

Mon Compte Mobilité

Configuration du Financeur MOB

# 

# Introduction au document

Ce document décrit les étapes à suivre nécessaires à la configuration d’un client pour un financeur ayant choisi d’utiliser la plateforme moB afin que le traitement des souscriptions à ses aides soit réalisé directement dans l’application MOB, par ses gestionnaires/superviseurs.

Les grandes étapes sont :

* Enregistrement d’un client confidentiel dans le fournisseur d’identité de moB

Seuls les paramètres indiqués sont à saisir (attention à la casse).

Les paramètres non listés sont ceux par défaut.

## Client Keycloak

Ce type de client OIDC est plutôt à destination des applications Backend. Il correspond à un compte de service.

Il permet le flux « Authorization Code Flow », le flux « Client Credentials » et de récupérer un jeton de longue durée (si demandé).

A la création, l’équipe MCM renseigne notamment le client ID et génère un client secret.

Une fois créée, le client ID et le client secret sont alors communiqués de façon sécurisée par l’équipe MCM au partenaire financeur.

## Informations requises

On note pour la suite les variables ci-dessous.

|  |  |  |
| --- | --- | --- |
| Nom variable | Description | Exemple |
| *FUNDER\_NAME* | nom du financeur (Entreprise/Collectivité) s’interfaçant avec MOB | fnogec |
| *Entreprises* | Liste des entreprises financeur |  |

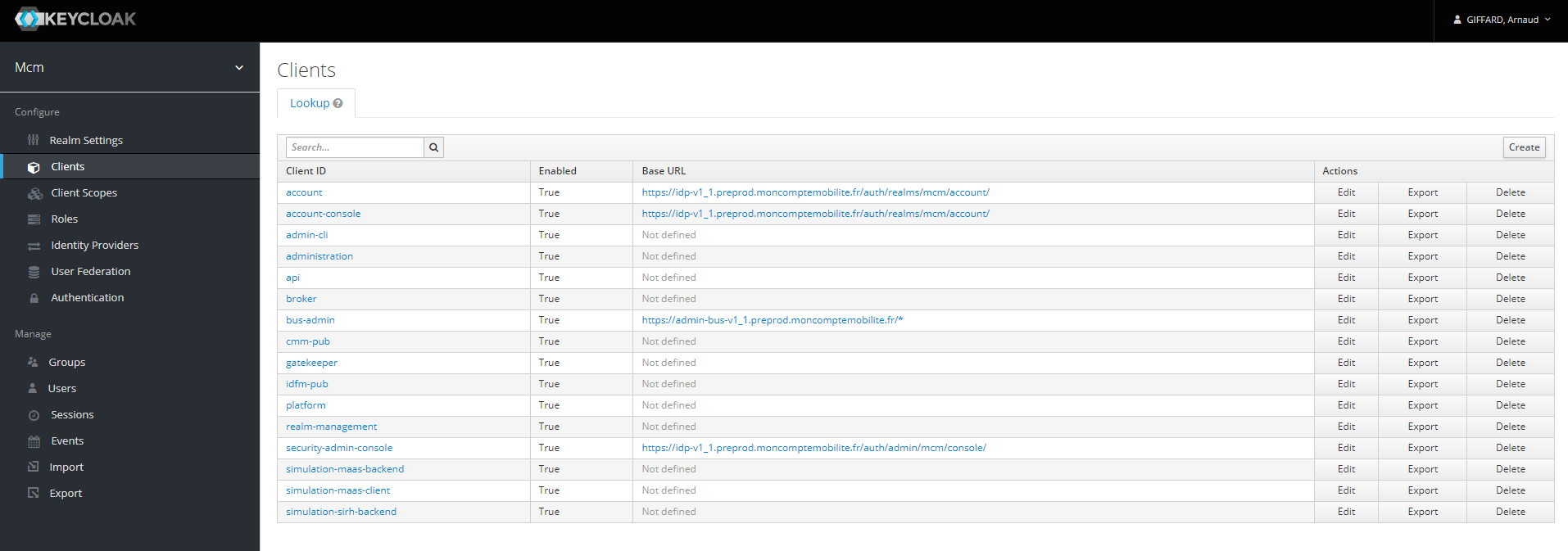
# Keycloak

## Client SIRH

### Client confidentiel

Dans cette section, on va s’intéresser à la création du client keycloak confidentiel qui sera utilisé par le Key Manager du financeur pour obtenir un jeton d’accès valide qui lui donnera accès à l’API /.

