

Configure Single Sign-on (SSO) with OneLogin

Document generated 10/23/2023

[PDF VERSION](#)

Tags | [Authentication](#) | [SSO](#) | [SAML](#) | [OneLogin](#) |

Admin privileges required

Applies to: Free Basic Business Enterprise

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

1. OneLogin Setup for Stack Overflow for Teams

In OneLogin, add a new SAML 2.0 Application. In this example, we used a *SAML Custom Connector (Advance)* application.

Once the application is created, go to the Configuration tab.

SAML Custom Connector (Advanced)

Info	Application details
Configuration	RelayState <input type="text"/>
Parameters	Audience (EntityID) <input type="text" value="https://sso.stackoverflow.com/c/[your_site]"/>
Rules	Recipient <input type="text" value="https://sso.stackoverflow.com/c/[your_site]/auth/saml2/post"/>
SSO	ACS (Consumer) URL Validator* <input type="text" value="https://sso.stackoverflow.com/c/[your_site]/auth/saml2/post"/> <div><i>i</i> *Required.</div>
Access	ACS (Consumer) URL* <input type="text" value="https://sso.stackoverflow.com/c/[your_site]/auth/saml2/post"/> <div><i>i</i> *Required</div>
Users	Single Logout URL <input type="text"/>
Privileges	
Setup	

The following can be used to fill in on this page.

- **RelayState:** This can remain empty.
- **Audience (EntityID)** is something you can make up. The URI doesn't need to exist, but will be used as the Audience Restriction URL you must add on the SO Admin Authentication settings. It is recommended to use the Assertion Consumer Service URL of your Team, which can be found on [https://stackoverflowteams.com/c/\[your_site\]/admin/access/authentication](https://stackoverflowteams.com/c/[your_site]/admin/access/authentication)
- **ACS (Consumer) URL & ACS (Consumer) URL Validator:** This is the Assertion Consumer Service URL of your Team, which can be found on [https://stackoverflowteams.com/c/\[your_site\]/admin/access/authentication](https://stackoverflowteams.com/c/[your_site]/admin/access/authentication)

You can leave the remaining as default.

Now go to the Parameters tab.

You must have at least one parameter for the user display name, email, and NameID attributes. All must be included in the SAML assertions, so when adding the custom parameters, make sure you check the Include in SAML assertion checkbox.

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

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Credentials are

☐ Configured by admin

☒ Configured by admins and shared by all users

SAML Custom Connector (Advanced) Field

Email

Name

NameID value

Edit Field Email

Name	Email
Value	<div>Email</div>
Flags	<input checked="" type="checkbox"/> Include in SAML assertion

CANCEL

DELETE


SAVE

2. Configure Stack Overflow Authentication Settings

In a new browser, open your Stack Overflow **Authentication** settings on Stack Overflow. Make sure *Single sign-on (SSO)* is selected.

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

On OneLogin click the SSO tab

SAML Custom Connector (Advanced)

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Enable SAML2.0

Sign on method
SAML2.0

X.509 Certificate
Standard Strength Certificate (2048-bit)
[Change](#) [View Details](#)

SAML Signature Algorithm
SHA-256

Issuer URL
<https://app.onelogin.com/saml/metadata/>

SAML 2.0 Endpoint (HTTP)
<https://>

SLO Endpoint (HTTP)
<https://>

You'll need to copy over to Stack Overflow the following fields according to what you got on OneLogin:

- **Single Sign-On Service Url:** that's the SAML 2.0 Endpoint on OneLogin.
- **Single Sign-On Service Protocol Binding:** do not change, leave as POST.
- **Issuer:** that's the Issuer URL on OneLogin.
- **Audience Restriction:** This is the Audience URL you set on the OneLogin Configuration tab.
- **Display Name Assertion:** This is the SAML Test Connector (IdP) Field, on the Parameters tab, for the user display name. In our example, that was the "Name" parameter.
- **Email Address Assertion:** should match the SAML Test Connector (IdP) Field, on the Parameters tab, for the user email. In our example, that was the "Email" parameter.
- **Job Title** (optional): should match the user job title attribute you entered on the Parameters tab.
- **Department** (optional): should match the user department attribute you entered on the Parameters tab.
- Leave all checkboxes unchecked.
- **Identity Provider Certificates:** copy and paste the certificate for your OneLogin setup. This can be found by clicking on View Details for the certificate generated by OneLogin in the screenshot above.

[Certificates /](#)

Standard Strength Certificate (2048-bit)

SHA256

Fingerprint



X.509 Certificate

X.509 Certificate



X.509 PEM

Download

3. Test Configure Authentication Settings for your Stack Overflow Team

Validate your certificate by pressing **Validate certificate** (you should get a green box with a success message).

Now press Authenticate and enable. You should all be good to go to [https://stackoverflowteams.com/c/\[your_site\]](https://stackoverflowteams.com/c/[your_site]) with your SSO.

If any issue arises you can use Debug SAML auth settings and View SAML request to find out where the issue might be occurring.

Identity Provider Certificates

Base64-encoded public keys used to verify SAML responses from the Identity Provider

t3d0Gj/r2tCoU/7MLmBRjj1w65jAGZqRwvFd4+moP0gF



Validate certificate

Cancel

Add another certificate

Authenticate and enable SSO

Debug SAML auth settings

View SAML request

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