<AppID>`

For **tenant-specific endpoints**, the `TenantDomainName` can be one of the following types:

- A registered domain name of an Azure AD tenant, such as: `contoso.onmicrosoft.com`.
- The immutable tenant ID of the domain, such as `72f988bf-86f1-41af-91ab-2d7cd011db45`.
- AppID, such as `37939f70-cf51-434d-91b6-9f7e68a34bcl`

For **tenant-independent endpoints**, the `TenantDomainName` is `common`. This document lists only the Federation Metadata elements that are common to all Azure AD tenants that are hosted at login.microsoftonline.com.



Step 4:

Verify the certificate, and send the metadataURL to Rydoo to proceed with further configuration.

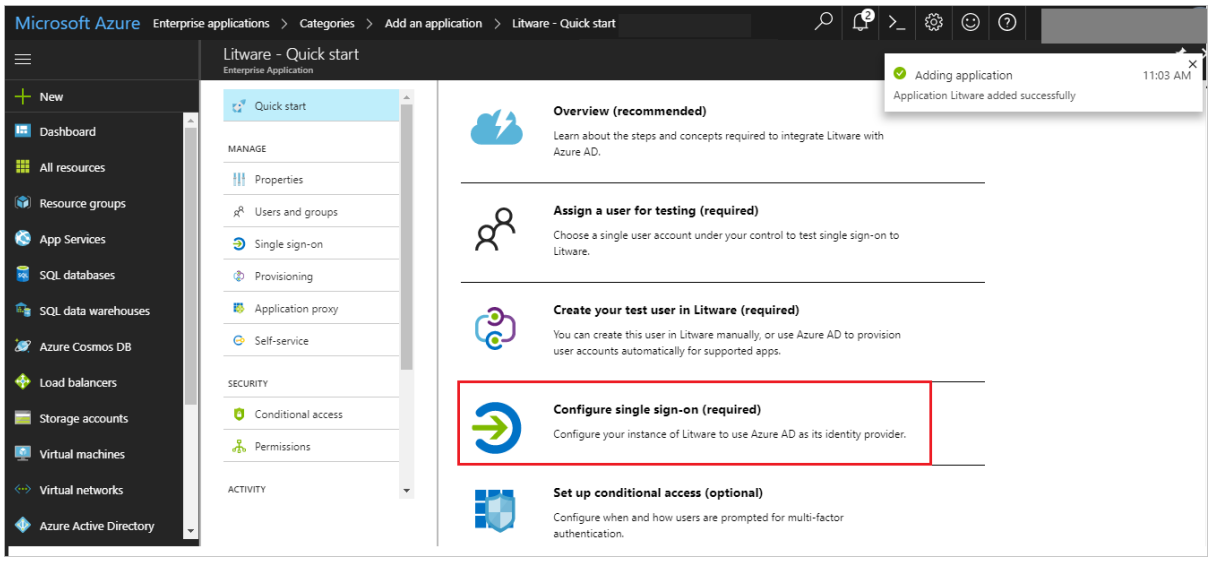
- You can configure the expiration date for at most 3 years.
- Check status of **Active** and then save the configuration.
- The correct notification email. When the active certificate is near the expiration date, Azure AD will send a notification to the email address configured in this field.

Note: MetadataURL should be shared with Rydoo first to proceed with configuration. Please do not remove the configuration after providing the metadataURL as this configuration would be used to set up connection between Rydoo and your

application. Once it's configured by Rydoo, necessary information will be shared to complete SAML configuration.

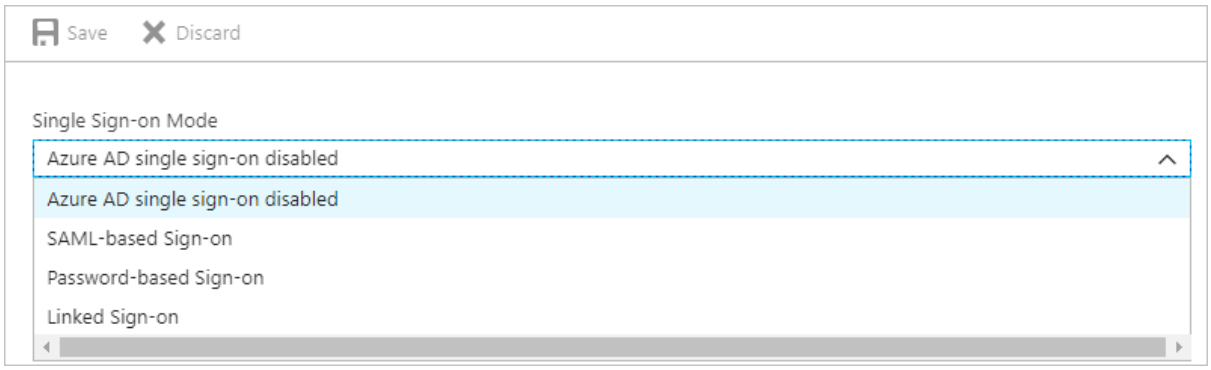
Step 5:

To start, select **Configure Single Sign-On** or click on **Single sign-on** from the application's left-hand navigation menu. The next screen presents the options for configuring single sign-on.



