Portainer - Configuration SSO Oauth avec keycloak

Difficulté : Confirmé

Notions : Authentification, SSO

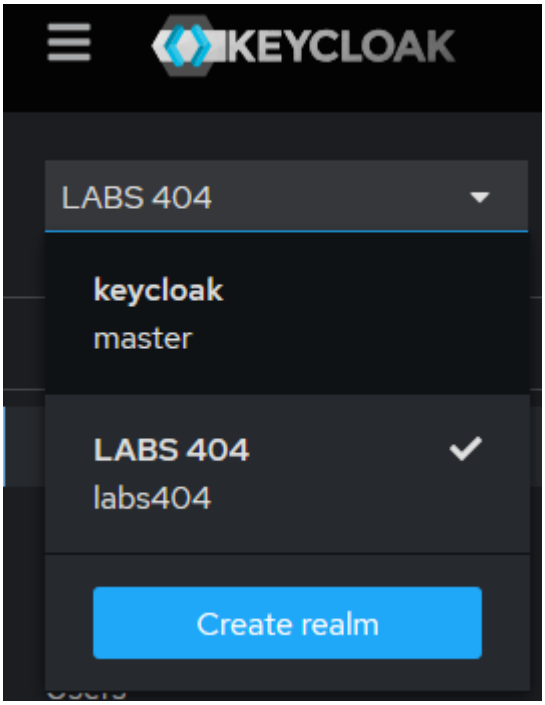
I. Introduction

Cette procédure à pour but d'expliquer le paramétrage de l'authentification SSO de portainer avec Keycloak.

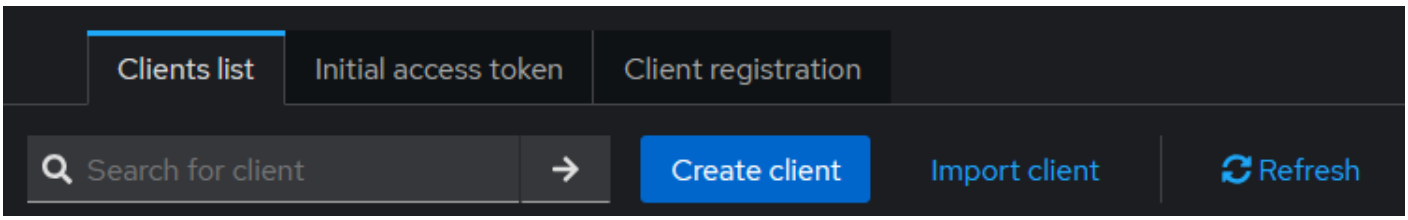
II. Côté Keycloak

2.1 Créer le client

Se connecter au keycloak et choisir le realm sur lequel ajouter le client portainer.



Cliquer sur '***Create client***'



Sélectionner le type '***OpenID Connect***'

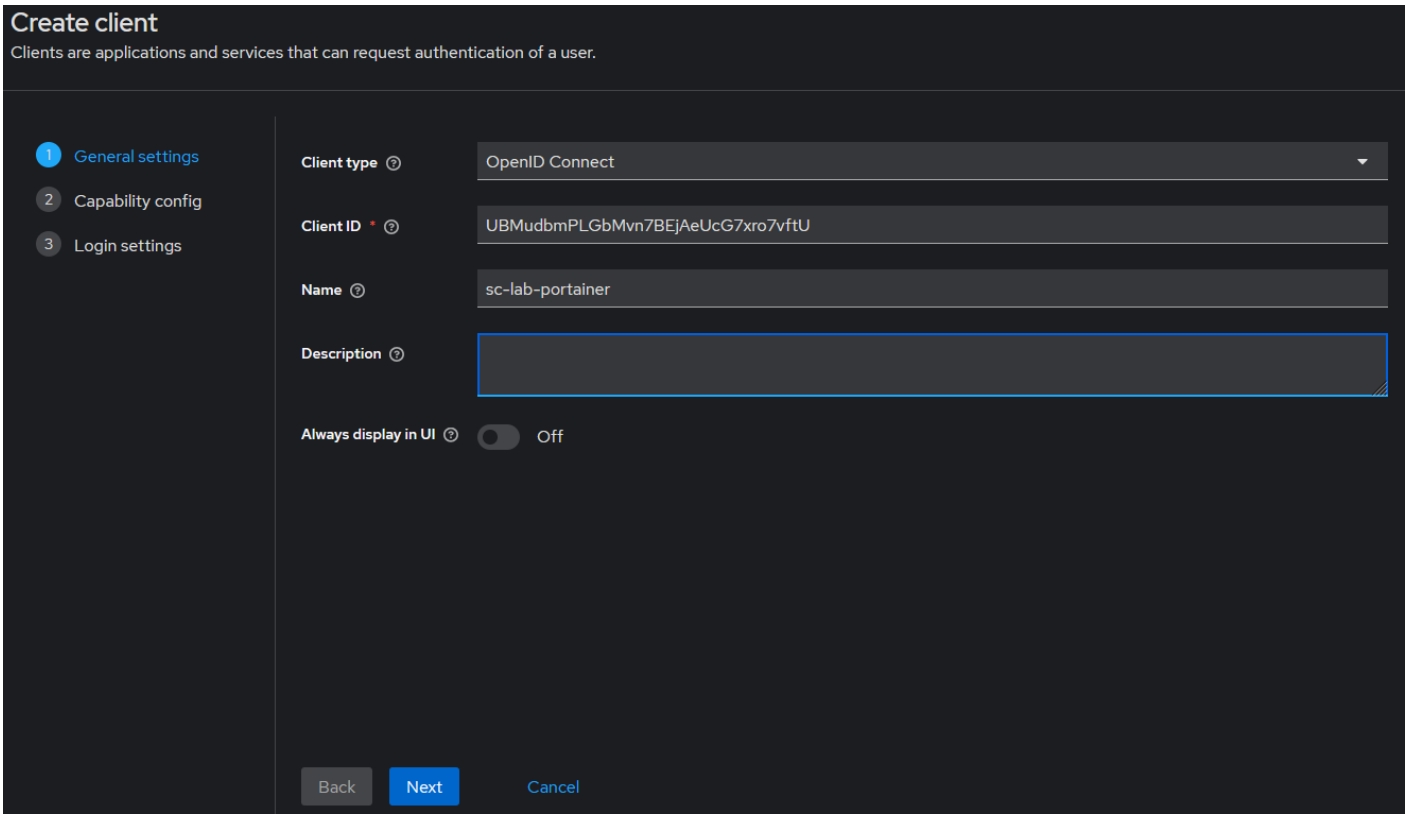
Générer ou définir un '***clientID***'.

