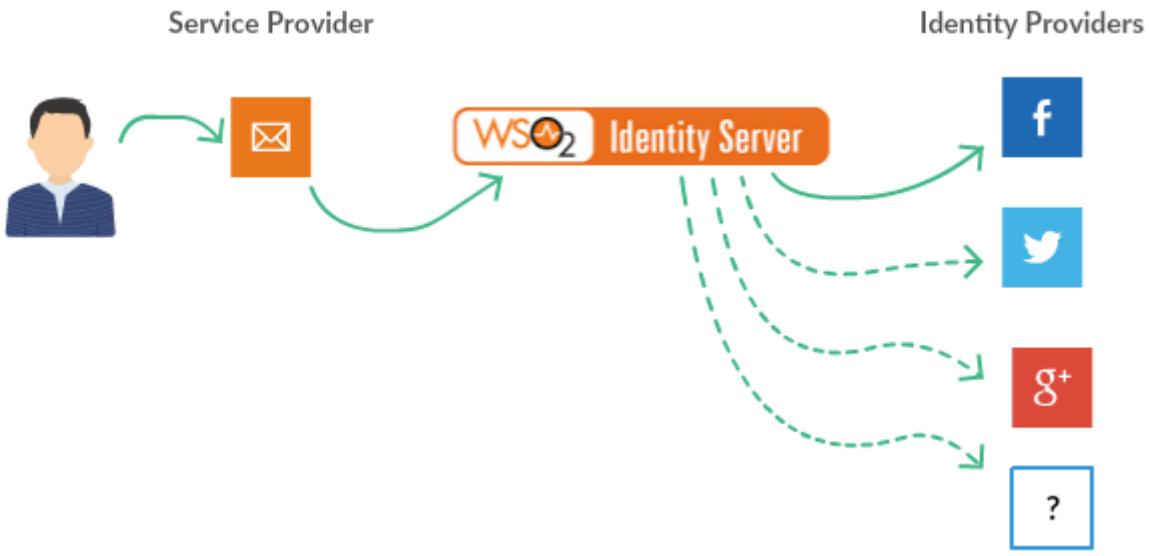
Piraveena Paralogarajah

229 Followers About Follow

Configuring Keycloak as a federated IDP in WSO2 Identity Server

Piraveena Paralogarajah Jun 1, 2019 · 5 min read



With WSO2 Identity Server, you can integrate different Identity Servers. So WSO2 Identity server will have trust relationships with that identity server and it will assert the identities belong to the other Identity providers.

Now we are going to configure keycloak as a federated IDP in WSO2 Identity Server.

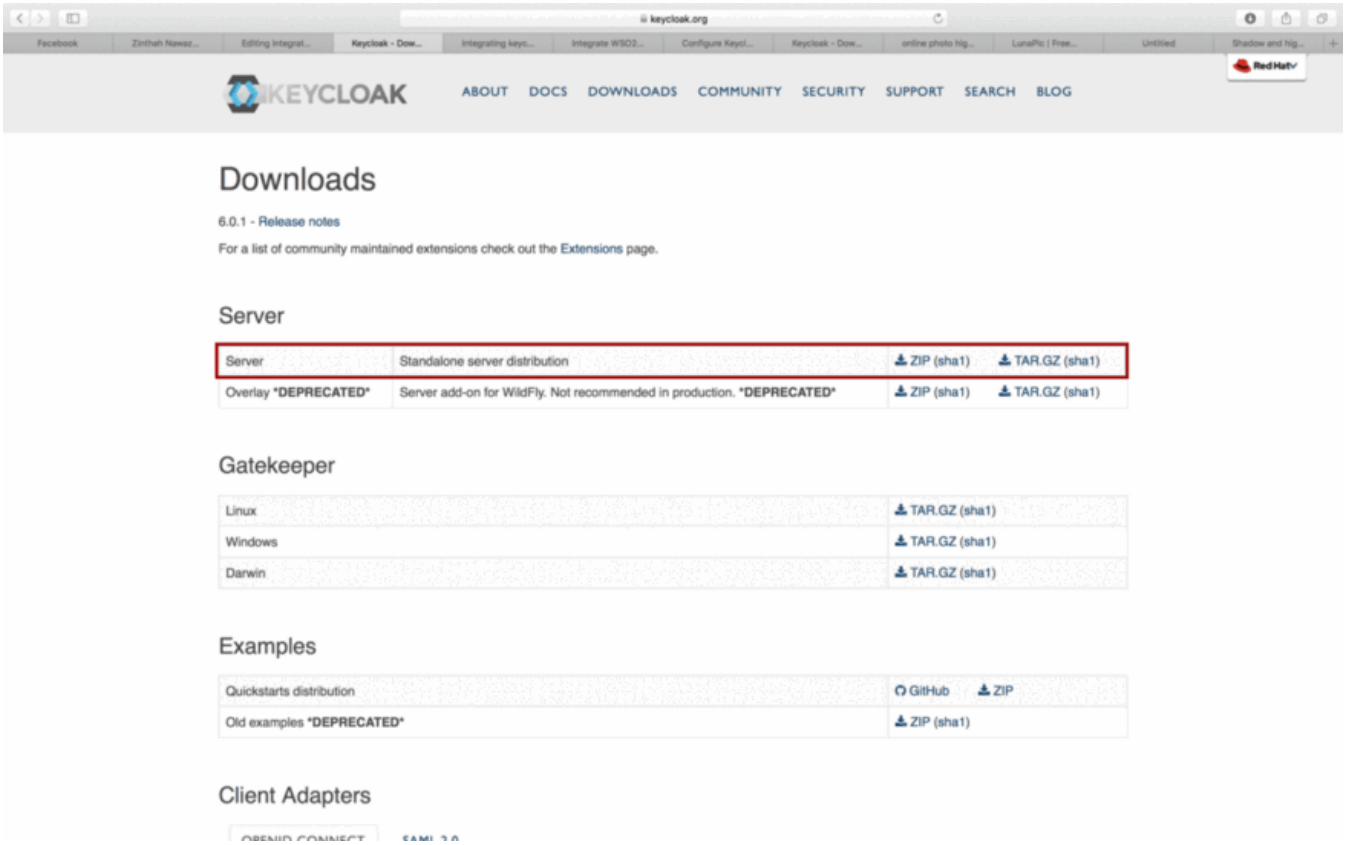
This can be done in 4 steps:

