

## Configure Single Sign-on (SSO) with Okta (preview)

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

Document generated 08/08/2025

[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.

**NOTE:** To configure SSO with Okta, you'll need administrator access to both Okta and SOE.

There are two ways to configure Okta for SSO authentication for your SOE site. We recommend using the Okta app integration method as described below, unless:

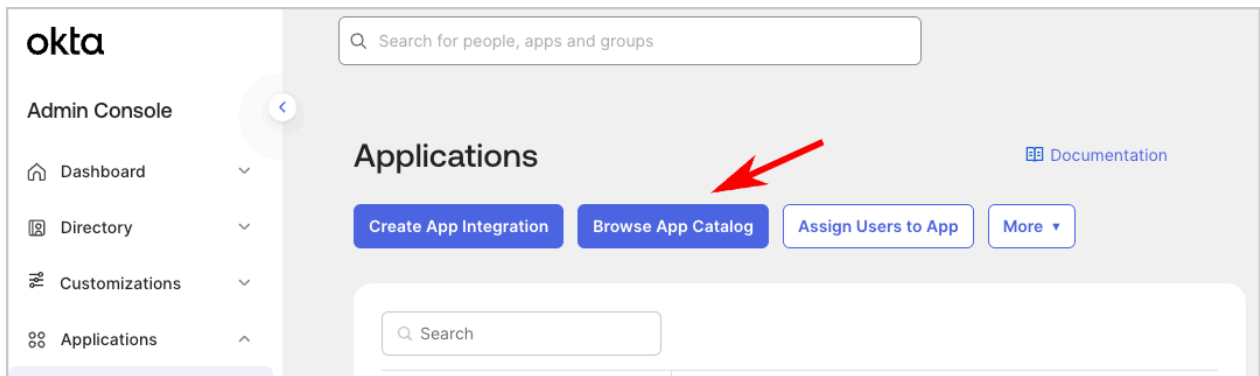
- You can't (or choose not to) access the Okta App Integration Catalog, or
- You need to add the user's job title and/or department SAML attributes

If either of these applies, skip down to the "[ALTERNATE MANUAL CONFIGURATION METHOD](#)" section.

