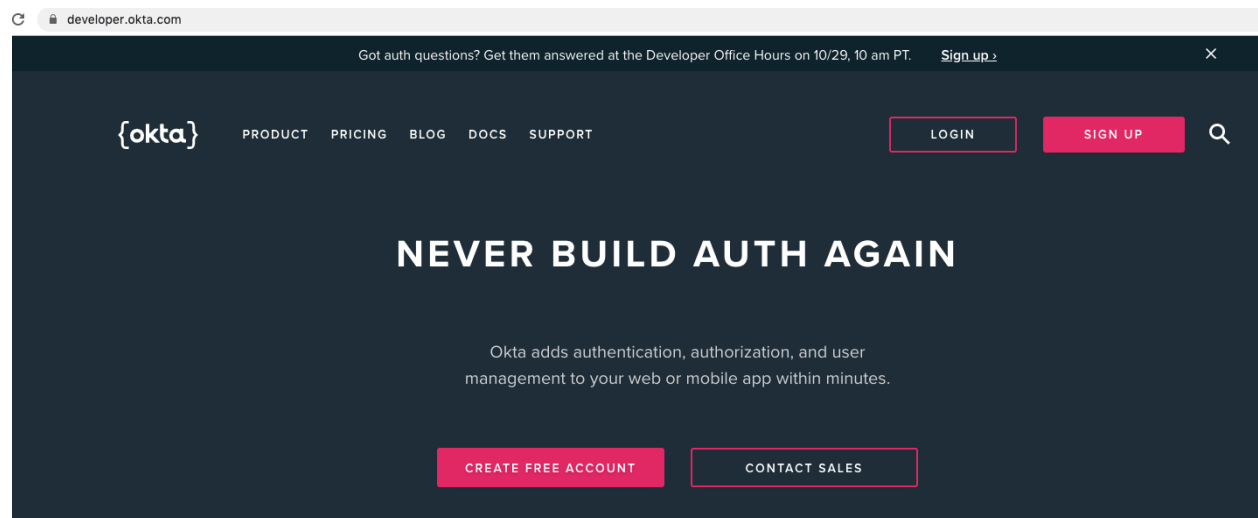


Create your Account with SSO Provider OKTA and create SSO Application for SAML in OKTA for SAML Integration

Setting up an SSO provider

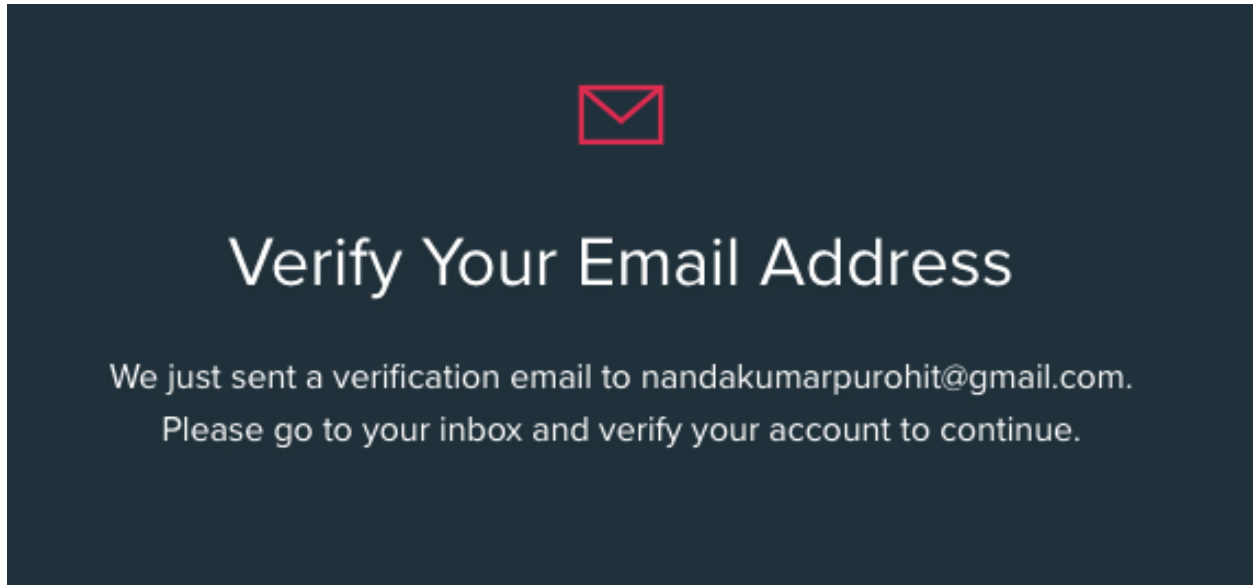
As detailed, we will be using Okta as our SSO provider to build our sample application, which covers Spring Security using SAML 2.0 as the authentication mechanism.

