

Portainer - Configuration SSO Oauth avec keycloak



Difficulté : Confirmé

Notions : Authentification, SSO

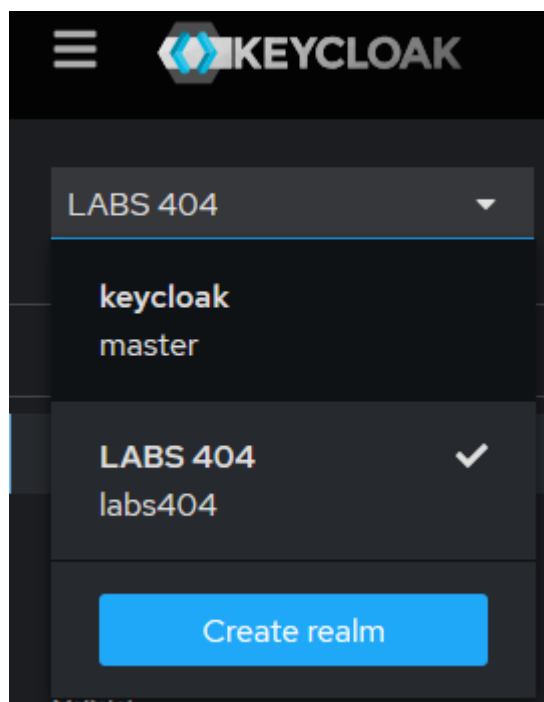
I. Introduction

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

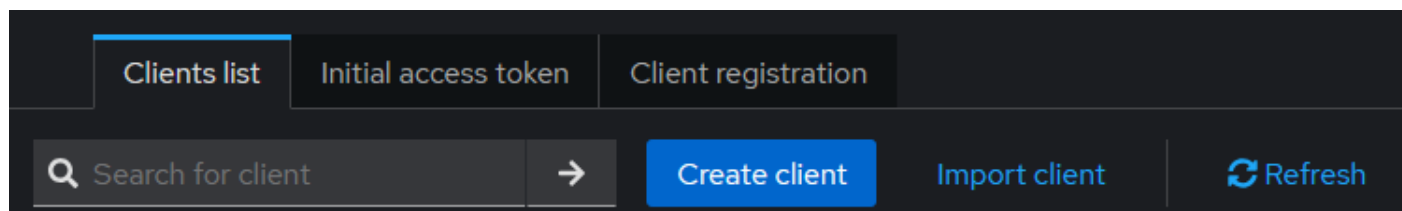
II. Côté Keycloak

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**'.

Create client

Clients are applications and services that can request authentication of a user.

1 General settings

2 Capability config

3 Login settings

Client type ⓘ

Client ID ⓘ

Name ⓘ

Description ⓘ

Always display in UI ⓘ

OpenID Connect

UBMudbmPLGbMvn7BEjAeUcG7xro7vftU

sc-lab-portainer

☐ Off

Back

Next

Cancel

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

Vérifier que les cases suivantes sont cochées.

Puis faire '**Next**'.

1

General settings

2

3

Login settings

Client authentication ?

On

Authorization ?

On

Authentication flow

☒ Standard flow ?

☐ Implicit flow ?

☒ OAuth 2.0 Device Authorization Grant ?

☐ OIDC CIBA Grant ?

☒ Direct access grants ?

☒ Service accounts roles ?

Back

Next

Cancel

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

Puis faire '**Save**'.

1

General settings

2

3

Login settings

Root URL ?

https://docker.labs404.fr/

Home URL ?

https://docker.labs404.fr/

Valid redirect URIs ?

https://docker.labs404.fr/*

+

Add valid redirect URIs

Valid post logout redirect URIs ?

https://docker.labs404.fr/#!/logout

+

Add valid post logout redirect URIs

Web origins ?