> *Il est possible d'utiliser un générateur afin de générer un e chaîne de 32 caractères. Par exemple : ici.*

> **Best Practice** *: 32 caractères avec minuscules, majuscules et chiffres.*

Choisir un nom parlant.

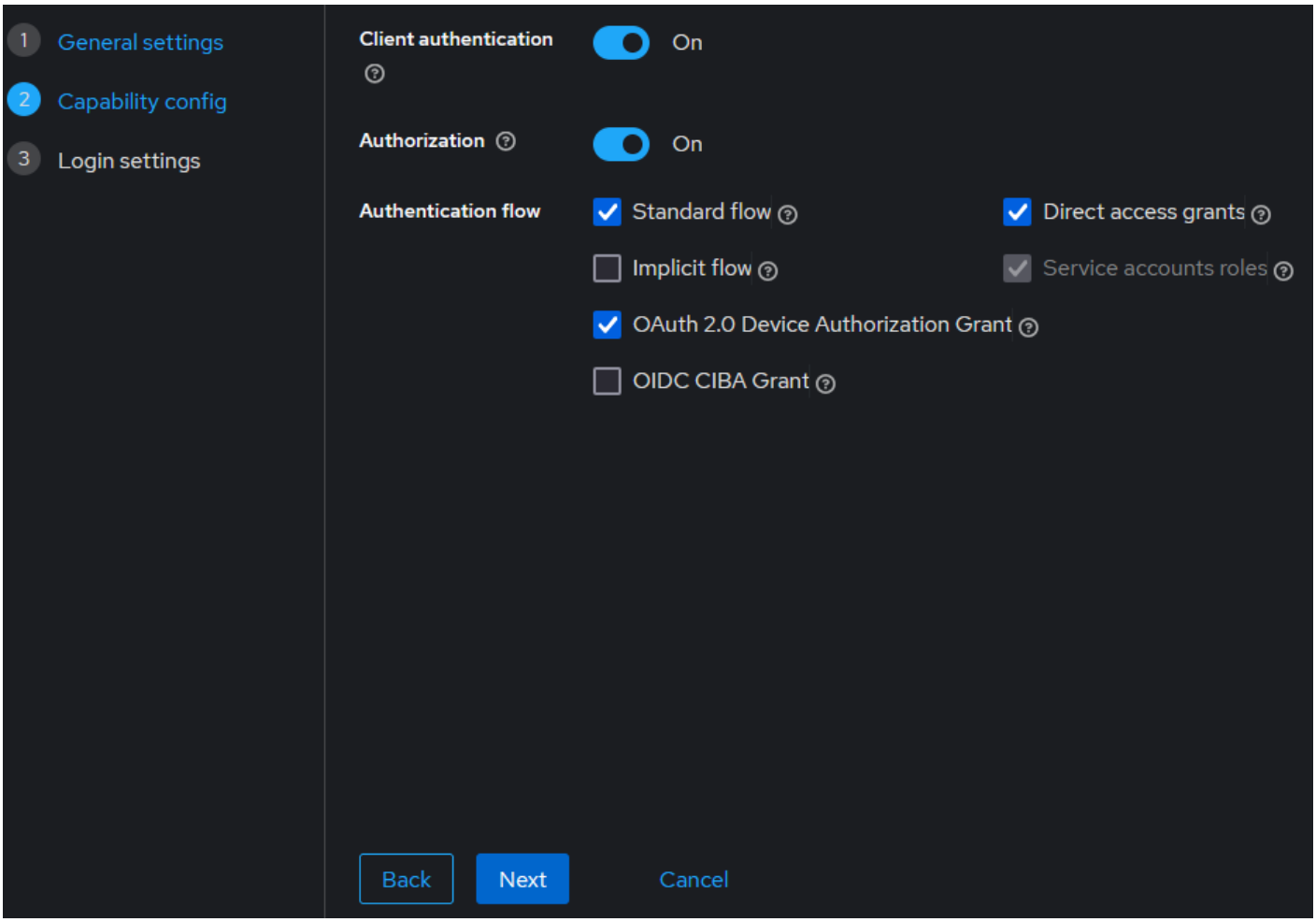
Puis faire '***Next***'.



