Configure Single Sign-on (SSO) with Okta

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

Document generated 08/18/2025

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

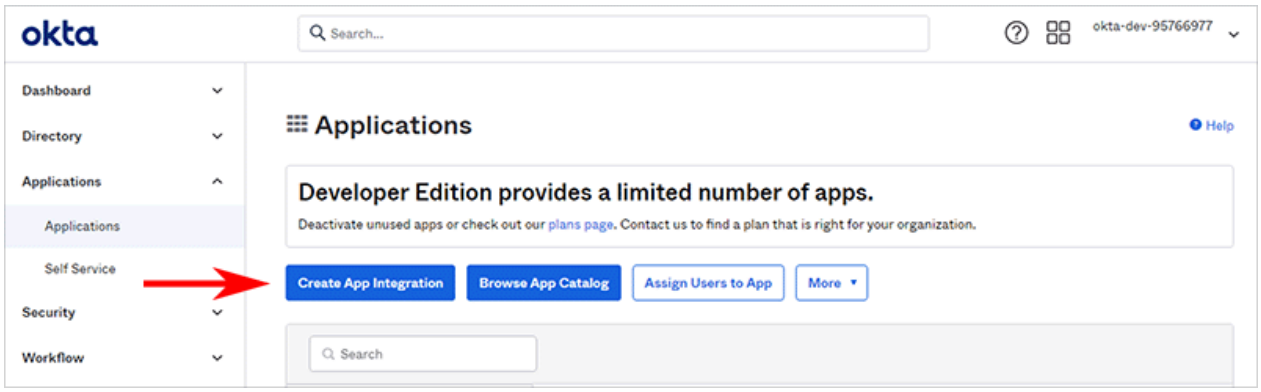
These instructions describe how to integrate your Stack Overflow for Teams Enterprise (SOE) site with Okta as your Identity Provider (IdP) for authentication. Once configured, your users will be able to use Okta and the Security Assertion Markup Language (SAML) for Single Sign-on (SSO) authentication 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.

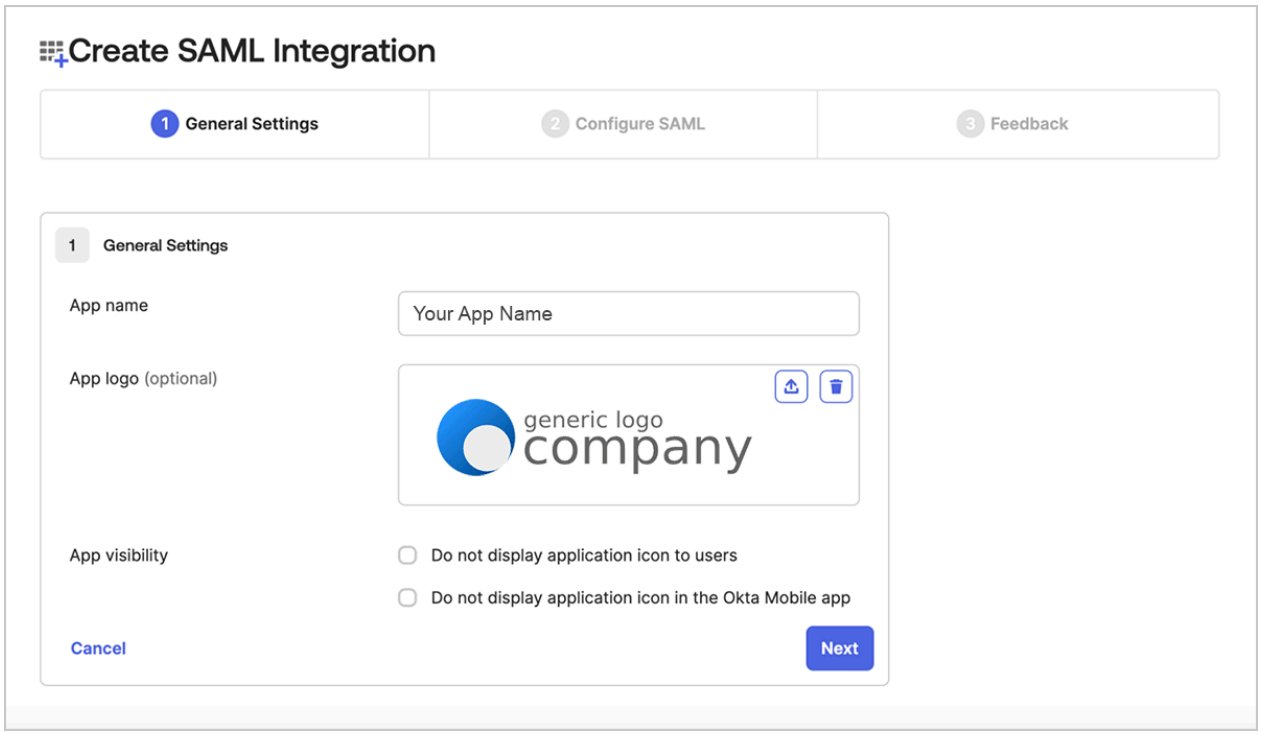
THIS ARTICLE APPLIES TO STACK OVERFLOW FOR TEAMS ENTERPRISE ONLY.
Other Stack Overflow for Teams users should read this article instead. Find your plan.
***NOTE:** To configure SSO with Okta, you'll need administrator access to both Okta and SOE.*