1. Configuring WSO2 Identity Server as a service provider in Keycloak

4. Configure a Service provider in WSO2 Identity Server

1. Configuring WSO2 Identity Server as a service provider in Keycloak

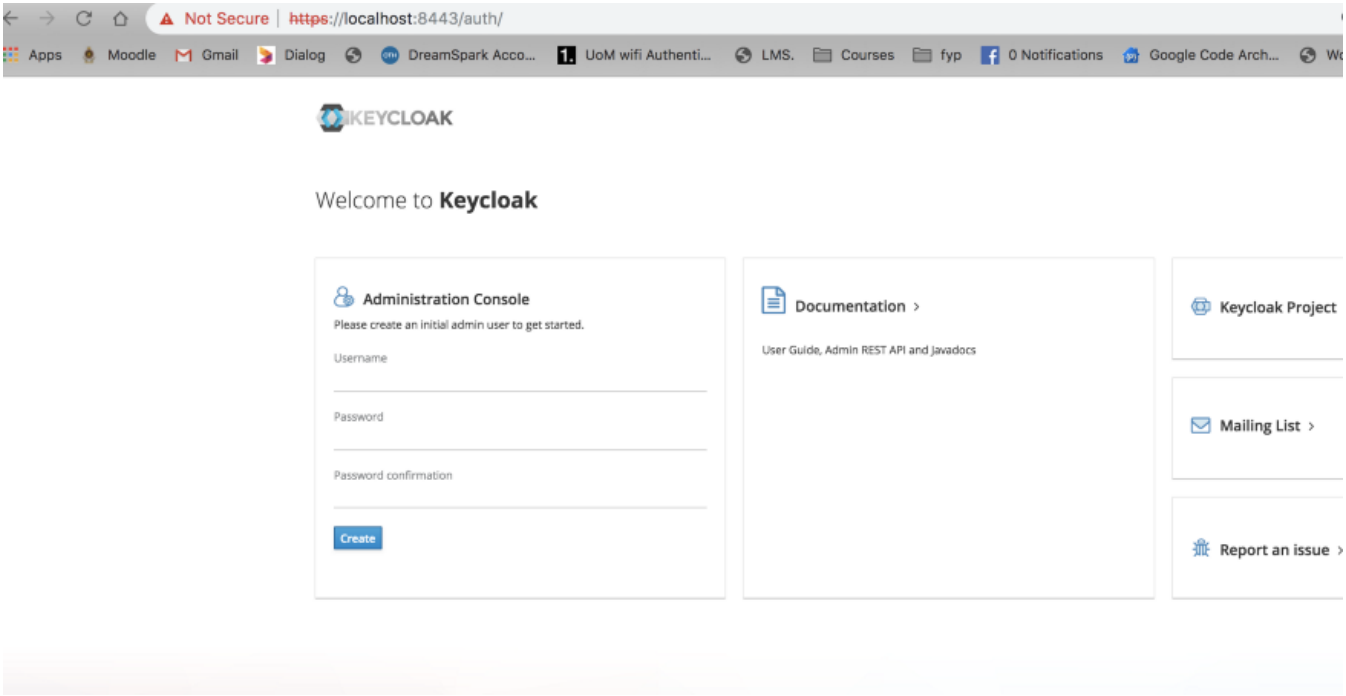
- Download keycloak from this keycloak official site