1. To set up an Okta user, perform the following steps:
Go to <https://developer.okta.com> and click on **SIGN UP**.



2. Enter the relevant details and click on **GET STARTED**. Okta will send you an email with your **Org Subdomain** and **Temporary Password**.

Click on the **ACTIVATE MY ACCOUNT** button in the email, enter your **Username** (email) and **Temporary Password**, and log in.



3. You will be presented with some more account-related information. Fill in the details and complete your account setup.

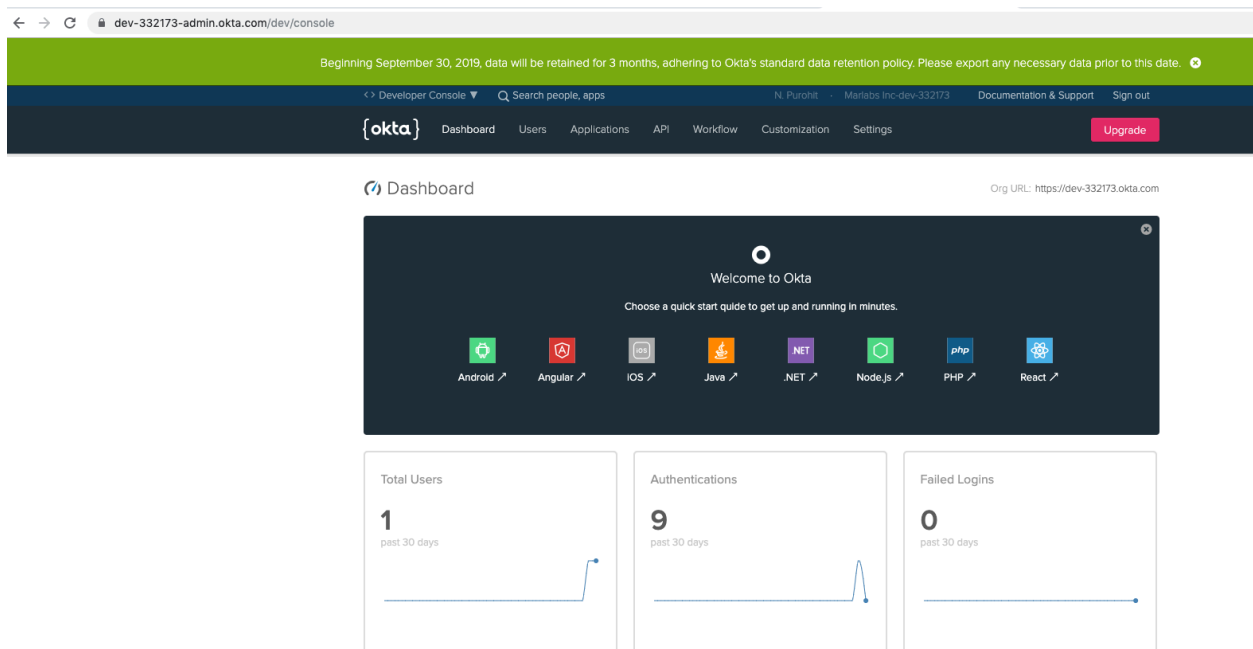
You now have an Okta account set up with one user (you) and no applications configured to do SSO.

Setting up an SSO Application in OKTA

4. Open your page in [**http://developer.okta.com**](http://developer.okta.com)

You will see this below page as a landing page

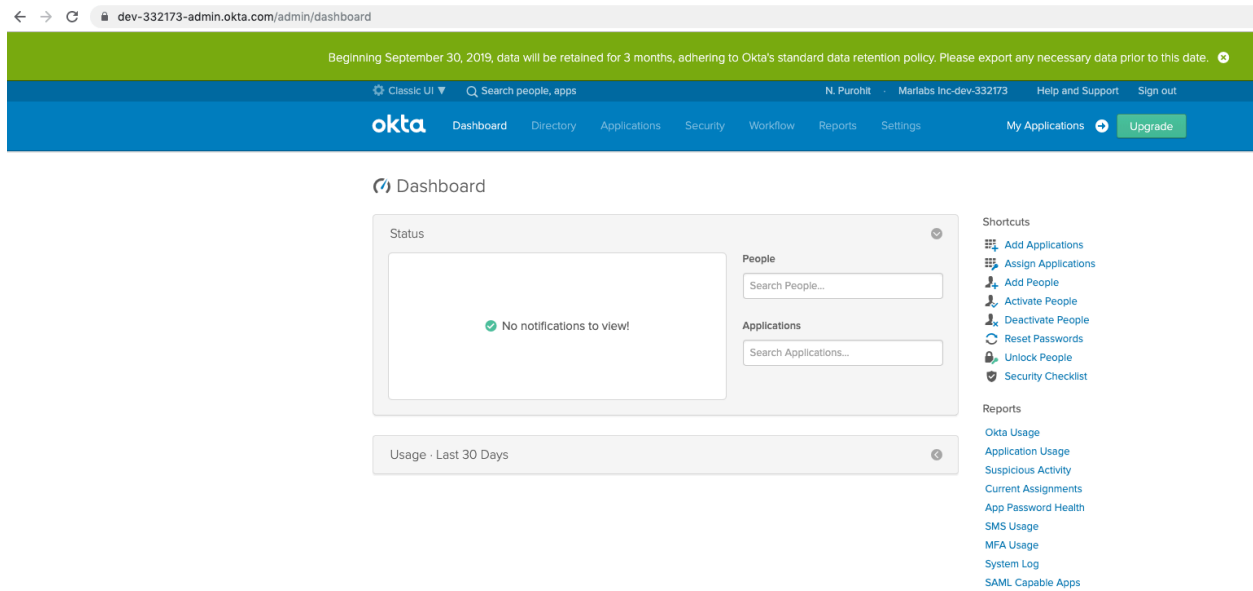
Note: If you do not see this page, then click on **Admin** button on Top Right and then you will see this page.