Sur la page suivante, activer '***Client authentication***' et '***Authorization***'.

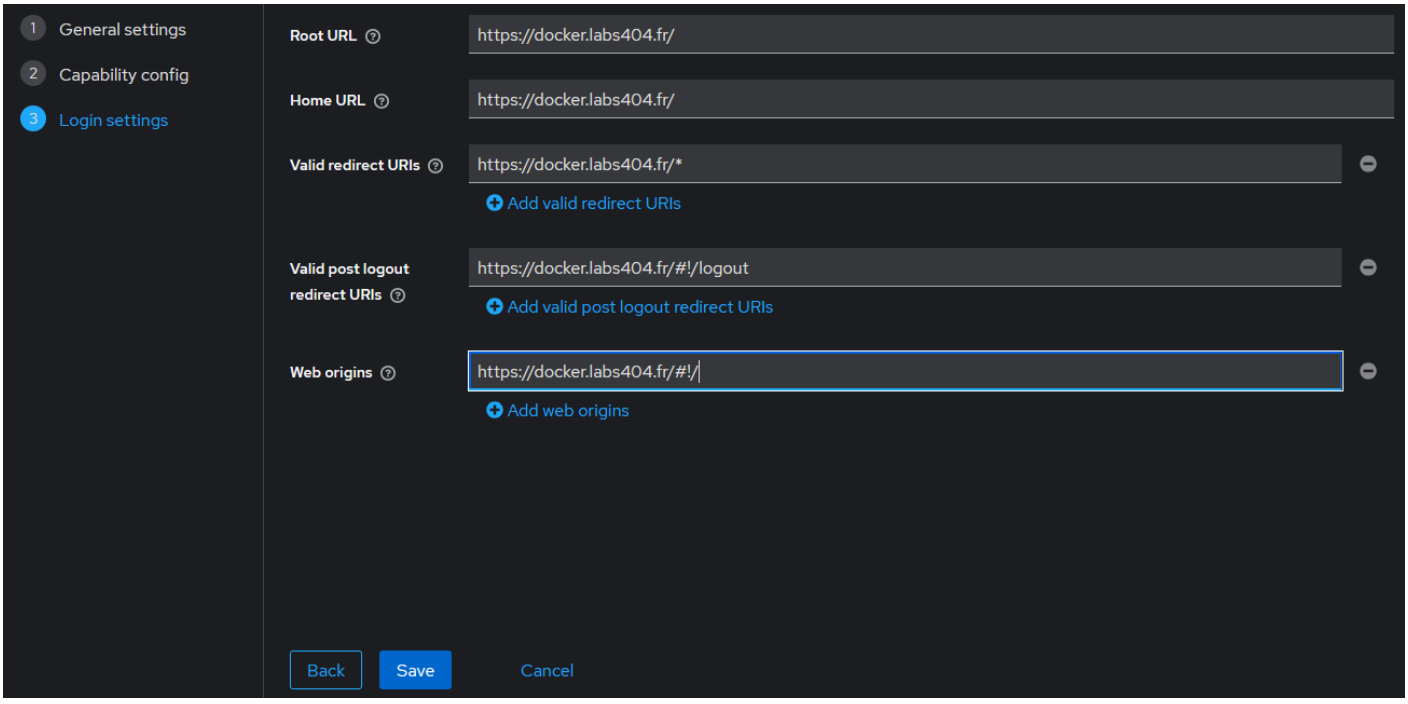
Vérifier que les cases suivantes sont cochées.

Puis faire '***Next***'.



Entrer les URL au format suivant (en modifiant les FQND).

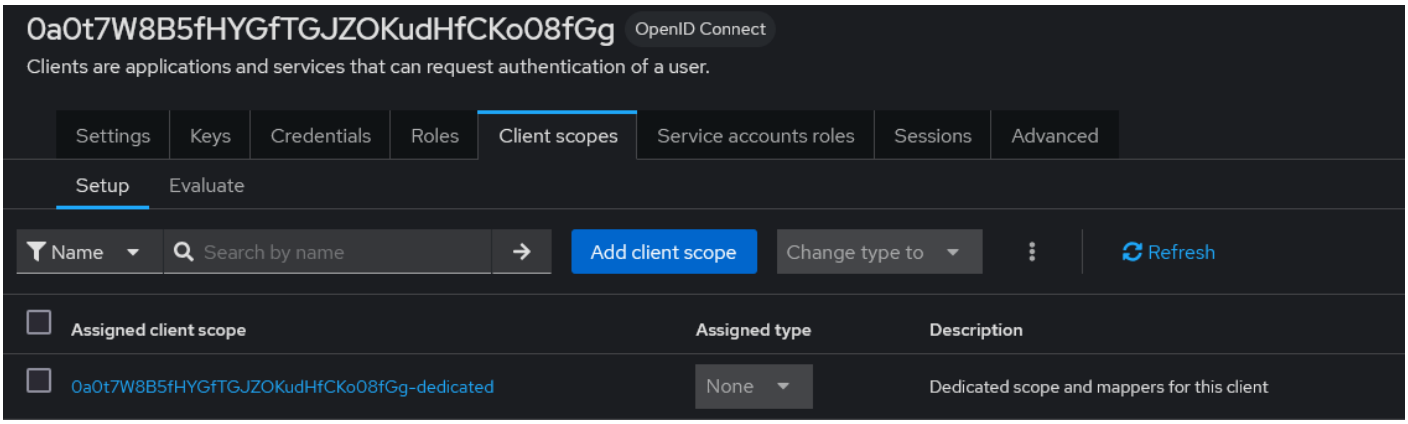
Puis faire '***Save***'.