Dans l’onglet Clients cliquer sur « Create ».



#### Ecran Add Client

**Client ID** : *FUNDER\_NAME*-backend (ex. fnogec-backend)

**Client Protocol :** openid-connect



Cliquer sur Save.

#### Onglet Settings

**Client Id** : *FUNDER\_NAME*-backend (ex. fnogec-backend)

**Name** : Key Manager *FUNDER\_NAME* (ex. Key Manager FNOGEC)

**Enabled** : ON

**Client protocol** : openid-connect

**Access type** : confidential

**Direct access grants enabled** : OFF

**Service account enabled** : ON

**Valid Redirect UrIs** : \*

Cliquer sur Save.

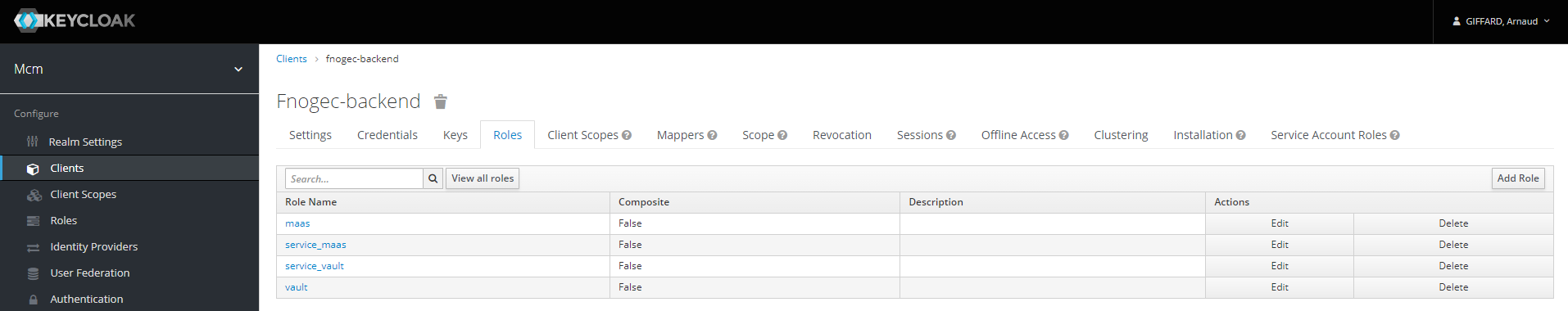
#### Onglet Credentials

Il faut récupérer le secret et le transmettre au financeur pour que son Key Manager puisse se connecter à notre fournisseur d’identité.

#### Onglet Roles

Dans cet onglet, il faut ajouter les rôles avec les noms suivants (attention à la casse) :