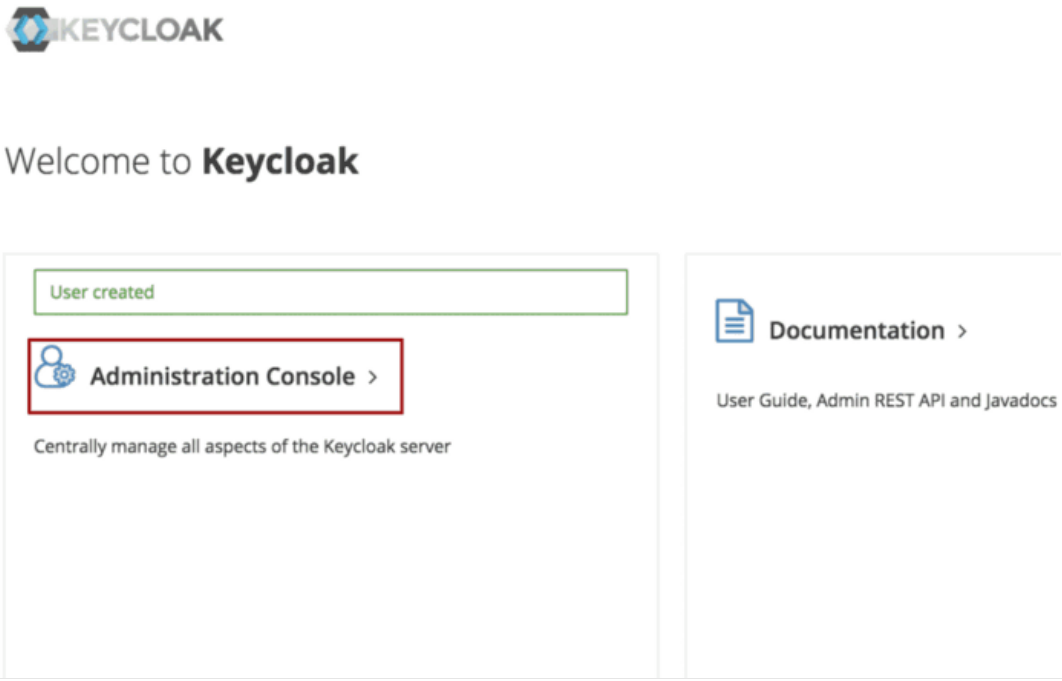
- Download and Unzip, and run the command

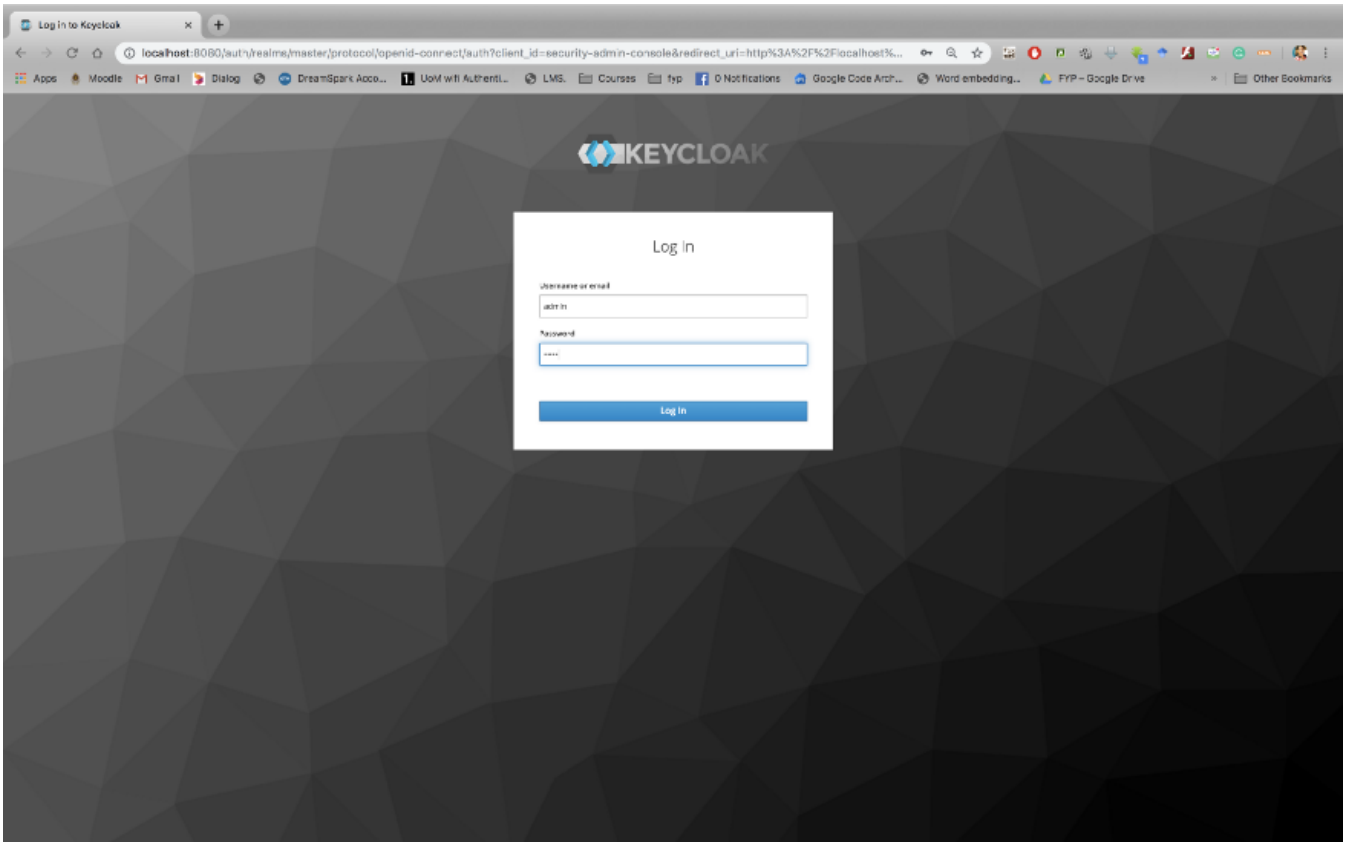
```
sh.standalone.sh
```

- Now you need to a setup a admin user to login to admin console. For that you will have to run add-user-keycloak script. If you have local access then you can create an admin user by logging on to auth portal. Go to https://localhost:8443/auth/ and create a admin user

