

PRE-RELEASE Configure Single Sign-on (SSO) with Okta

Set up Stack Internal Enterprise for SAML authentication with Okta.

Document generated 11/21/2025

[PDF VERSION](#)

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

Applies to:

Free

Basic

Business

Enterprise

ADMIN PRIVILEGES REQUIRED

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

NOTE: This document is in pre-release, and should not be used for SSO setup. Follow the instructions in the [Configure Single Sign-on \(SSO\) with Okta](#) article instead.

Overview

These instructions describe how to integrate your Stack Internal Enterprise site with Okta as your identity provider 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.

NOTE: In SSO terminology, Okta is the identity provider (IdP) and your Stack Internal Enterprise site is the service provider (SP). We'll use the terms IdP and SP throughout this article.

Stack Internal Enterprise supports the following features with Okta:

- IdP-initiated SSO
- SP-initiated SSO
- Just-in-time provisioning
- Force authentication

When setting up SAML authentication, you'll configure your Stack Internal Enterprise 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 Stack Internal Enterprise.

There are two ways to configure Okta for SSO authentication for your Stack Internal Enterprise 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

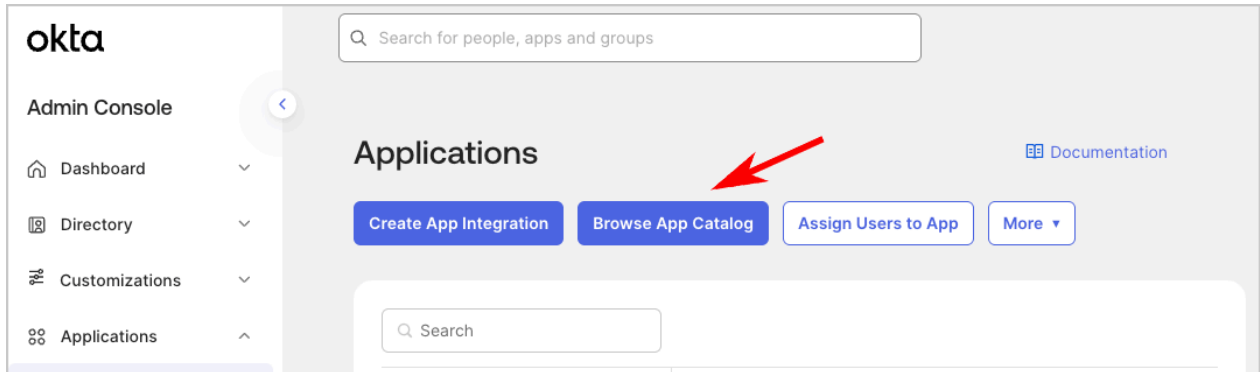
- You need to add the user's job title and/or department SAML attributes

