



Okta Identity Management Requirements for People First and Chatbot

Configuration Instructions

Version: 1.1

Prepared by: Mark Lloyd

Date Reviewed: Oct 2020

Classification: Company Confidential

people first


Powered by MHR International

Table of Contents

1	Summary	3
2	Creating a People First Okta application	4
3	Creating an Okta authorisation server	8

1 Summary

This document provides information on how to:

- Create a People First Okta application
- Create an Okta authorisation server

Whilst progressing through this document some key information will need to be retained and sent to us in order for us to configure your people first system to work with your Okta identity manager.

----- KEY INFORMATION REQUIRED BY MHR -----

Key information required by MHR in order to configure your People First to work with your Okta identity manager :-

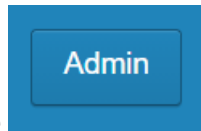
Your Okta People First Application Client ID : (Section 2.15) :

Your Okta Authorisation Server Metadata URI : (Section 3.8) :


Please forward the above information to MHR.

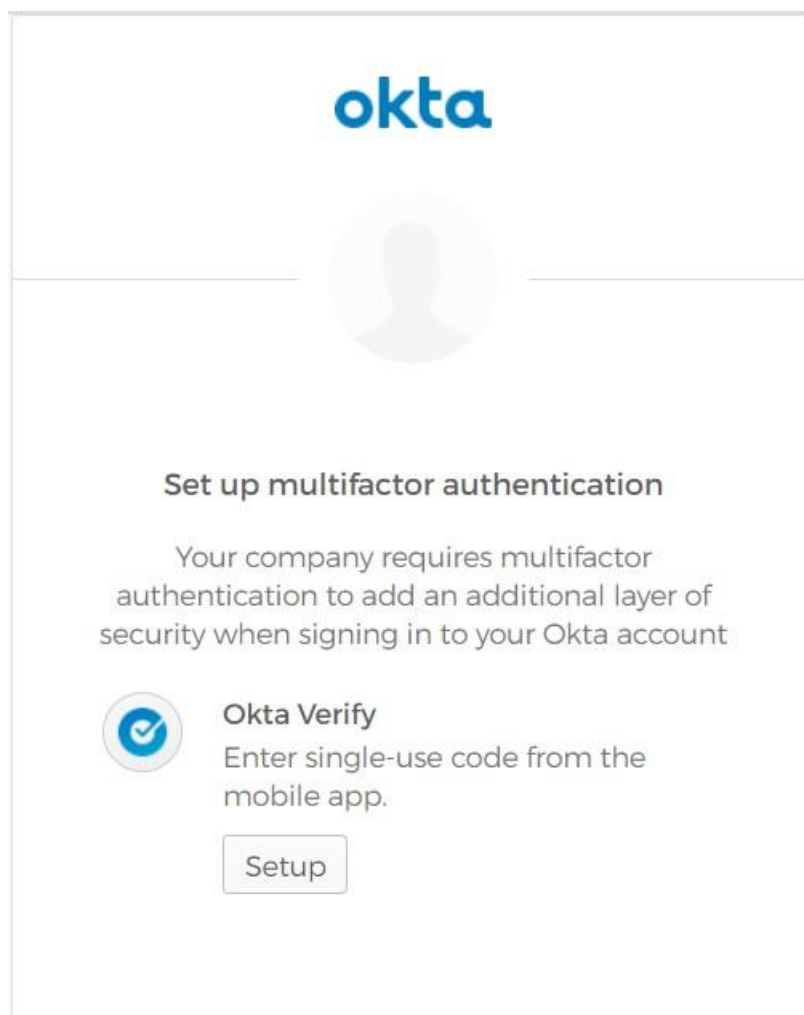
2 Creating a People First Okta application

- 1) Sign into your Okta identity manager
- 2) Select *Your apps* from your user profile dropdown menu



- 3) Click on the  button at the top of the screen

- 4) **NB:** You may be asked to set up MFA, if so, click the  button and follow the instructions



- 5) To continue configuring the Okta app

A blue rectangular button with rounded corners containing the text "Add App" in white.

Click on the button to select *Use single sign on* and then click on the

A green rectangular button with rounded corners containing the text "Create New App" in white.

button

6) In the Platform dropdown select “Single Page App (SPA)” and click on the

A green rectangular button with rounded corners containing the text "Create" in white.

button

7) Enter “People First” for the Application name

8) Enter “<https://login.people-first.com/redirect/>” for the Login redirect URIs

9) Ensure “Implicit” is checked in the *Allowed grant types*

10) NB: Logout Redirect URLs – not required

A green rectangular button with rounded corners containing the text "Save" in white.

11) Click on the button.

General Settings
Edit

APPLICATION

Application label: People First

Application type: Single Page App (SPA)

Allowed grant types: Client acting on behalf of a user

- Authorization Code
- Implicit
- Allow ID Token with implicit grant type
- Allow Access Token with implicit grant type

LOGIN

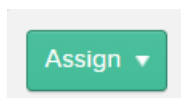
Login redirect URIs: <https://login.people-first.com/redirect/>

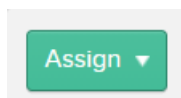
Logout redirect URIs:

Login initiated by: App Only

Initiate login URI:

12) Click on the Assignments tab



13) Click the  button and select the appropriate option to assign any people or groups of people, from your Okta directory, who require user access to People First

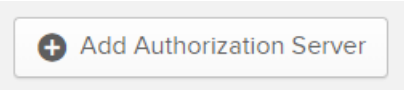
14) Save your changes and then click “Done”

15) Make a note of the Okta People First application **client id** generated.