5. You must change the UI to **Classic UI** by hovering on the Menu **Developer Console** on Top left



6. Classic UI page looks like this



6. Click on the **Add Applications** under **Shortcuts** link on the Right side

Shortcuts

 [Add Applications](#)

7. Click on the **Create New App** button. Select **Web** as the platform, select the **SAML 2.0** radio button, and click on the **Create** button.

[← Back to Applications](#)

 **Add Application**

Can't find an app?

Create New App

[Apps you created \(1\) →](#)

[← Back to Applications](#)

 **Add Application**

Can't find an app?

Create New App

[Apps you created \(1\) →](#)

INTEGRATION PROPERTIES

Any

[Supports SAML](#)

[Supports Provisioning](#)

CATEGORIES

4me	4me
-----	-----

Create a New Application Integration

Platform

Web

Sign on method

☒ SAML 2.0

Uses the SAML protocol to log users into the app.

☐ OpenID Connect

Uses the OpenID Connect protocol to log users into an app you've built.

Create

Cancel

8. In the **App name** field, enter your app name, keep the rest of the fields as they are, and click on the **Next** button.

Create SAML Integration

1 General Settings

2 Configure SAML


3 Feedback

1 General Settings

App name

MyAnotherSAMLApp

App logo (optional) ?



Browse..

Upload Logo

App visibility

☐ Do not display application icon to users

☐ Do not display application icon in the Okta Mobile app

Cancel

Next

9. In the **Single sign on URL** field, enter the URL as **https://localhost:8443/saml/SSO**.

In the **Audience URI** field, enter the URI as **https://localhost:8443/saml/metadata**.

Keep the rest of the fields as they are, and click on the **Next** button.

Create SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

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

[Show Advanced Settings](#)

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

Name	Name format (optional)	Value
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text"/>
Add Another		

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>
Add Another		

B Preview the SAML assertion generated from the information above

[< > Preview the SAML Assertion](#)

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

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

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](#)

10. Click on the radio button that says **I'm an Okta customer adding an internal app**.

11. Select the checkbox that says, **This is an internal app that we have created**, and click on the **Finish** button.

Create 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

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.


Previous

Finish

12. You will see the following screen after application is created

oktaDashboardDirectoryApplicationsSecurityWorkflowReportsSettingsMy ApplicationsUpgrade

← Back to Applications



MyAnotherSAMLApp

ActiveView Logs

GeneralSign OnMobileImportAssignments


SettingsEdit

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

Application username formatOkta username

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

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Sign On Policy

Add Rule

Priority	Rule name	Status	Actions
1	Default sign on rule	Active	Not editable

CONDITIONS

User assigned this app

Anywhere

ACTIONS

Allow access

Sign On Policy

A sign on policy is a set of rules that determine how users access this application. For example, you can deny access when a specific user or group of users is off network.