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

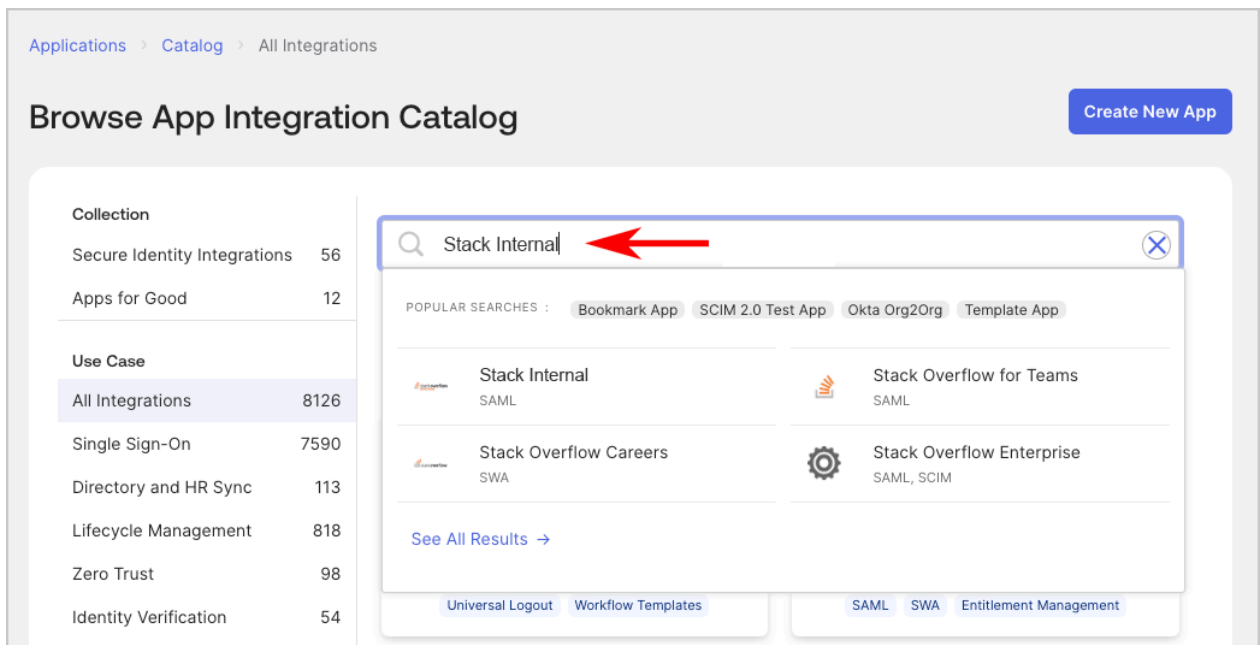
OKTA APP INTEGRATION METHOD

Install the Stack Internal Enterprise SAML application for Okta

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



2. Search for "Stack Internal".

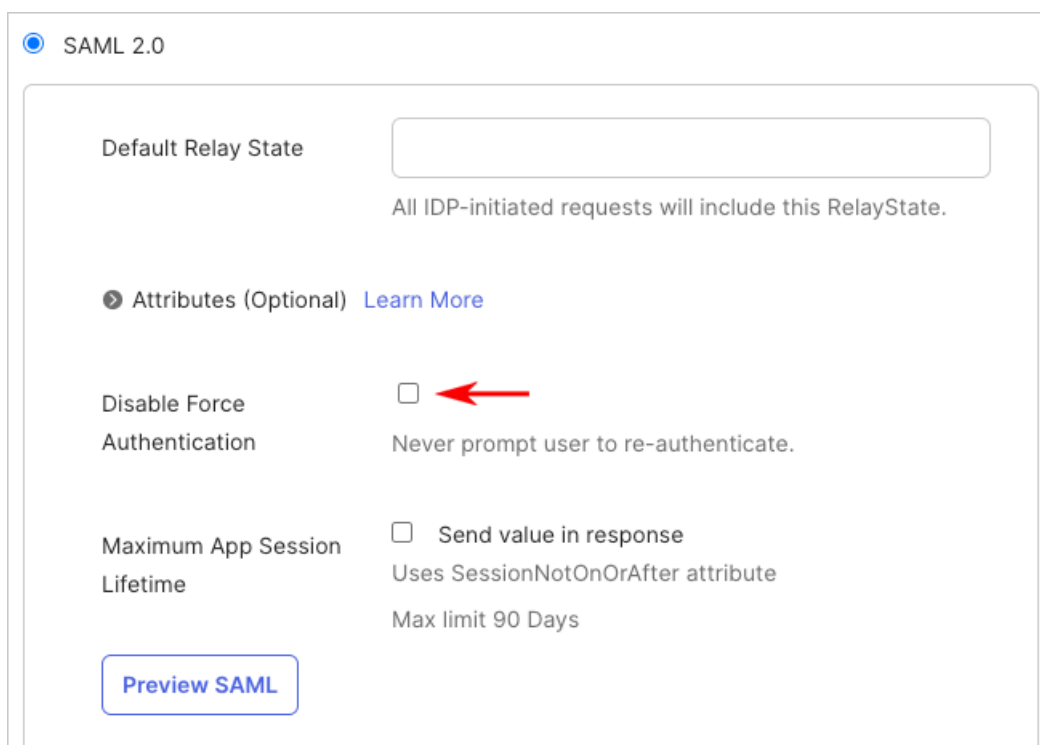


3. On the "General Settings" tab, enter an **Application label** (we suggest "Stack Internal"). Enter your Stack Internal Enterprise site's full URL in the Okta **subdomain** field. Click **Done**.

You can force your users to sign in with SSO every time they log in by telling Stack Internal Enterprise to ignore previous user authentication sessions. To do this, you'll need to change configuration settings in both Okta and Stack Internal Enterprise.

In the Stack Internal Enterprise Application in Okta:


1. Go to the "Sign On" tab.
2. Click **Edit Settings**.