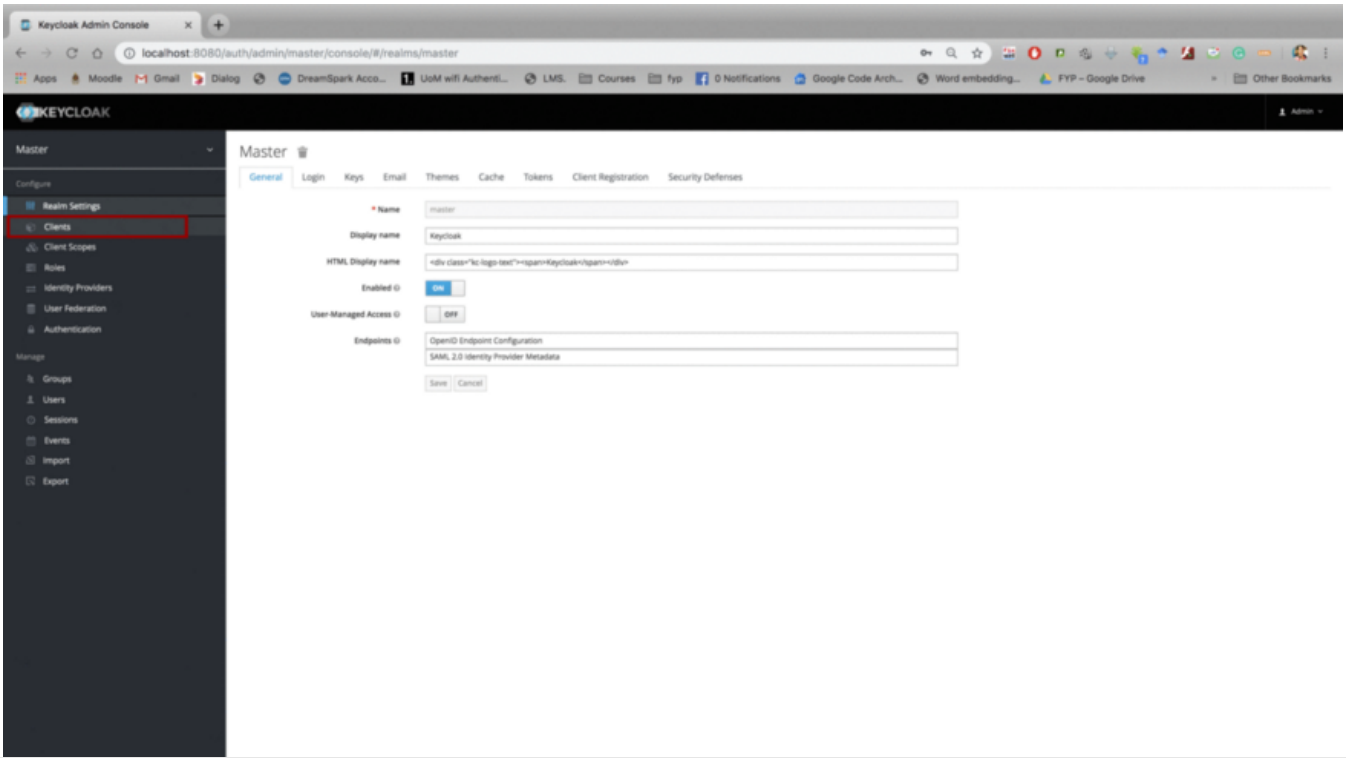


- Once the user got created, you can see a success message.
- Click on **Administration Console.** You will be prompted username / password page. Enter registered admin user's username and password'

