

Riskpal integration with okta

All Riskpal users have the ability to configure a default Identity Provider to power Single Sign On (SSO). This article details how to configure Okta as the primary Identity Provider to facilitate SSO with the Riskpal application.

Supported Features

Service Provider (SP)-Initiated Authentication (SSO) Flow - This authentication flow occurs when the user attempts to log in to the application from Riskpal.

For account creation you will need to contact Riskpal. Email address: info@riskpal.co.uk

Requirements

In order to proceed with configuring login with SSO through Okta, you must:

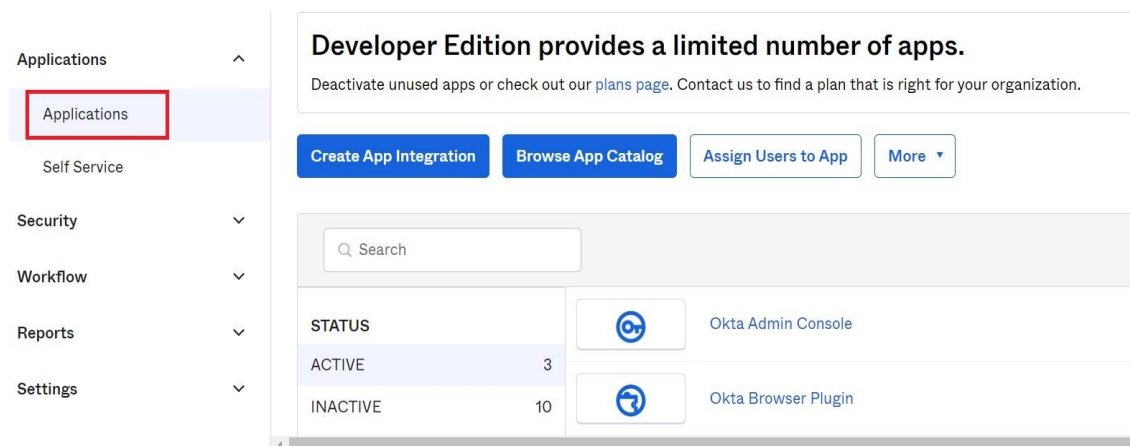
- Have access to an Okta tenant
- Be an Okta administrator to that tenant
- Have contacted Riskpal for integration

Please email tom.bacon@riskpal.co.uk for the integration

Configuration Steps

Step 1: Setting up Riskpal App in Okta

1. Go to Applications under Applications



2. On the Applications page, select Browse App Catalog

Developer Edition provides a limited number of apps.
Deactivate unused apps or check out our [plans page](#). Contact us to find a plan that is right for your organization.

Create App Integration **Browse App Catalog** Assign Users to App More

Search

STATUS	
ACTIVE	3
INACTIVE	10

Okta Admin Console

Okta Browser Plugin

3. Search for Riskpal App and add it

Last updated: March 6, 2023

+ Add Integration

Riskpal

Okta Verified Overview

4. Add an Application label and click Done

General settings - Required

Application label: Riskpal
This label displays under the app on your home page

Application Visibility:
☐ Do not display application icon to users
☐ Do not display application icon in the Okta Mobile App

Cancel Done

General settings
All fields are required for application

5. Click on Sign on tab ,in that click on edit

General **Sign On** Mobile Import Assignments Okta API Scopes

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.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

About

OpenID Connect allows users to sign-on to applications using the OpenID Connect protocol.

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

6. In Credentials details section change the Application username format to “Email”

configuration.

Credentials Details

Application username format Email

Update application username on Create and update

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

Save

7. Once the App is added, you will have to assign users to the app under the Assignments tab. This will enable users to log into Riskpal app using Okta. To add users, navigate to the Assign to People option under Assign option on Assignments Page. If you already have a group you can choose the Assign to Groups option and assign the entire group.

General Sign On Mobile Import **Assignments** Okta API Scopes

Assign **Convert assignments**

Assign to People

Assign to Groups

Groups

Type

01101110
01101111
01101100
01101100
01101101
01101110
01100111

REPORTS

Current As

Recent Un

SELF SERVICE

You need service for

8. You can add people by clicking the Assign option next to their name. After you have all the people click the Done button

Assign Riskpal to People

hiral

hiral panchal hiral+123@souqbox.net	Assign
Hiral Panchal hiral+53@souqbox.net	Assign
hiral panchal hiral+128@souqbox.net	Assign
hiral panchal hiral+46@souqbox.net	Assign
hiral Panchal hiral+22@souqbox.net	Assign
hiral Panchal hiral+145@souqbox.net	Assign

Step 2: Enabling SSO in Riskpal App

1. You will require Client ID and Client secret key

← Back to Applications



Riskpal

Active

View Logs Monitor Imports

General

Sign On

Mobile

Import

Assignments

Okta API Scopes

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.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

☒ OpenID Connect

Client ID

Ooabqkg9qwHmgbbqTQ4x7

Public identifier for the client that is required for all OAuth flows.