3 Creating an Okta authorisation server

1) Go to the Okta Admin portal

2) Click on the Security tab and select the API option

3) On the Authorization Servers tab, click the  button or alternatively you can customise the “default” authorisation server

4) For the Name enter “PeopleFirstIdP”

5) For the Audience – enter the Okta People First application **client id** generated previously


6) For the Description enter “Identity provider for People First”

7) Click the  button

8) Make a note of the **Metadata URI**

Settings		Edit
Name	PeopleFirstIdP	
Audience	<your Audience ID>	
Description	Identity provider for People First	
Issuer	https://<your Okta domain name>.okta.com/oauth2/<your Issuer ID>	
Metadata URI	https://<your Okta domain name>.okta.com/oauth2/<your Issuer ID>/well-known/oauth-authorization-server	
Signing Key Rotation ?	Automatic	
Last Rotation	29 Sep 2020	

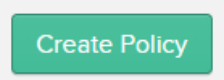
9) **NB:** You must add a policy for users to be able to logon (if you customised the default IdP this may be unnecessary as it has a policy out of the box)

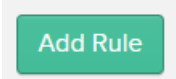
10) Go to the “Access Policies” tab and click on the  button

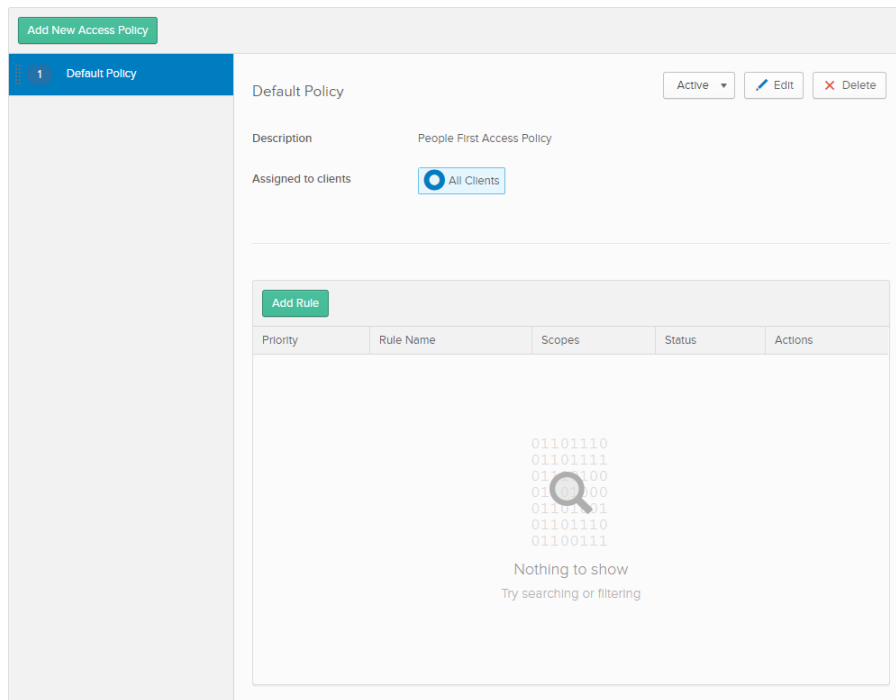
11) For the Name enter “Default Policy”

12) For the Description enter “People First Access Policy”

13) For Assign to, ensure All clients is selected

14) Click on the  button

15) On the next screen, click on the  button



16) For the Rule Name enter “People First Policy Rule”

17) All other settings can be left as defaults

Add Rule

Rule Name

IF **Grant type is**

- Client acting on behalf of itself
 - Client Credentials
- Client acting on behalf of a user
 - Authorization Code
 - Implicit
 - Resource Owner Password

AND **User is**

- Any user assigned the app
- Assigned the app and a member of one of the following:

AND **Scopes requested**

- Any scopes
- The following scopes:

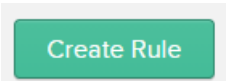
THEN **Use this inline hook**

AND **Access token lifetime is**

AND **Refresh token lifetime is**

but will expire if not used every

18)



19) Click on the  button

Please raise a case with the MHR service desk, passing on the key information recorded in this document, so that your People First system can be configured with your identity provider



Global Head Quarters

People First
Ruddington Hall
Loughborough Road
Nottingham
NG11 6LL
UK
+44 (0) 1159 456 000

EMEA Head Quarters

People First
The Greenway, Block C
Ardilaun Court
112-114 St Stephen's Green
Dublin 2
Ireland
+353(1) 6532147

US Head Quarters

People First
Suite 550
11921 Freedom Drive
Two Fountain Square
Reston, Virginia
20190 USA
+1 (0703) 397 5182

APAC Head Quarters

People First
9 Raffles Place
Level 6
Republic Plaza 1
Singapore
048619
+65 981 57 815



people first