



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
<i>FUNDER_NAME</i>	nom du financeur (Entreprise/Collectivité) s'interfaçant avec MOB	fnogec
<i>Entreprises</i>	Liste des entreprises financeur	

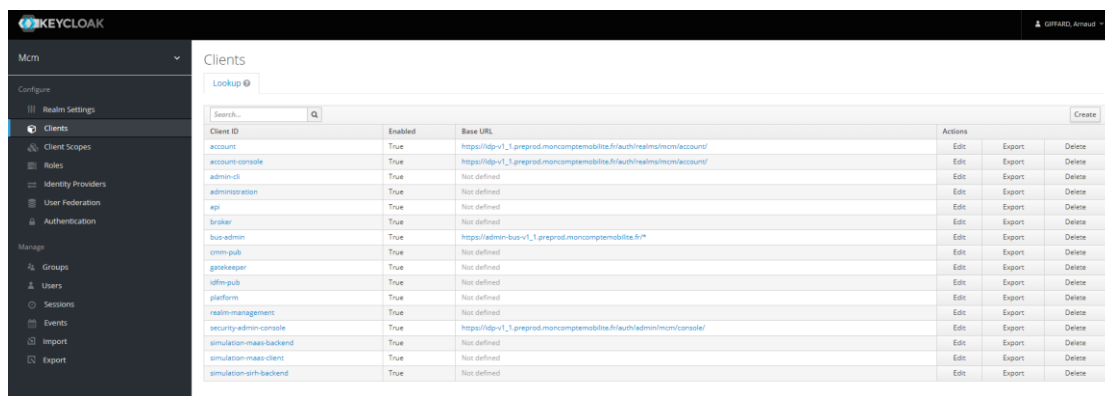
Keycloak

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 ».

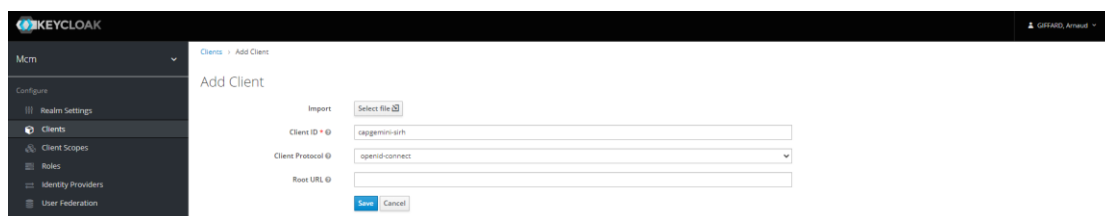


Client ID	Enabled	Base URL	Actions
account	True	https://idp-v1_1.preprod.moncomptemobilite.fr/auth/realms/mcm/account/	Edit Export Delete
account-console	True	https://idp-v1_1.preprod.moncomptemobilite.fr/auth/realms/mcm/account/	Edit Export Delete
admin-cli	True	Not defined	Edit Export Delete
admin-console	True	Not defined	Edit Export Delete
api	True	Not defined	Edit Export Delete
broker	True	Not defined	Edit Export Delete
bus-admin	True	https://admin-bus-v1_1.preprod.moncomptemobilite.fr/	Edit Export Delete
crm-pub	True	Not defined	Edit Export Delete
gatekeeper	True	Not defined	Edit Export Delete
idm-pub	True	Not defined	Edit Export Delete
platform	True	Not defined	Edit Export Delete
realtime-management	True	Not defined	Edit Export Delete
security-admin-console	True	https://idp-v1_1.preprod.moncomptemobilite.fr/auth/admin/mcm/console/	Edit Export Delete
simulation-maas-backend	True	Not defined	Edit Export Delete
simulation-maas-client	True	Not defined	Edit Export Delete
simulation-sirh-backend	True	Not defined	Edit Export Delete

Ecran Add Client

Client ID : *FUNDER_NAME*-backend (ex. fnogec-backend)

Client Protocol : openid-connect



Import

Client ID

Client Protocol

Root URL

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 Urls : *

Cliquer sur Save.

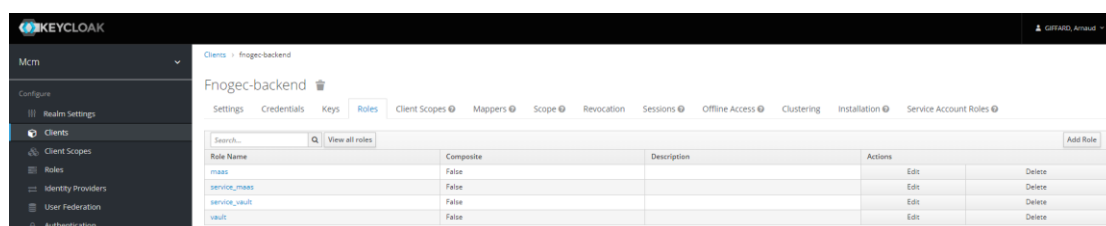
Onglet Credentials

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) :

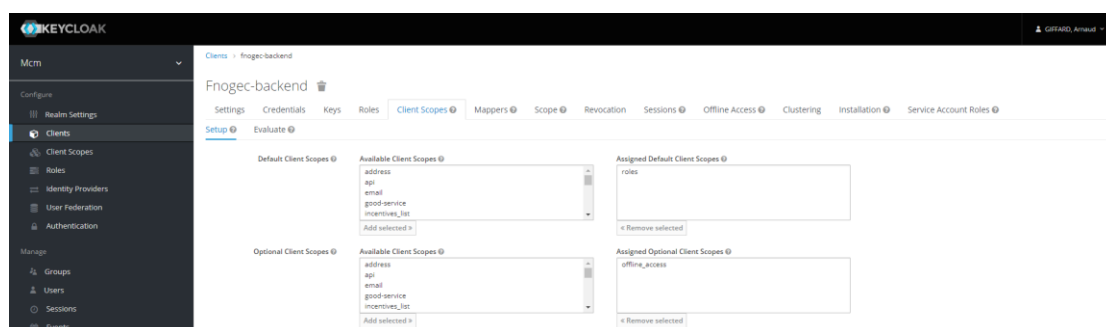
- vault
- service_vault



Onglet Client Scopes

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

- Default client scopes
 - o roles
 - o funders-clients (pour le rendre accessible dans l'écran de création d'une entreprise, à retirer par la suite)
- Assigned optional scopes
 - o 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.


