

## Mise en place d'un serveur d'authentification « Keycloak »

### Objectif

Gagner du temps et déporter votre authentification avec Keycloak.

### Présentation de l'outil Keycloak

**Keycloak** est un outil de gestion des identités et d'authentification. Il est utilisé pour le SSO, c'est-à-dire, que pour plusieurs services, on délègue l'identification par Keycloak. Pour cela, il implémente les standards OAuth 2.0 avec les protocoles sous-jacents **OpenID** ou **SAML**.

Il offre les fonctionnalités suivantes :

- ✓ Authentification unique
- ✓ Adaptateurs clients
- ✓ Protocoles standards
- ✓ Console d'administration
- ✓ Console de gestion des comptes utilisateur

### Comment fonctionne-t-il ?

Le principe de keycloak est le suivant : tout utilisateur non authentifié sera redirigé vers la page de connexion Keycloak. Après une connexion réussie, l'utilisateur est redirigé vers l'application mais avec un en-tête d'autorisation supplémentaire. Lors de cet accès, l'application n'a qu'à vérifier le jeton fourni. Lors des appels aux services API back-end, les applications front-end devront fournir le même jeton d'autorisation dans l'en-tête de la demande. Le service backend utilisera les informations contenues dans le jeton pour authentifier l'utilisateur avec keycloak et autoriser l'accès aux points de terminaison.

### Utilisation de Keycloak

1. Télécharger l'outil **Keycloak** via le lien suivant : <https://www.keycloak.org/>

**Remarque** : pour des raisons de compatibilité de version, nous allons utiliser **V12**

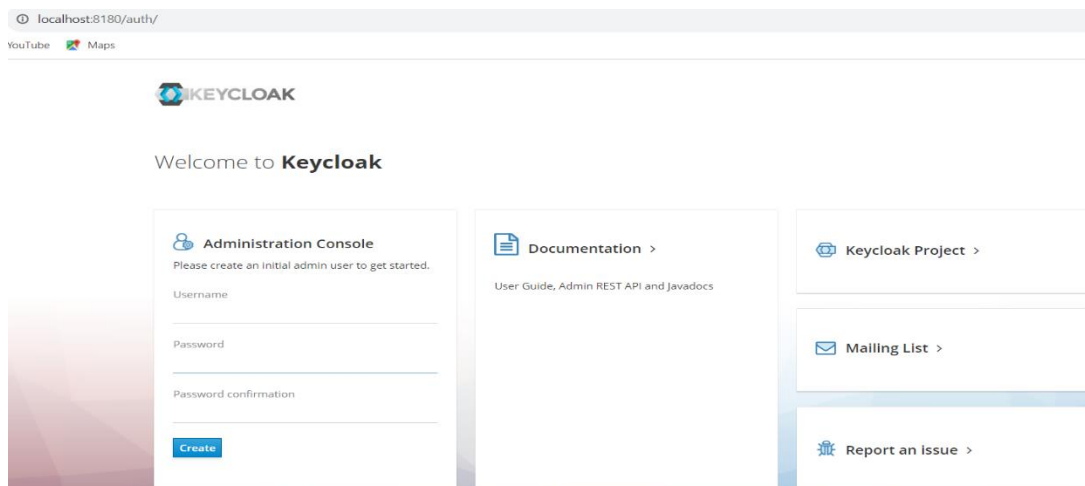
Après avoir téléchargé **Keycloak 12.0.4**, faire l'extraction de fichier ZIP dans un répertoire de votre choix sur votre système.