3. Uncheck the **Disable Force Authentication** option.



☒ SAML 2.0

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

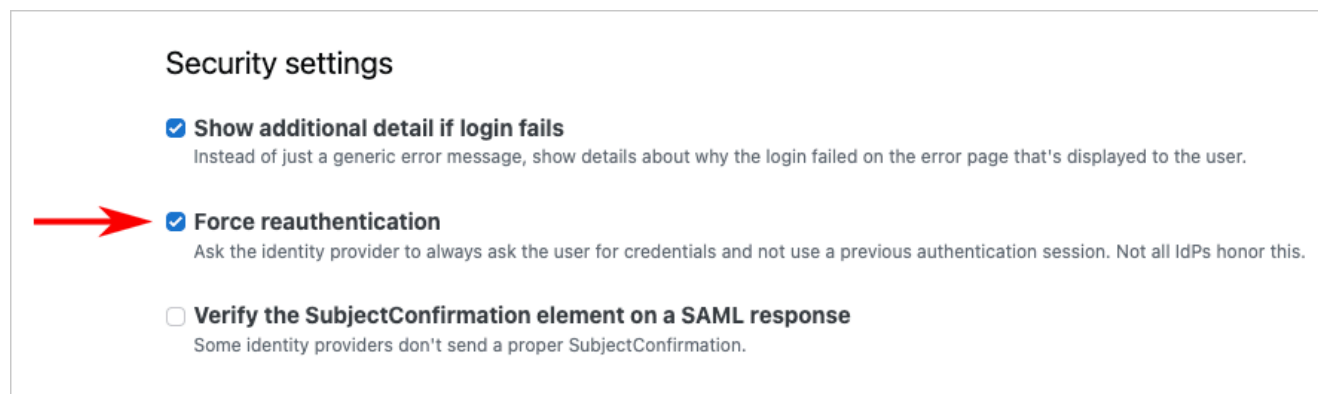
Attributes (Optional) [Learn More](#)

Disable Force Authentication ☐ 
Never prompt user to re-authenticate.

Maximum App Session Lifetime ☐ Send value in response
Uses SessionNotOnOrAfter attribute
Max limit 90 Days


[Preview SAML](#)

4. Go to the Stack Internal Enterprise admin settings "Authentication" menu.
5. Under "Security settings", check **Force reauthentication**.



Security settings

☒ **Show additional detail if login fails**
Instead of just a generic error message, show details about why the login failed on the error page that's displayed to the user.

 ☒ **Force reauthentication**
Ask the identity provider to always ask the user for credentials and not use a previous authentication session. Not all IdPs honor this.

