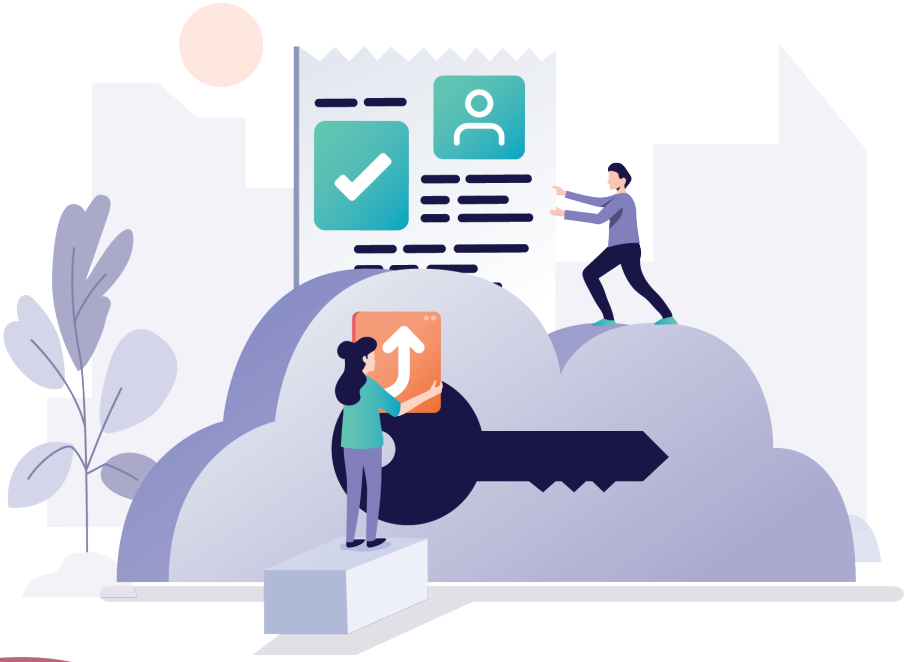
rydoo

Rydoo Single-Sign-On

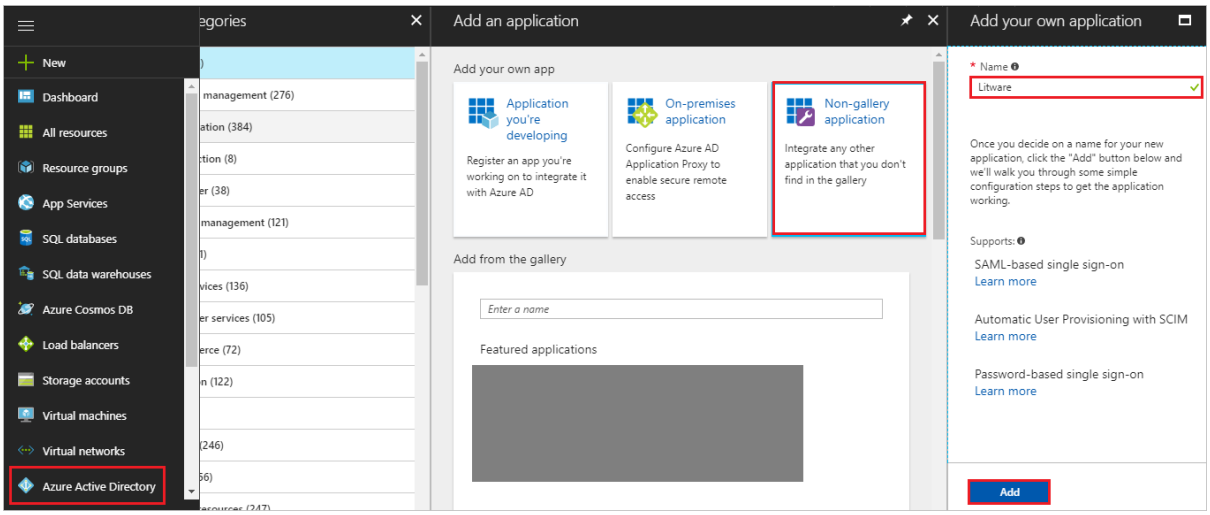
Support



Configure Rydoo single sign-on using Azure Active Directory

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. Browse to the **Active Directory > Enterprise Applications > New application > Non-gallery application** section, select **Add**, and then **Add an application from the gallery**.



In the app gallery, you can add Rydoo by selecting the **Non-gallery application** tile that is shown in the search results if Rydoo app wasn't found. After entering a Rydoo name, you can configure the single sign-on options and behavior.