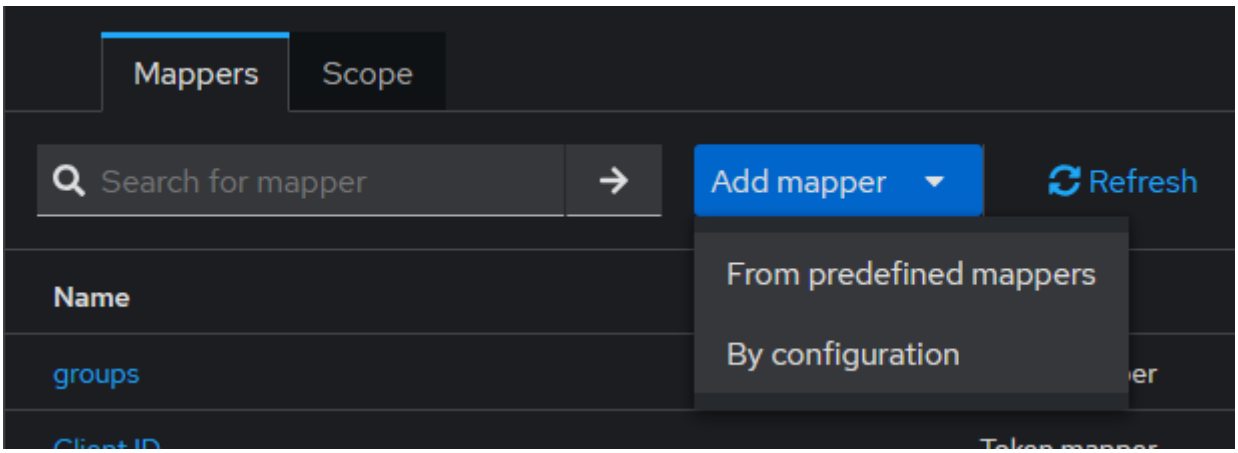
2.2 Préparer la synchro des groupes

Afin de pouvoir gérer les droits depuis le keycloak et synchroniser les groupes, aller dans l'onglet '***Client scope***'.

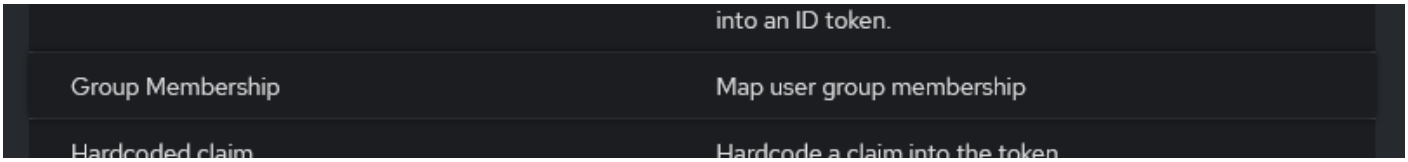
Choisir le client scope au nom du client suivi de '***-dedicated***'.



Faire '***Add Mapper***' puis '***By Configuration***'.



Choisir '***Group Membership***'.