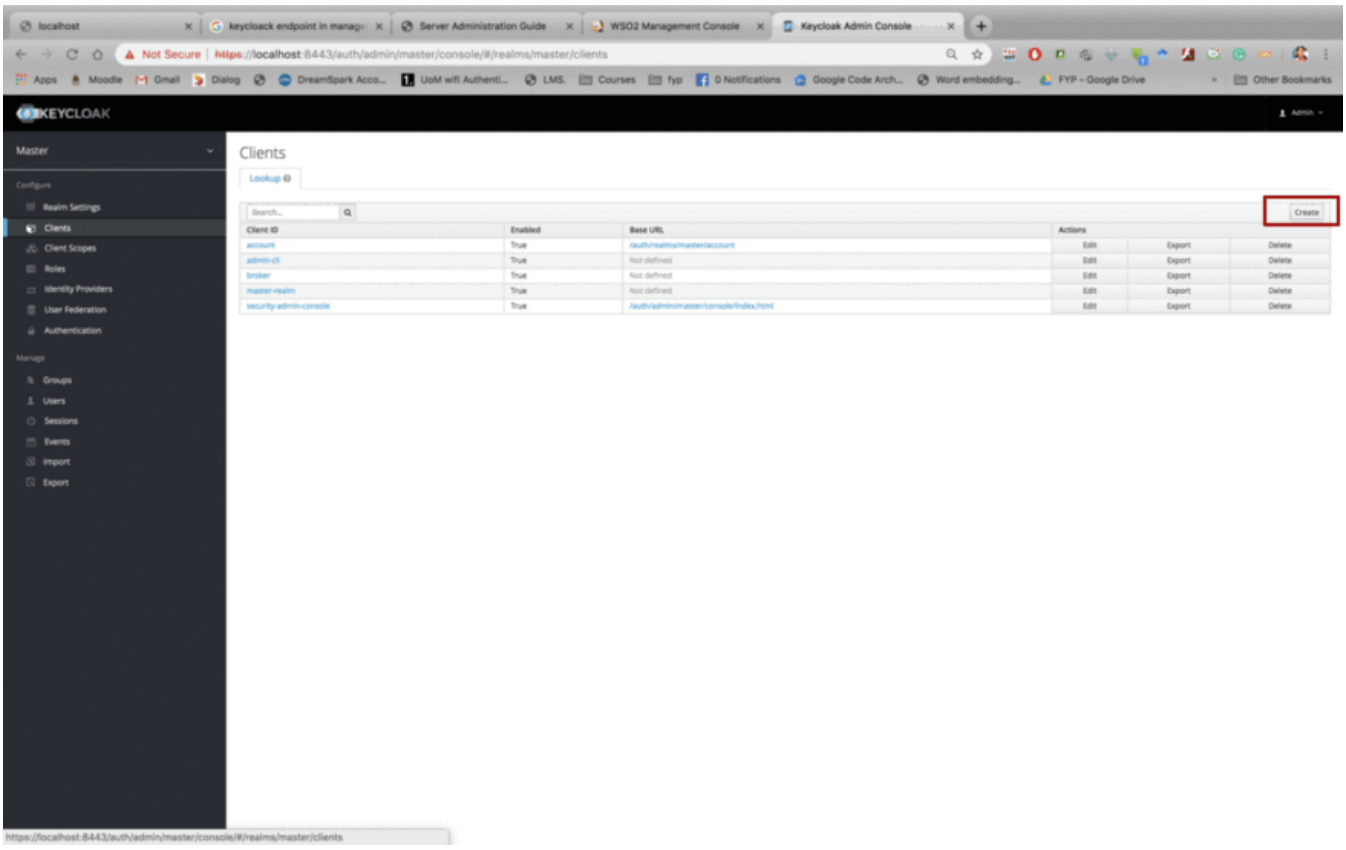




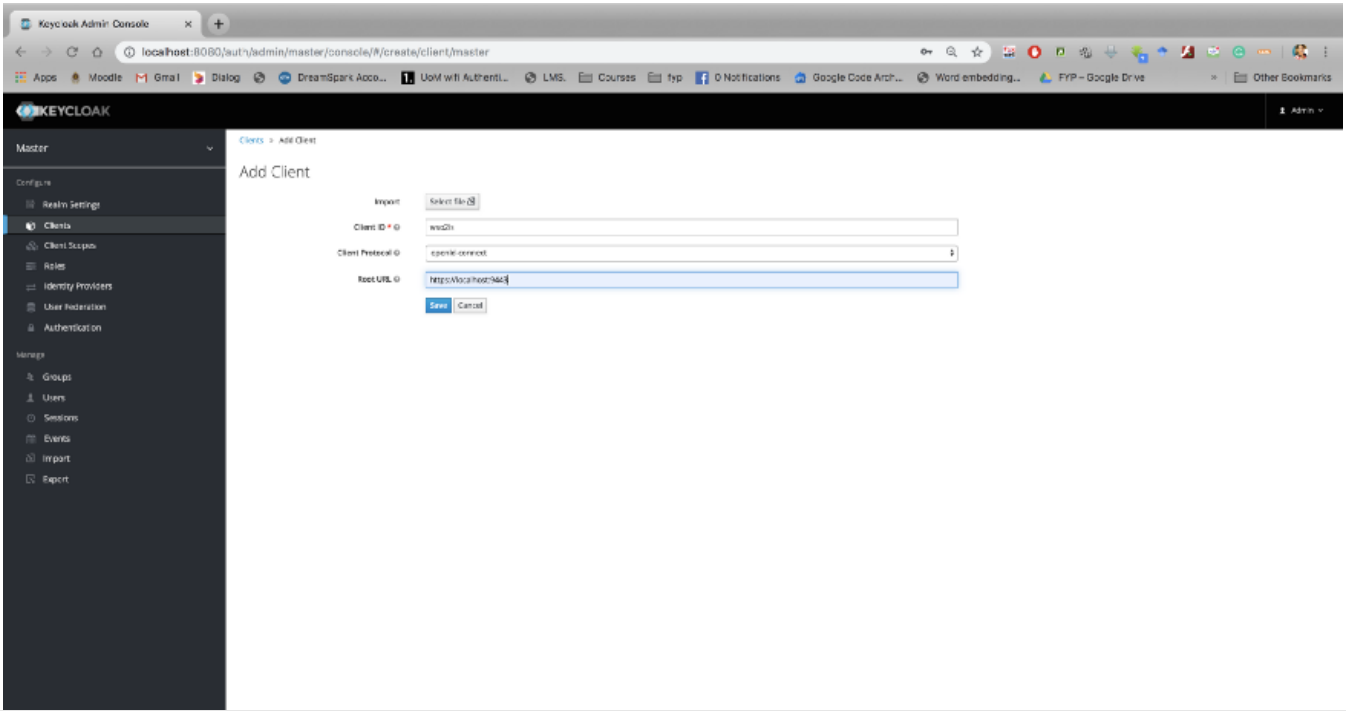
- Now you need to configure WSO2 Identity server as a service provider in Keycloak Identity Server. Click on Clients menu.