Quick tip: As a best practice, use the search function to check to see if the application already exists in the application gallery. If the app is found and its description mentions single sign-on, then the application is already supported for federated single sign-on.

Review certificate expiration data, status, and email notification

When you create a Gallery or 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 the application. For details on the certificate format, see the application's SAML documentation.

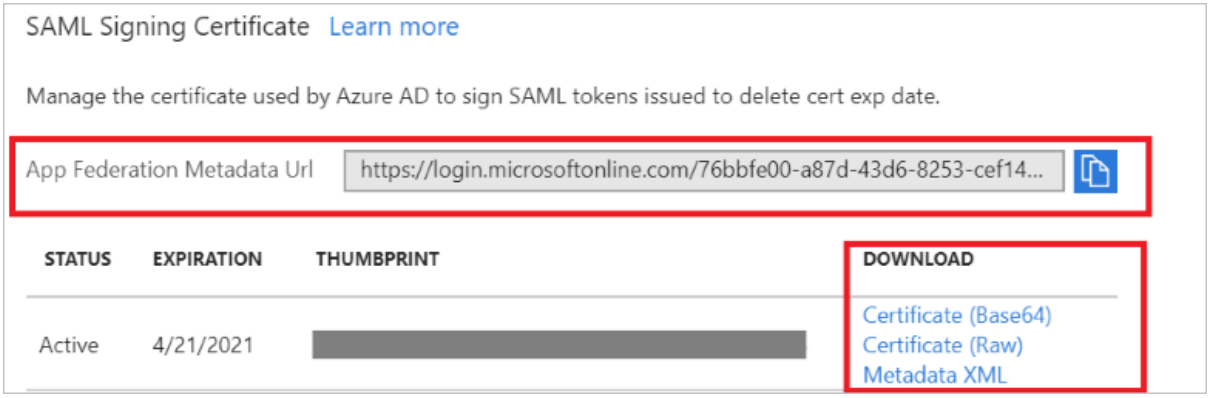
From Azure AD, you can download the certificate in Base64 or Raw format. In addition, you can get the certificate by downloading the application metadata XML file or by using the App federation metadata URL.

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`

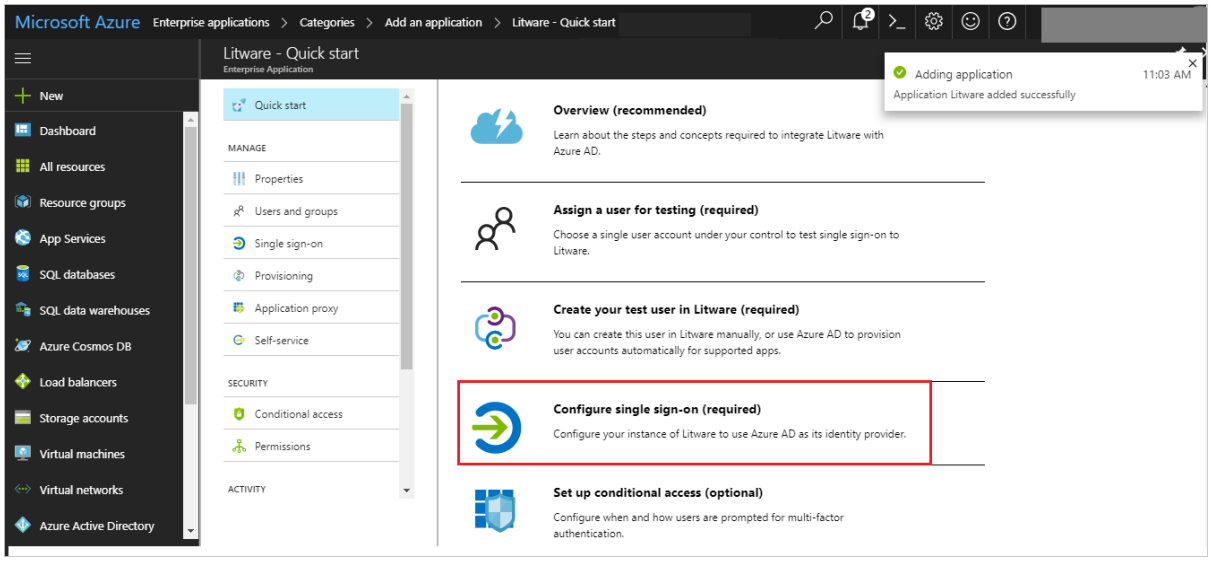
For **tenant-independent endpoints**, the `TenantDomainName` is `common`. This document lists only the Federation Metadata elements that are common to all Azure AD tenants that are hosted at login.microsoftonline.com.