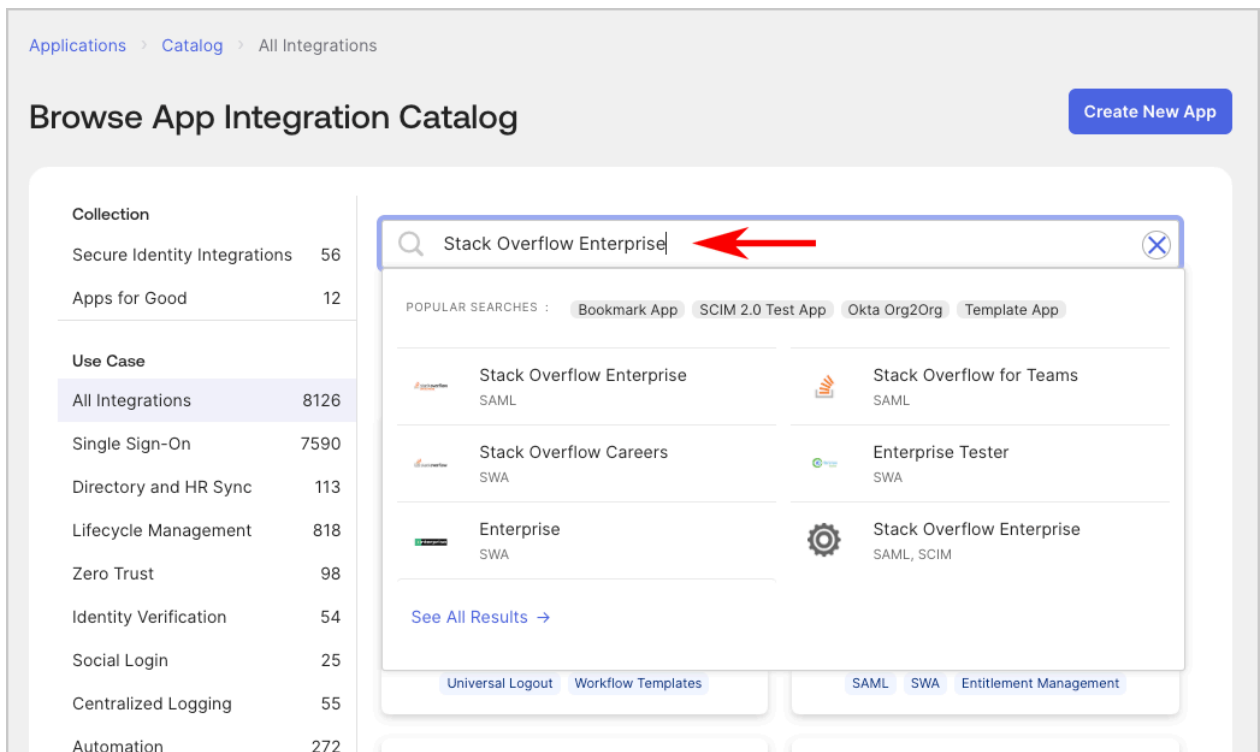
## OKTA APP INTEGRATION METHOD

### Install the SOE SAML application for Okta

1. In Okta, click **Applications**, then **Browse App Catalog**.









2. Search for "Stack Overflow Enterprise".



3. On the "General Settings" tab, enter an **Application label** (we suggest "Stack Overflow Enterprise"). Enter your SOE site's full URL in the Okta **subdomain** field. Click **Done**.



## Metadata details

Metadata URL	<a href="https://dev-21852446.okta.com/app/exkp06hkgb009V4pk5d7/sso/saml/metadata">https://dev-21852446.okta.com/app/exkp06hkgb009V4pk5d7/sso/saml/metadata</a>  <a href="#">Copy</a>
▼ Hide details	
Sign on URL	<a href="https://dev-21852446.okta.com/app/dev-21852446_stackoverflowforteams_1/exkp06hkgb009V4pk5d7/sso/saml">https://dev-21852446.okta.com/app/dev-21852446_stackoverflowforteams_1/exkp06hkgb009V4pk5d7/sso/saml</a>  <a href="#">Copy</a>
Sign out URL	<a href="https://dev-21852446.okta.com">https://dev-21852446.okta.com</a>  <a href="#">Copy</a>
Issuer	<a href="http://www.okta.com/exkp06hkgb009V4pk5d7">http://www.okta.com/exkp06hkgb009V4pk5d7</a>  <a href="#">Copy</a>
Signing Certificate	<div> <a href="#">Download</a></div> <div> <a href="#">Copy</a></div>

2. In a new browser tab, log in to your SOE instance as an administrator. In the left-hand menu, click **Admin settings**, then **Authentication**. Click **Use SAML 2.0** (if not already enabled).
3. On Okta's "Sign On" tab, use the **Copy** links to add the following values to your SOE settings. If you see a setting that's not listed here, leave it unchanged.
  - **Assertion consumer service URL** Enter the SAML 2.0 post URL of your SOE site ([https://\[your\\_site\].stackenterprise.co/auth/saml2/post](https://[your_site].stackenterprise.co/auth/saml2/post)).
  - **Single sign-on service URL** Copy the **Sign On URL** value from Okta and paste it here.
  - **Issuer** Copy the **Issuer** value from Okta and paste it here.
  - **Audience restriction** Enter the SAML 2.0 post URL of your SOE site (same as above: [https://\[your\\_site\].stackenterprise.co/auth/saml2/post](https://[your_site].stackenterprise.co/auth/saml2/post)).
  - **Use Subject/NameID as the user identifier** Enable this checkbox.
  - Fill in the **Name** value from the Okta "Attribute Statements" tab for each of the following:
    - **Display name assertion** displayName
    - **Email address assertion** email
  - **Identity provider certificates** Click the Okta **Signing Certificate Copy** link, and paste the results here.

Validate your certificate by clicking **Validate Certificate**. If your certificate passes verification, you'll see a green box with a success message.

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: 15537D5D50D7C762B187129AE3BECB122878E9F3  
SignatureAlgorithm: sha256RSA

Validate Certificate

Remove Certificate

Add another Certificate

## Assign users to the Okta application

On the Okta "Assignments" tab, assign your users (and/or groups) with the **Assign** button.

