



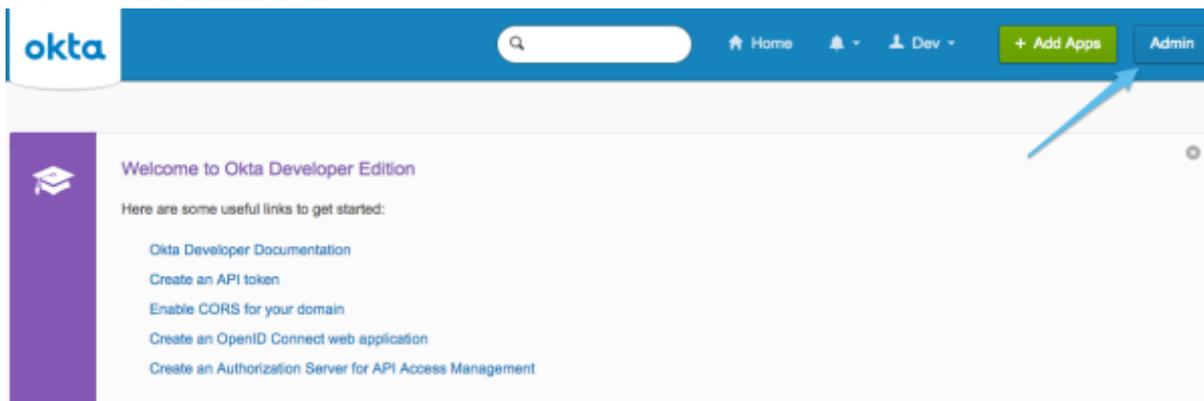
[In Okta](#)
[In Wepow](#)

The first step in configuring an application to support SAML based Single Sign-On from Okta is to set up an application in Okta.

In Okta

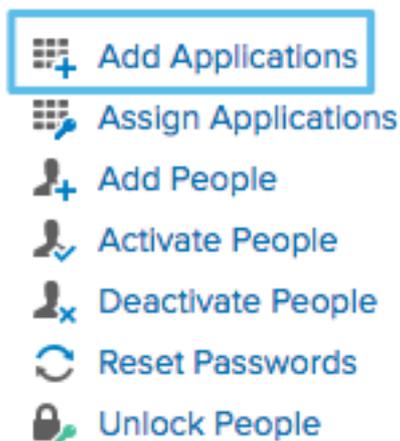
Here is how to set up a SAML application in Okta:

1. Click on the blue Admin button



2. Click on the Add Applications shortcut

Shortcuts



3. Click on the green Create New App button



Okta Dashboard Directory Applications Security Reports Settings My Applications

← Back to Applications

➕ Add Application

Q| All A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

<p>Can't find an app?</p> <p>Create New App</p> <p>Apps you created (0) →</p> <p>INTEGRATION PROPERTIES</p> <p>Any</p> <p>Supports SAML</p> <p>Supports Provisioning</p>	Teladoc Okta Verified	Add
	&frankly Okta Verified ✓ SAML	Add
	1000ft Okta Verified	Add
	101domains.com Okta Verified	Add

- In the dialog that opens, select the SAML 2.0 option, then click the green Create button

Create a New Application Integration

Platform: Web

Sign on method:

- Secure Web Authentication (SWA)
Users credentials to sign in. This integration works with most apps.
- SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

Create Cancel

- In Step 1 General Settings, enter Example SAML Application in the App name field, then click the green Next button.



1 General Settings

App name: Wepow

App logo (optional): [Upload Logo]

App visibility:

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

Cancel [Next]

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

6. In Step 2 Configure SAML, section A SAML Settings, create the Single sign on URL <https://wepowsubdomain.wepowapp.com/sso/saml/consume> For the recipient, destination URLs use <https://wepowapp.com>. For "Audience URI" wepowapp.com. Select "Name ID format" and set to "EmailAddress" and "Application username" set to "Email"

A SAML Settings

GENERAL

Single sign on URL: <https://okta.wepowapp.com/sso/saml/consume>

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Recipient URL: <https://wepowapp.com>

Destination URL: <https://wepowapp.com>

Audience URI (SP Entity ID): wepowapp.com

Default RelayState: [Empty]

If no value is set, a blank RelayState is sent

Name ID format: EmailAddress

Application username: Email

Show Advanced Settings

What does this form do?
This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?
The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate
Import the Okta certificate to your Identity Provider if required.