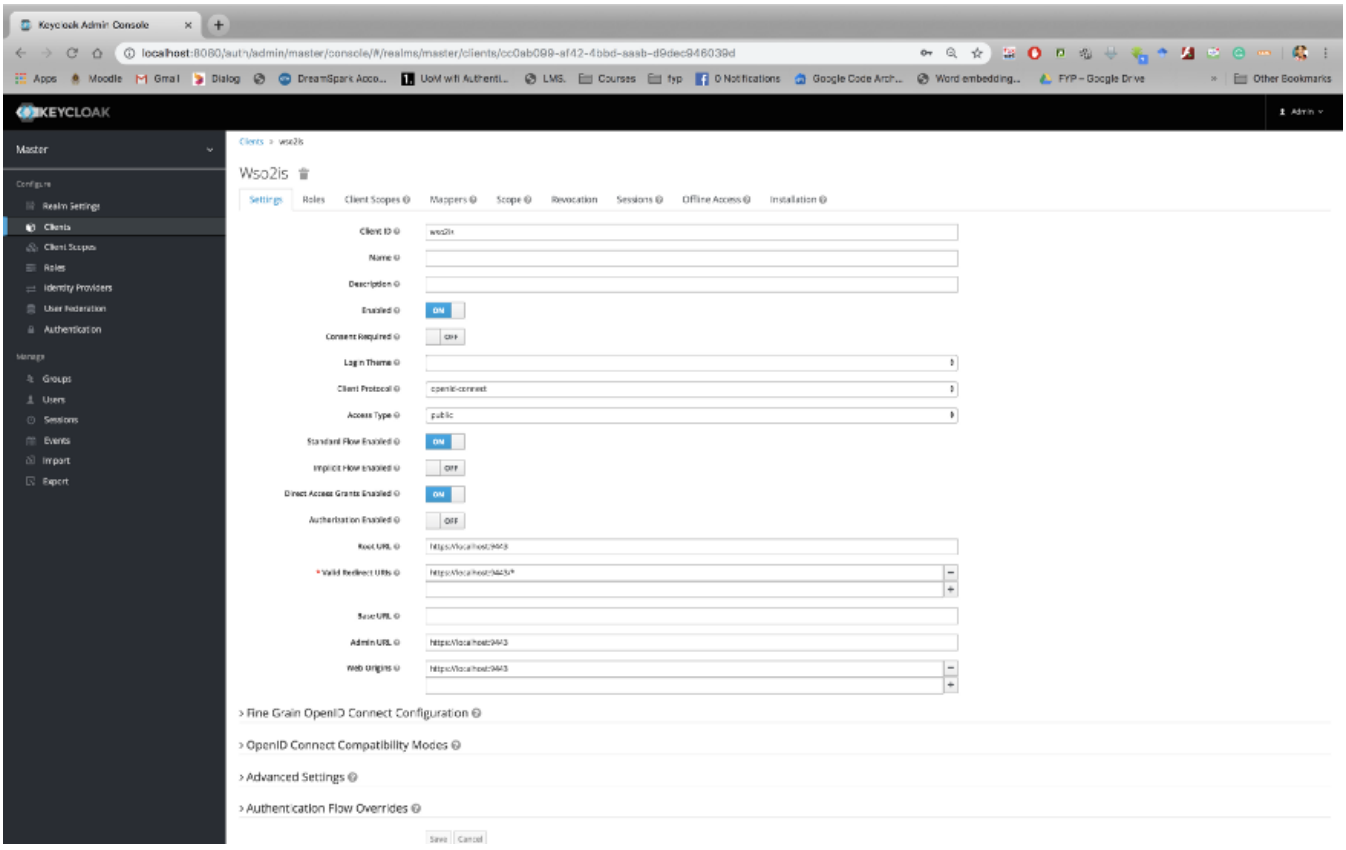
- Now you can see some service providers already configured. Click on **Create** button and create a new service provider.