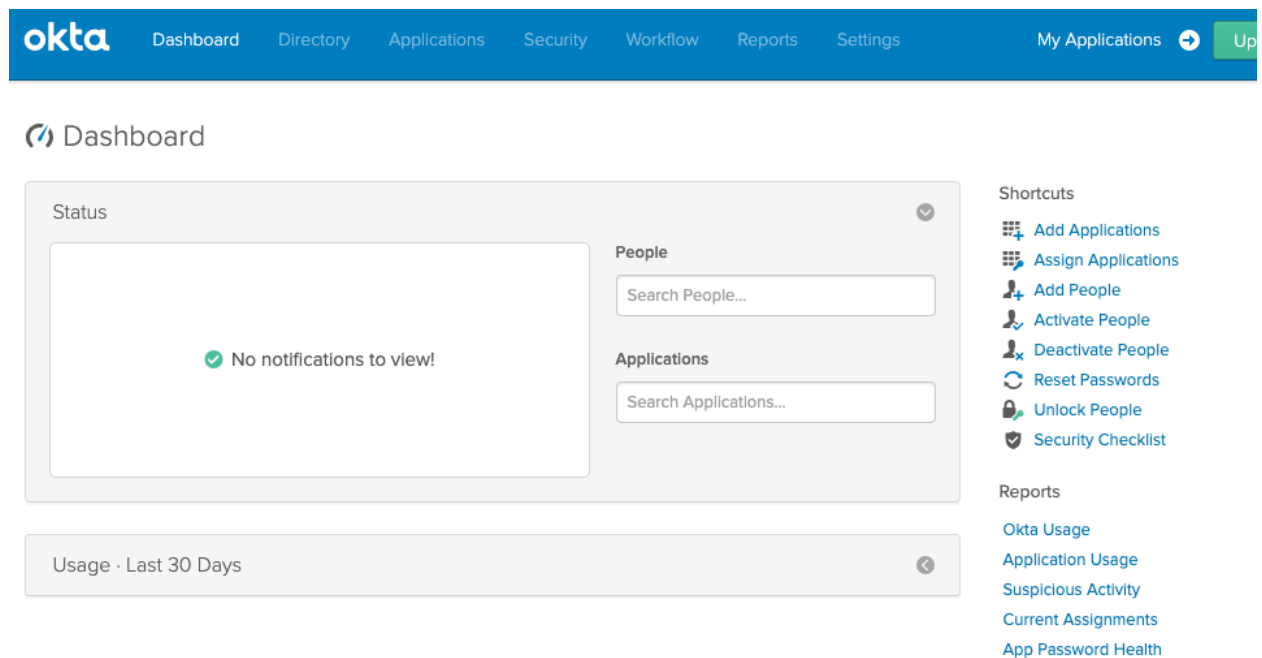
Every application starts with a default rule that allows access to anyone assigned the app from anywhere.

Rule Priority

You can determine rule precedence by setting the priority number. For example, a rule with a priority value of 1 has first priority and takes precedence over all other rules.

Setting up an SSO Application in OKTA

13. Navigate to the **Dashboard** and click on the **Assign Applications** under **Shortcuts**.



14. Click on the created application (in the **Applications** section) on the left, click on your username (on the **People** section) on the right, and click on the **Next** button

[← Back to Applications](#)

Assign Applications




1 Assign Apps to People

2 Confirm Assignments

Cancel

Next

Applications 1

Search		
<input type="checkbox"/>	Application & Label	Sign-on
<input checked="" type="checkbox"/>	 MyAnotherSAMLApp	SAML 2.0
<input type="checkbox"/>	 MySampleApp	SAML 2.0
<input type="checkbox"/>	 DemoSAMLApp	OpenID Connect
First Previous 1 Next Last		

People 1

Search by person	
<input checked="" type="checkbox"/>	Person & Username
<input checked="" type="checkbox"/>	Nandakumar Purohit nandakumarpurohit@gmail.com
Active	
First Previous 1 Next Last	

Cancel

Next

15. On the next page, click on the **Confirm Assignments** button, and you will be done assigning the application to a user

[← Back to Applications](#)

Assign Applications

1 Assign Apps to People

2 Confirm Assignments

Review your assignments before confirming

[Previous](#)

[Cancel](#)

[Confirm Assignments](#)


Assignment Summary

Applications (1)


- MyAnotherSAMLApp

People (1)

- Nandakumar Purohit

 MyAnotherSAMLApp needs additional information entered before it can be assigned.

Enter user attributes

 MyAnotherSAMLApp
MyAnotherSAMLApp · SAML 2.0

Enter user-specific attributes

Search

Username defaults to [Okta username](#)

Person	User specific fields
Nandakumar Purohit	<div>Username<div>nandakumarpurohit@gmail.com</div></div>

Showing 1 - 1 of 1

[Previous](#)

[Cancel](#)

[Confirm Assignments](#)

16. You will see the following screen after assigning the application to your account.

okta

[Dashboard](#)[Directory](#)[Applications](#)[Security](#)[Workflow](#)[Reports](#)[Settings](#)[My Applications](#)[Upgrade](#)

Applications

Help

Add ApplicationAssign ApplicationsMore

Q Search

STATUS

ACTIVE3

INACTIVE0

DemoSAMLApp
Client ID: 00a1osvs0tB8EYqRk357

▼

MyAnotherSAMLApp

▼

MySampleApp

▼