## 2. Starter le serveur comme suit :

Accédez au répertoire où vous avez extrait Keycloak (keycloak-12.0.4\bin) et exécutez la commande suivante pour le démarrer : standalone.bat -Djboss.http.port=8180

```
D:\ESPRIT\Cours\MS-2023_2024\keycloak-12.0.4\keycloak-12.0.4\bin>standalone.bat -Djboss.http.port=8080
```

Maintenant, vous pouvez lancer le serveur en tapant **localhost:8180**

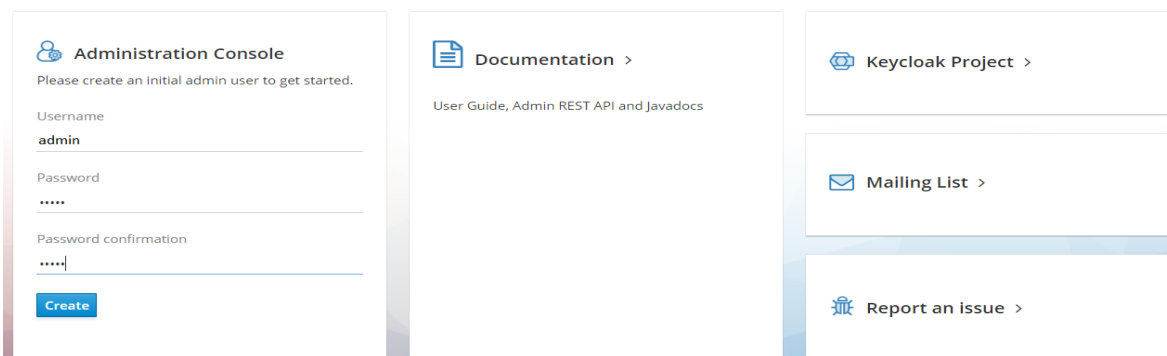


## 3. Se connecter au serveur

- Veuillez consulter le console administrateur pour se connecter en tant qu'administrateur en utilisant les données suivantes comme il est mentionné dans la figure ci-dessous :