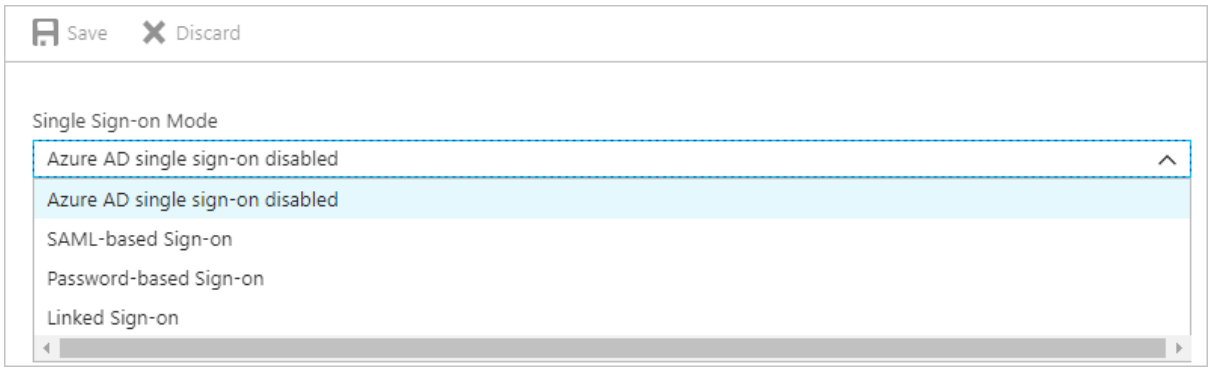
Verify the certificate, and send the metadataURL to Rydoo to proceed with further configuration.

- The desired expiration date. You can configure the expiration date for at most 3 years.
- A status of active. If the status is inactive, change the status to active. To change the status, check **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 to proceed with configuration. Once it's configured by Rydoo, necessary information will be shared to complete SAML configuration.



Adding an application this way provides a similar experience to the one available for pre-integrated applications. 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. The options are described in the next sections of this article.



SAML-based single sign-on

Select this option to configure SAML-based authentication for the application. This requires that the application support SAML 2.0. You should collect information on how to use the SAML capabilities of the application before continuing. Complete the following sections to configure single sign-on between the application and Azure AD.
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. 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.

  The following is an example of how the Identifier or Issuer appears in the SAML request sent by the application to Azure AD:

  Copy

```
<samlp:AuthnRequest
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
ID="id6c1c178c166d486687be4aaf5e482730"
Version="2.0" IssueInstant="2013-03-18T03:28:54.1839884Z"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://www.contoso.com<
/Issuer>
</samlp:AuthnRequest>
```

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.

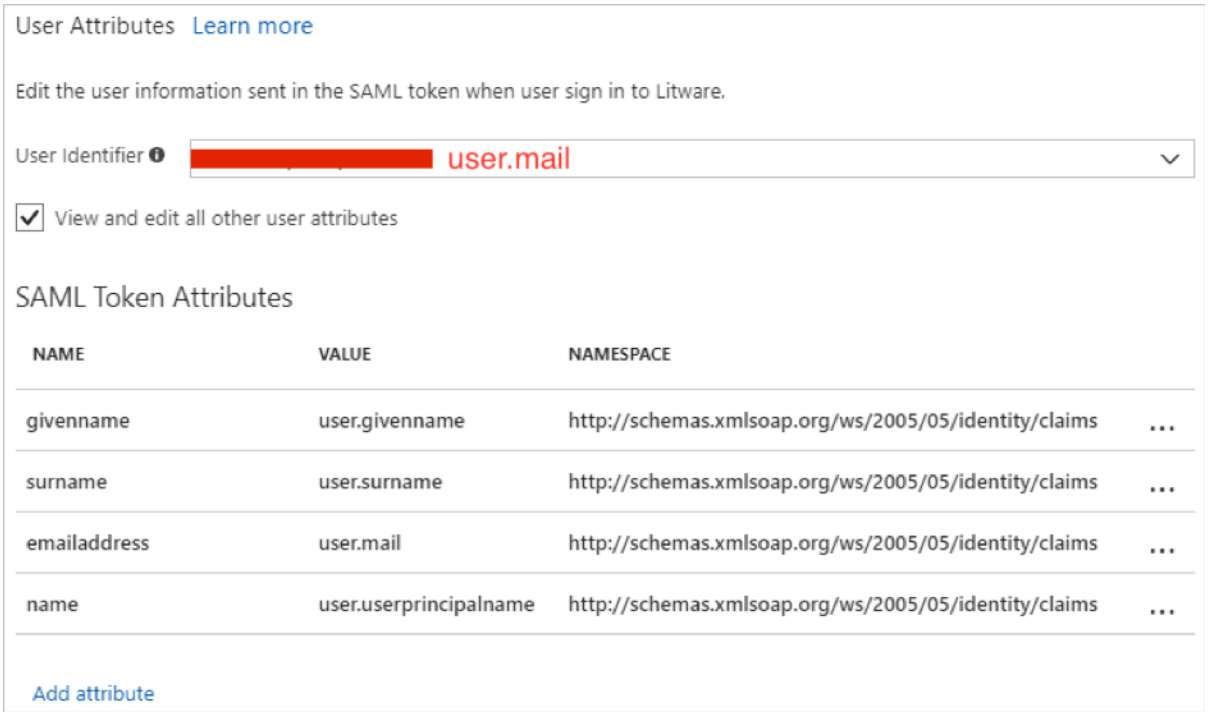
NOTE: Company name to be changed accordingly based on information provided by Rydoo.