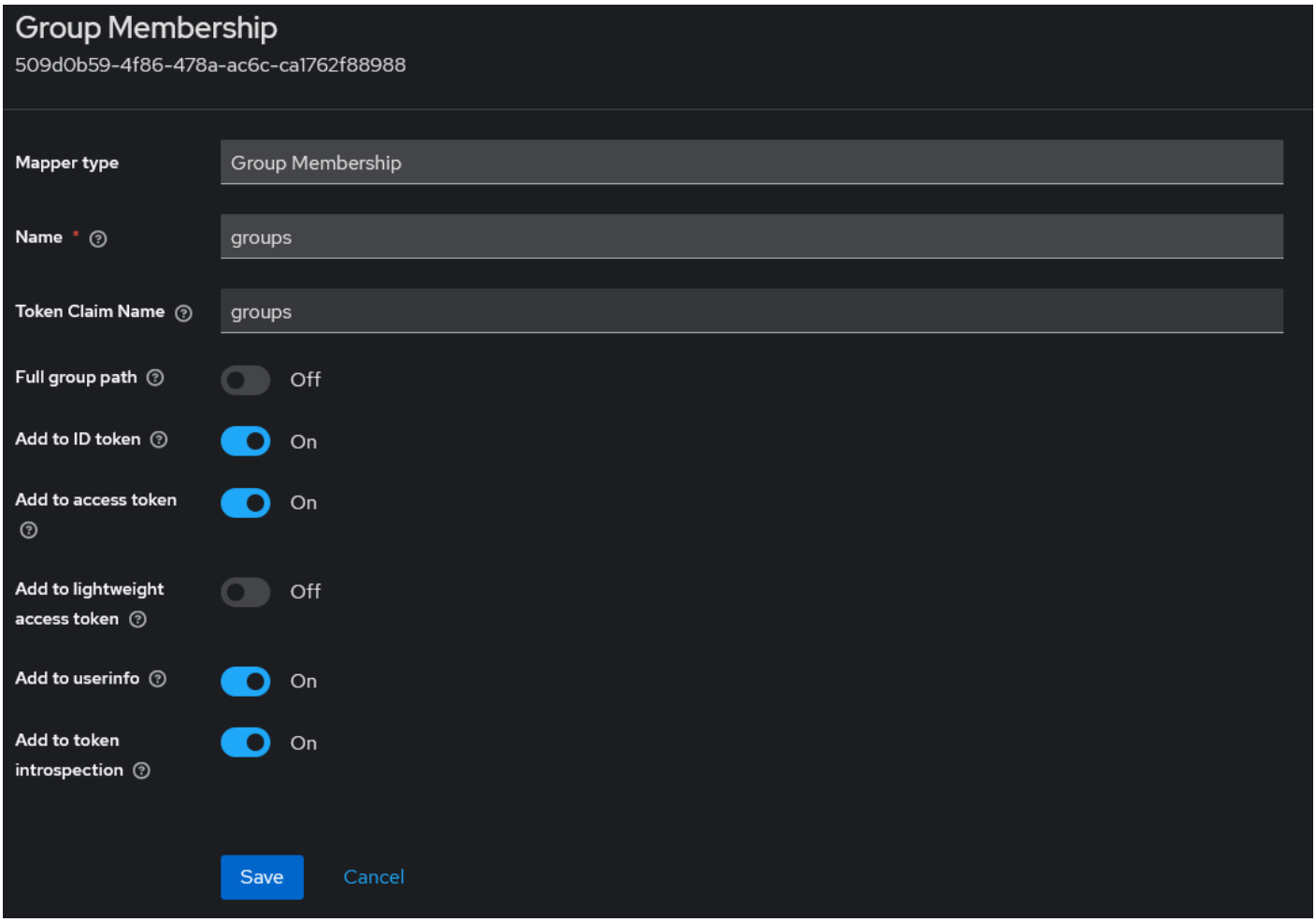


Définir le nom du ***mapper*** en '***groups***'.

Définir le Token ***claim name*** en '***groups***'.

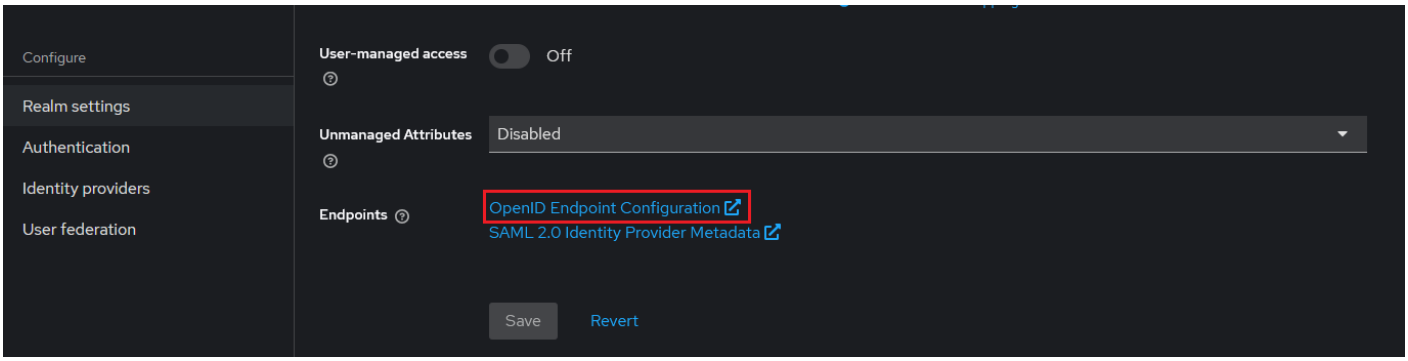
Vérifier que les fonctions suivantes soit activées / désactivées.

Puis faire '***Save***'.

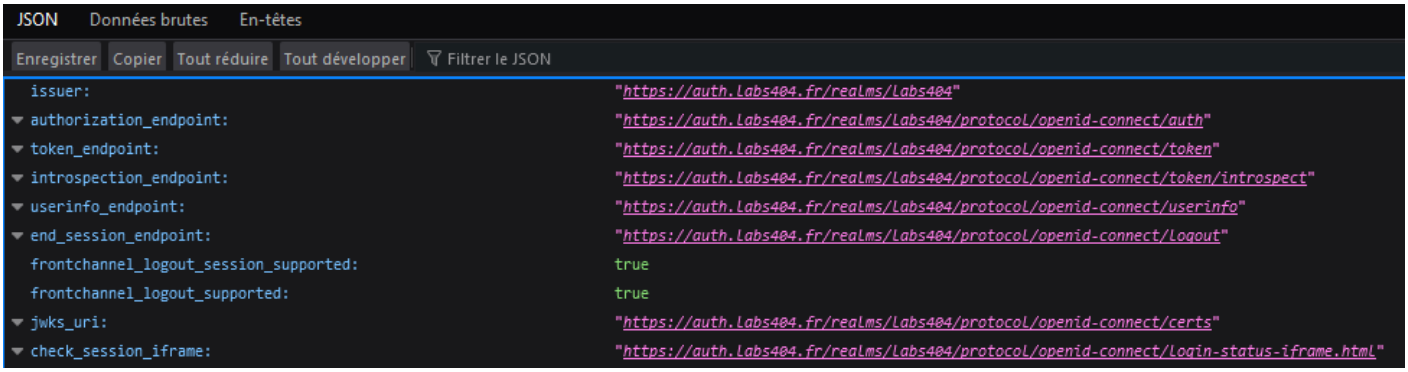


2.3 Récupérer les URL

Pour récupérer les URL, sélectionner le realm et faire '***Realm settings***' puis cliquer sur '***OpenID Endpoint Configuration***'.



