Keycloak with Okta SAML Provider

31 May 2018, 20:30

keycloak / keycloak-v-3.4 / advanced-features / security / Okta / SAML / Identity Brokering / SAML Identity provider

Keycloak with Okta SAML Provider

The post describes how to integrate Keycloak with Okta SAML Provider

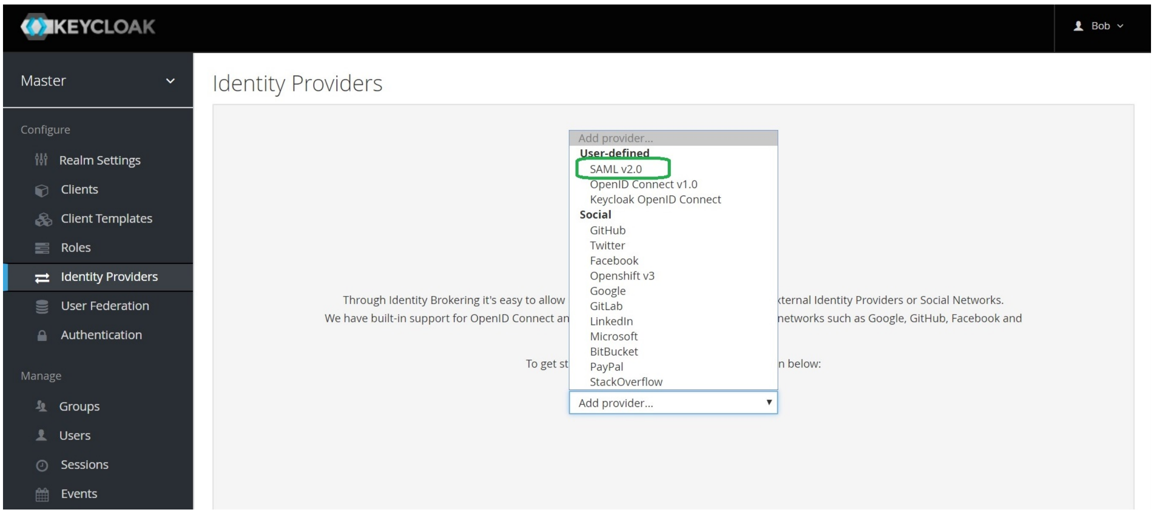
Configuration

We need to configure Keycloak and Okta in parallel. First, you need to add the SAML provider in Keycloak, then you need to add a SAML application in Okta using the Keycloak provider metadata.

Finally you need to import the SAML application metadata into the Keycloak provider.

Add SAML provider in Keycloak

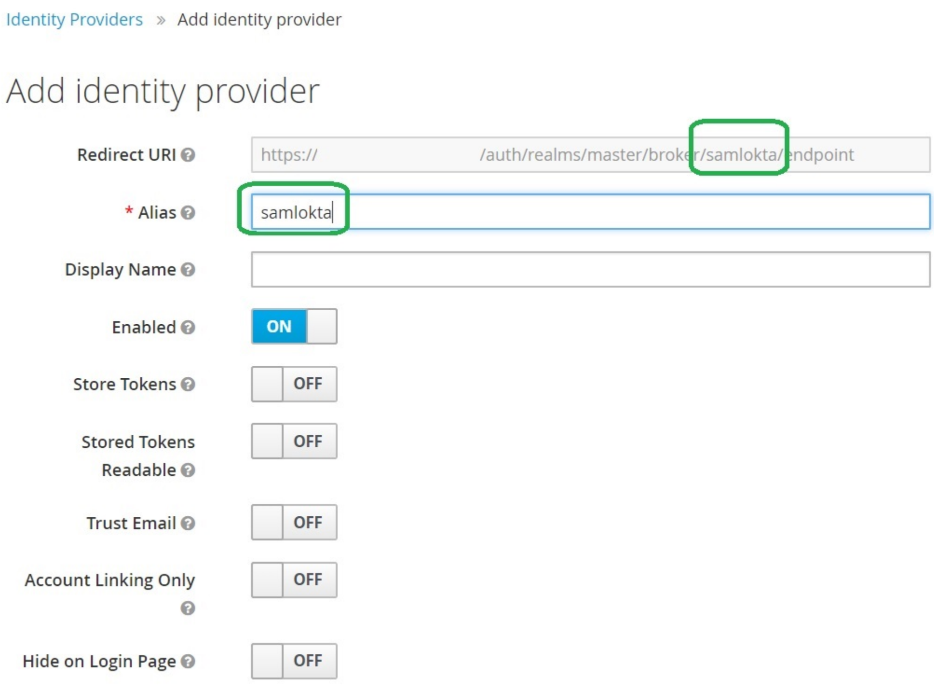
Open Keycloak admin page, open **Identity Providers**, select the **SAML v2.0** provider from the list of providers.



