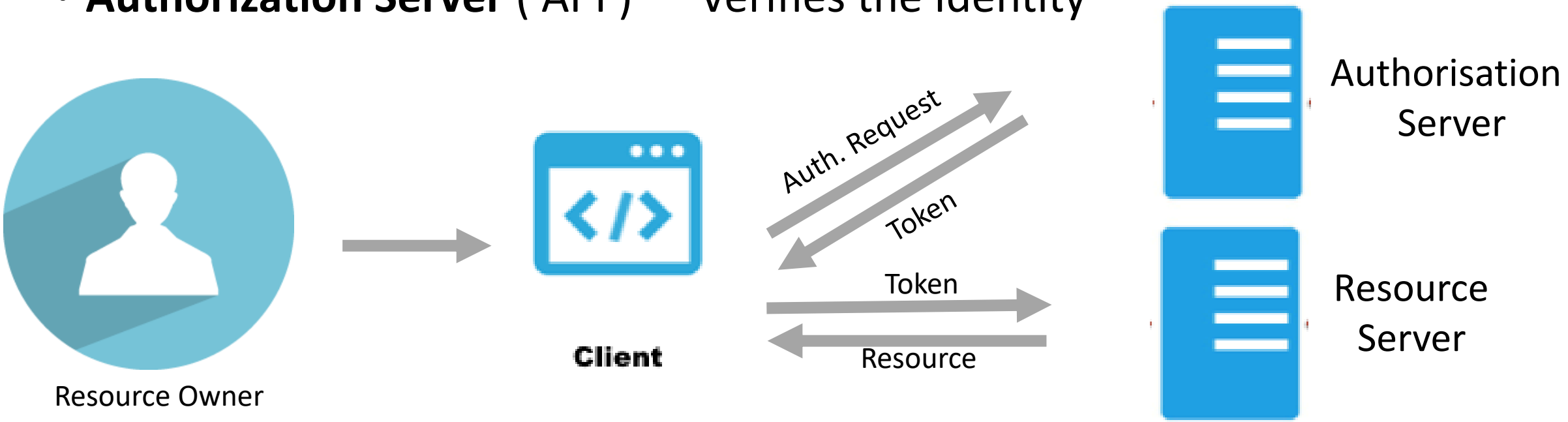
OAuth 2 Introduction

- Roles
- Grant Types
- Flows
- Demo

OAuth Roles

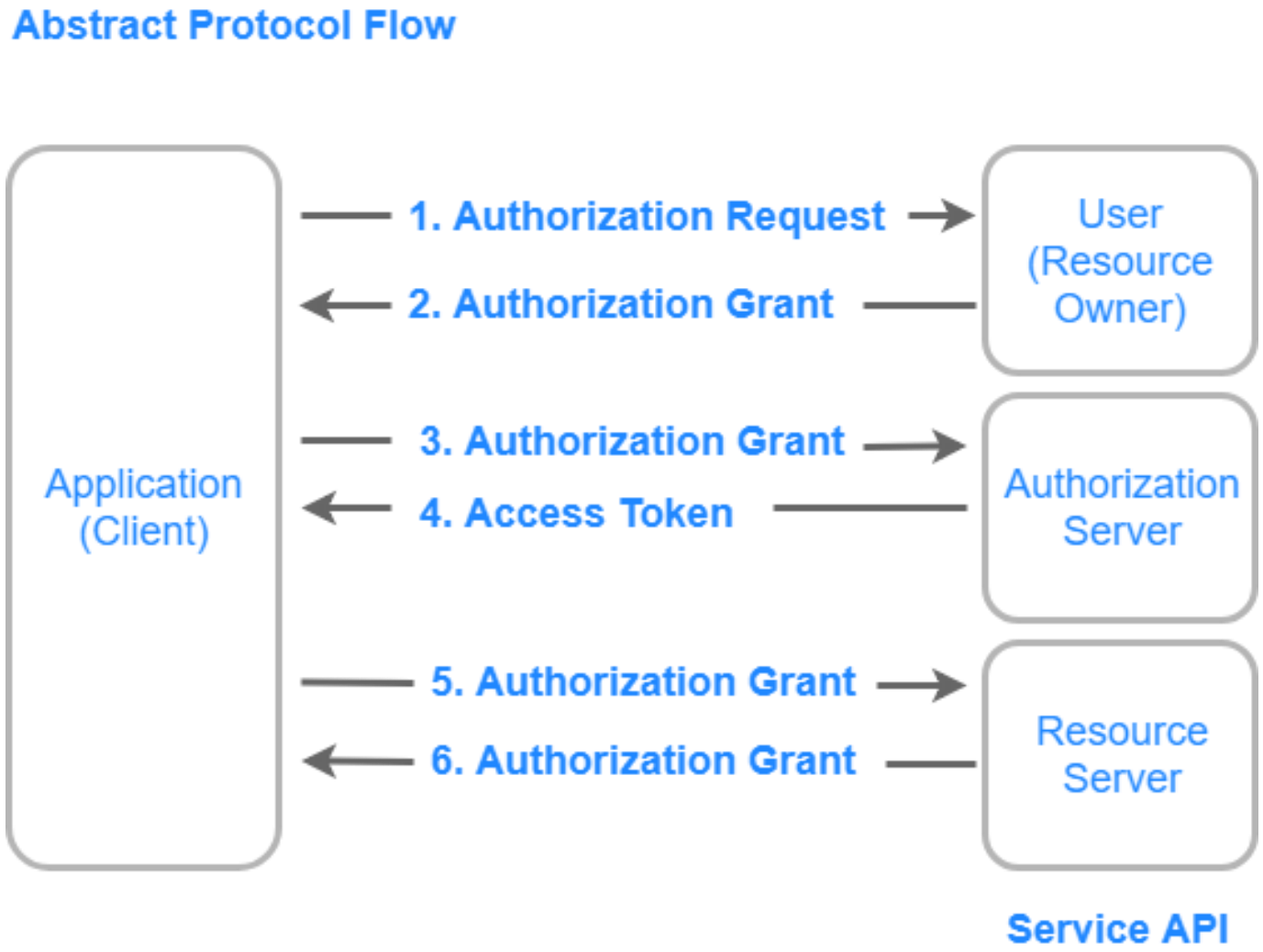
- **Resource Owner** (User)
- **Client** (Application that wants to access user account)
- **Resource Server** (API) Hosts User Accounts
- **Authorization Server** (API) Verifies the Identity