Une page s'affiche et permet de récupérer les URL.

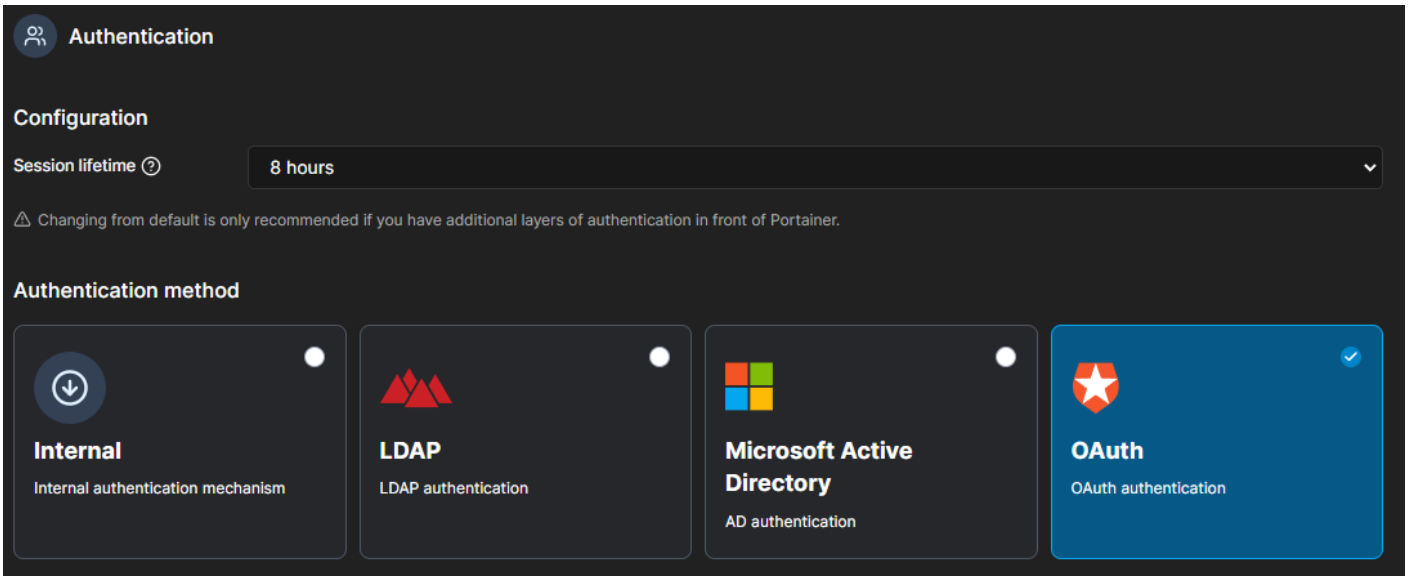


II. Côté Portainer

Se connecter au Portainer.

Aller dans '***Settings --> Authentication***'

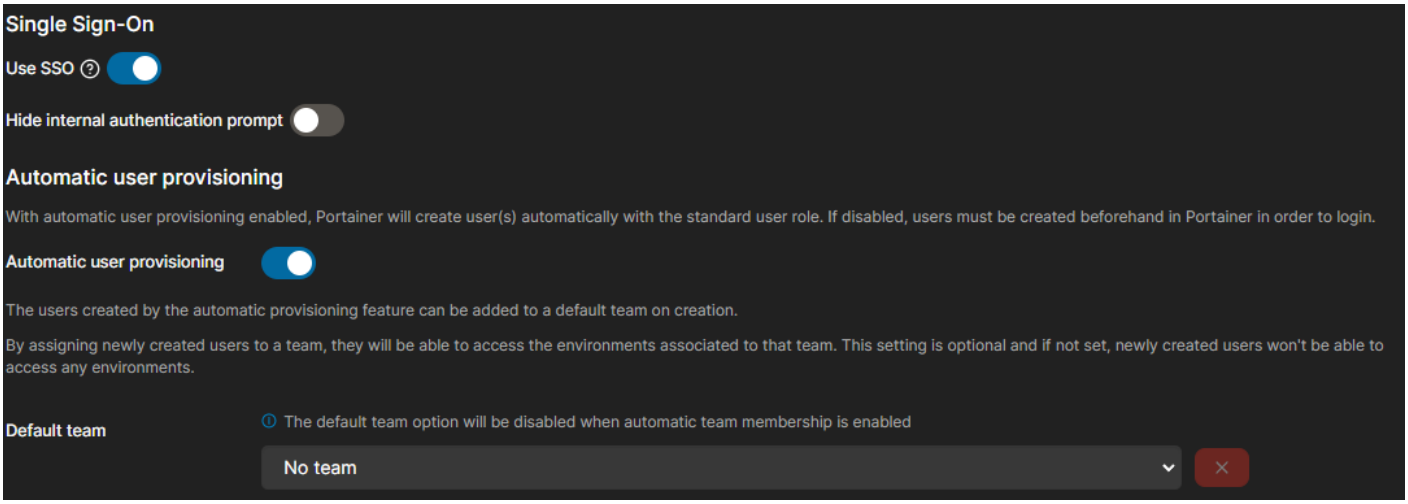
Sélectionner '***Oauth***'



Activer '***Use SSO***' et '***Automatic user provisioning***'.

Laisser la ***Default Team*** en '***No Team***'.