Keycloak SAML Identity Providers documentation is here

Configure SAML provider in Keycloak

Provide the **alias**. Note that it is part of **Redirect URI**



Identity Providers » Add identity provider

Add identity provider

Redirect URI: https:// /auth/realms/master/broker/samlokta/endpoint

* Alias: samlokta

Display Name:

Enabled: ON

Store Tokens: OFF

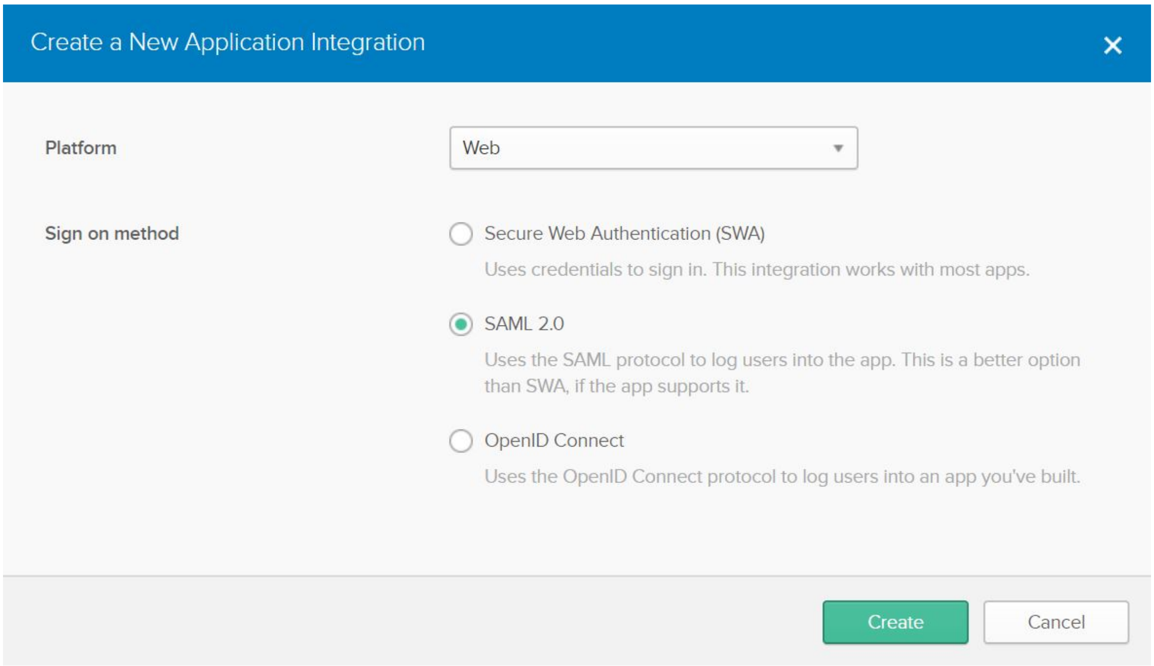
Stored Tokens Readable: OFF

Trust Email: OFF

Account Linking Only: OFF

Hide on Login Page: OFF

Add SAML application in Okta



Create a New Application Integration

Platform: Web

Sign on method

○ Secure Web Authentication (SWA)

Uses credentials to sign in. This integration works with most apps.