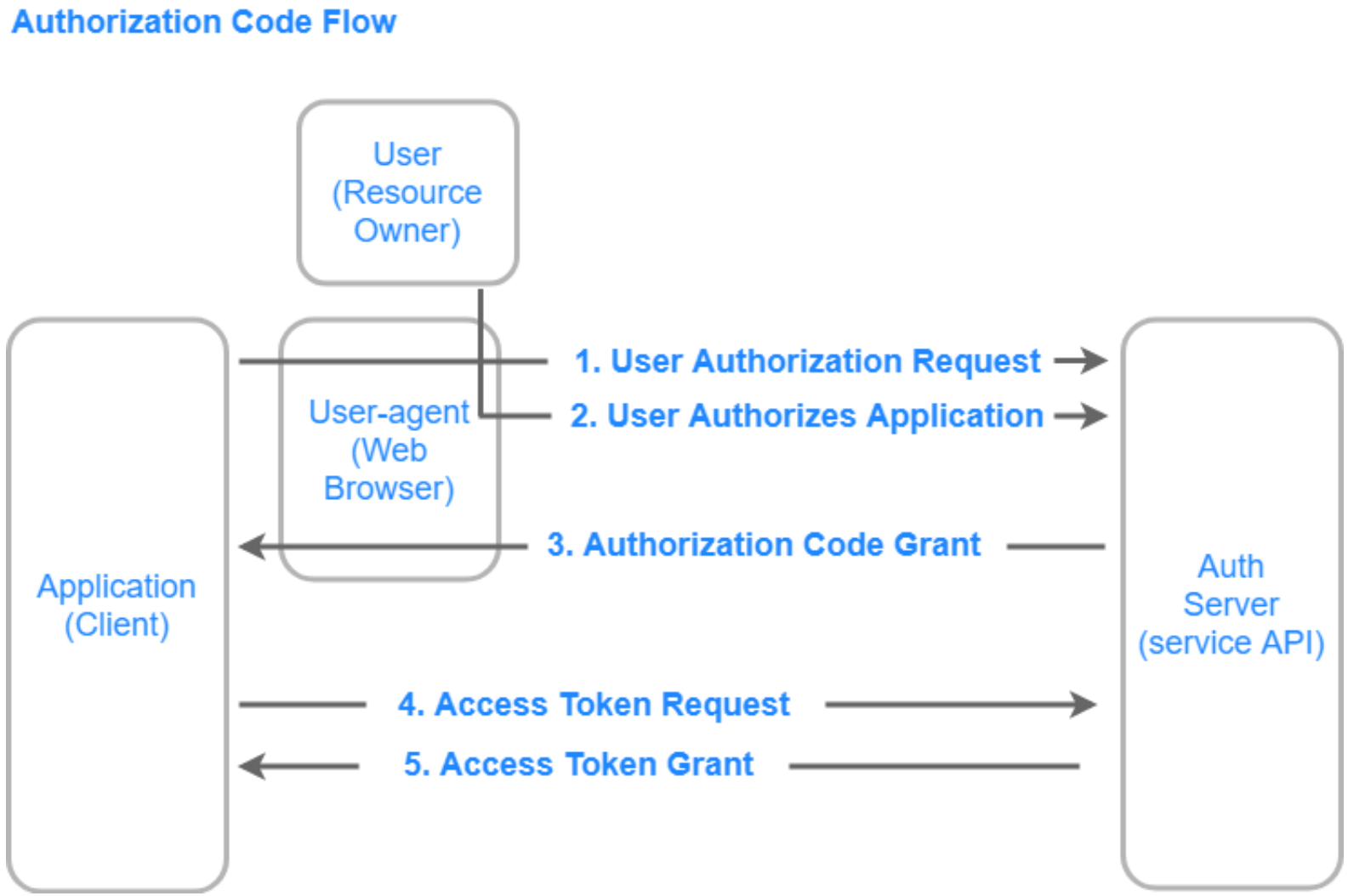
Authorization Grant

- **1. Authorization Code**: used with server-side Applications
- **2. Implicit**: used with Mobile Apps or Web Applications (applications that run on the user's device)
- **3. Resource Owner Password Credentials**: used with trusted Applications, such as those owned by the service itself
- **4. Client Credentials**: used with Applications API access, example use case, changing application settings (authorization based on with client_id, client_secret)
