**Keycloak Authorization 서버 설정**

**Keycloak, JWT기반 OAuth2 책임의 분산 (1/3) : 마이크로서비스와 OAuth2 구성요소인 Authorization Server/ Client/ Resource Server를 활용해 Single Sign-On 구현 모형을 실습한다. OAuth2에서 Authorization Server로 Keycloak을 설치하고 설정하는 방법을 간단하게 실습한다.**

10분 이내 완료

[**INTO THE LAB**](https://labs.msaez.io/#/courses/cna-full/cna-full-aws/Keycloak-OAuth2-1)

**Instruction**

**Keycloak기반 OAuth2 - Authorization Svr**

**OAuth2 Stackholders**

* **Gateway를 OAuth2 Client로, 주문 마이크로서비스를 Resource Server로 설정한다.**
* **Keycloak 서버를 설치하고 접속하여 기본설정과 사용할 User를 등록한다.**
* **OAuth2의 Grant type을 'authorization\_code’를 적용한다.**
* **Platform에서 작업이 원활히지 않을 경우, Local에서 수행한다.**

**Local 머신에 IDE(IntelliJ, VSCode)와 JDK 11 이상이 설치되어 있어야 한다.**

**Keycloak 시작**

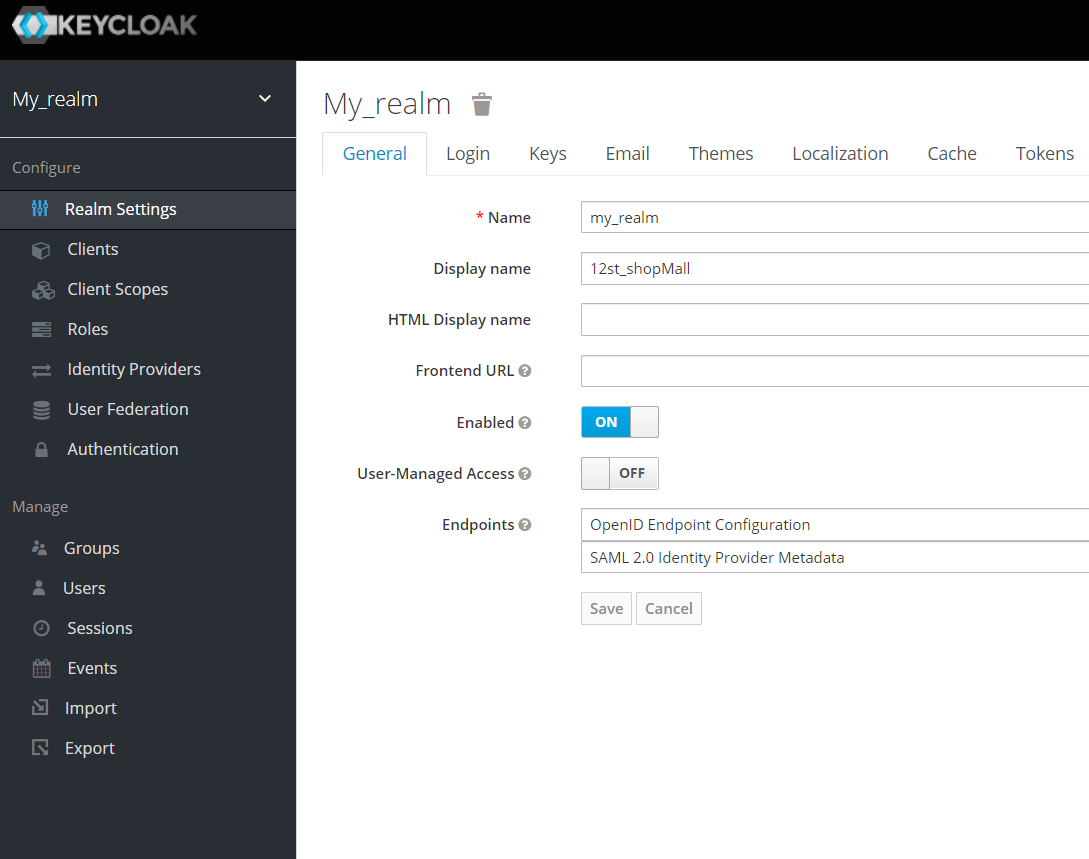
* **Redhat이 만든 Keycloak 서버는 8080포트를 기본 사용한다.**
* **bin 폴더 하위에 OS에 맞는 Script를 실행한다.**