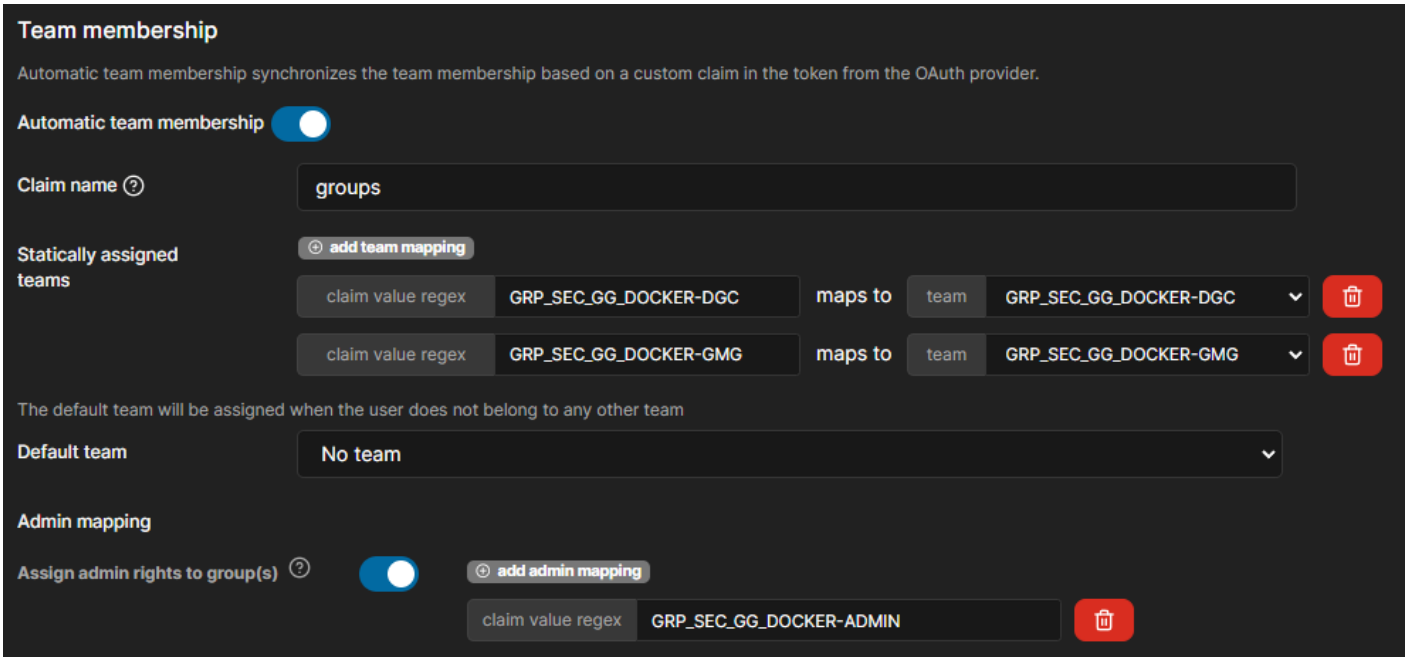
> **Note** : Activer 'Hide internal authentication prompt' forcera la page de login SSO et désactivera l'authentification interne. Il sera toutefois possible d'y accéder en ajoutant ***/#!/internal-auth*** à la suite de l'url.



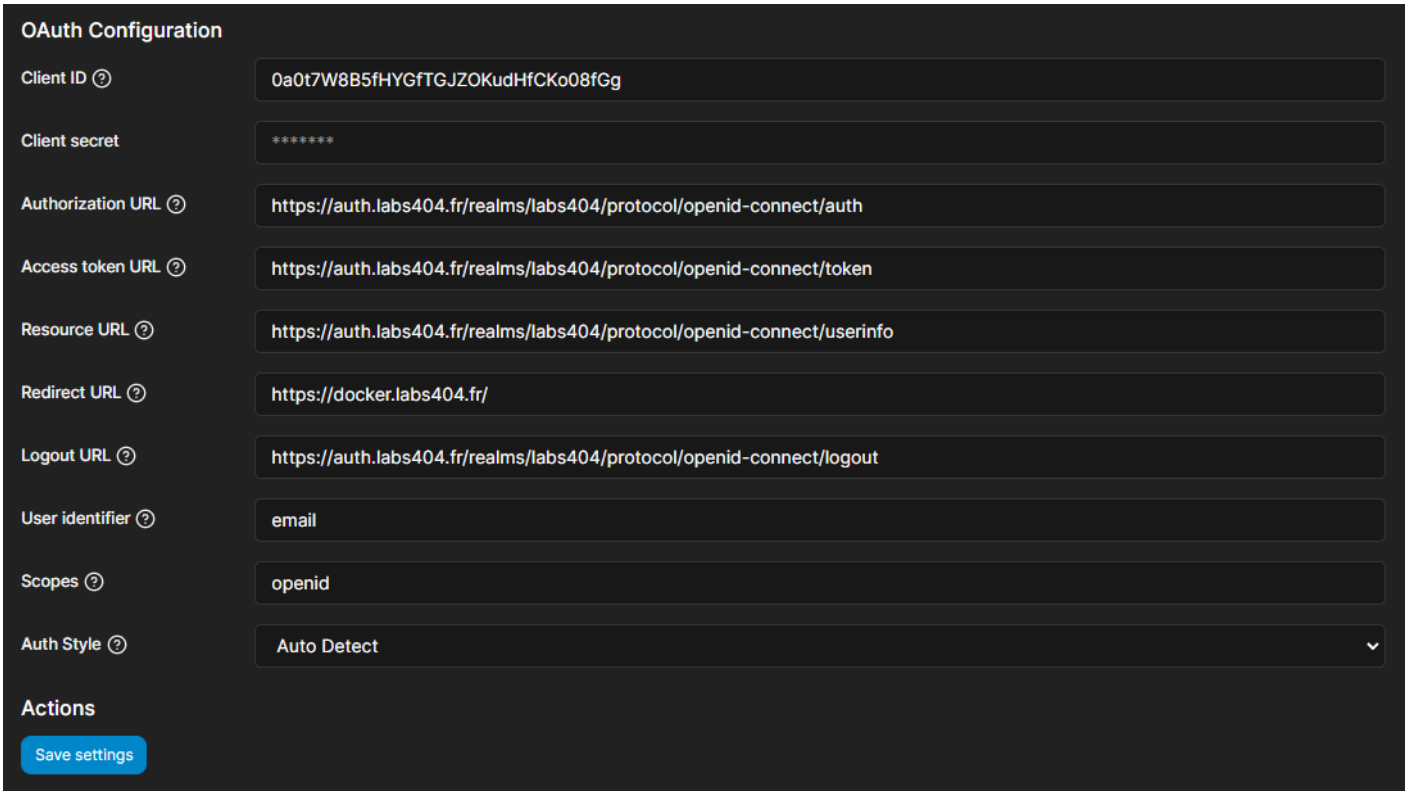
Activer '***Use SSO***' et '***Automatic Team membership***'.