- **5. Refresh token grant**: used to obtain an access token with a refresh token

General Overview



1. Authorisation Code Grant Type



1. Authorisation Code Grant Type

- 1. Application requests AUTHORISATION_CODE

https://cloud.digitalocean.com/v1/oauth/authorize?response_type=code&client_id=CLIENT_ID&redirect_uri=CALLBACK_URL&scope=read

- 2. User authorizes
- 3. Application receives AUTHORISATION_CODE

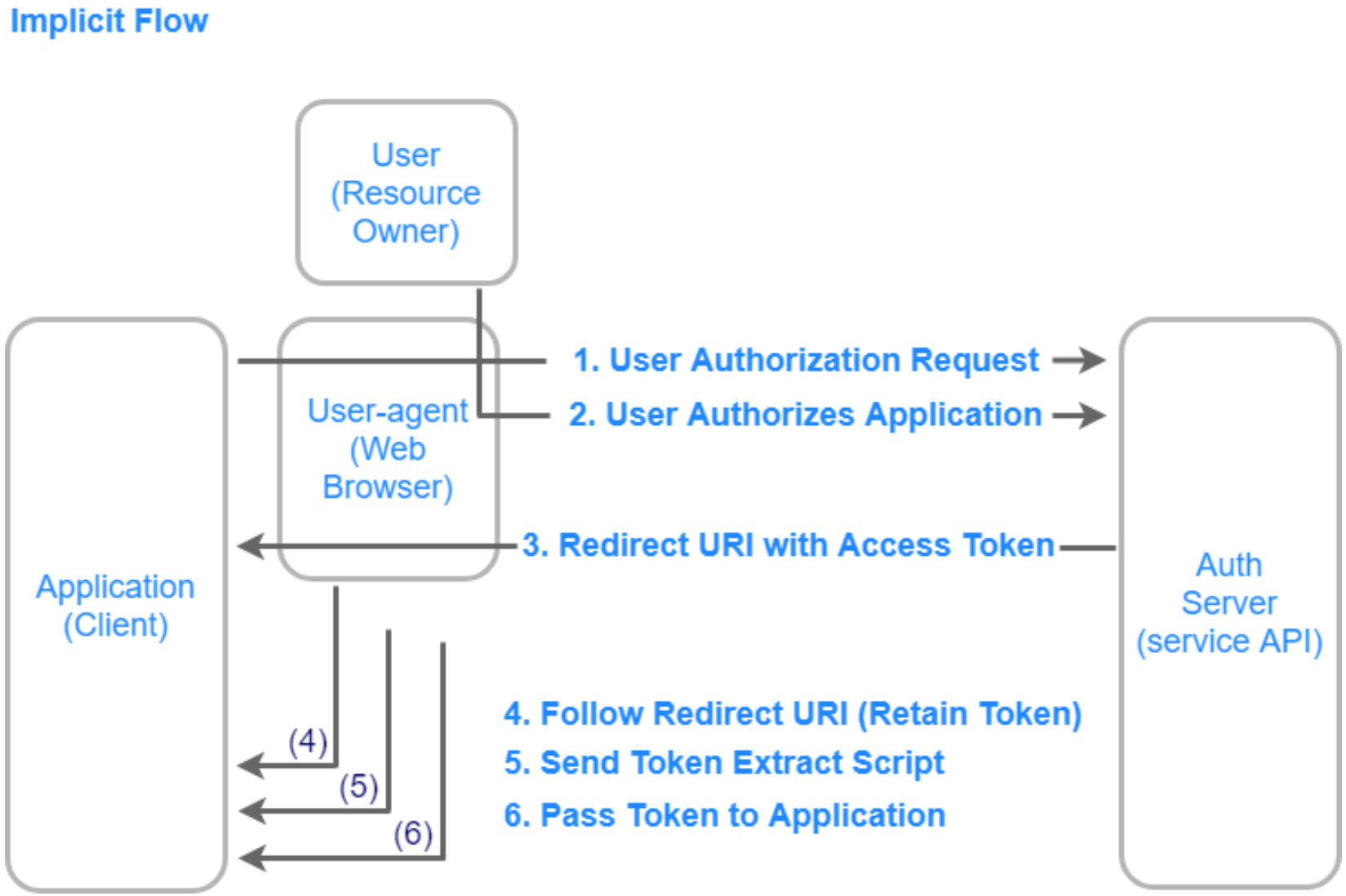
https://dropletbook.com/callback?code=AUTHORIZATION_CODE