**cd keycloak/bin**

**chmod 744 ./kc.sh**

**./kc.sh start-dev**

* **웹브라우저에서 Keycloak 관리콘솔(**[**http://localhost:8080/**](http://localhost:8080/)**)에 접속한다.**
* **관리자 계정이 (admin/admin)으로 등록되어 있다.**
* **'Administration Console’을 눌러 콘솔로 진입한다.**

****

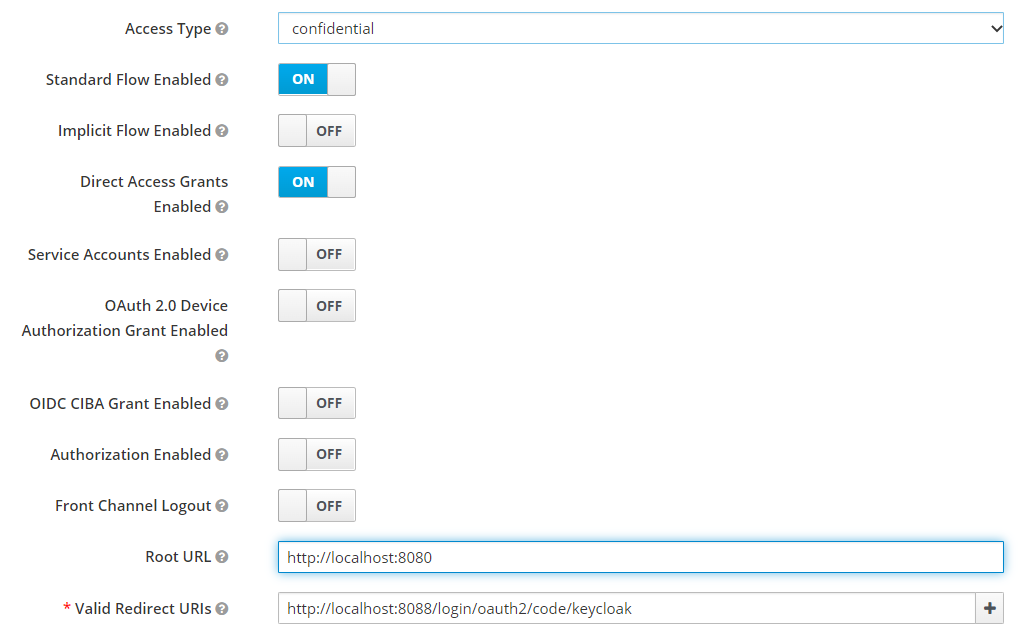
**Keycloak 설정**

* **Realm 추가**
* **‘test-realm’ 이름으로 Root 관리단위인 Realm을 추가한다.**
* **추가된 Realm에서 Token의 Lifespan을 1시간으로 조정한다.**
* **Client 등록**
* **왼쪽 메뉴 Client를 눌러, Realm 범주의 Client를 추가한다.**
* **‘test-client’ 이름으로 OAuth2 CLIENT를 등록한다.**

**Root URL:**[**http://localhost:8080**](http://localhost:8080/)

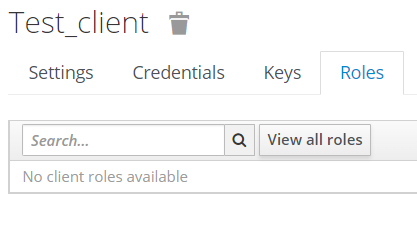
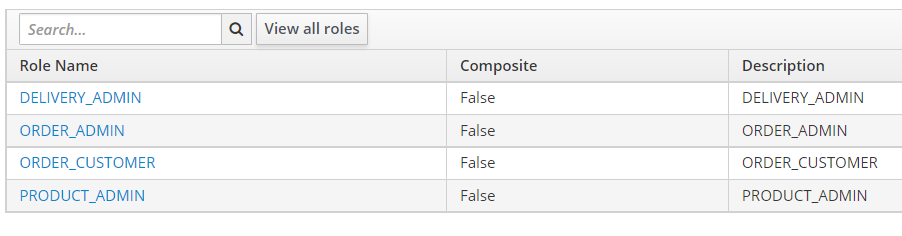
* **'Save’를 눌러 저장한다.**
* **Client의 OAuth2 설정을 추가한다.**