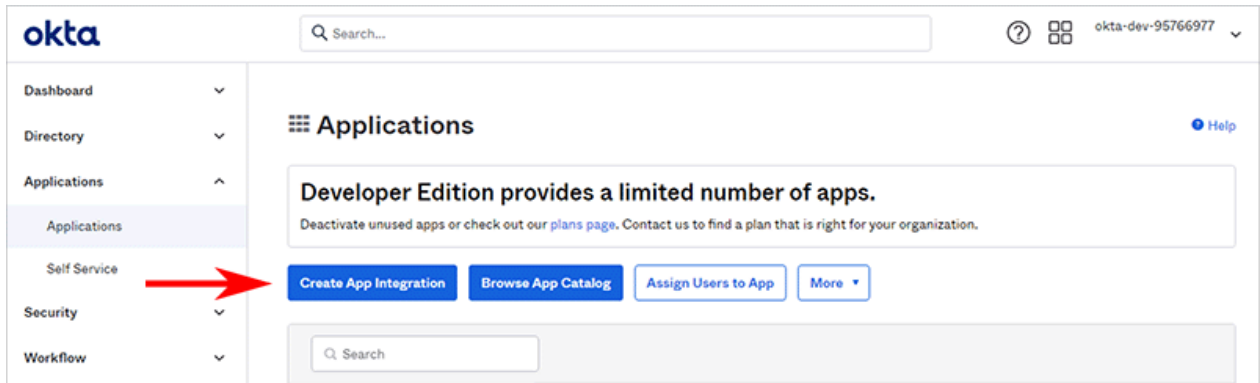
☐ **Verify the SubjectConfirmation element on a SAML response**
Some identity providers don't send a proper SubjectConfirmation.

ALTERNATE MANUAL CONFIGURATION METHOD

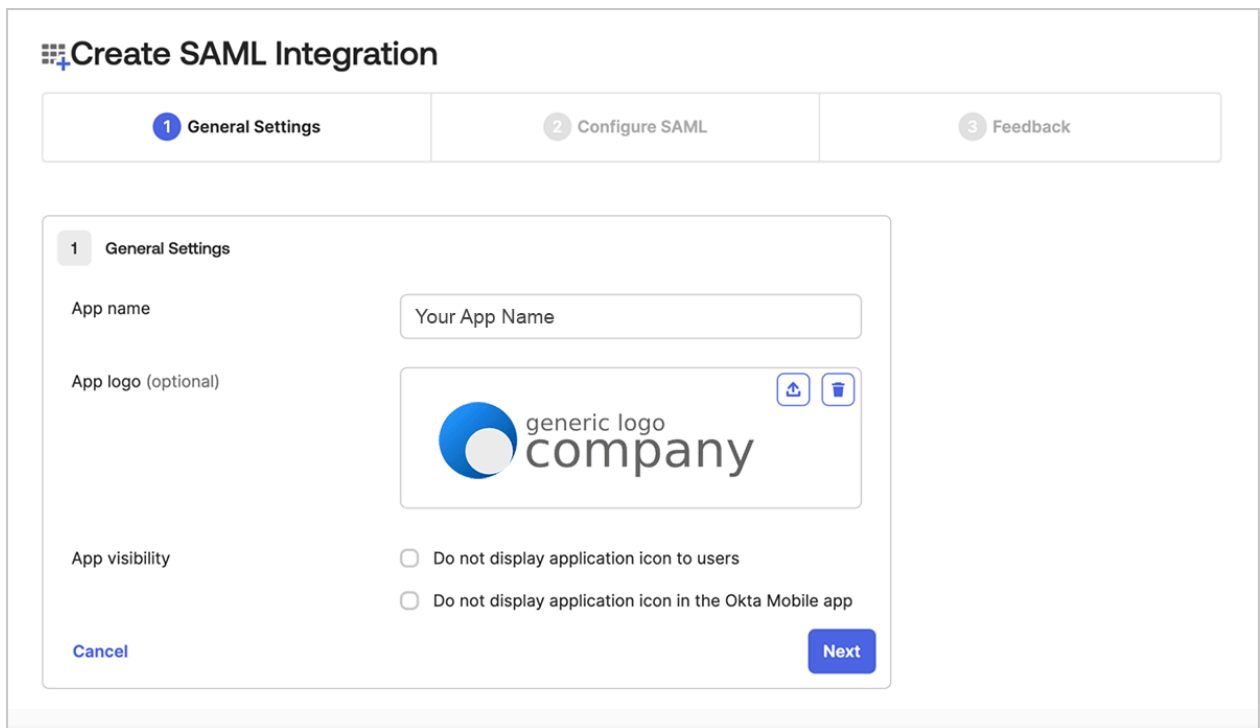
NOTE: The following steps allow for manual configuration of Okta SSO. Use this process if you can't (or choose not to) access the Okta App Integration Catalog, or need to add the user job title and department data fields.