- 4. Application requests ACCESS_TOKEN

https://cloud.digitalocean.com/v1/oauth/token?client_id=CLIENT_ID&client_secret=CLIENT_SECRET&grant_type=authorization_code&code=AUTHORIZATION_CODE&redirect_uri=CALLBACK_URL

- 5. Application receives ACCESS _ TOKEN

2. Implicit Grant Type



2. Implicit Grant Type

1. Application requests authorisation

https://cloud.digitalocean.com/v1/oauth/authorize?response_type=token&client_id=CLIENT_ID&redirect_uri=CALLBACK_URL&scope=read

2. **User Authorizes Application**

- **Step 3: User-agent Receives Access Token with Redirect URI**

https://dropletbook.com/callback#token=ACCESS_TOKEN

- **Step 4: User-agent Follows the Redirect URI**
- **Step 5: Application Sends Access Token Extraction Script**
- **Step 6: Access Token Passed to Application**

3. Grant Type: Resource Owner Password Credentials

1. Requesting a Token Based on User Credentials

https://oauth.example.com/token?grant_type=password&username=USERNAME&password=PASSWORD&client_id=CLIENT_ID

4. Grant Type: Client Credentials

1. Requesting Token Based on Application Credentials

https://oauth.example.com/token?grant_type=client_credentials&client_id=CLIENT_ID&client_secret=CLIENT_SECRET

5. Grant Type: Refresh Token

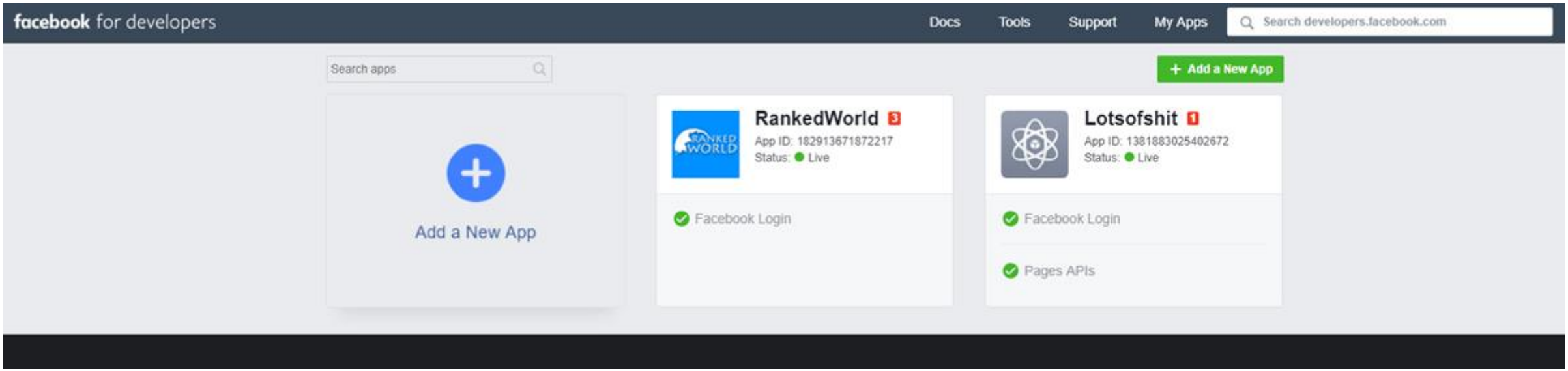
1. Requesting Token Based on a Refresh Token

https://cloud.digitalocean.com/v1/oauth/token?grant_type=refresh_token&client_id=CLIENT_ID&client_secret=CLIENT_SECRET&refresh_token=REFRESH_TOKEN