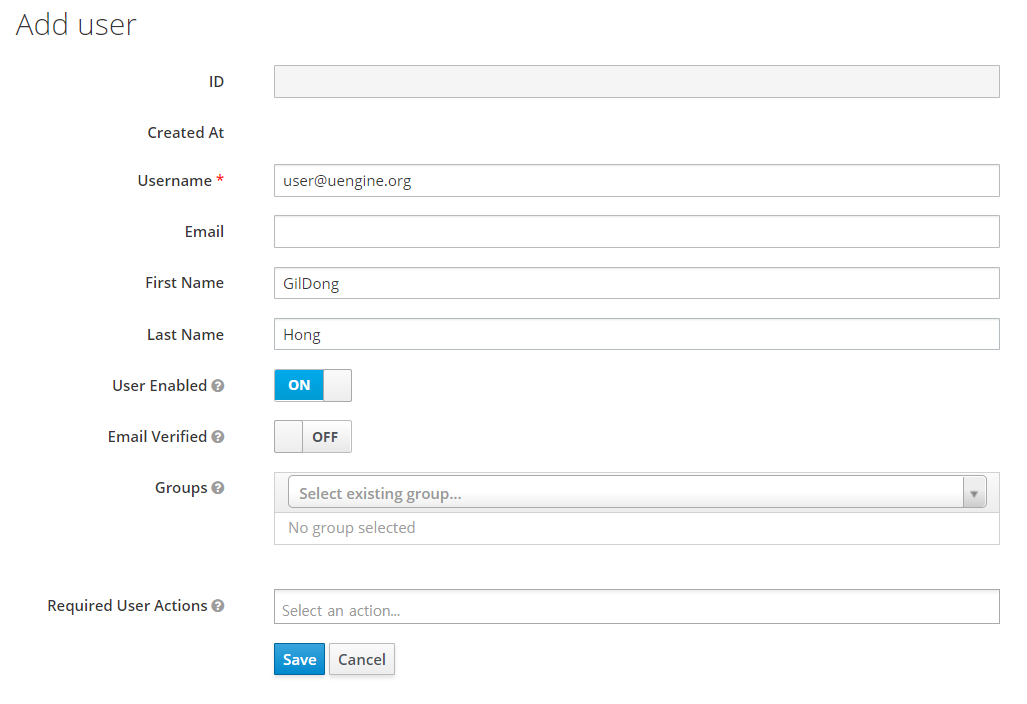
**Redirect URI:**[**http://localhost:8088/login/oauth2/code/keycloak**](http://localhost:8088/login/oauth2/code/keycloak) **Access Type: public에서 confidential로 설정  
OAuth2의 “Client Credentials” 타입이 활성화된다.**

****

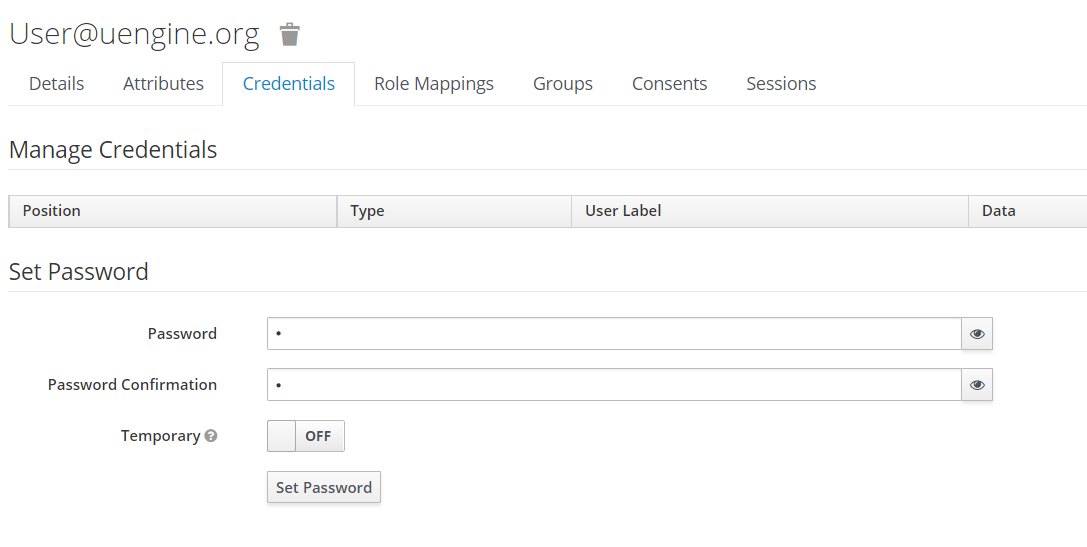
* **'Save’를 눌러 저장한다.**
* **‘Credentials’ 탭을 눌러, Client의 Secret 정보가 발급됨을 확인한다.**