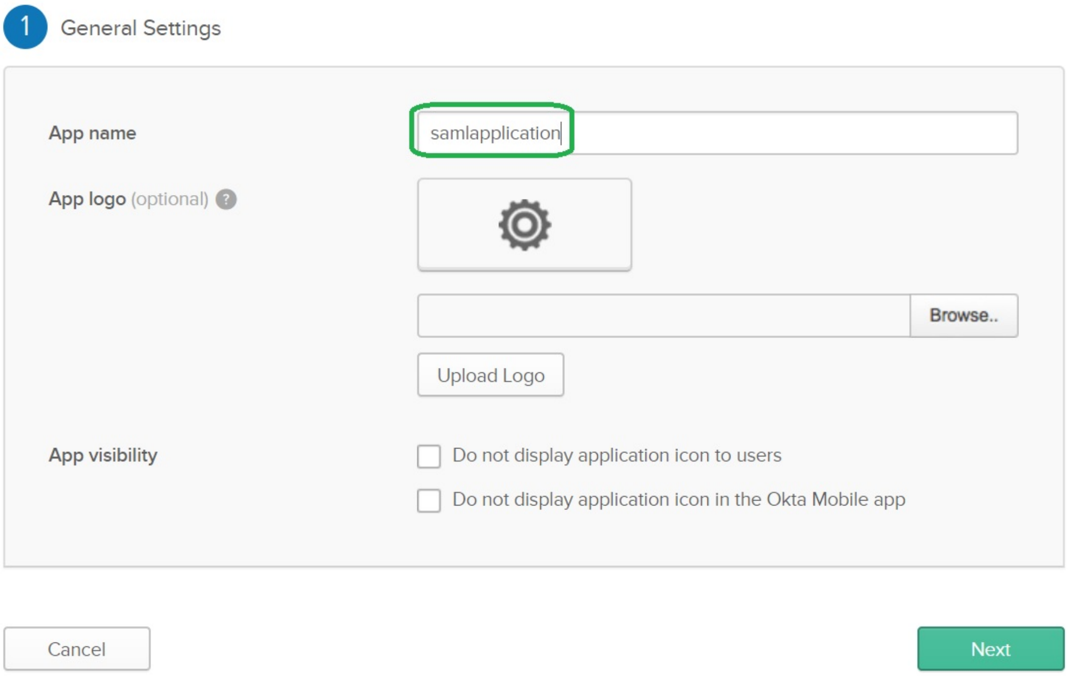
● SAML 2.0

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.

Provide the application name



1 General Settings

App name: samlapplication

App logo (optional)