**Login :admin, Password :admin, Password confirmation : admin**

Welcome to **Keycloak**

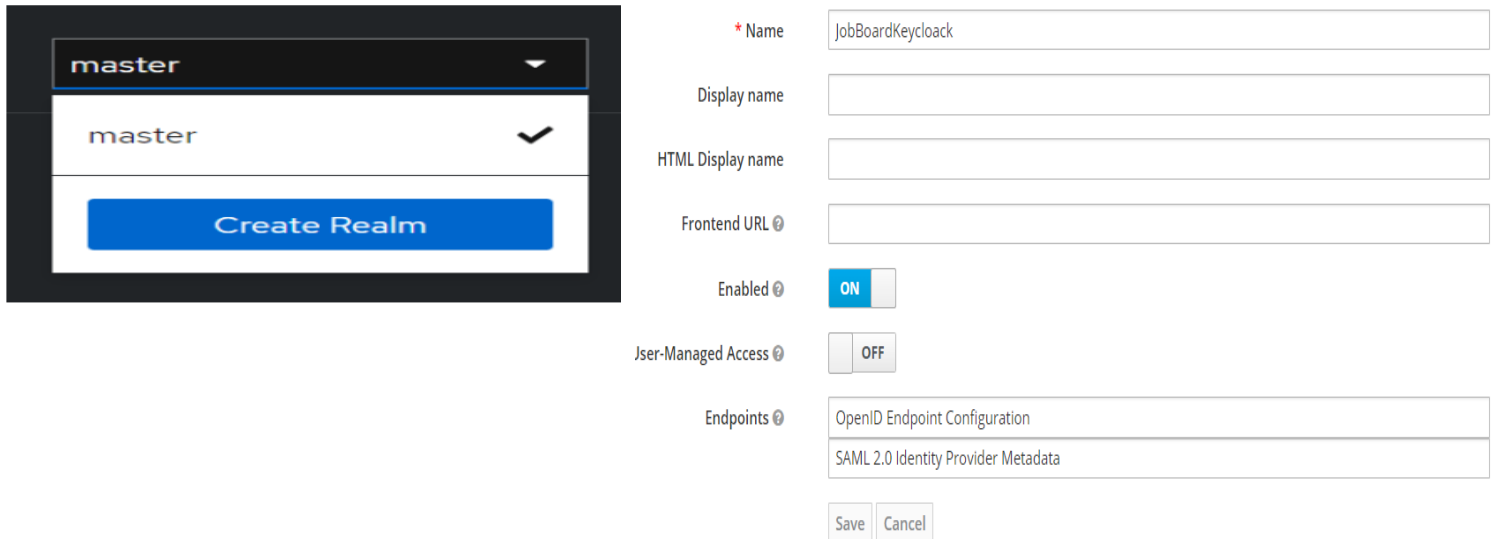


Une connexion réussie, nous amène par la suite vers un realm par défaut

NB : Un **realm** fait référence à un domaine de sécurité et d'administration dans lequel les utilisateurs, les applications et les rôles sont gérés.

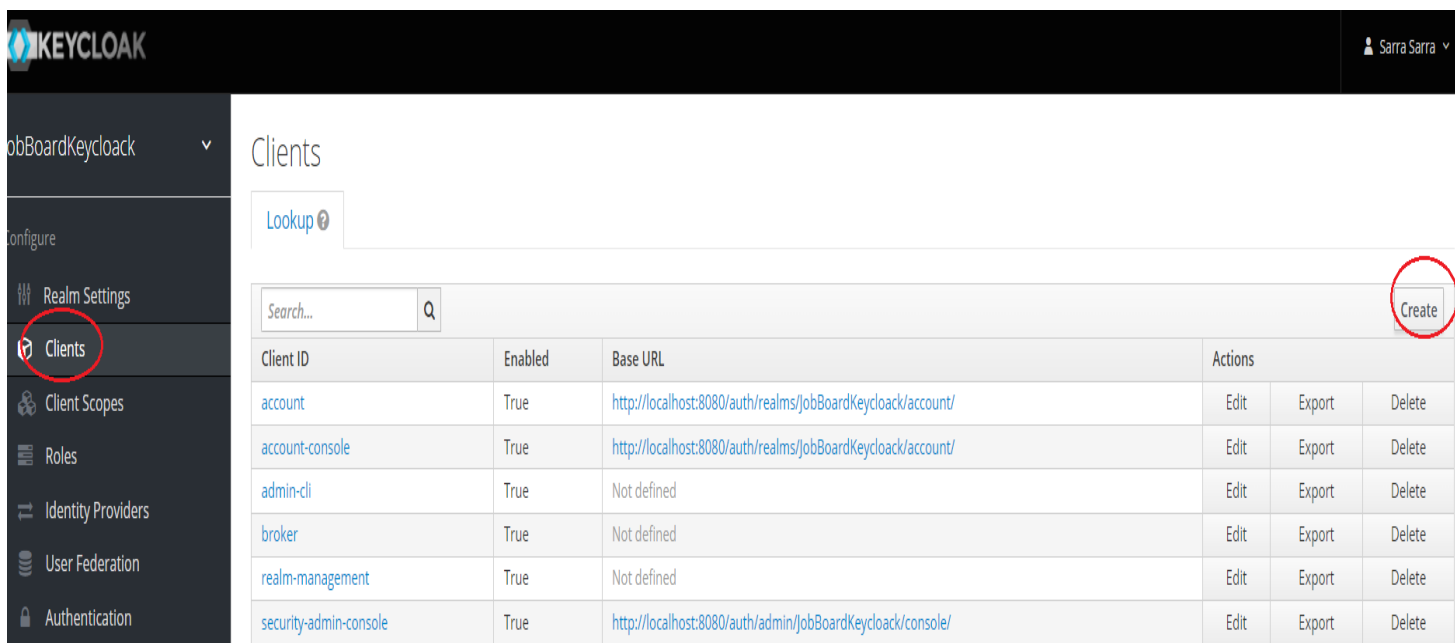
#### 4. Création d'un realm et des clients

- Dans la liste à gauche, vous pouvez ajouter un realm et le nommer JobBoardKeycloak



The image shows two parts of the Keycloak interface. On the left is a modal dialog for creating a new realm. It has a dropdown menu with 'master' selected, a checkmark, and a blue 'Create Realm' button. On the right is the 'Create Client' form. It includes fields for 'Name' (filled with 'JobBoardKeycloak'), 'Display name', 'HTML Display name', and 'Frontend URL'. There are toggle switches for 'Enabled' (ON) and 'User-Managed Access' (OFF). The 'Endpoints' section lists 'OpenID Endpoint Configuration' and 'SAML 2.0 Identity Provider Metadata'. At the bottom are 'Save' and 'Cancel' buttons.