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**.

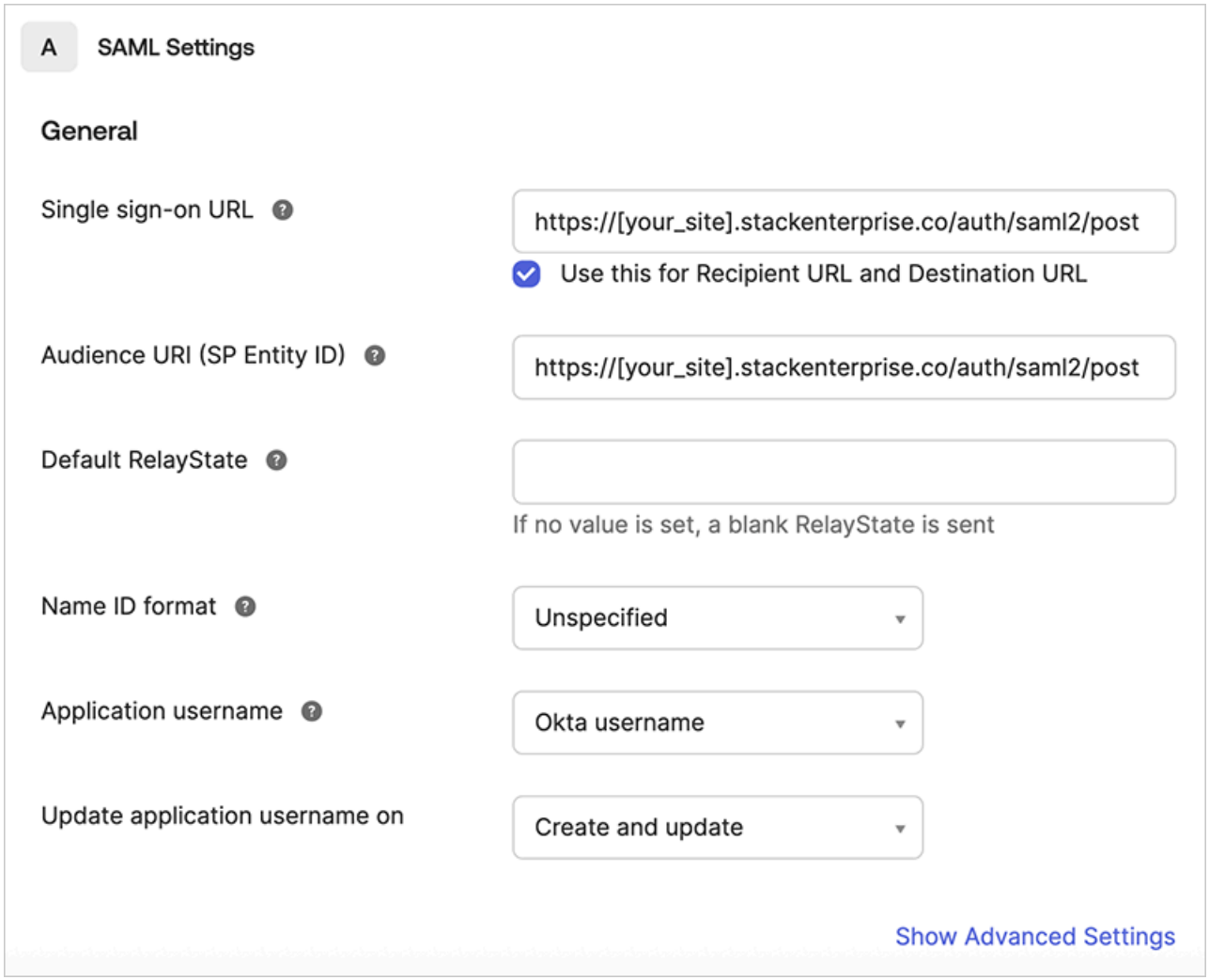


Configure Okta SAML settings

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**).
- **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**).
- **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).*



Set attribute statements