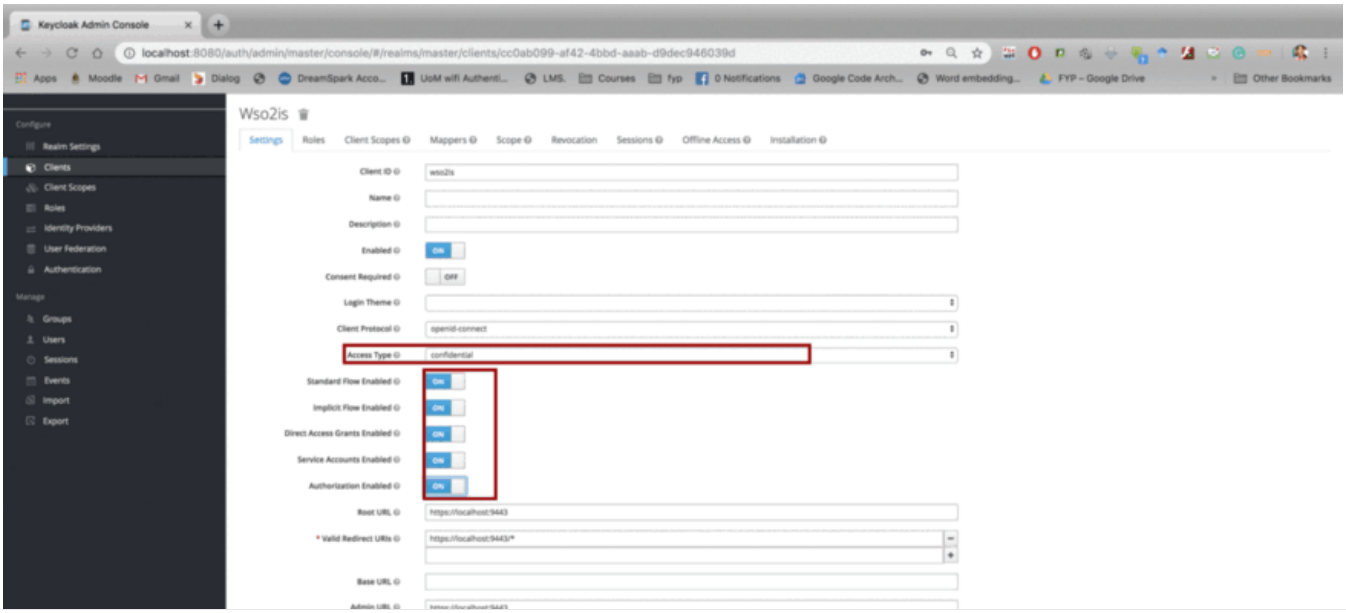
- Enter the client ID and client protocol and root URL of the service provider (Here WSO2 Identity server will act as a service provider to Keycloak Identity Server)

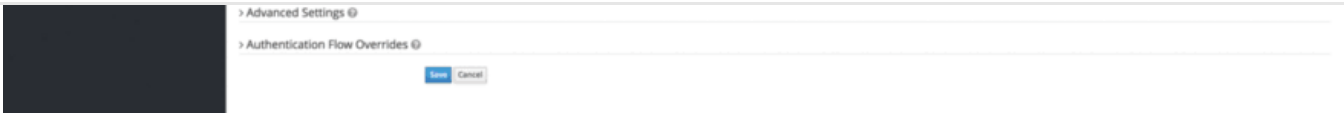


- Once you create the service provider, you will be redirected to the service provider details.