About

OpenID Connect allows users to sign-on to applications using the OpenID Connect protocol.

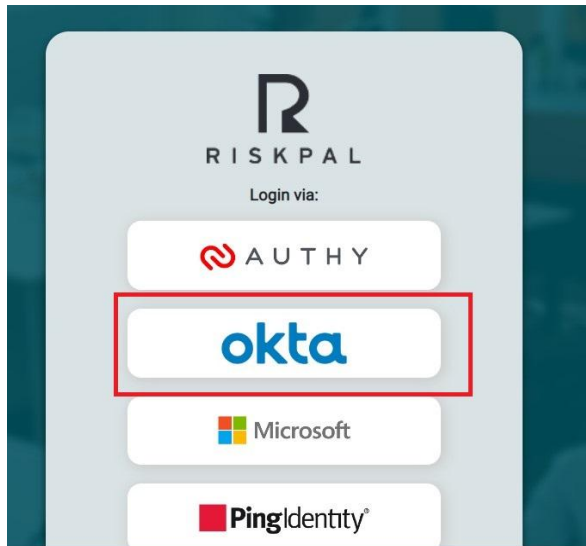
Application Username

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

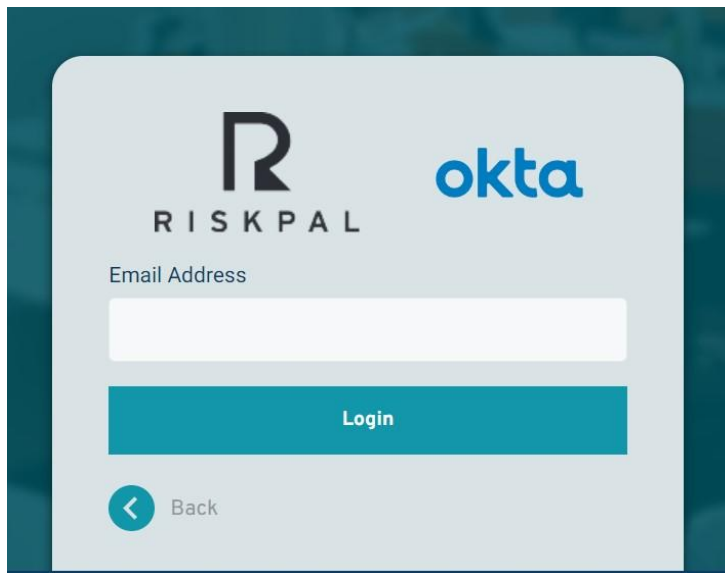
If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Issuer URL will be of the format <https://your-company.okta.com> for example <https://riskpal.okta.com>. Also if URL has **-admin** suffix for example <https://your-company-admin.okta.com>, just remove the suffix and only use <https://your-company.okta.com>(**https://** is required)

2. Please contact info@riskpal.co.uk or tom.bacon@riskpal.co.uk to submit your Client ID, client secret and Issuer URL. Please don't mail the details on the mentioned email.
3. Login to Okta through Riskpal <https://www.riskpal.co.uk/login> , Please click on okta:



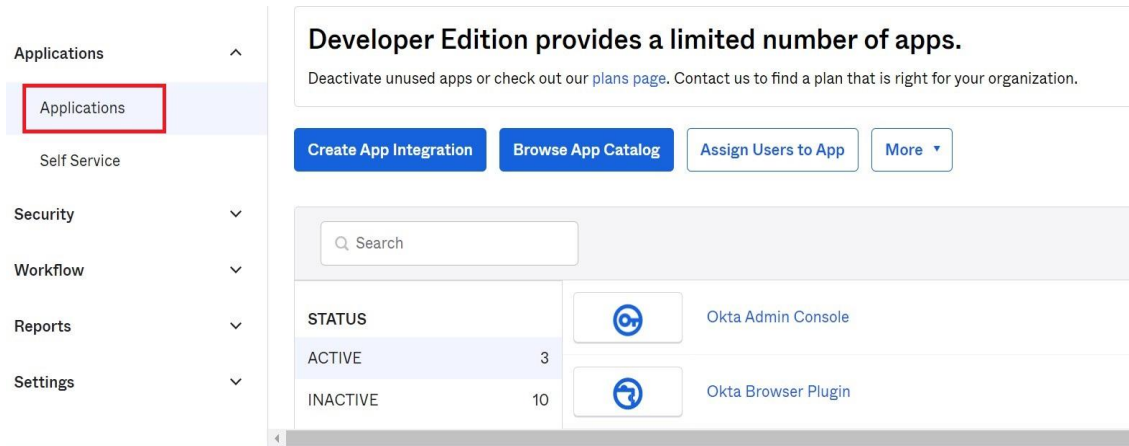
4. Enter your email address, click on Login