Review or customize the claims issued in the SAML token

When a user authenticates to the application, Azure AD will issue a SAML token to the app that contains information (or claims) about the user that uniquely identifies them. By default this includes the user's username, **email address**, first name, and last name.

You can view or edit the claims sent in the SAML token to the application under the **Attributes** tab.

`NameIDPolicy` is provided, It should be configured in **emailAddress** format.
The `Format` attribute can have only one of the following values; any other value results in an error.



Set up target application

To configure the application for single sign-on, locate the application's documentation. To find the documentation, scroll to the end of the SAML-based sign-on configuration page, and then click on **Configure**.

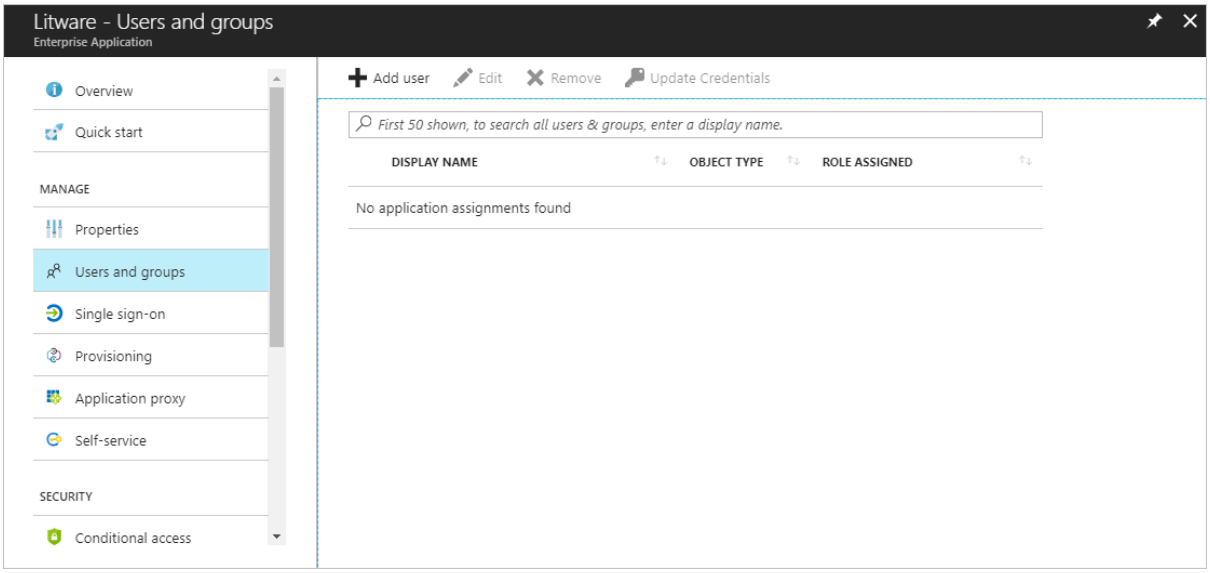
The required values vary according to the application. The Sign-On and Sign-Out service URL both resolve to the same endpoint, which is the SAML request-handling endpoint for your instance of Azure AD. The SAML Entity ID is the value that appears as the Issuer in the SAML token that is issued to Rydoo.

Rydoo will provide the metadata file with relevant information like sign-In URL to the endpoint and the EntityID.

Assign users and groups to your SAML application

Once your application has been configured to use Azure AD as a SAML-based identity provider, then it is almost ready to test. As a security control, Azure AD will not issue a token allowing a user to sign into the application unless Azure AD has granted access to the user. Users may be granted access directly, or through a group membership.

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.

Test the SAML application

Before testing the SAML application, you must have set up the application with Azure AD, and assigned users or groups to the application.