

Configure Single Sign-on (SSO) with Okta

Set up Stack Overflow for Teams Enterprise for SAML authentication with Okta.

Document generated 12/06/2024

[PDF VERSION](#)

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

Applies to: Free Basic Business Enterprise

ADMIN PRIVILEGES REQUIRED

This documentation is for **Stack Overflow for Teams Enterprise**. Free, Basic, and Business users can access their documentation [here](#). [Find your plan](#).

Overview

These instructions describe how to integrate your Stack Overflow for Teams Enterprise (SOE) 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.

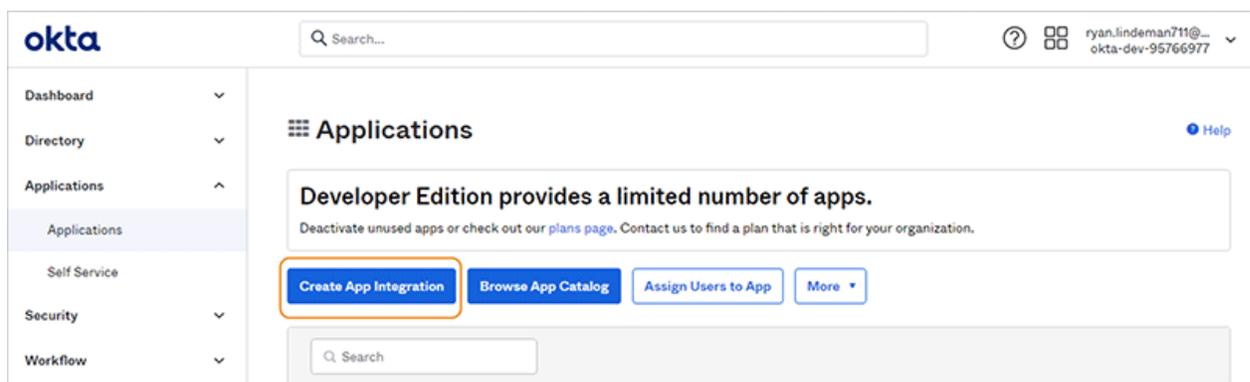
When setting up SAML authentication, you'll configure your SOE site and the Okta IdP in a back-and-forth process. We recommend having a browser tab open to each site.

THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.

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

Create a new Okta SAML application

1. From the Applications page in Okta, click **Create App Integration**. Add a new custom Application.



2. Choose **SAML 2.0** as **Sign-on method**.

Create a new app integration ✕

Sign-on method

[Learn More](#) 

- OIDC - OpenID Connect**
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.
- SAML 2.0**
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.
- SWA - Secure Web Authentication**
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.
- API Services**
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

[Cancel](#) [Next](#)

3. For General Settings choose any **App name** and **App logo** (optional) that makes sense for your organization.

Create SAML Integration

1 General Settings 2 Configure SAML

1 General Settings

App name: Stack Overflow for Teams

App logo (optional) 



App visibility

Do not display application icon to users

Do not display application icon in the Okta Mobile app

[Cancel](#) [Next](#)

Configure Okta SAML settings

1. In a new browser window or tab, open your SOE site and click **Admin settings** in the left-hand menu. Click **Authentication**, then **Configure SAML 2.0**.

CUSTOMIZE

ACCESS MANAGEMENT

CONTENT

INTEGRATION AND APPS

COMMUNICATION

MAINTENANCE

Authentication

Control how Users get access to the site



Let's choose and configure an authentication method.
How would you like to control how users access the site?

[Use SAML 2.0](#) [Use Active Directory](#)

2. Return to the SAML Settings for Okta and add the following information.

- **Single sign-on URL** This is the `/auth/saml2/post` URL of your SOE instance. This is also your **Assertion consumer service URL** on SOE.

Authentication

Control how Users get access to the site

Currently authenticating using **No Authentication** [Configure Active Directory](#)

SAML 2.0 settings

Assertion consumer service URL
This is the `/auth/saml2/post` URL of your Stack Overflow Enterprise instance. Please make sure the Domain Name (FQDN) is correct.
e.g., `https://soetest.com/auth/saml2/post`

- **Audience URI** This is something you can make up. On the SOE authentication settings, this will be used as the **Audience Restriction**. A good suggestion is to use the sample URL provided on the SOE authentication settings page.

Audience restriction Optional

If empty, does not restrict login based on audience. Otherwise, we expect the SAML response to contain this.
e.g., `https://soetest.com/auth/saml2/info`

- **Default Relay State** Leave this blank.
- **Name ID Format** Choose **Unspecified**.
- **Application Username** Use a value that will be static for users. Okta username will work.

3. Click **Show Advanced Settings** and check the following settings.

- Set **Response** to **Signed**. Stack Overflow Enterprise will not accept unsigned responses.
- Leave **Assertion Encryption** as **Unencrypted**.

Encrypt assertions (optional)

You can also encrypt the assertion if desired. In that case, you need to upload the public key of your signing certificate to Okta. Your SOE instance also needs both the private and public keys, and how you'll provide those depends on your deployment type.

- For on-premise deployments, you need to provide the certificate into the Windows Certificate Store at **Local Machine** -> **Personal**. You must do this on all web servers running SOE.
- For cloud-hosted deployments, [reach out](#) to Stack Overflow support with your certificates and we'll upload them to your SOE site.

A SAML Settings

General

Single sign on URL ?

 Use this for Recipient URL and Destination URL Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

[Hide Advanced Settings](#)

Response ?

