

Configure Single Sign-on (SSO) with Okta

How to set up Stack Overflow for Teams for SAML SSO authentication with Okta.

Document generated 05/16/2025

[PDF VERSION](#)

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

ADMIN PRIVILEGES REQUIRED

Applies to: Free Basic Business Enterprise

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

Overview

These instructions describe how to integrate your Stack Overflow for Teams Basic or Business site with Okta as your Identity Provider (IdP) for authentication. Once configured, your users will be able to use Okta and the Security Assertion Markup Language (SAML) for Single Sign-on (SSO) authentication into your site. You can learn more about SAML in our [SAML Authentication Overview](#) document.

When setting up SAML authentication, you'll configure your Stack Overflow for Teams site and the Okta IdP in a back-and-forth process. We recommend having a browser tab open to each site.

THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS BASIC AND BUSINESS ONLY.

Stack Overflow for Teams Enterprise users should read [this article](#) instead. [Find your plan](#).

Configure Okta SAML settings

From the *Applications* page in Okta, click *Browse App Catalog*. That will take you to the Application Directory, from which you can search for **Stack Overflow for Teams**.

Then Click *Add* to begin set up.

- Dashboard ▼
- Directory ▼
- Applications ▲
 - Applications
 - Self Service
- Security ▼
- Workflow ▼
- Reports ▼
- Settings ▼

← Back to Applications

Browse App Integration Catalog

Create New App

CATEGORIES	
All Integrations	7227
Analytics	659
Apps for Good	2
Collaboration and Productivity	1322
Developer Tools	638
Directories and HR Systems	384
Data Privacy and Consent Management	10
Identity Proofing	5
Identity Governance and Administration	17
CRM and Marketing	736
Security	733

INTEGRATIONS

Stack Overflow for Teams	SAML
Stack Overflow Enterprise	SAML
Stack Overflow Careers	SWA
Userflow	SAML
Stackdriver	SWA

[See All Results](#)

Give the application a name (we recommend sticking to the default *Stack Overflow for Teams*). Then Click *Done*.

On the Application page, click the *Sign On* tab, then open *View Setup Instructions* in a separate browser. We will be using details from this page in setup.



Stack Overflow for Teams

Active ▾



[View Logs](#) [Monitor Imports](#)

General

Sign On

Mobile

Import

Assignments

Settings

[Cancel](#)

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)



SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Disable Force
Authentication



Never prompt user to re-authenticate.

[Preview SAML](#)



SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

Identity Provider metadata is available if this application supports dynamic

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`



Configure Okta authentication settings

On the Stack Overflow for Teams Application page on Okta, click the *Edit* button

Enter the **Customer ID** under *Advance Sign-on Settings* then press *Save*

- Your **Customer ID** can be found in the *Assertion Consumer Service URL* on Stack Overflow Authentication Settings
For example: If your *Assertion Consumer Service URL* is `https://sso.stackoverflow.com/c/acme/auth/saml2/post`, your **Customer ID** is `acme`.

Settings Cancel

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

i SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State
All IDP-initiated requests will include this RelayState.

Attributes (Optional) [Learn More](#)

Disable Force Authentication Never prompt user to re-authenticate.

[Preview SAML](#)

⚙️ SAML 2.0 is not configured until you complete the setup instructions.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

Advanced Sign-on Settings

These fields may be required for a Stack Overflow for Teams proprietary sign-on option or general setting.

Customer ID
Enter your Customer ID. Refer to the Setup Instructions above to obtain this value.

Configure Stack Overflow for Teams SAML settings

From the Okta *View Setup Instructions* skip to **Step 4**

Copy and paste the **Single Sign-On Service URL** given here to the Single Sign-On Service URL textbox on Stack Overflow Authentication settings.

Copy and paste the **Issuer** given here to the Issuer textbox on Stack Overflow Authentication settings.

For the following fields on Stack Overflow, you can enter:

Audience Restriction: `https://stackoverflow.com`

Display Name Assertion: `displayname`

Email Address Assertion: `email`

You can also add the following optional SAML attributes:

- Job title (as `jobTitle`)
- Department (as `department`)

When Okta includes `jobTitle` and `department` in the SAML response, your Stack Overflow for Teams site automatically updates these user data fields on login. It will then display these fields on the user profile page.

Copy and paste the **Identity Provider Certificate** given here to the Identity Provider Certificate on Stack Overflow Authentication settings.

4 Follow the steps below:

- **Method:** Select **Single sign-on**.
- **Assertion Consumer Service URL:** Make a copy of the portion marked in red. This is your **Customer ID**.

For example: If your **ACS URL** is `https://sso.stackoverflow.com/clacme/auth/saml2/post`, your **Customer ID** is `acme`.

- **Single sign-on Service Url:** Copy and paste the following:

```
https://dev-95766977.okta.com/app/stackoverflowteams/ex[REDACTED]sso/saml
```

- **Single sign-on Service Protocol Binding:** Select `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.

- **Issuer:** Copy and paste the following:

```
http://www.okta.com/[REDACTED]
```

- **Audience Restriction:** Enter `https://stackoverflow.com`.
- **Display Name Assertion:** Enter `displayname`.
- **Email Address Assertion:** Enter `email`.
- **Identity Provider Certificates:** click **Add another certificate**, then copy and paste the following:

```
-----BEGIN CERTIFICATE-----  
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF  
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF  
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF  
00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 88 99 AA BB CC DD EE FF
```

Save and test Stack Overflow for Teams SAML settings

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/{addyourteam}` 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/7MLmBRji1w65jAGZqRwvFd4+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](#).