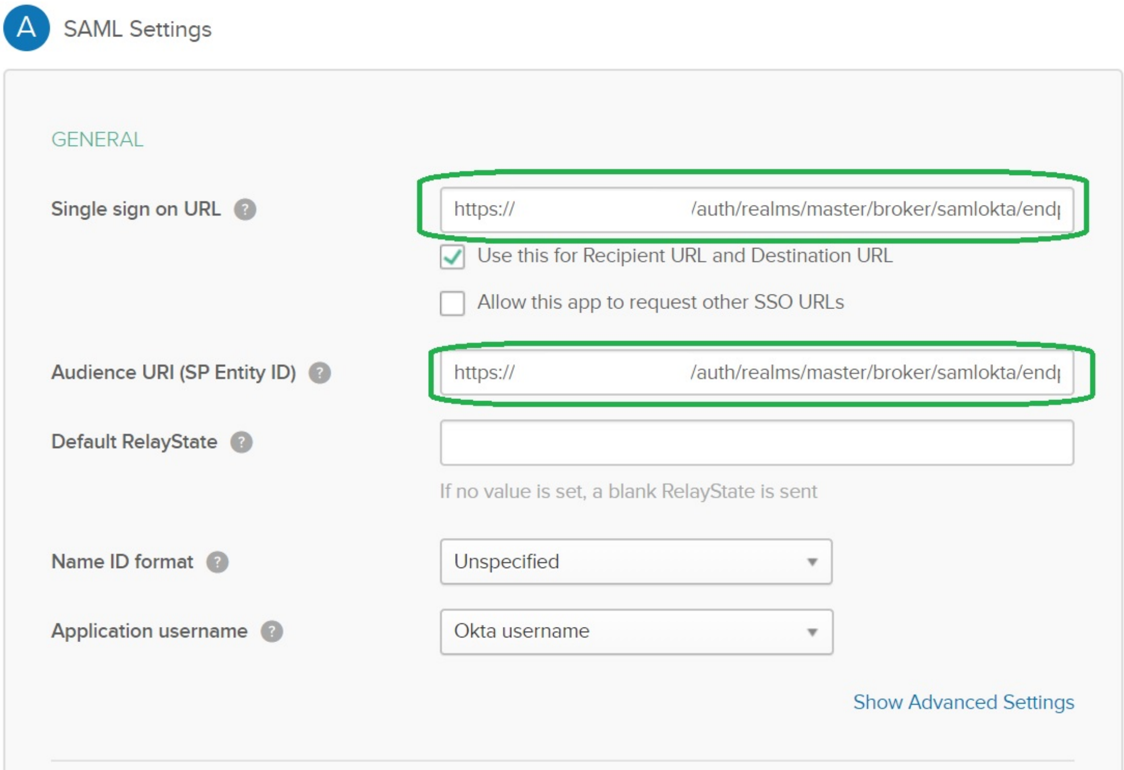
App visibility:

□ Do not display application icon to users

□ Do not display application icon in the Okta Mobile app

Configure SAML Settings

Copy Keycloak’s **Redirect URI** to the **Single sign on URL** and **Audience URI (SP Entity ID)** settings



A SAML Settings

GENERAL

Single sign on URL: https:// /auth/realms/master/broker/samlokta/end

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https:// /auth/realms/master/broker/samlokta/end

Default RelayState:

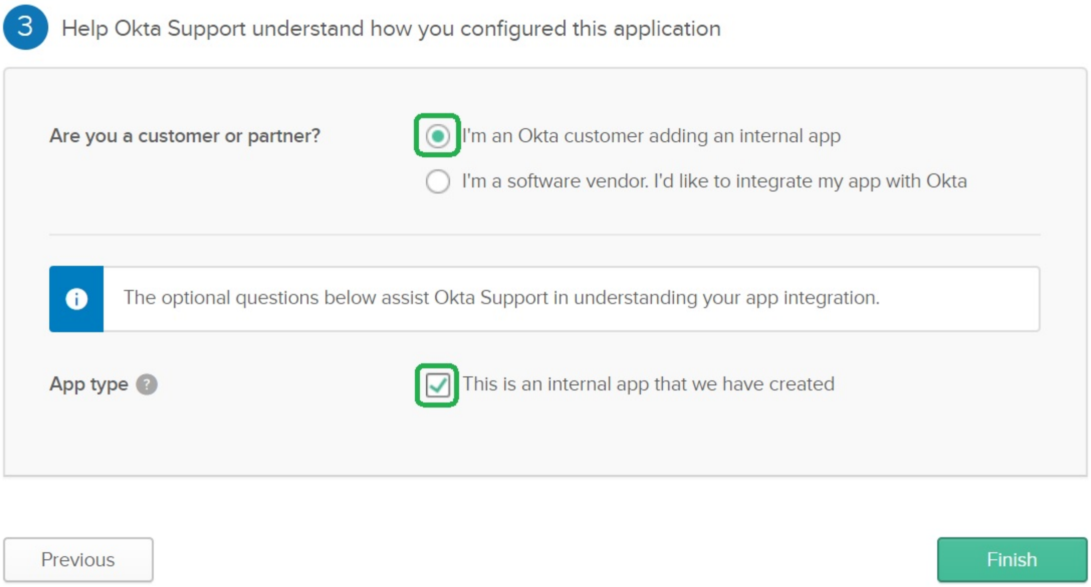
If no value is set, a blank RelayState is sent