Définir les nom des groupes Keycloak à synchroniser et les associer aux groupes du portainer

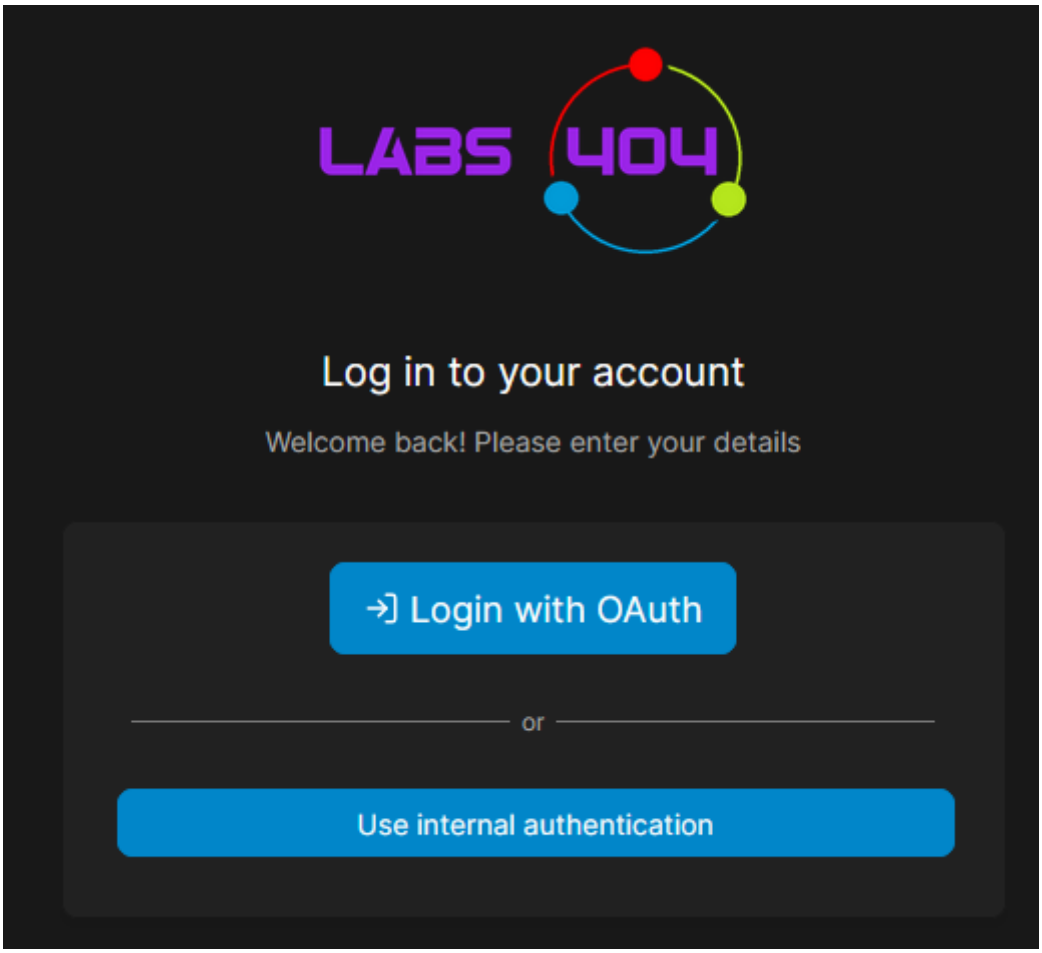
Définir le groupe administrateur.



Définir les url de configuration comme suit en remplaçant, puis faire '***Save***'.



Tout est prêt et la nouvelle page de connexion inclut désormais l'option d'authentification.



Revision #2
Created 2026-07-30 07:35:53 UTC by Olivier
Updated 2026-07-30 08:19:09 UTC by Olivier