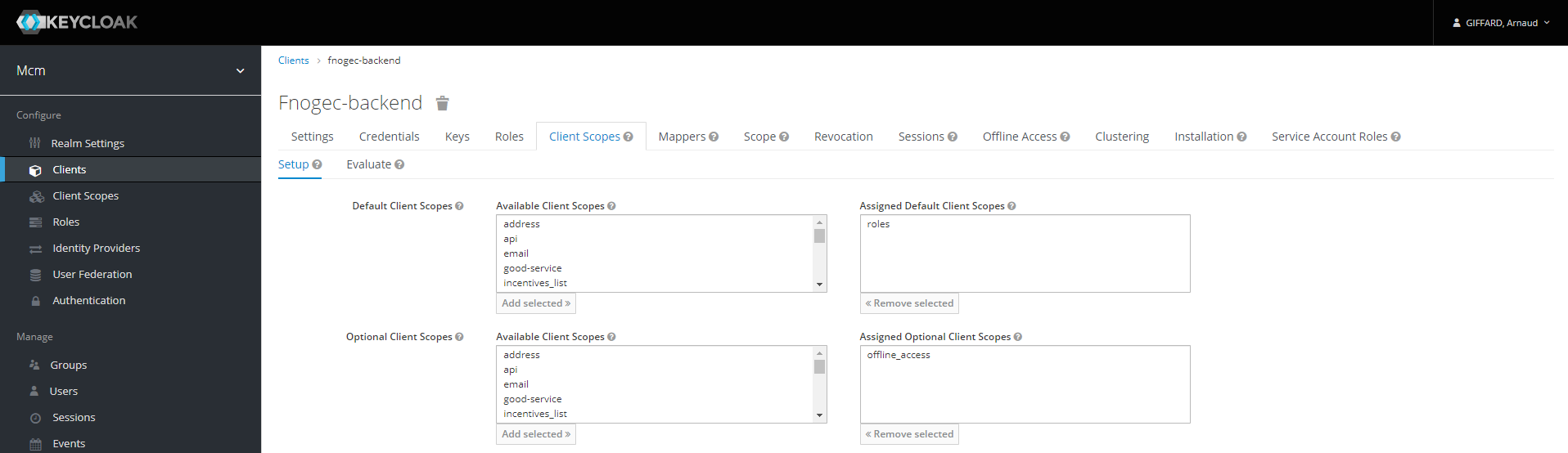
* *vault*
* *service\_vault*



#### Onglet Client Scopes

Dans cet onglet, il faut retirer les rôles non nécessaires. Le client doit avoir les scopes suivants :

* Default client scopes
  + roles
  + funders-clients (pour le rendre accessible dans l’écran de création d’une entreprise, à retirer par la suite)
* Assigned optional scopes
  + offline\_access



#### Onglet Mappers

Dans cet onglet, il faut ajouter/modifier 2 mappers avec la configuration ci-dessous.

##### vault\_name

Cliquer sur Create.

**Name** : vault\_name

**Mapper type** : Hardcoded claim

**Token claim name** : vault\_name

**Claim value** : *FUNDER\_NAME-backend*

**Claim json type** : String

**Add to ID token** : OFF

**Add to access token** : ON

**Add to userinfo** : OFF

Cliquer sur Save.

##### vault\_role

Cliquer sur Create.

**Name** : vault\_role

**Mapper type** : Hardcoded role

**Rôle** : sélectionner le client rôle *FUNDER\_NAME-backend*, et sélectionner le rôle *service\_vault*.

Cliquer sur Save.

##### groups

Cliquer sur Create.