Name ID format: Unspecified

Application username: Okta username

Configure the application type

Configure the application type and press **Finish**



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

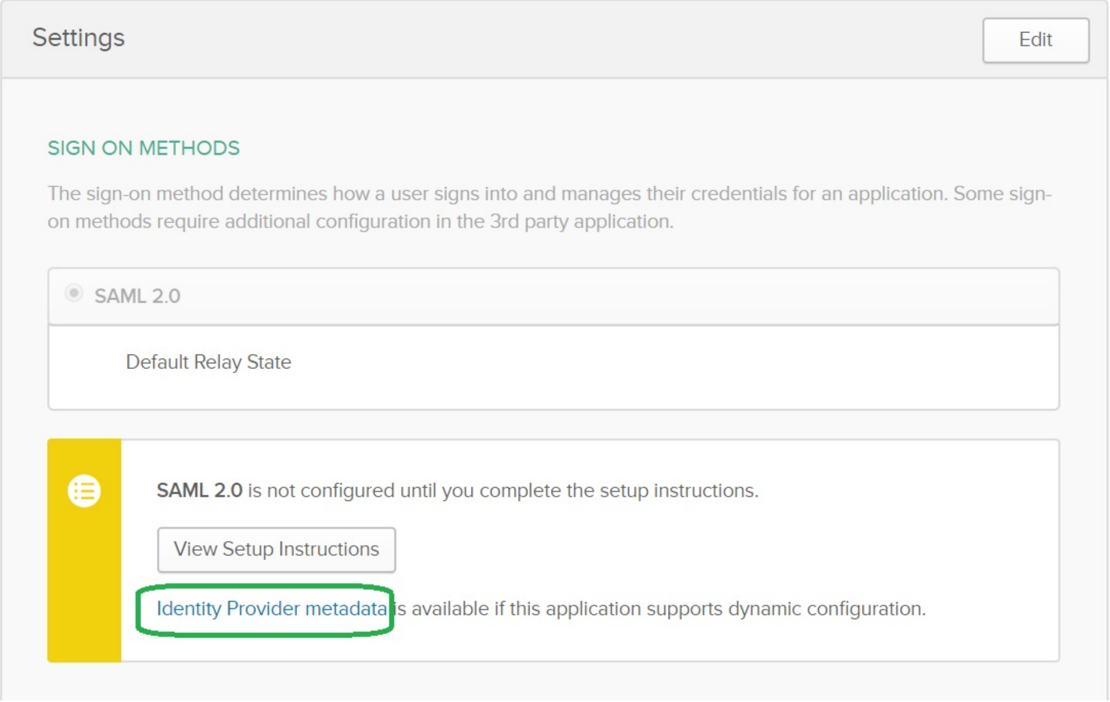
○ I'm a software vendor. I'd like to integrate my app with Okta

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

App type ☑ This is an internal app that we have created

Copy the metadata link

We have added the application to Okta, now we need to copy the **Identity Provider metadata** link and import it into Keycloak.