**NOTE:** You can't test your SSO configuration until you've assigned users.

GeneralSign OnProvisioningImportAssignments

Assign ▼Convert assignments ▼

Search...People ▼

Filters

PeopleGroups

Person	Type
	01101110
	01101111
	01101100
	01101100
	01101101
	01101110
	01100111

No users found

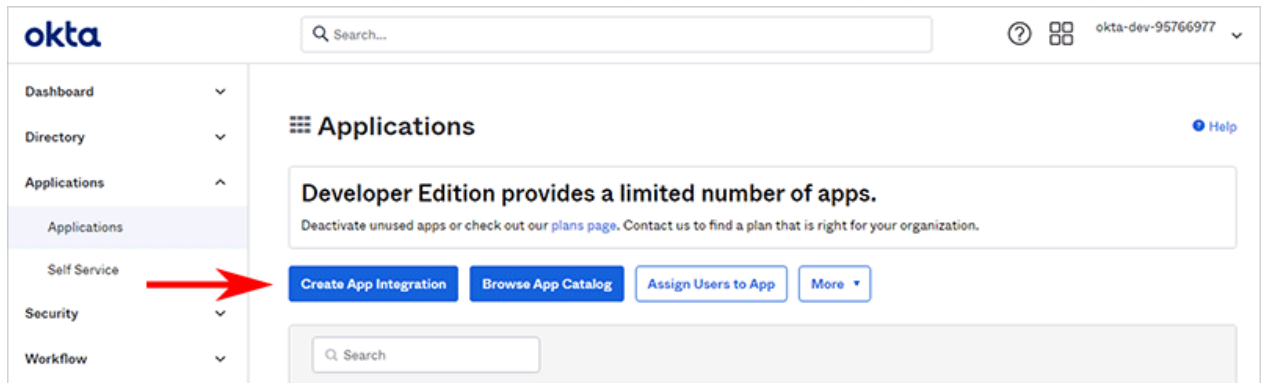
This completes the main Okta application configuration. Jump down to the "[Save and test SOE SAML settings](#)" section below to save and verify your settings.

## ALTERNATE MANUAL CONFIGURATION METHOD

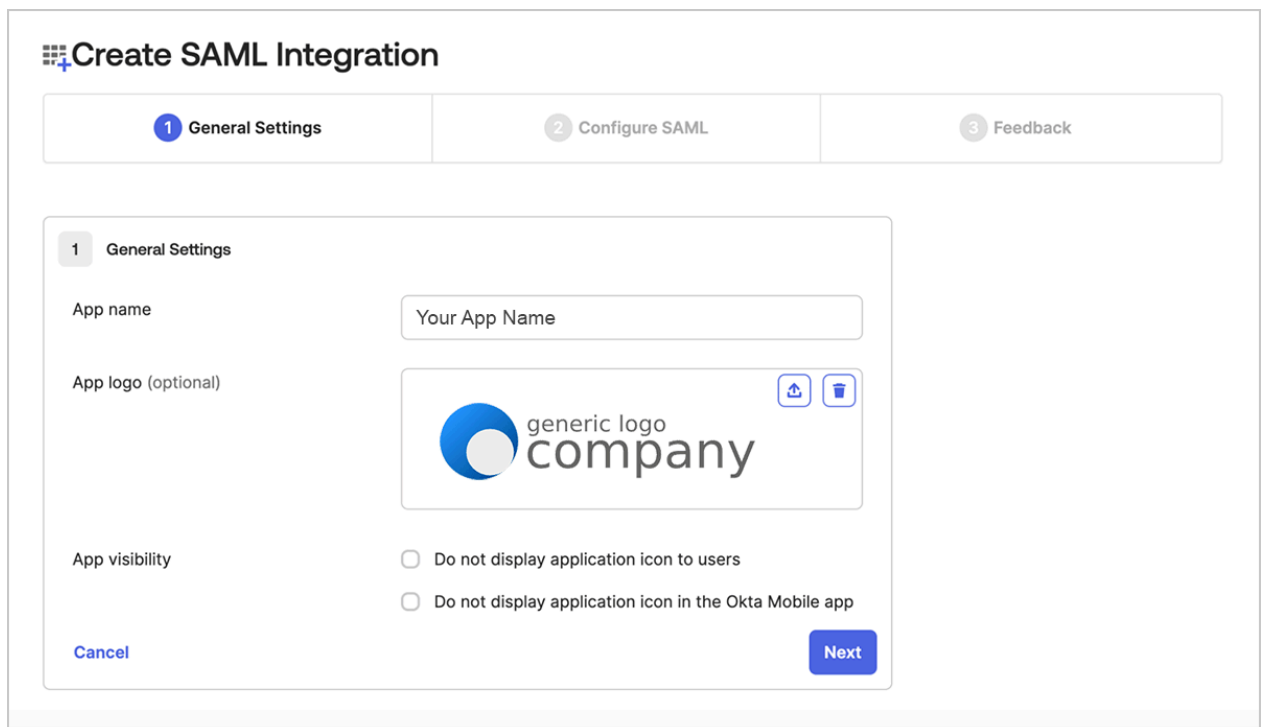
**NOTE:** The following steps allow for manual configuration of Okta SSO. Use this process if you can't (or choose not to) access the Okta App Integration Catalog, or need to add the user job title and department data fields.