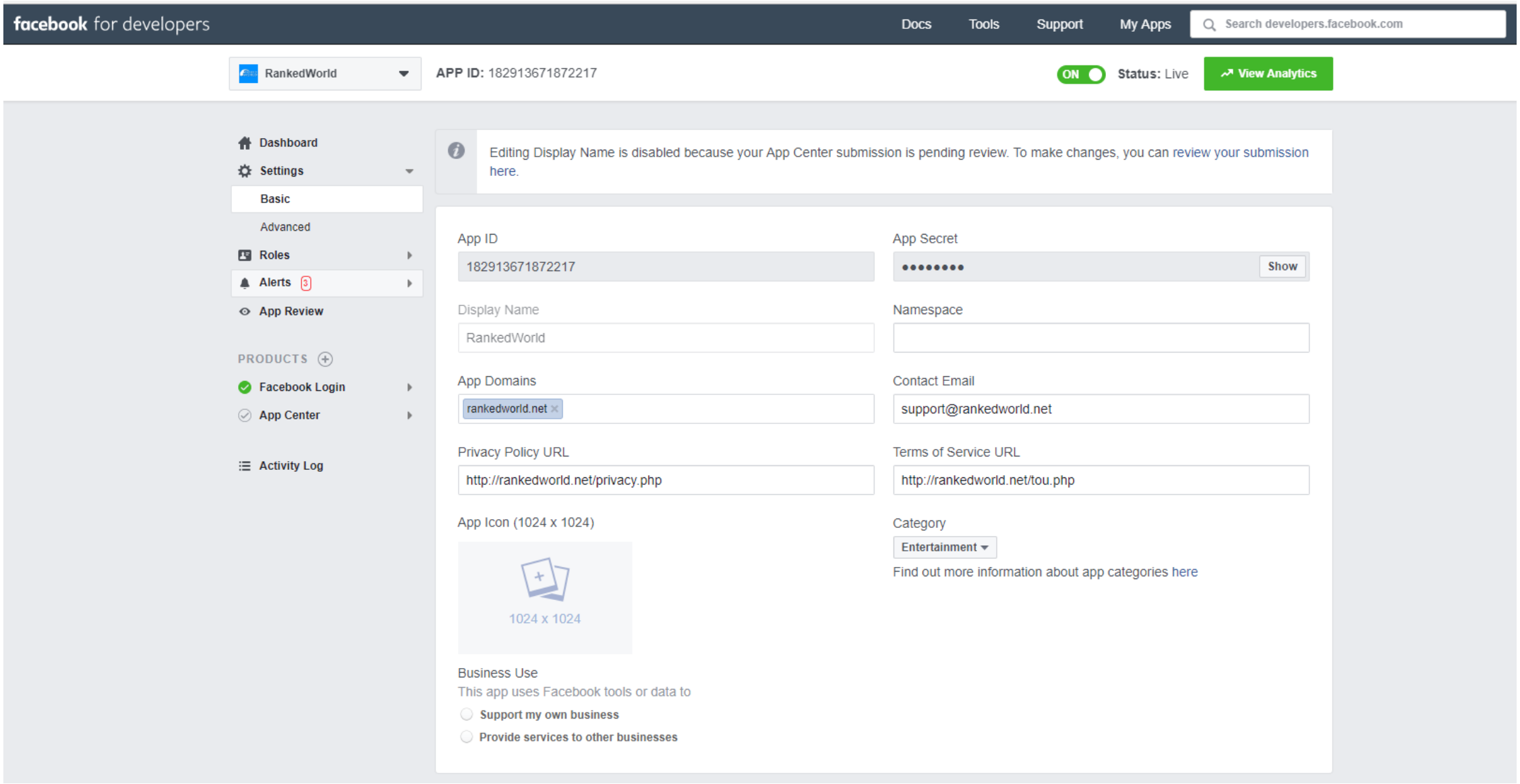
facebook APP Configuration

1. Facebook APP Creation
2. Set Redirect URL
3. Facebook APP Configuration

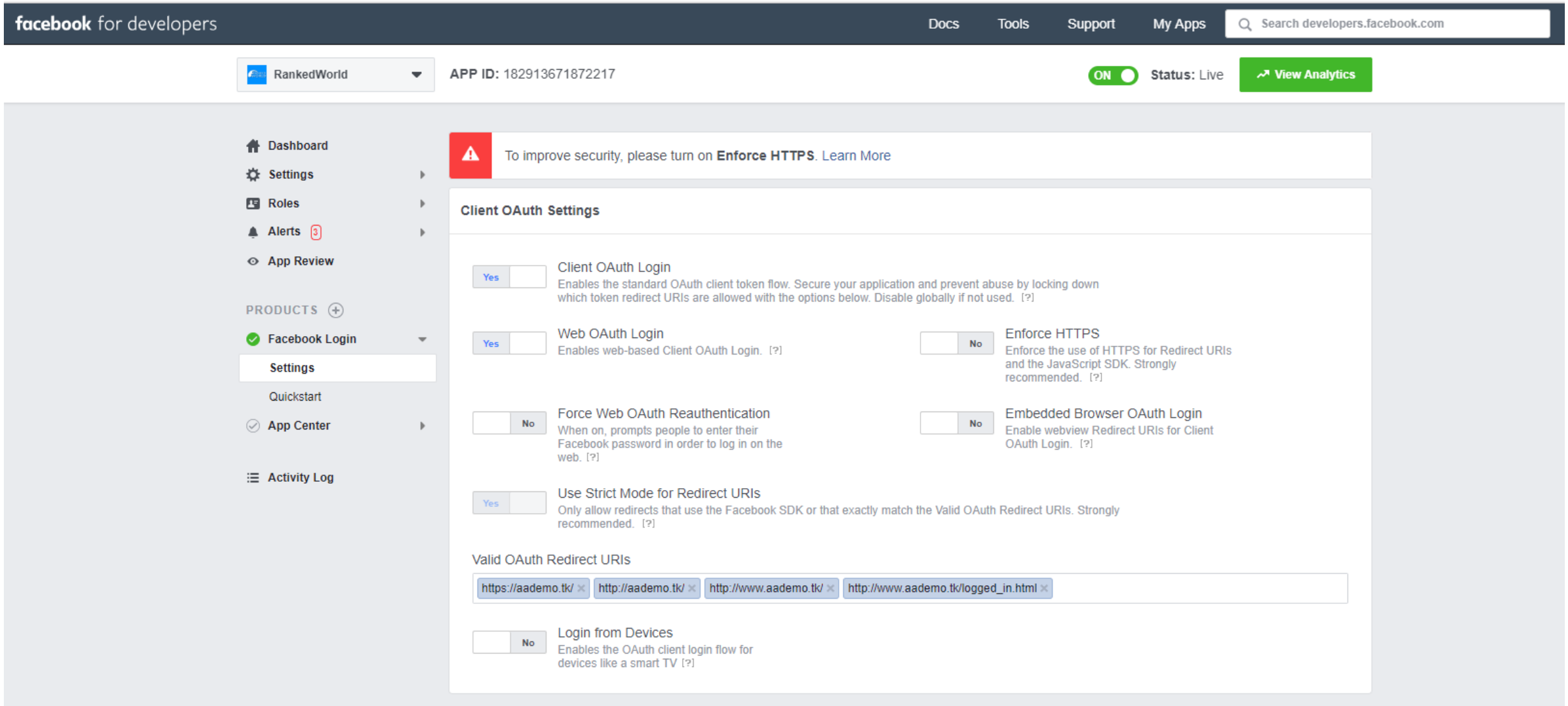
1. Facebook APP Creation



2. Check Basic Information