- Sous le nouveau realm crée, vous pouvez ajouter de nouveaux clients de la manière suivante :



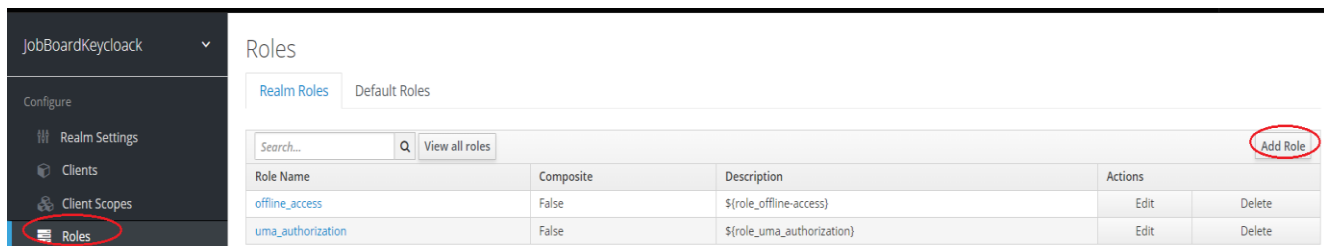
The image shows the 'Clients' page in the Keycloak admin console for the 'JobBoardKeycloak' realm. The left sidebar has 'Clients' highlighted with a red circle. The main area shows a table of existing clients. A 'Create' button in the top right corner is also circled in red. The table has columns for Client ID, Enabled, Base URL, and Actions (Edit, Export, Delete).

| Client ID              | Enabled | Base URL  | Actions            |
|------------------------|---------|---|--------------------|
| account                | True    | <a href="http://localhost:8080/auth/realms/JobBoardKeycloak/account/">http://localhost:8080/auth/realms/JobBoardKeycloak/account/</a> | Edit Export Delete |
| account-console        | True    | <a href="http://localhost:8080/auth/realms/JobBoardKeycloak/account/">http://localhost:8080/auth/realms/JobBoardKeycloak/account/</a> | Edit Export Delete |
| admin-cli              | True    | Not defined   | Edit Export Delete |
| broker                 | True    | Not defined   | Edit Export Delete |
| realm-management       | True    | Not defined   | Edit Export Delete |
| security-admin-console | True    | <a href="http://localhost:8080/auth/admin/JobBoardKeycloak/console/">http://localhost:8080/auth/admin/JobBoardKeycloak/console/</a>   | Edit Export Delete |

A ce niveau là, vous avez besoin d'ajouter un URL valide : [http://localhost:8080/\\*](http://localhost:8080/*)

#### 5. Création de rôles et d'utilisateurs

Veillez choisir l'option Real rôle et le nommer « **user** » comme le montre la figure ci-dessous



- Nous avons maintenant un rôle « user » qui peut être attribué aux utilisateurs, mais comme il n'y a pas encore d'utilisateurs, allons sur la page Utilisateurs et ajoutons-en un : « **user1** ».
- Nous pouvons maintenant accéder à l'onglet Informations d'identification. Nous définissons le mot de passe par « user ».
- Maintenant, nous allons attribuer l'utilisateur créé au rôle **user** :

**Veuillez choisir user->sélectionner l'utilisateur user1->Role mappings  
->Dans la table Available roles, veuillez sélectionner l'utilisateur user1.**

Pour vérifier que l'utilisateur a été ajouté, veuillez choisir l'option Roles comme le montre la figure ci-dessous