https://docker.labs404.fr/#!/

+

Add web origins

Back

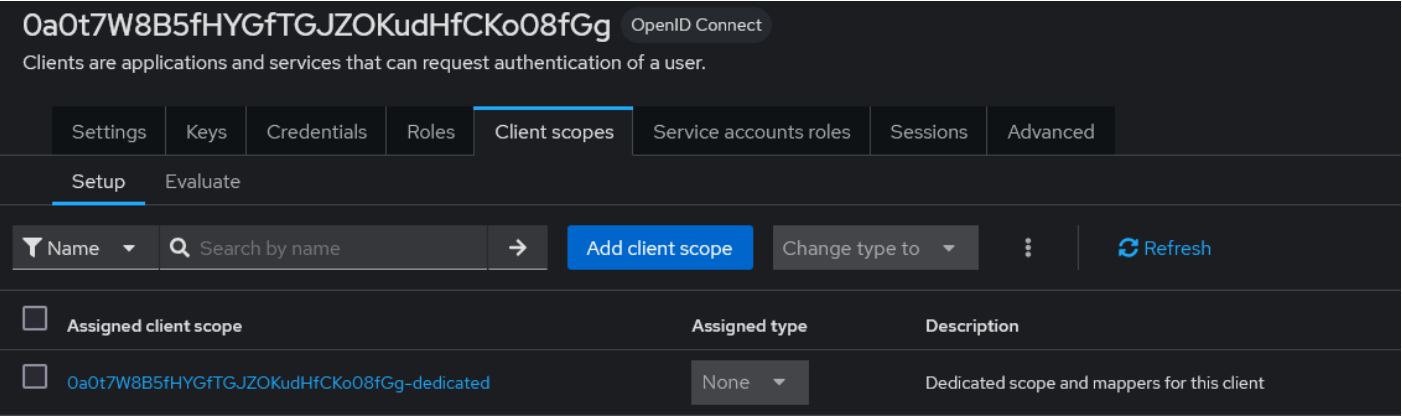
Save

Cancel

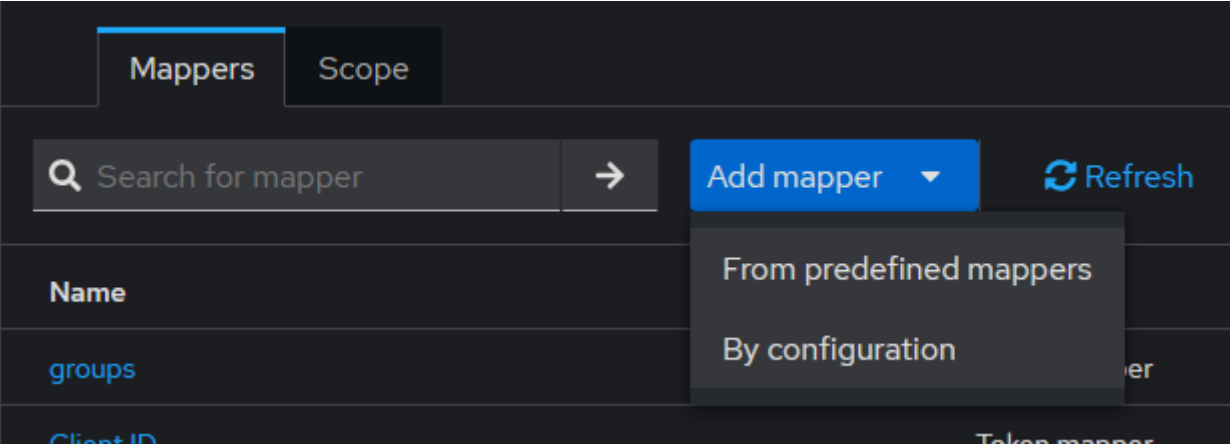
2.2 Préparer la synchro des groupes

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

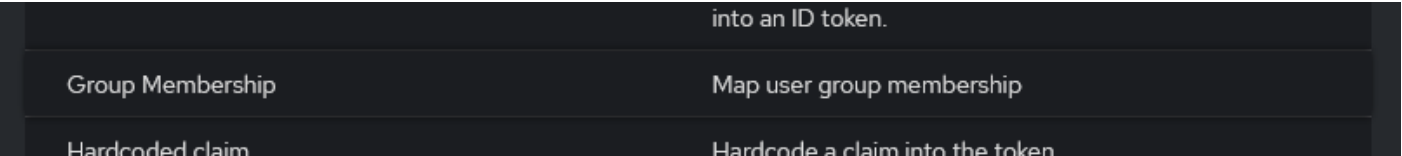
Choisir le client scope au nom du client suivi de '**-dedicated**'.



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



Choisir '**Group Membership**'.