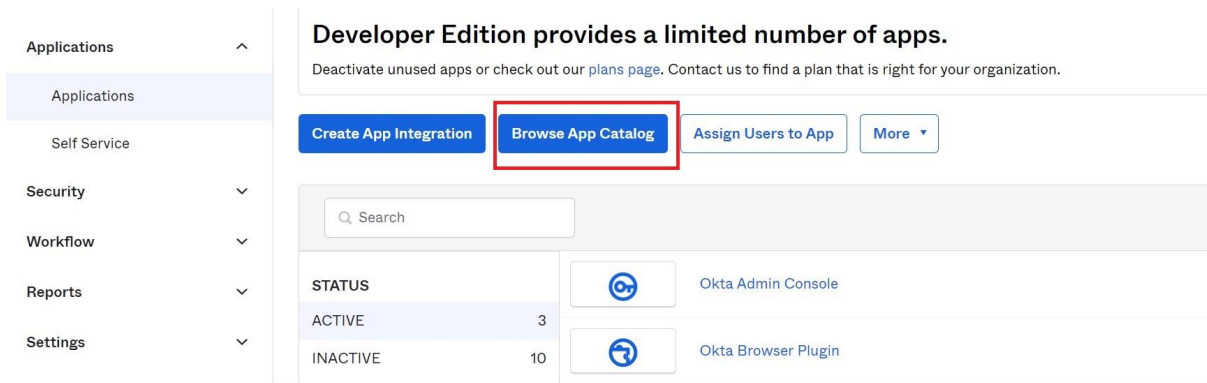
5. If you are already logged into your okta portal, you would be directly logged into the system or redirected to the respective okta portal.

Accessing Riskpal through Okta portal

1. Go to Applications under Applications



2. On the Applications page, select Browse App Catalog



3. Search for Bookmark App to add

Browse App Integration Catalog

Use Case	
All Integrations	7529
Apps for Good	9
Automation	28
Centralized Logging	11
Directory and HR Sync	25
Bot or Fraud Detection	3
Identity Proofing	12
Identity Governance and Administration (IGA)	9

Search Bookmark App

Search results for "Bookmark App"

★ All Integrations

Bookmark App

Bookmark App for apps which don't yet have Okta integrations

4. Click on add integration to add the application

Last updated: October 21, 2021

[+ Add Integration](#)



Bookmark App

5. Add "Application label" as Riskpal and URL as ["https://riskpal.co.uk/login?oktaOIN=true"](https://riskpal.co.uk/login?oktaOIN=true) and click on done

Application label

Riskpal App

This label displays under the app on your home page

URL

<https://riskpal.co.uk/login?oktaOIN=true>

The URL of the sign-in page for this app

Request Integration

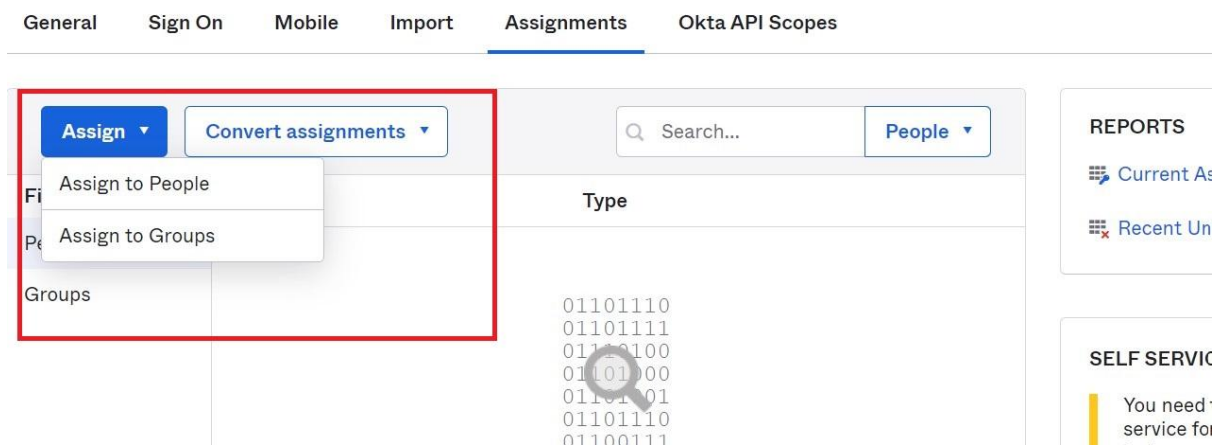
☐

Would you like Okta to add an integration for this app?

Application Visibility

☐ Do not display application icon to users

9. Once the App is added, you will have to assign users to the app under the Assignments tab. This will enable users to log into Riskpal app using Okta. To add users, navigate to the Assign to People option under Assign option on Assignments Page. If you already have a group you can choose the Assign to Groups option and assign the entire group.



10. You can add people by clicking the Assign option next to their name. After you have all the people click the Done button

If you experience any issues or have any questions, please reach out to info@riskpal.co.uk to engage our support staff.