Settings

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

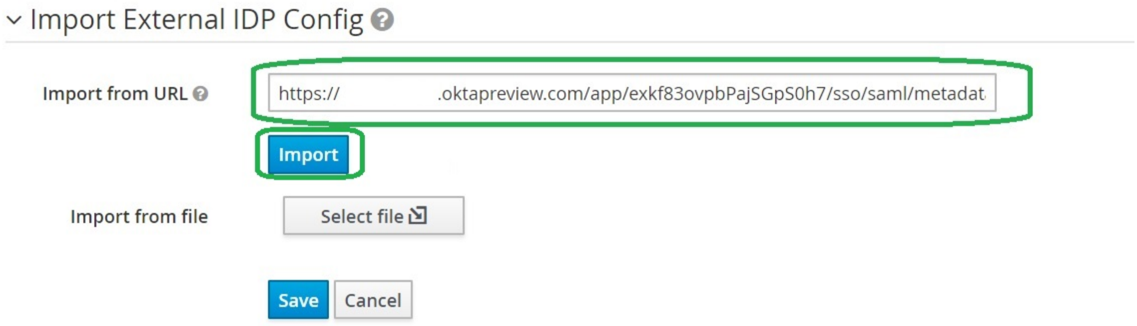
SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

Note that you need to assign people to the application

Import Okta SAML metadata into Keycloak

Paste the metadata link into the **Import from URL** area and press on the **Import** button