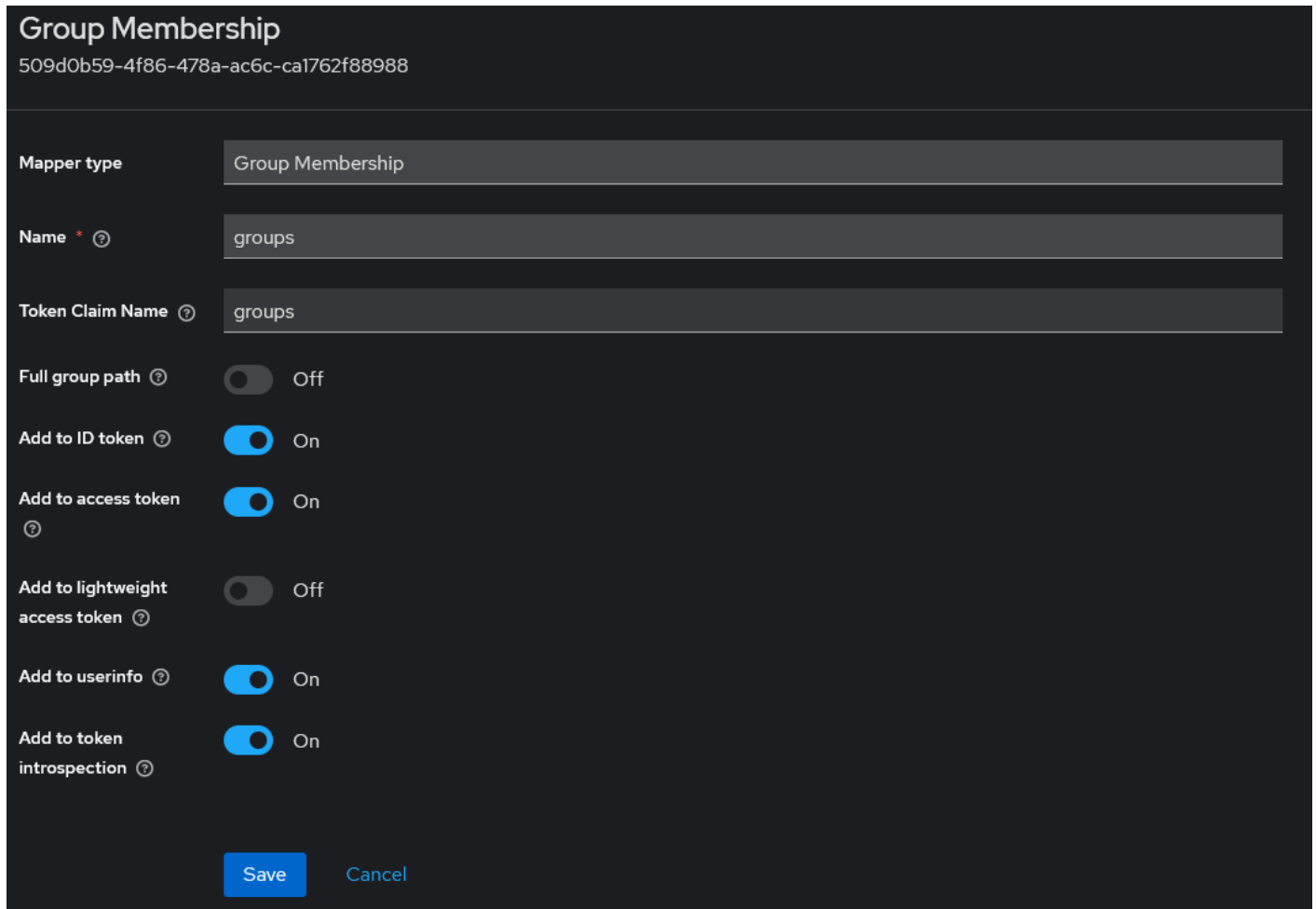


Définir le nom du **mapper** en '**groups**'.

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

Vérifier que les fonctions suivantes soit activées / désactivées.

Puis faire '**Save**'.

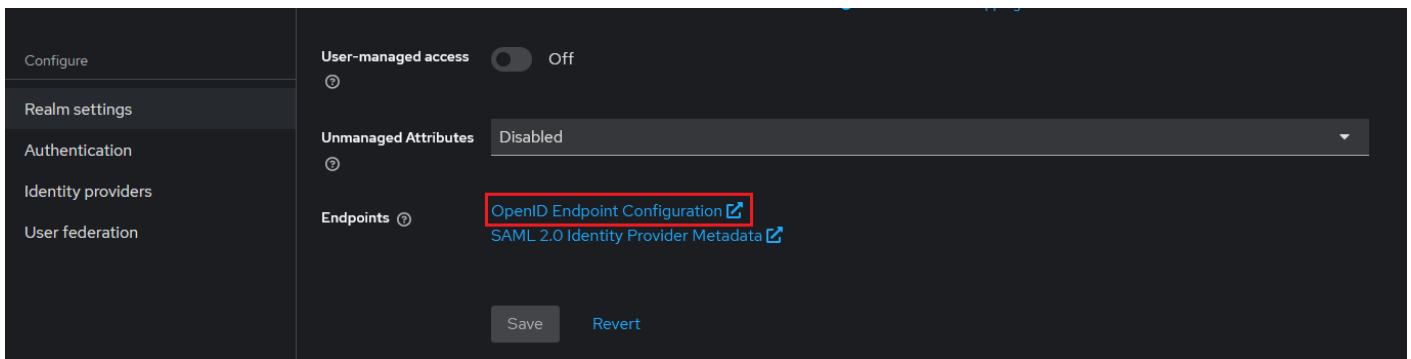


The screenshot shows a configuration window titled "Group Membership" with a unique ID "509d0b59-4f86-478a-ac6c-ca1762f88988". It contains several input fields and toggle switches. The "Mapper type" is set to "Group Membership". The "Name" and "Token Claim Name" fields both contain the text "groups". There are seven toggle switches: "Full group path" is Off, "Add to ID token" is On, "Add to access token" is On, "Add to lightweight access token" is Off, "Add to userinfo" is On, "Add to token introspection" is On, and "Add to token introspection" is On. At the bottom, there are "Save" and "Cancel" buttons.

