

Configure Single Sign-on (SSO) with Entra ID

Document generated 10/23/2023

[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.

NOTE: Before October 2023, Entra ID was called Azure Active Directory (Azure AD).

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.

App registrations

[+ New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

 Try out the new App registrations search preview! Click to enable the preview. →

 Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates for these libraries. [Learn more](#)

[All applications](#) [Owned applications](#) [Deleted applications \(Preview\)](#)

 Start typing a name or Application ID to filter these results

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).

Save
Discard
Got feedback?

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Platform configurations

Depending on the platform or device this application is targeting, additional configuration may be required such as redirect URIs, specific authentication settings, or fields specific to the platform.

+ Add a platform

Web

2. Configure URLs

Now edit the following URLs under Basic SAML Configuration:

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.

- **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.

Display name : [Stack Overflow non-premium](#)
 Application (client) ID : c3cbd98b-3c04-417b-a633-51df1fcac147
 Object ID : ee70a6fe-968e-4ff2-a178-92db2fb15f83
 Directory (tenant) ID : c2c4c2c2-b302-41d2-8c88-03850bed4af0
 Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)
 Redirect URIs : [1 web, 0 spa, 0 public client](#)
 Application ID URI : [Add an Application ID URI](#)
 Managed application in I... : [Stack Overflow non-premium](#)

3. Configure Attributes

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

The screenshot shows the 'Token configuration' page for an application named 'Stack Overflow non-premium'. The 'Optional claims' section is highlighted with an orange box. It contains a table with the following data:

Claim	Description
acct	User's account status in tenant
<input checked="" type="checkbox"/> email	The addressable email for this user, if the user has one
upn	An identifier for the user that can be used with the user name...

The 'Token type' section is also highlighted with an orange box. It shows 'SAML' selected as the token type. The text below it says: 'Access and ID tokens are used by applications for authentication. [Learn more](#)'.

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 Entra ID application, download the Certificate (Base 64) to save the certificate file on your computer.

The screenshot shows the 'Endpoints' page for the 'Stack Overflow non-premium' application. The 'Federation metadata document' endpoint is highlighted with an orange box. The URL for this endpoint is: <https://login.microsoftonline.com/c2c4c2c2-b302-41d2-8c88-03850bed4af0/federationmetadata/2007-06/federationmetadata.xml>

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.

☒ **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

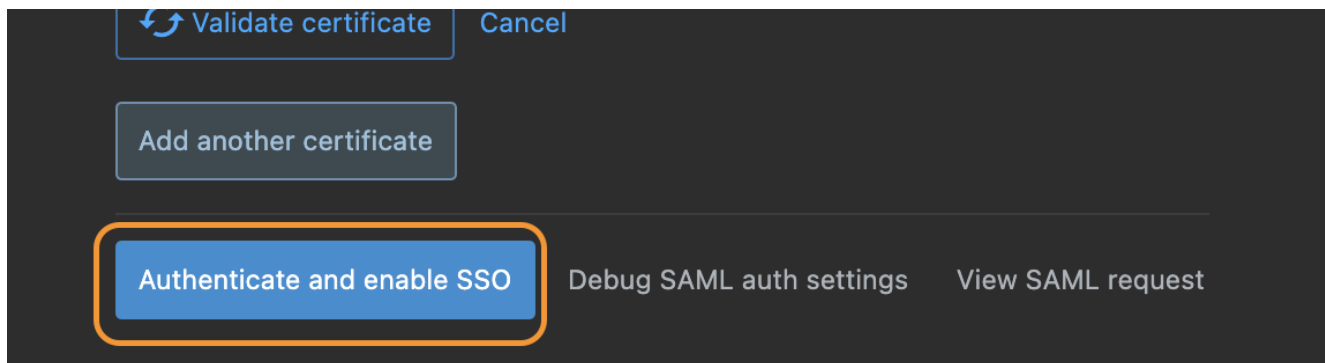
e.g. URL to FederationMetadata.xml

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.



- **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**.

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