Download Okta Certificate

Select "Name ID format" and set to "EmailAddress" and "Application username" set to "Email"

7. In the Attribute Statements section, add three attribute statements:
1. FirstName set to user.firstName
 2. LastName set to user.lastName



3. Email set to user.email
4. "is_owner" set to isMemberOfGroupName("WepowOwner") ? "true" : "false"
5. "wepow_team_1" set to "isMemberOfGroupName("Engineering") ? "Engineering" : null"
6. "wepow_role_1" set to "isMemberOfGroupName("Engineering") ? "admin" : null"

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
first_name	Unspecified	user.firstName	×
last_name	Unspecified	user.lastName	×
is_owner	Unspecified	isMemberOfGroupName("WepowOwner") ? "t	×
wepow_team_1	Unspecified	isMemberOfGroupName("Engineering") ? "En	×
wepow_role_1	Unspecified	isMemberOfGroupName("Engineering") ? "ad	×
Email	Unspecified	user.email	×

[Add Another](#)

Click Next to continue.

8. In Step 3 Feedback, select I'm an Okta customer adding an internal app, and This is an internal app that we have created, then click Finish.

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

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

App type **3**

This is an internal app that we have created

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

Why are you asking me this?
This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.



- The Sign On section of your newly created Example SAML Application application appears. Keep this page open in a separate tab or browser window. You will return to this page later in this guide and copy the Identity Provider metadata link.

(To copy that link, right-click on the Identity Provider metadata link and select Copy)

General **Sign On** 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.

SAML 2.0

Default Relay State

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

View Setup Instructions

[Identity Provider metadata](#) Copy this link ports dynamic configuration.

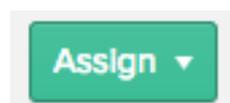
CREDENTIALS DETAILS

Application username format

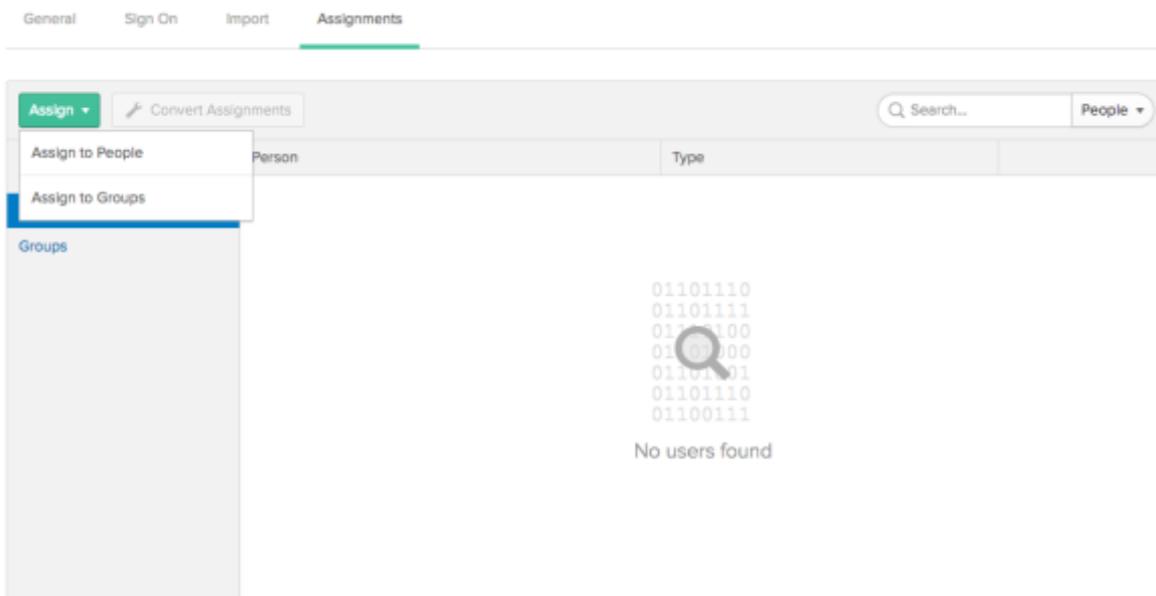
Password reveal Allow users to securely see their password (Recommended)

- Right-click on the Assign Application section and select Open Link In New Tab (so that you can come back to the Sign On section later).