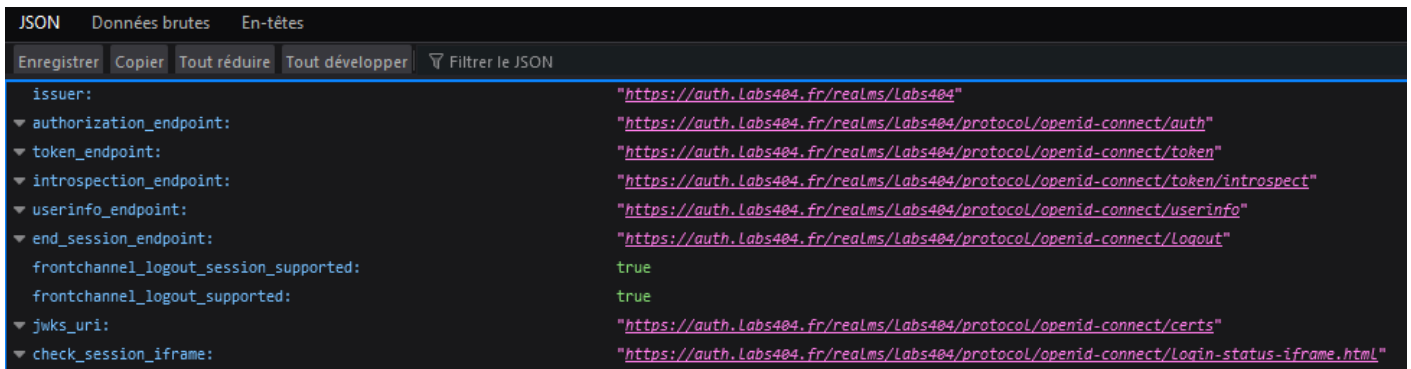
Configuration Item	Value / State
Mapper type	Group Membership
Name *	groups
Token Claim Name	groups
Full group path	Off
Add to ID token	On
Add to access token	On
Add to lightweight access token	Off
Add to userinfo	On
Add to token introspection	On

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**'

 **Authentication**

Configuration

Session lifetime ⓘ 8 hours ▼

⚠ Changing from default is only recommended if you have additional layers of authentication in front of Portainer.

Authentication method


Internal
Internal authentication mechanism


LDAP
LDAP authentication


Microsoft Active Directory
AD authentication


OAuth
OAuth authentication

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.

Single Sign-On

Use SSO ⓘ ☒

Hide internal authentication prompt ☐

Automatic user provisioning

With automatic user provisioning enabled, Portainer will create user(s) automatically with the standard user role. If disabled, users must be created beforehand in Portainer in order to login.

Automatic user provisioning ☒

The users created by the automatic provisioning feature can be added to a default team on creation.

By assigning newly created users to a team, they will be able to access the environments associated to that team. This setting is optional and if not set, newly created users won't be able to access any environments.

Default team ⓘ The default team option will be disabled when automatic team membership is enabled

No team ▼ ✕

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.

Team membership

Automatic team membership synchronizes the team membership based on a custom claim in the token from the OAuth provider.

Automatic team membership ☒

Claim name ?

Statically assigned teams ⊕ add team mapping

claim value regex	GRP_SEC_GG_DOCKER-DGC	maps to	team	GRP_SEC_GG_DOCKER-DGC	
claim value regex	GRP_SEC_GG_DOCKER-GMG	maps to	team	GRP_SEC_GG_DOCKER-GMG	

The default team will be assigned when the user does not belong to any other team

Default team

Admin mapping

Assign admin rights to group(s) ? ☒ ⊕ add admin mapping

claim value regex	GRP_SEC_GG_DOCKER-ADMIN	
-------------------	-------------------------	--

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

OAuth Configuration

Client ID ?

Client secret

Authorization URL ?

Access token URL ?

Resource URL ?

Redirect URL ?

Logout URL ?

User identifier ?

Scopes ?

Auth Style ?

Actions

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



Log in to your account

Welcome back! Please enter your details

→] Login with OAuth

or

Use internal authentication

Revision #2

Created 2026-07-30 07:35:53 UTC by Olivier

Updated 2026-07-30 08:19:09 UTC by Olivier