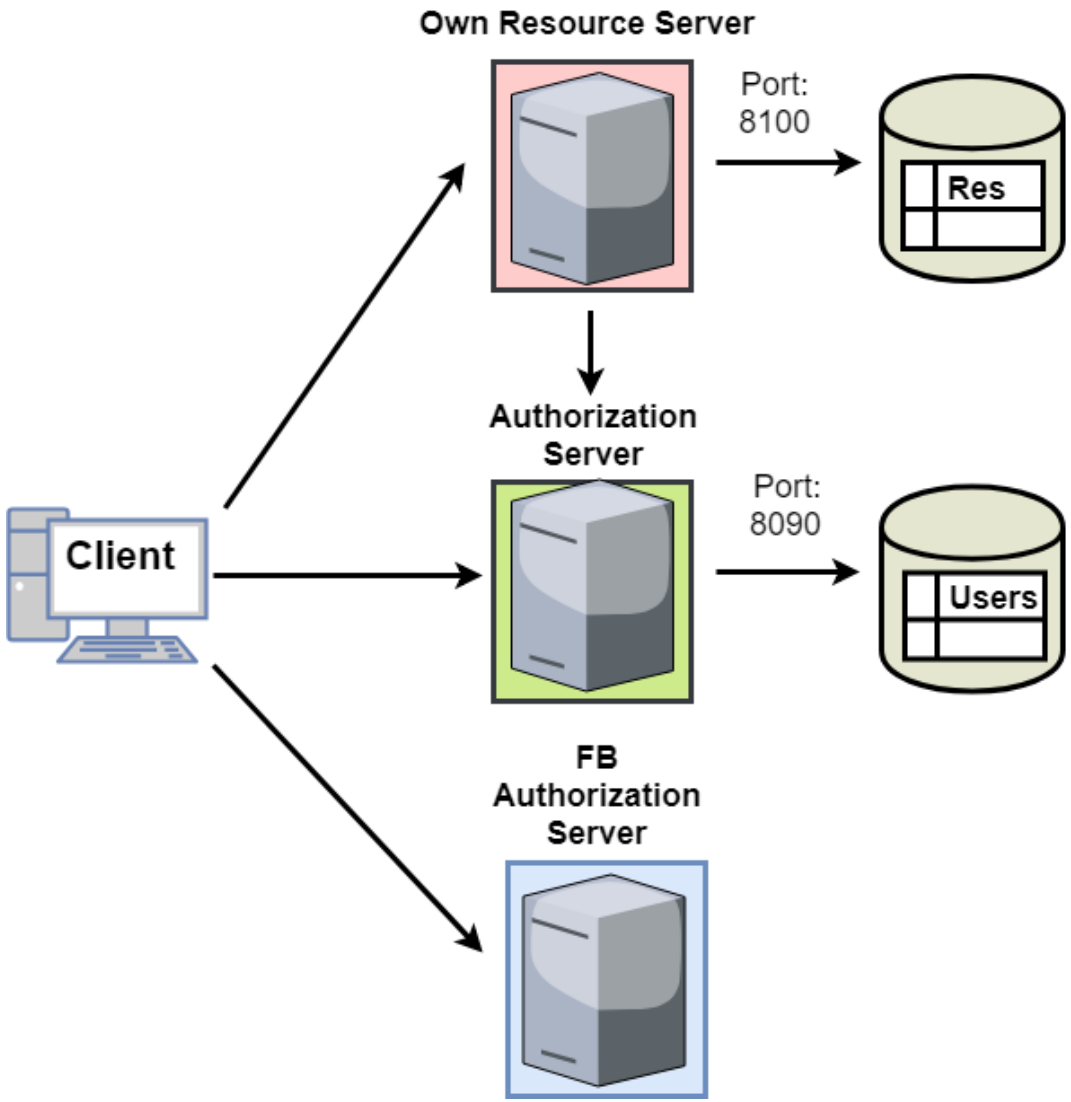
3. Facebook APP Configuration



OAuth MicroService Architecture Integration

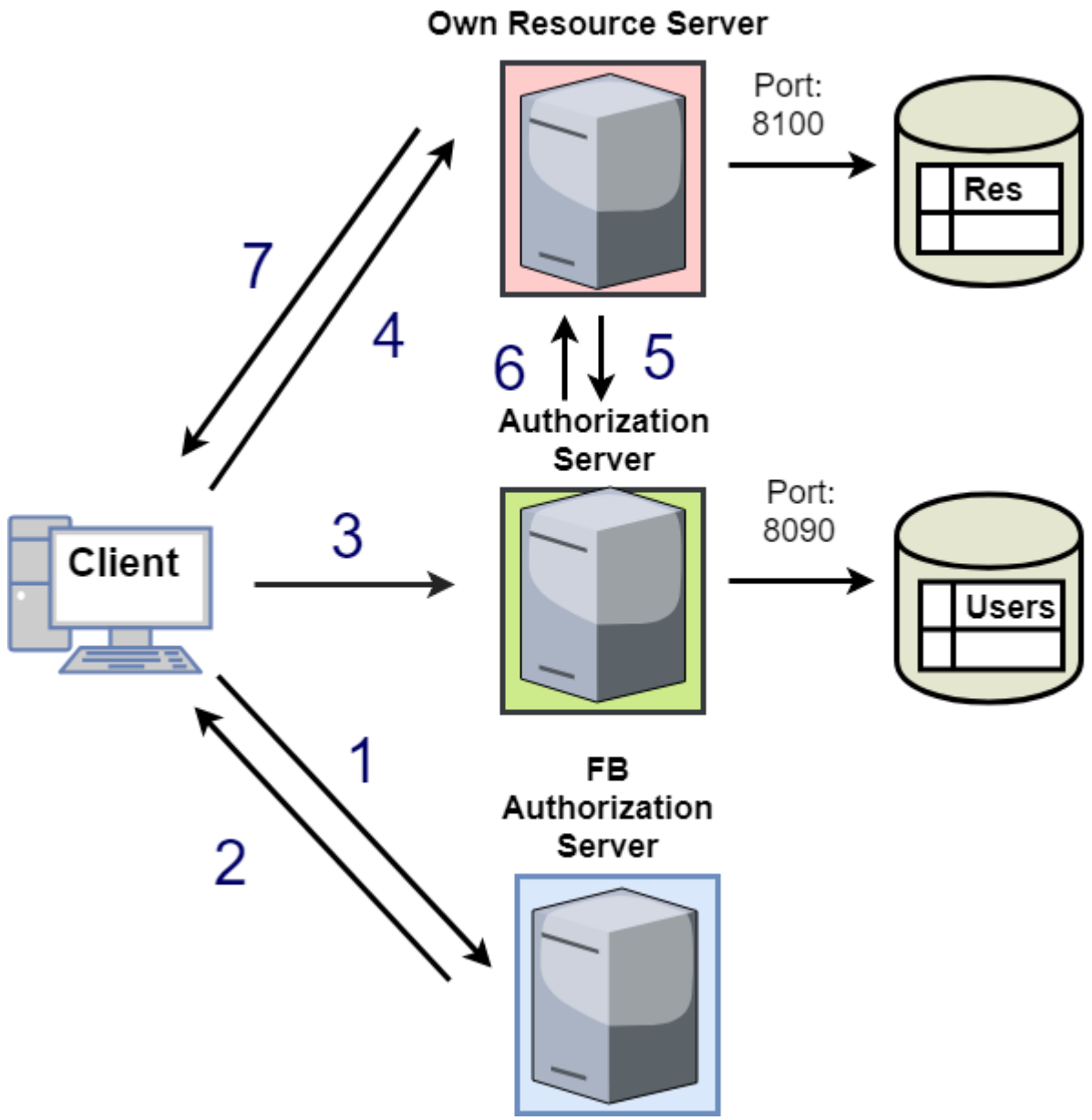
1. General Overview
2. Implicit Flow
3. Authorization Code Flow

1. General Overview



2. Implicit Flow

1. Access Token Request
2. User Receives Access Token
3. Client Registers User
4. Client Requests Resource
5. Resource Server Checks Token
6. Authorization Server Responds
7. User Receives Resource