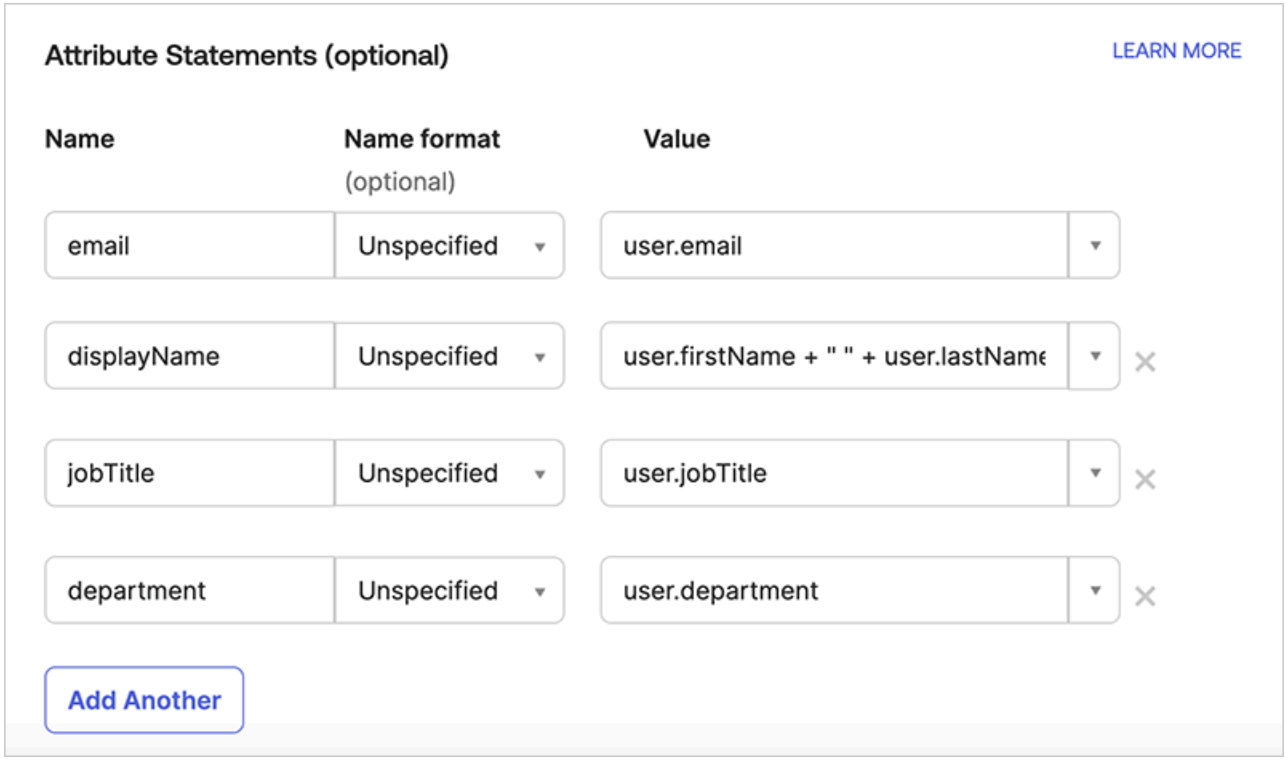
Attributes are user information values passed from Okta to SOE as part of the login process. You'll need to define at least two SAML attributes: user email and name. This involves giving each attribute a name (which you'll later enter into SOE) and choosing which Okta values to attach to each attribute.

