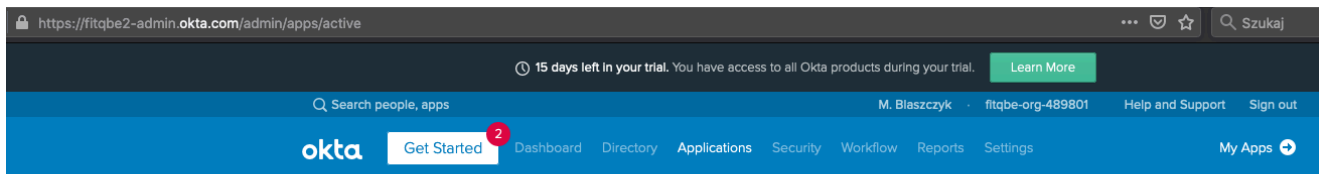


Instrukcja tworzenia aplikacji OAuth2 w usłudze Okta, w celu realizacji integracji z Fitqbe

1. Integracja oparta jest o protokół OAuth2 oraz authorization code flow, Fitqbe potrzebuje jedynie najniższe uprawnienie: profile, email, openid, offline_access (aby weryfikować czy konto nie zostało zablokowane). To uprawnienie umożliwia nam odczytywanie jedynie podstawowych danych konta pojedynczego użytkownika, który zdecydował się na integrację konta Fitqbe z Okta.
2. Do integracji konieczne jest stworzenie aplikacji w panelu administracyjnym Okta: [https://\[tenant\]-admin.okta.com/admin/getting-started](https://[tenant]-admin.okta.com/admin/getting-started), administrator usługi Okta musi tutaj zalogować się.
3. Następnie wejść w zakładkę aplikacji i kliknąć „Add Application”






4. Następnie kliknąć na „Create New App” po prawej stronie



← Back to Applications

 Add Application

Create New App

CATEGORIES	Search...	
Featured	Featured Integrations See all	
API Management 6		 Active Directory Provisioning
Apps 5991		 Atlassian Cloud SAML, SWA, Provisioning
Apps for Good 12		 DocuSign SAML, SWA, Provisioning
CASB 3		
Directories and HR Systems 12		

5. Na ekranie konfiguracji należy wybrać opcję: Web oraz OpenID Connect i kliknąć „Create”

Create a New Application Integration [X]

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.

Create **Cancel**

6. Następnie należy uzupełnić poszczególne pola wartościami i kliknąć „Save”:

1) Fitqbe

2)





3) <https://webhooks.fitqbe.com/authentication/connect/okta>

 Create OpenID Connect Integration


GENERAL SETTINGS


Application name

Application logo (Optional) 

 X


CONFIGURE OPENID CONNECT

Login redirect URIs 


Logout redirect URIs 

7. Następnie kliknąć przycisk „Edit” po prawej stronie, tak aby można było edytować poniższe wartości. Chcemy zaznaczyć pole „Refresh Token” w sekcji „Allowed grant types”.

← Back to Applications



Fitqbe22

Active ▼  [View Logs](#)