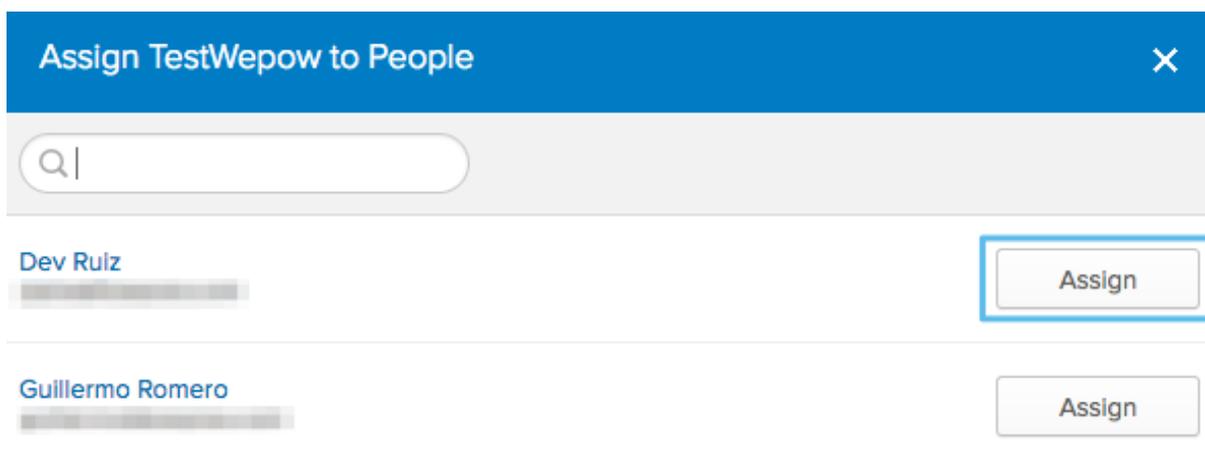
In the new tab that opens, click on the Assign button



- A dialog titled Assign to people will open. Type your username into the search box, select the checkbox next to your username, then click the green Next button



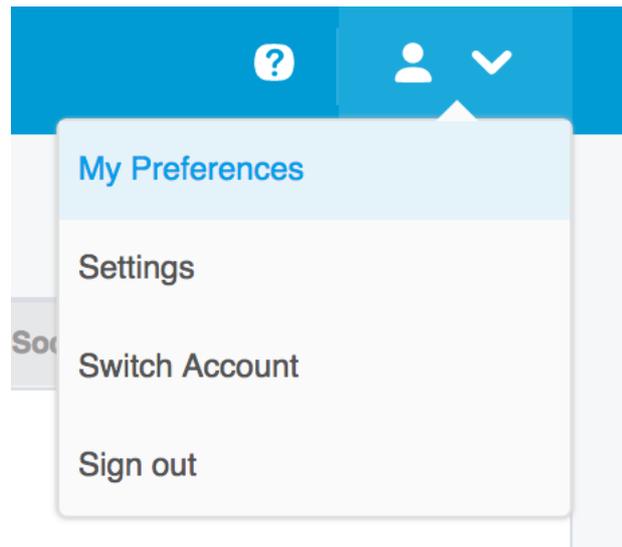
12. You will be prompted to Enter user-specific attributes. Just click the green Confirm Assignments button to keep the defaults.



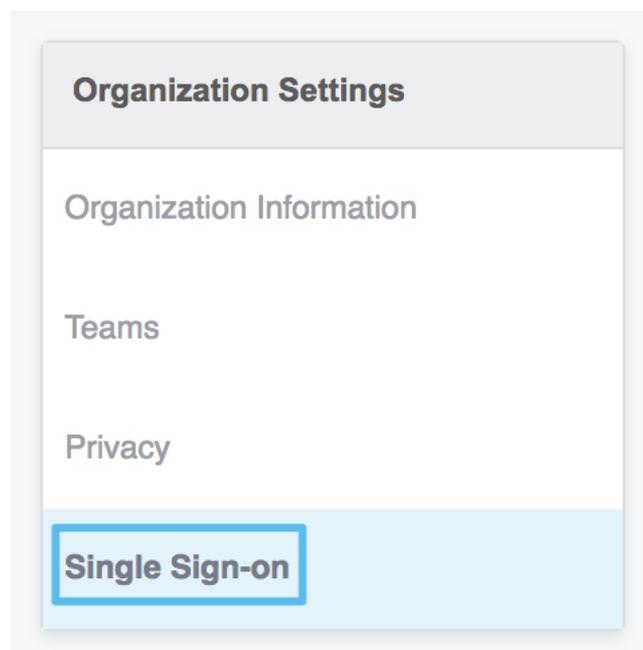
You are now ready to configure SAML in your application. The information in the tab you opened in step #9 contains the information that you™ll need to configure SAML in your application.

In Wepow

1. Enter to the Wepow App, and go to "My preferences"



2. From the section "Organization Settings" click on Single Sign-on



3. Select the option "SAML 2.0 and go back to Okta and pull the information from step #9.