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.

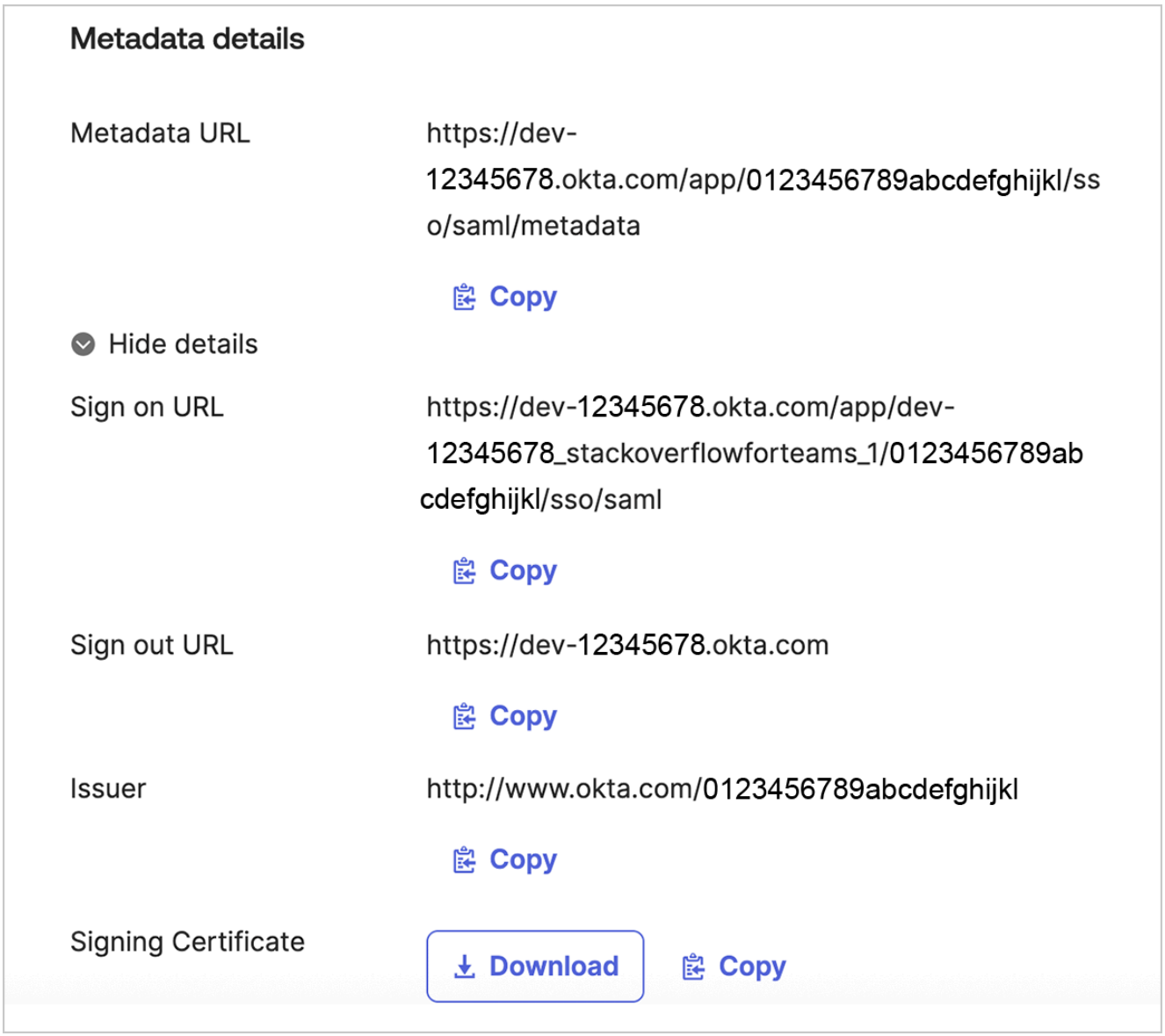
- **jobTitle** (optional) The user's job title. Set **Value** to **user.jobtitle**.
- **department** (optional) The user's department. Set **Value** to **user.department**.