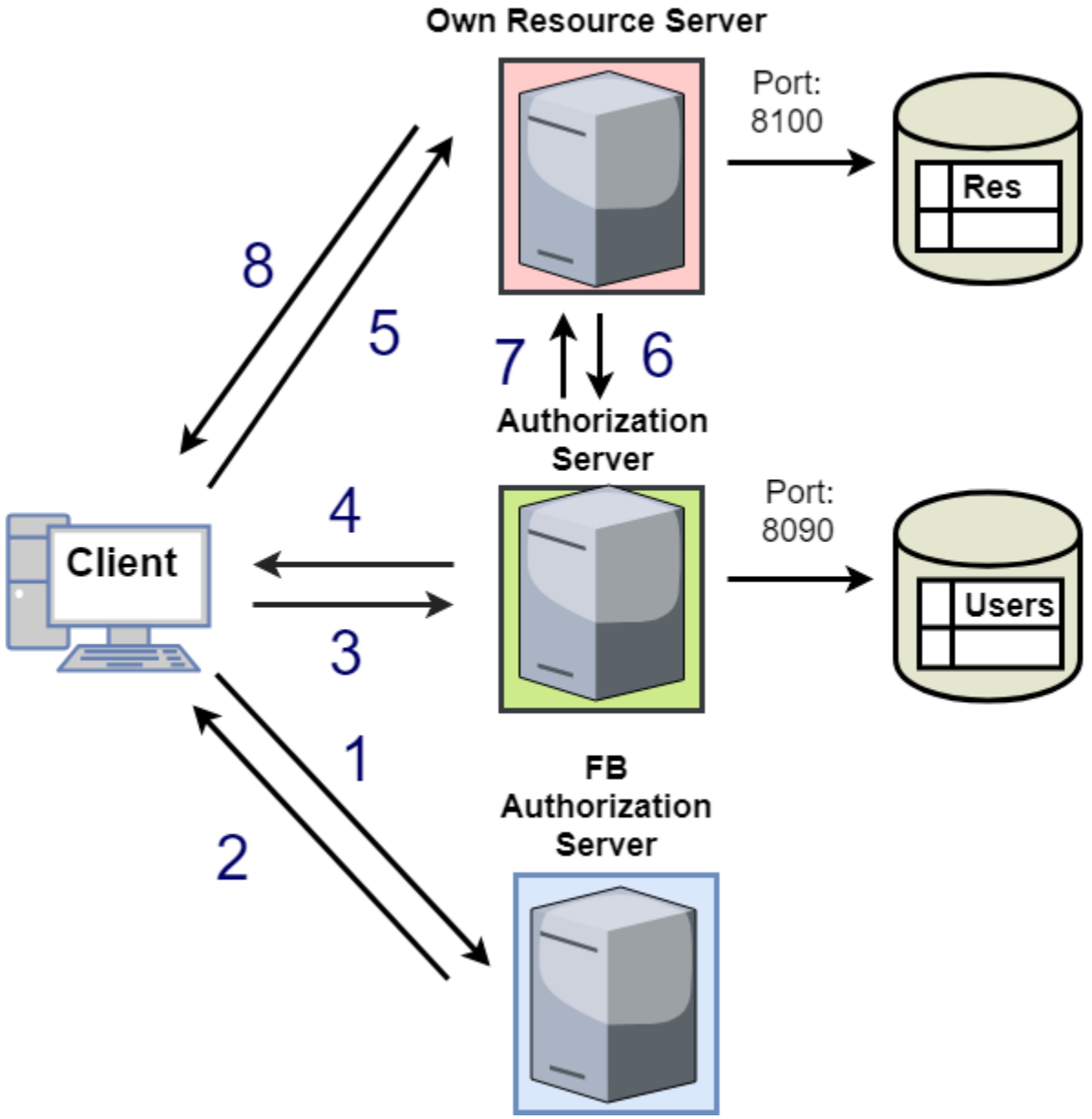


3. Authorization Code Flow

1. Authorization Code Request
2. User Receives Authorization Code
3. Client Sends Auth Code

(in the Background Code -> Token)

4. Client Receives App Token
5. Client Requests Resource
6. Resource Server Checks Token
7. Authorization Server Responds
8. User Receives Resource



Auth Code – Access Token Exchange

- Request Authorization Code
- var facebookAuthEndpoint = “https://www.facebook.com/v2.10/dialog/oauth” +

```
"? response_type= code " +
"& client_id= 182913671872217 " +
"& redirect_uri= http://www.aademo.tk/logged_in.html” +
+ "& scope= public_profile user_friends”;
```

- Request Access Token
- var userEndpoint = "https://graph.facebook.com/v2.10/oauth/access_token?" +

```
"client_id=1829136718722217&" +
"redirect_uri=http://www.aademo.tk/logged_in.html&" +
"client_secret=b6b84d379d3d5006ecaf0eb2dd6f0cac&" +
"code=" + code;
```

Demo

http://www.aademo.tk

Thank You!

- Resources used:
  - https://www.digitalocean.com/community/tutorials/an-introduction-to-oauth-2
  - https://dzone.com/articles/oauth2-implicit-grant-flow-example-using-facebook
  - https://developers.facebook.com/docs/php/howto/example_retrieve_user_profile
  - https://developers.facebook.com/docs/facebook-login/access-tokens
  - https://developers.facebook.com/docs/facebook-login/manually-build-a-login-flow
- Resources Created
  - https://github.com/kkocs/OAuth2_Demo