Step 6:

Rydoo works with SAML protocol, so to configure SSO, select this option to configure **SAML-based authentication for the application**. This requires that the application support SAML 2.0. Complete the subsequent sections to configure single sign-on between Rydoo and Azure AD.



Step 7:

Enter basic SAML configuration

To set up Azure AD, enter the basic SAML configuration. You can manually enter the values or upload a metadata file to extract the value of the fields.
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.

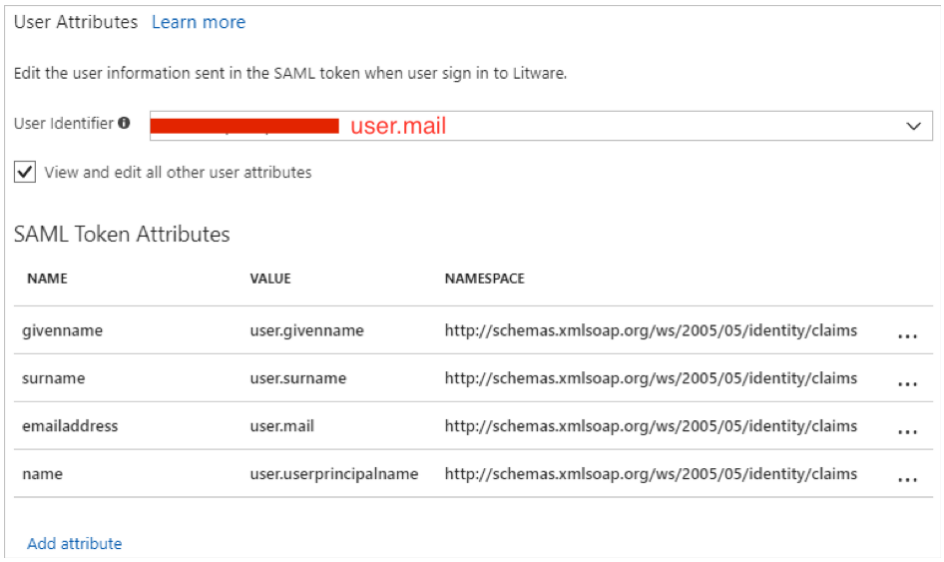
- **Identifier** - should uniquely identify the application for which single sign-on is being configured. https://accounts.rydoo.com/ should be configured.

- **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. https://accounts.rydoo.com/saml/**CompanyName**/Acs should be configured.

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

- **NameIDPolicy –** EmailAddress should be configured. Additional attributes like first name and last name may also be configured.

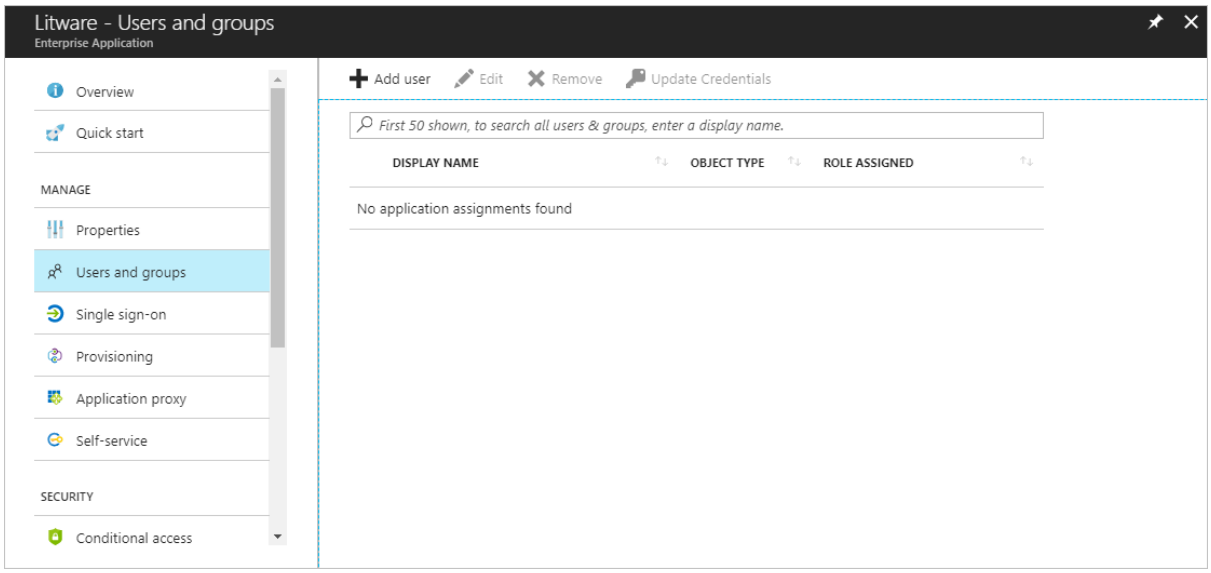
Review or customize the claims issued in the SAML



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.