

Configure Single Sign-on (SSO) with Entra ID Enterprise Application

Document generated 09/29/2023

[PDF VERSION](#)

Tags | [Authentication](#) | [SSO](#) | [SAML](#) | [Azure AD](#) | [Entra ID](#) |

Admin privileges required

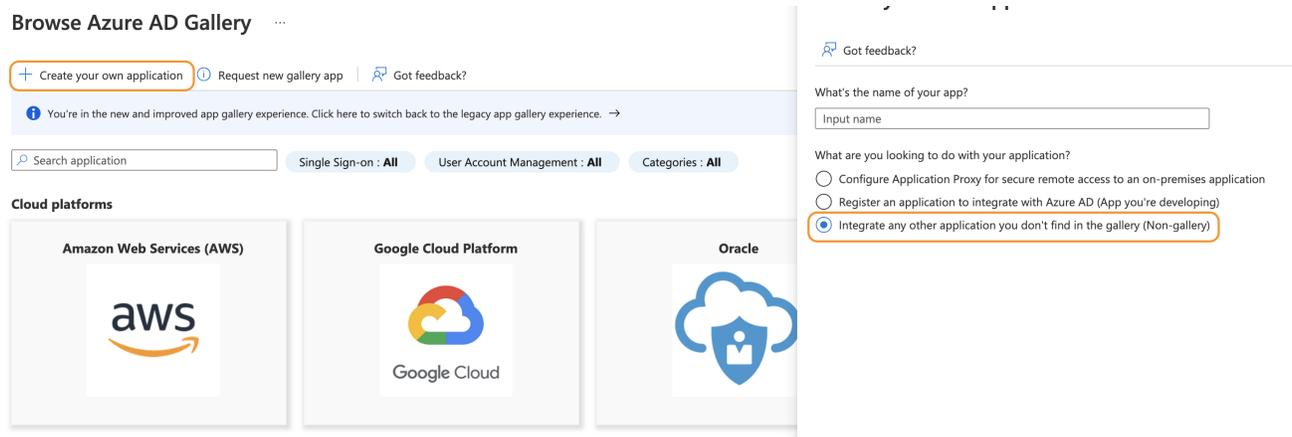
Applies to: Free Basic Business Enterprise

Enterprise users can access their documentation [here](#). [Find your plan](#).

To use SAML 2.0 Authentication with **Entra ID Enterprise Application**, go to your Entra ID Portal and add a new Enterprise Application. You need to click on Entra ID → Enterprise applications → Create your own application. If you cannot find the Entra ID menu, look into More Services and search for Entra ID.

1. Create a new Application

Now enter the name for your app (e.g. Stack Overflow for Teams), select the non-gallery application option, then click create.



Once the application loads, click on the Single sign-on option. Then click on SAML (or, depending on your Entra ID version, select SAML-based sign-on on the dropdown menu).

Overview

Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators (Preview)
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- ...

Properties

Name: Stack Overflow for Team...

Application ID: 8e8213de-26db-44ca-9f...

Object ID: 2599ed7a-7921-474c-9b...

Getting Started

- 1. Assign users and groups**
Provide specific users and groups access to the applications
[Assign users and groups](#)
- 2. Set up single sign on**
Enable users to sign into their application using their Azure AD credentials
[Get started](#)
- 3. Provision User Accounts**
Automatically create and delete user accounts in the application
[Get started](#)
- 4. Conditional Access**
Secure access to this application with a customizable access policy.
[Create a policy](#)
- 5. Self service**
Enable users to request access to the application using their Azure AD credentials
[Get started](#)

2. Configure URLs

Now edit the following URLs under Basic SAML Configuration:

Set up Single Sign-On with SAML

Read the [configuration guide](#) for help integrating Stack Overflow for Team Premium.

1 Basic SAML Configuration [Edit](#)

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	<i>Optional</i>
Relay State	<i>Optional</i>
Logout Url	<i>Optional</i>

- **Identifier (Entity ID):** Must be unique per application. We recommend you set this field to **StackOverflowForTeams**. You'll enter this value into your Stack Overflow Teams auth settings as **Issuer** and **Audience Restriction**. *Before moving on make sure the Entity ID checkbox for "Default" is checked.
- **Reply URL:** Enter your Team's **Assertion Consumer Service URL** into the **Reply URL** field. You can find this URL in your **Authentication** settings on Stack Overflow.