[Clients](#) > [simulation-maas-backend](#) > [Mappers](#) > [groups](#)


Groups


Protocol  openid-connect


ID 2749fd55-7d36-4c7f-85a2-31da45a2b8a1


Name  groups


Mapper Type  Group Membership

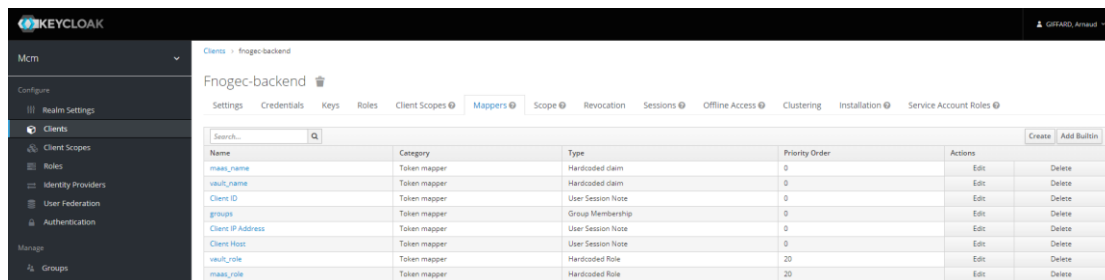
Token Claim Name  membership

Full group path  ☒ ON

Add to ID token  ☐ OFF

Add to access token  ☒ ON

Add to userinfo  ☐ OFF

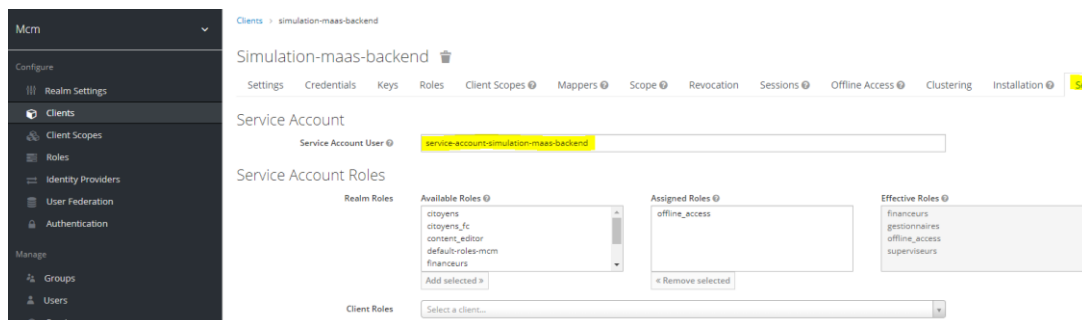


The screenshot shows the Keycloak Admin Console interface. The left sidebar contains navigation links for 'Configure' (Realm Settings, Clients, Client Scopes, Roles, Identity Providers, User Federation, Authentication) and 'Manage' (Groups, Users, Sessions). The main content area is titled 'Frogoc-backend' and shows the 'Mappers' tab. A table lists various mappers:

Name	Category	Type	Priority Order	Actions
mail_name	Token mapper	Hardcoded claim	0	Edit, Delete
vault_name	Token mapper	Hardcoded claim	0	Edit, Delete
Client ID	Token mapper	User Session Note	0	Edit, Delete
groups	Token mapper	Group Membership	0	Edit, Delete
Client IP Address	Token mapper	User Session Note	0	Edit, Delete
Client Host	Token mapper	User Session Note	0	Edit, Delete
vault_role	Token mapper	Hardcoded Role	20	Edit, Delete
mail_role	Token mapper	Hardcoded Role	20	Edit, Delete

Onglet Service Account Roles

Dans cet onglet, cliquer sur le service account : **service-account-FUNDER_NAME-backend**



The screenshot shows the 'Service Account Roles' configuration page for the 'simulation-maas-backend' client. The 'Service Account User' is set to 'service-account-simulation-maas-backend'. The 'Service Account Roles' section displays:


- Realm Roles:** A list of available roles including 'citoyens', 'citoyens_fc', 'content_editor', 'default-roles-mcm', and 'financeurs'. The 'Add selected >' button is visible.
- Assigned Roles:** A box containing the 'offline_access' role. The '< Remove selected' button is visible.
- Effective Roles:** A box showing the resulting roles: 'financeurs', 'gestionnaires', 'offline_access', and 'superviseurs'.


At the bottom, there is a 'Client Roles' dropdown menu with the text 'Select a client...'.


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


Service-account-simulation-maas-backend


Details Attributes Credentials Role Mappings **Groups** Consents Sessions Identity Provider Links


Group Membership 





 /entreprises/Enterprise Test 1


 /entreprises/Enterprise Test 2


 /entreprises/Enterprise Test 3


 /financeurs/gestionnaires


 /financeurs/superviseurs


Available Groups 





 admins


 citoyens


 collectivités


 Mulhouse


 simulation-maas


 entreprises


 Capgemini


 Enterprise Test 1


 Enterprise Test 2


 **Enterprise Test 3**

 SIRH

 kadmiri

 financeurs

 gestionnaires

 superviseurs

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).