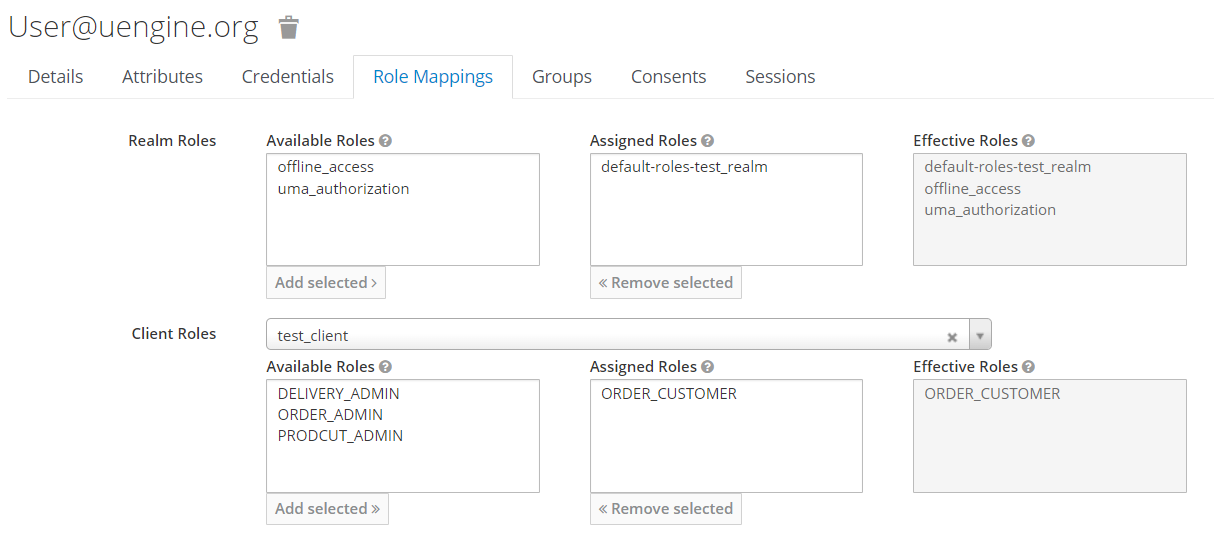
**권한(Role) 및 사용자 설정**

* **‘Roles’ 탭을 눌러 Client의 Local Role을 추가한다.  
  **
* **아래 목록처럼 나타나도록 Role 이름을 부여한다.  
  **
* **왼쪽 메뉴에서 Users를 눌러 사용자를 등록한다.**

**사용자 정보는 Custom하게 생성해 본다. (User와 Admin 계정포함)  
**

* **등록 후, Credentials 탭에서 비밀번호를 등록하는데 이때, Temporary를 Off로 설정한다.**

****

* **User 등록이 끝나면, Role과 사용자를 매핑한다.**
* **등록한 사용자 각각에서 ‘Role Mappings’ 탭을 눌러 Client의 Local Role을 선택해 준다.  
  **

**User 계정에는 ‘ORDER\_CUSTOMER’ 역할 매핑  
Admin 계정에는 ‘ORDER\_ADMIN’, ‘ORDER\_CUSTOMER’ 역할 매핑**

* **이로써, 간단하게 Keycloak 설정을 마무리한다.**

**CheckPoints**

1. 모든 요구사항을 만족하는가