## Create a new Okta SAML application

1. In Okta, click **Applications**, then **Create App Integration**.



2. Choose **SAML 2.0** as **Sign-on method**.
3. On the "General Settings" tab, enter an **App name**. If desired, upload an **App logo**.



## Configure Okta SAML settings

On the "Configure SAML" tab, configure the following fields:

- **Single sign-on URL** Enter your SOE SAML URL ([https://\[your\\_site\].stackenterprise.co/auth/saml2/post](https://[your_site].stackenterprise.co/auth/saml2/post)).
- **Audience URI (SP Entity ID)** Enter any unique value. We suggest using your SOE SAML URL (same as above: [https://\[your\\_site\].stackenterprise.co/auth/saml2/post](https://[your_site].stackenterprise.co/auth/saml2/post)).
- **Default Relay State** Leave blank.

- **Name ID format** Select **Unspecified**.
- **Application username** This field identifies the user record, so set this to a user attribute that is unique and will never change (for example: **Okta username**).

**NOTE:** It's important to select an **Application username** source field that is both unique and unchanging. A user's email address, for example, is unique but not unchanging (an updated email address would result in SOE creating a new, duplicated account for that user).

A
SAML Settings

General

Single sign-on URL ?

https://[your\_site].stackenterprise.co/auth/saml2/post

☒ Use this for Recipient URL and Destination URL

Audience URI (SP Entity ID) ?

https://[your\_site].stackenterprise.co/auth/saml2/post

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Unspecified

Application username ?

Okta username

Update application username on

Create and update

[Show Advanced Settings](#)

## Set attribute statements

Attributes are user information values passed from Okta to SOE as part of the login process. You'll need to define at least two SAML attributes: user email and name. This involves giving each attribute a name (which you'll later enter into SOE) and choosing which Okta values to attach to each attribute.

Define the SAML attributes **Name** and **Value** as follows:

- **email** The user's email address. Set **Value** to **user.email**.
- **displayName** The user's name as it should appear in SOE. If you have a custom Okta field with the full user name, set **Value** to that field. You can also concatenate fields with the "+" operator (for example: **user.firstName + " " +**

`user.lastName`).

You can also define optional user job title and department attributes. Populating and sending these attributes on login allows you to use SOE's [Connectivity](#) feature.

- **jobTitle** (optional) The user's job title. Set **Value** to `user.jobtitle`.
- **department** (optional) The user's department. Set **Value** to `user.department`.

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

Name	Name format (optional)	Value	
email	Unspecified ▼	user.email	▼
displayName	Unspecified ▼	user.firstName + " " + user.lastName	▼ ✕
jobTitle	Unspecified ▼	user.jobTitle	▼ ✕
department	Unspecified ▼	user.department	▼ ✕

Add Another

After configuring attributes, click **Next**.

## BOTH METHODS: Save and test SOE SAML settings

To complete the SSO setup, click **Save Settings** on the SOE authentication settings page.



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 \(IdP\)](#)

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.

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.

Properly configuring SAML authentication can be tricky. For more information on troubleshooting, see the [SAML Authentication Troubleshooting](#) article. You can also [reach out](#) to Stack Overflow support for help.