**Name** : groups

**Mapper type** : Group Membership

**Token claim name** : membership

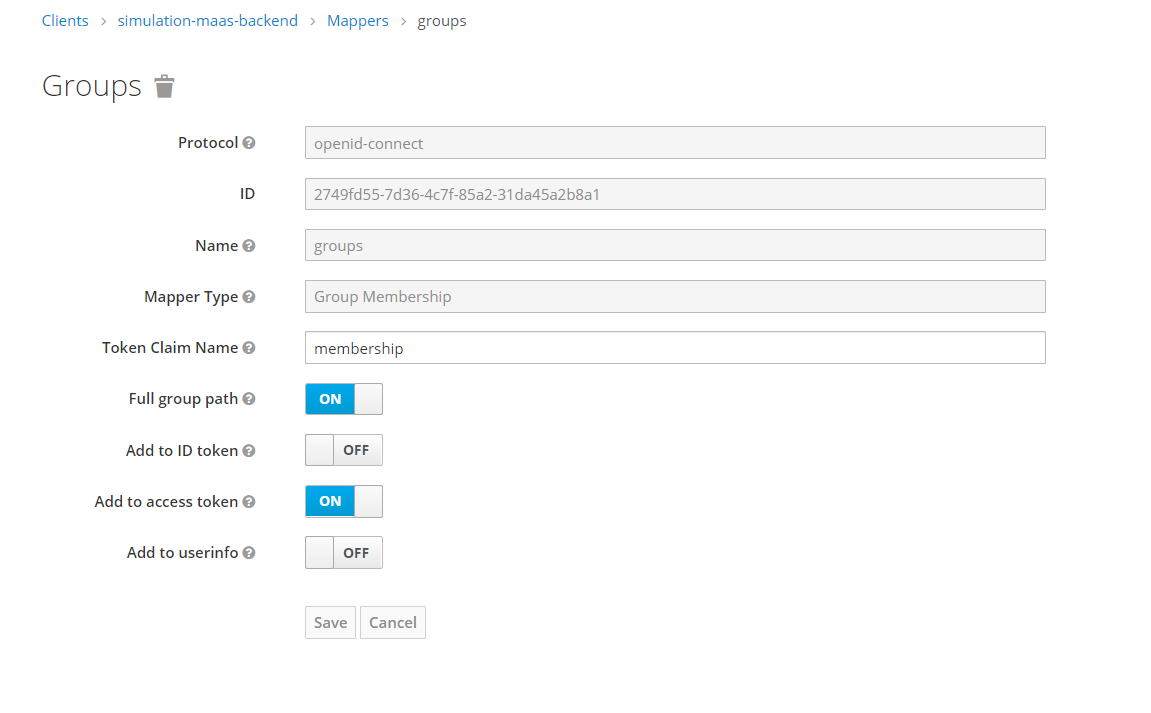
**Full group path** : ON

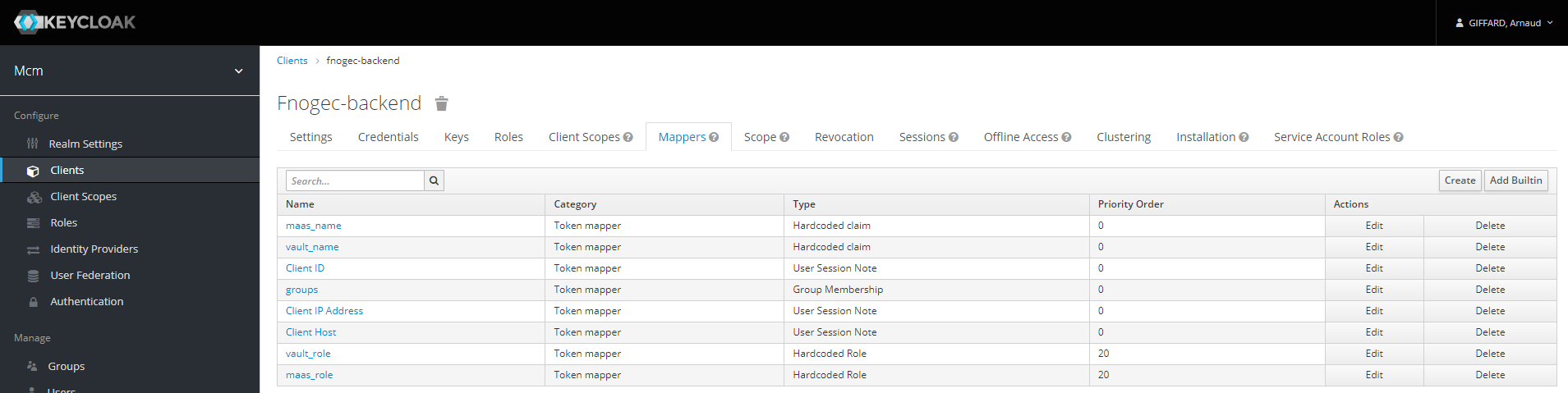
**Add to ID token** : OFF

**Add to access token** : ON

**Add to userinfo** : OFF

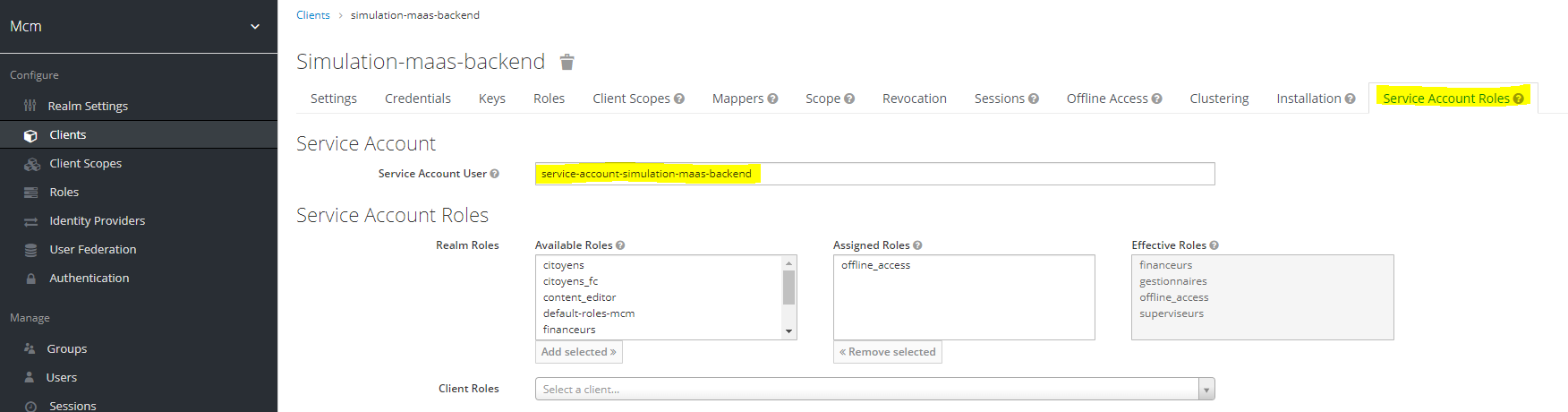
Cliquer sur Save.



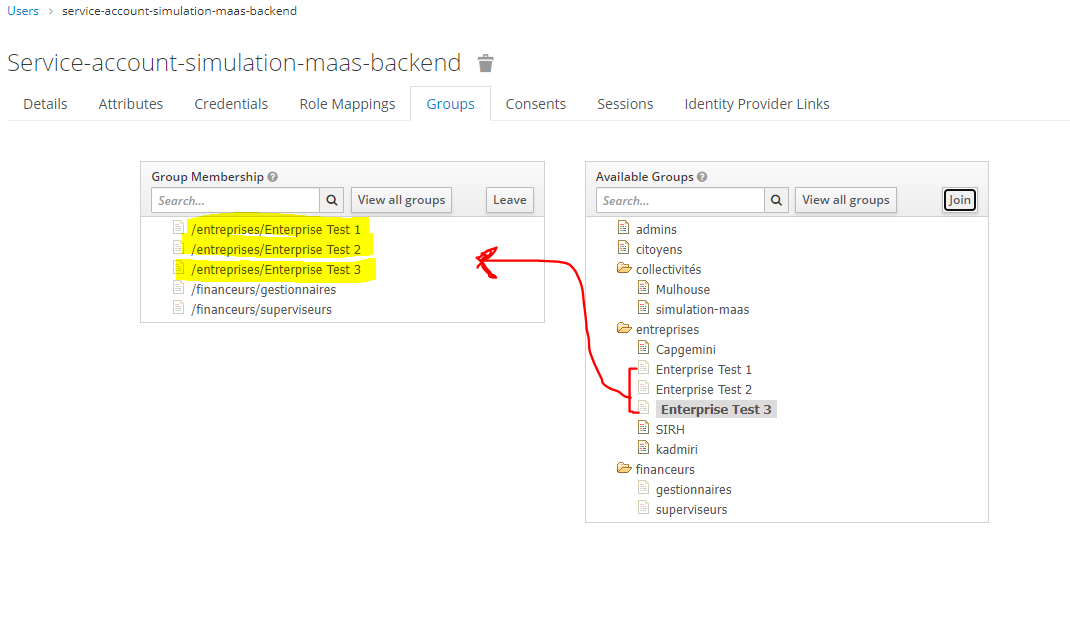


#### Onglet Service Account Roles

Dans cet onglet, cliquer sur le service account : **service-account-FUNDER\_NAME-backend**



Keycloak redirige vers une nouvelle page afin d’ajouter les **groups correspondant aux enterprises pour lesquelles ce client vault sera utilisé**. Pour chacune, la slectionner et cliquer sur Join.



## Invoquer l’API

Le fournisseur d’identités permet de donner un JWT, contenant un jeton d’accès.

Pour l’API moB, ce jeton d’accès est un Bearer Token.

Si ce jeton d’accès est expiré, il faudra demander un nouveau jeton d’accès avec les credentials liés au client (client\_id / client\_secret).