Authentication

Setup your Team's authentication method. This determines how users login and join your Team.

 [Looking to manage users?](#)

Single sign-on (SSO)

This is the safest and most efficient option for members to join and login to your team.

[Learn more about SSO](#)

RECOMMENDED

Email domain

Anyone with your organization's verified email domain will be able to join.

You will still be able to invite users manually.

Manual invitations

Invite new users by email.

Identity provider (IdP) settings

Making any changes on this page may cause breaking authentication methods for all your Team members and revoke their access. If you'd like help making changes, [contact Customer Support](#).

Assertion Consumer Service URL

This setting cannot be changed and is for informational purposes.

`https://sso.stackoverflow.com/c/[your_site]/auth/saml2/post`



3. Configure Attributes

On the user Attributes tab, make sure the user email is being included in the SAML response.

User Attributes & Claims		 Edit
givenname	user.givenname	
surname	user.surname	
emailaddress	user.mail	
name	user.userprincipalname	
Unique User Identifier	user.userprincipalname	

You can also add the following optional attributes. When configured and included in the SAML response, Stack Overflow for Teams automatically updates these user data fields on login.

- Job Title
- Department

4. Configure Attributes

In the SAML Signing Certificate section of your Azure AD application, download the Certificate (Base 64) to save the certificate file on your computer.

3

SAML Signing Certificate

Status	Active
Thumbprint	[REDACTED]
Expiration	[REDACTED]
Notification Email	[REDACTED]
App Federation Metadata Url	[REDACTED]
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

5. Set up Users and/or Groups

Do not forget to add users and/or groups to the application, under the Users and groups menu.

6. Set up Authentication settings on Stack Overflow for Teams

We must now set up our Team for using this Entra ID enterprise app. Open the Team Auth Settings page on a separate tab: [https://stackoverflowteams.com/c/\[your_team\]/admin/auth-settings](https://stackoverflowteams.com/c/[your_team]/admin/auth-settings)

You'll need to fill the following fields according to what you got on your Entra ID App:

- **Single Sign-On Service Url:** that's the Login URL of your Entra ID application.

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/c2c4c2c2-b302-...
Azure AD Identifier	https://sts.windows.net/c2c4c2c2-b302-41d2-8c8...
Logout URL	https://login.microsoftonline.com/c2c4c2c2-b302-...

[View step-by-step instructions](#)

- **Single Sign-On Service Protocol Binding:** do not change, leave as POST
- **Issuer and Audience Restriction:** that's the Identifier (Entity ID) URI you chose (see above)

- **Display Name Assertion:** for Entra ID apps, the display name assertion is usually <http://schemas.microsoft.com/identity/claims/displayname> or <http://schemas.microsoft.com/identity/claims/name>. If you want to be 100% sure, check your attributes list.
- **Email Address Assertion:** for Entra ID apps, the email assertion is usually <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress>. If you want to be 100% sure, check your Federation Metadata xml, and search for Email. The correct value will be whatever is described in the Uri attribute.
- Leave all checkboxes unchecked
- **Identity Provider Certificates:** open the certificate file you downloaded from your Entra ID app and copy/paste the contents of that file.

(Optional) Automate the renewal of certificates

Once you have set up SSO according to the above instructions, you can set up a Federation Metadata URL to automate the renewal of the Identity Provider Certificates. If you choose not to, the certificate will have to be updated by an admin every year, or access to the Team will be interrupted.

To set this up, click on the *Automatically update certificates periodically* checkbox, and paste your Federation Metadata URL from Entra ID, into the field that appears. Click Save, and you're all set.

Verify the SubjectConfirmation element on a SAML Response?

Automatically update certificates periodically

Requires federation metadata URL to be set.

Federation Metadata URL

A FederationMetadata.xml file that can be downloaded anonymously over https

Need help? Submit an issue or question through our [support portal](#).