Assertion Signature ?

Signature Algorithm ?

Digest Algorithm ?

Assertion Encryption ?

Encryption Algorithm ?

Key Transport Algorithm ?

Encryption Certificate ?

Enable Single Logout ?

 Allow application to initiate Single Logout

Assertion Inline Hook

Authentication context class ?

Honor Force Authentication ?

<input type="checkbox"/>	<input type="text" value="Yes"/>
SAML Issuer ID ?	<input type="text" value="http://www.okta.com/\${org.externalKey}"/>

4. Set attribute statements.

Minimum requirements for SAML Assertion:

- **Email Address**
- **Display Name**
- **Unique user identifier** This should never change for a user (e.g., Okta offers an "employee number" field, but you need to populate this for every user—it cannot be empty).

Attribute Statements (optional) [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text" value="email"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.email"/> ▼
<input type="text" value="login"/>	<input type="text" value="Unspecified"/> ▼	<input type="text" value="user.login"/> ▼ ✕
<input type="text" value="displayName"/>	<input type="text" value="Unspecified"/> ▼	<input +="" \"="" type="text" user.lastname"="" value="user.firstName + \"/> ▼ ✕

[Add Another](#)

5. Finish Okta setup.

- Select **I'm an Okta customer adding an internal app.**
- For **App type**, check **This is an internal app that we have created.**

Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

I'm an Okta customer adding an internal app

I'm a software vendor. I'd like to integrate my app with Okta

The optional questions below assist Okta Support in understanding your app integration.

App type 

This is an internal app that we have created

[Previous](#) [Finish](#)

Why are you...
This form pro...
useful backgr...
your app. Tha...
appreciate it.

Configure SOE SAML settings

1. After you save the application, click the **Sign On** tab.
2. Click **View Setup Instructions** and open the link in a new browser window or tab. This page shows setup and configuration documentation, as well as the URLs you'll need to continue the setup.



Stack Overflow for Teams

Active ▾



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

[General](#)

[Sign On](#)

[Mobile](#)

[Import](#)

[Assignments](#)

Settings

[Edit](#)

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

Default Relay State



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.

Credentials Details

1 Identity Provider Single Sign-On URL:

https://dev-95766977.okta.com/app/ [REDACTED]

2 Identity Provider Issuer:

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

3 X.509 Certificate:

```

-----BEGIN CERTIFICATE-----
[REDACTED]
-----END CERTIFICATE-----

```

[Download certificate](#)

3. Add the following values to your SOE authentication settings.

- **Identity Provider Single Sign-On URL** Copy this value to the SOE **Single Sign-On Service URL** field.
- **Identity Provider Issuer** Copy this value to the SOE **Issuer** field.
- **Audience Restriction** Enter the example value provided on SOE authentication settings.
- **User Identifier Assertion** The value used on Okta for this (for example: login, UID, etc.).
- **Display Name Assertion** Set to **displayName**.
- **Email Address Assertion** Set to **email**.
- **X.509 Certificate** Copy this value to the SOE **Identity Provider Certificate** field.

4. Set **Use Subject/NameID as User Identifier** field.

Use Subject/NameID as user identifier is checked by default, which allows the IdP to specify the user identifier based on your SAML app configuration. This is the recommended setting.

Use Subject/NameID as user identifier

If not checked, please enter a User Identifier below. If checked, the User Identifier Assertion will be used. Please make sure to use a stable identifier (e.g., Persistent) that doesn't change (e.g., don't use Transient)

If you uncheck this option, you can manually specify a **User identifier assertion** of your choice. Be sure to choose a user identifier that will never change (for example: login or user ID). Email address is *not* a good choice for user identifier, as email addresses can change.

5. Validate your certificate by clicking **Validate Certificate**. You should see a green box with a success message. If you don't, make sure you copied and pasted the full text of the certificate.

```
Issuer: E=info@okta.com, CN=dev-95766977, OU=SSOProvider, O=Okta, L=San Francisco, S=California, C=US
Subject: E=info@okta.com, CN=dev-95766977, OU=SSOProvider, O=Okta, L=San Francisco, S=California, C=US
Valid: Jun 10 2021 to Jun 10 2031
Thumbprint: 15537D5D50D7C762B187129AE38ECB122878E9F3
SignatureAlgorithm: sha256RSA
```

[Validate Certificate](#) [Remove Certificate](#)

[Add another Certificate](#)

Save and test SOE SAML settings

To complete the SSO setup, click **Save Settings**.

When saving settings, SOE will first perform an authentication test. If the test succeeds, SOE will apply your new authentication settings. Logged-in users stay logged in, as all active user sessions remain valid.

If the test fails, SOE will not apply the authentication settings. You'll stay on the SAML settings page so you can troubleshoot and correct problems.

This test acts as a safety net to keep invalid authentication settings from locking users (yourself included) out of your site. If you do find your users locked out of your site, reach out to Stack Overflow product support for help.

You can also click **Test currently saved SAML configuration** to display technical details about your SAML authentication. You'll find these helpful for understanding what information your IdP and SOE exchange. This is also useful when troubleshooting.

[Save settings](#)

Additional links

[Test currently saved SAML configuration](#)

- [Set up additional Access Rules](#)
- [Download SAML 2.0 EntityDescriptor that can be imported into Identity Provider \(IdP\)](#)
- [Parse SAML 2.0 EntityDescriptor from Identity Provider \(IdP\)](#)

If you can't resolve the authentication errors, [reach out](#) to Stack Overflow support for help.