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 Stack Internal Enterprise SAML URL (`https://[your_site].stackenterprise.co/auth/saml2/post`).
- **Audience URI (SP Entity ID)** Enter any unique value. We suggest using your Stack Internal Enterprise 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 Stack Internal Enterprise 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 Stack Internal Enterprise 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 Stack Internal Enterprise) 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 Stack Internal Enterprise. If you have a custom Okta field with the full user name, set **Value** to that field. You can also concatenate fields using the `${user.firstName} ${user.lastName}` formula.

You can also define optional user job title and department attributes. Populating and sending these attributes on login allows you to use Stack Internal Enterprise'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

A third optional attribute is external ID. You can set this to hold a unique ID for each user (for example: employee number). Stack Internal Enterprise will then display this ID on the user's profile page.

- **ExternalId** (optional) The user's unique ID. Set **Value** to **user.employeeNumber** (or any other unique user ID you defined in Okta).

After configuring attributes, click **Next**.

BOTH METHODS: Configure and test Stack Internal Enterprise SAML settings

1. Click to select the "Sign On" tab. Under the "Metadata details" heading, click **More details**. Keep this tab open for easy access to the metadata values.

Metadata details

Metadata URL <https://dev-12345678.okta.com/app/0123456789abcdefghijkl/sso/saml/metadata>

 [Copy](#)

▼ Hide details

Sign on URL https://dev-12345678.okta.com/app/dev-12345678_stackoverflowforteams_1/0123456789abcdefghijkl/sso/saml

 [Copy](#)

Sign out URL <https://dev-12345678.okta.com>

 [Copy](#)

Issuer <http://www.okta.com/0123456789abcdefghijkl>

 [Copy](#)

Signing Certificate

 [Download](#)

 [Copy](#)

2. In a new browser tab, log in to your Stack Internal Enterprise site 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 Stack Internal Enterprise 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 Stack Internal Enterprise 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 Stack Internal Enterprise 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

- **Job Title assertion** jobTitle (optional)
- **Department assertion** department (optional)
- **External ID** externalId (optional)
- **Identity provider certificates** Click **View SAML setup instructions** in the bottom right corner of the "Sign On" tab. Copy the entire value shown in the **X.509 Certificate** field and paste it 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: 15537D5D50D7C762B187129AE38ECB122878E9F3
 SignatureAlgorithm: sha256RSA

Validate Certificate
Remove Certificate

Add another Certificate

To complete the SSO setup, click **Save Settings** on the Stack Internal Enterprise 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, Stack Internal Enterprise will first perform an authentication test. If the test succeeds, Stack Internal Enterprise will apply your new authentication settings. Logged-in users stay logged in, as all active user sessions remain valid.

If the test fails, Stack Internal Enterprise 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 Stack Internal Enterprise exchange.

SP-initiated SSO

Once you've fully configured your Okta application, the user sign-in process will start with your Stack Internal Enterprise site and proceed as follows:

1. The user navigates to your Stack Internal Enterprise site ([https://\[your_site\].stackenterprise.co](https://[your_site].stackenterprise.co)), which initiates the sign-in process.
2. The Okta sign-in page appears, prompting the user to sign in with their Okta credentials.
3. If the user credentials are valid, Okta redirects the user to their home page on your Stack Internal Enterprise site.

Getting help

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.