General **Sign On** Assignments

General Settings

Cancel

APPLICATION

Application label

Application type Web

Allowed grant types

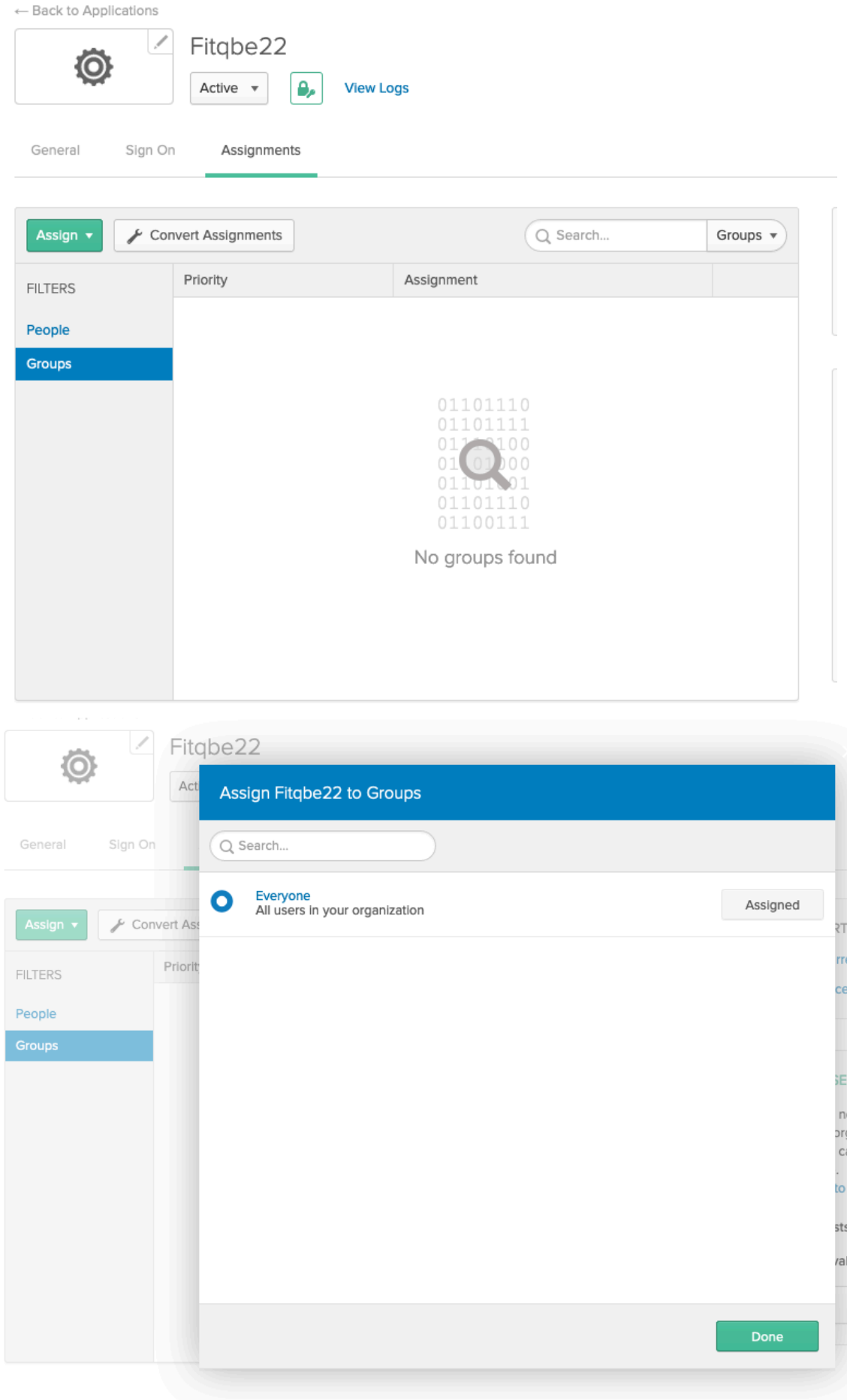
Client acting on behalf of itself

- Client Credentials

Client acting on behalf of a user

- Authorization Code
- Refresh Token
- Implicit (Hybrid)

8. Następnie należy przypisać do aplikacji wszystkich użytkowników w Okta. Najłatwiej to zrobić przez przypisanie grupy Everyone:



- Ostatnim krokiem jest skopiowanie danych dostępowych „Client ID” i „Client secret”. Dane proszę przesłać w formie poufnej do osoby kontaktowej w Fitqbe.

Client Credentials

Edit

Client ID

📄

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

Client secret

👁️📄

Secret used by the client to exchange an authorization code for a token. This must be kept confidential! Do not include it in apps which cannot keep it secret, such as those running on a client.