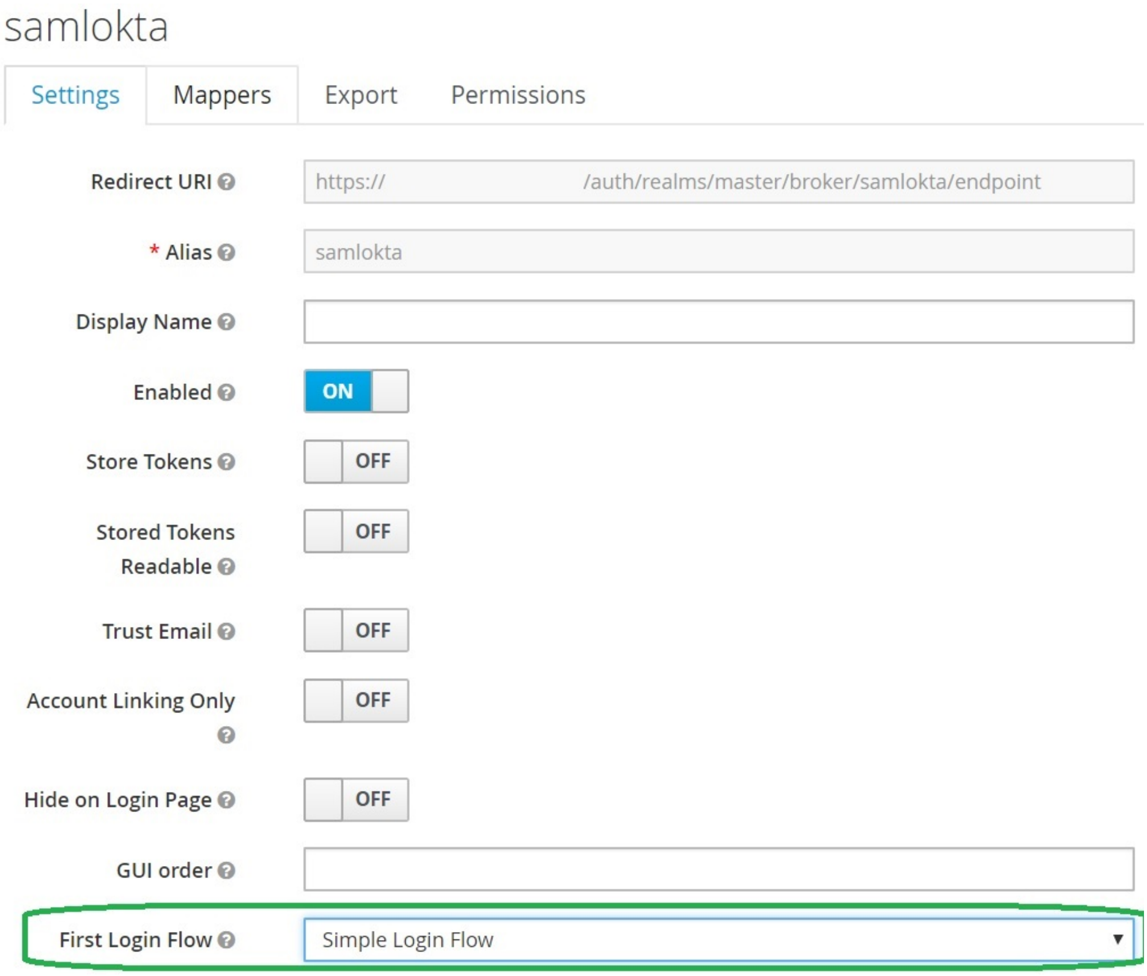
Import External IDP Config

Import from URL: https:// .oktapreview.com/app/exkf83ovpbPajSGpS0h7/sso/saml/metadat

Configure First Login Flow

In my previous post I have described how to add Simple Keycloak First Login Flow

Let’s configure the flow and then save the provider configuration



samlokta

Redirect URI: https:// /auth/realms/master/broker/samlokta/endpoint

* Alias: samlokta

Display Name:

Enabled: ON

Store Tokens: OFF

Stored Tokens Readable: OFF

Trust Email: OFF

Account Linking Only: OFF

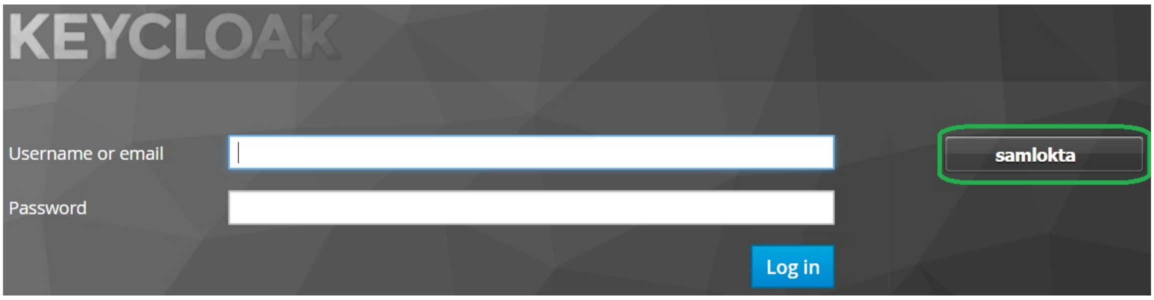
Hide on Login Page: OFF

GUI order:

First Login Flow: Simple Login Flow

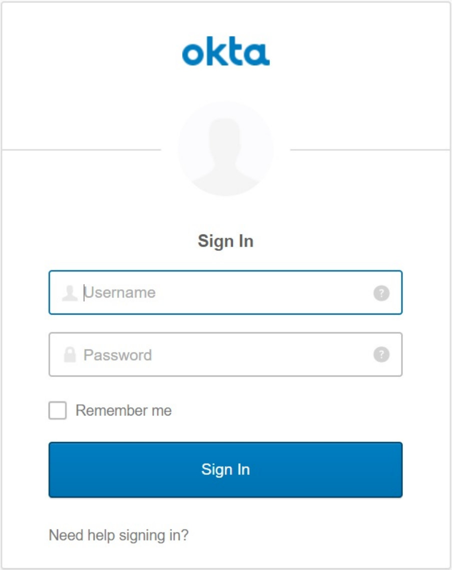
Login using Okta SAML

You open the login and surprise!
We have the additional button that allows us to login to Keycloak using Okta SAML provider:



Note that you can configure **Display Name** in the provider configuration and to set more friendly name.

When you press on the button you will be redirected to Okta.



Enjoy Okta SAML integration

‹ Simple Keycloak First Login Flow

OpenID Connect presentation ›