After configuring attributes, click **Next**.

Check **This is an internal app that we have created**, then click **Finish**.

Navigate to the "Sign On" tab. Under the "Metadata details" heading, click **More details**. You're now ready to configure SOE.



Configure SOE SAML settings

Open a new tab in your browser and log in to SOE as an administrator. Click **Admin settings** in the left-hand menu, then **Authentication**. Click **Use SAML 2.0** (if not already enabled).

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**).
- **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** Copy the **Audience URI (SP Entity ID)** value from Okta and paste it here.
- **Use Subject/NameID as user identifier** Enable this checkbox.

- Fill in the **Name** value from the Okta "Attribute Statements" tab for each of the following:
  - **Display name**
  - **Job Title**
  - **Department**
  - **External ID**
- **Identity provider certificates** Click the **Signing Certificate**'s **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.

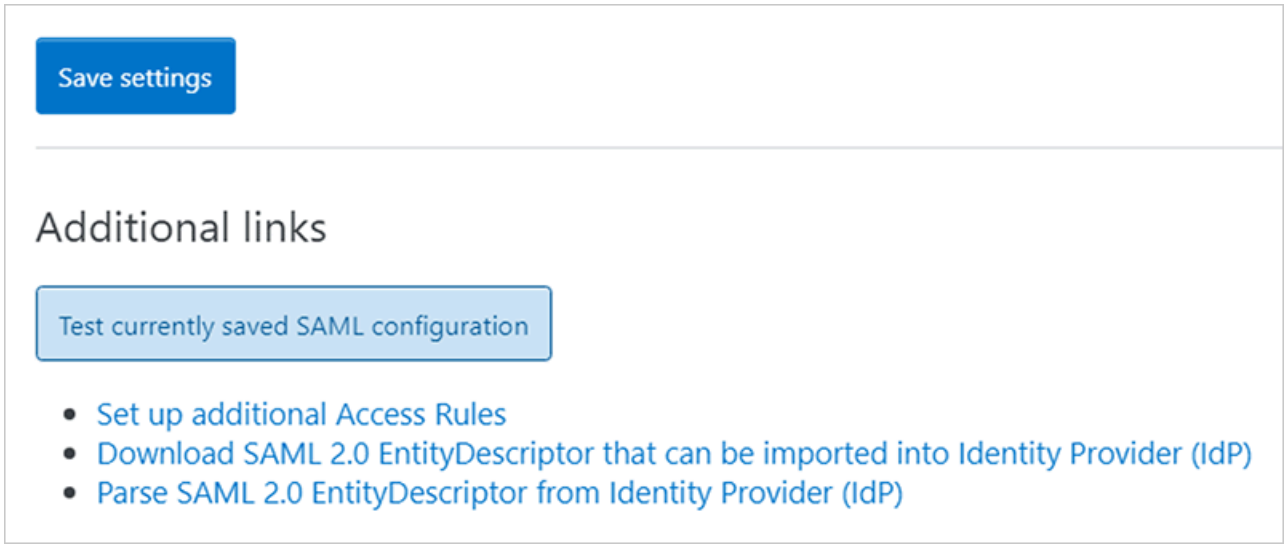
Save and test SOE SAML settings

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.

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.