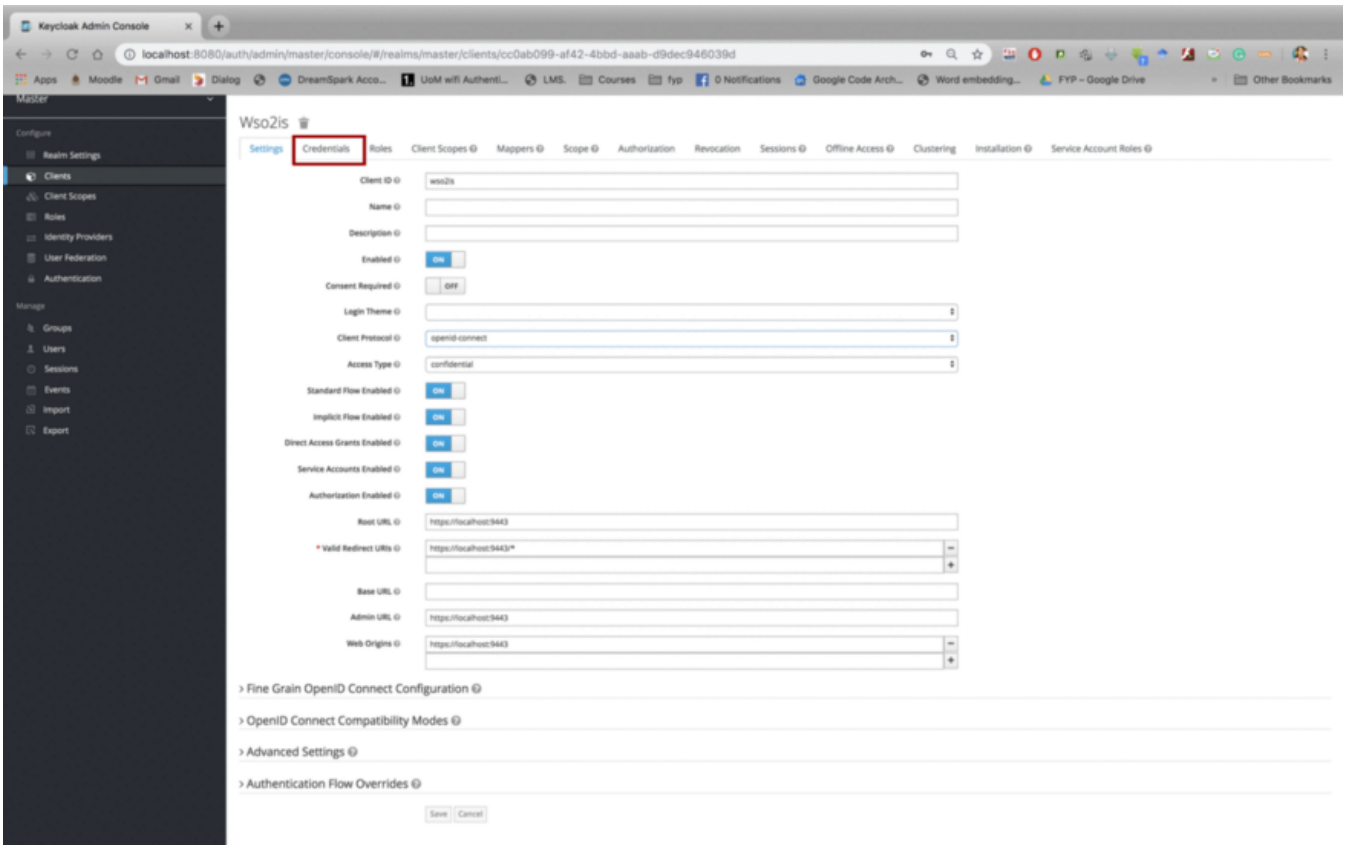


- Enable all **grant types** using the management console of Keycloak. Make sure the access type is **confidential.** That will create a client secret for the service provider. And click on save button to update your changes.

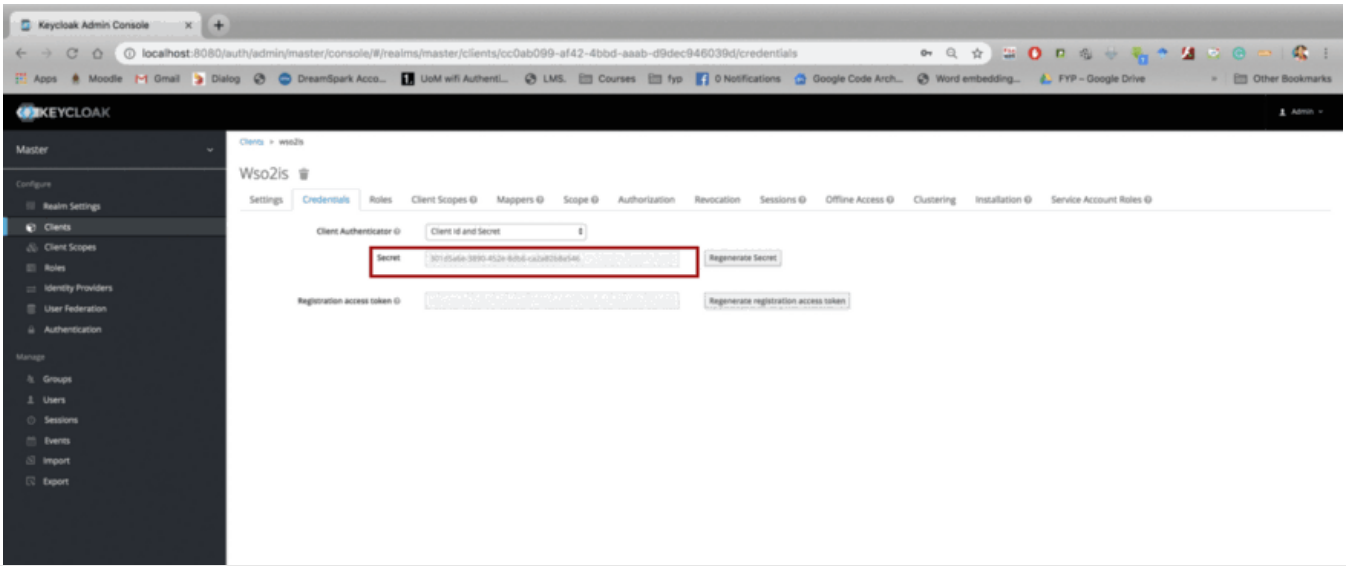


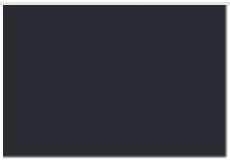


- Once you select Access Type to **confidential** new tab will be appeared as Credentials. There you can extract client secret. Now you saved the changed. Now you can see credentials tab. Click on **credential** tab.



- Now you can view the **client secret** of the service provider you created



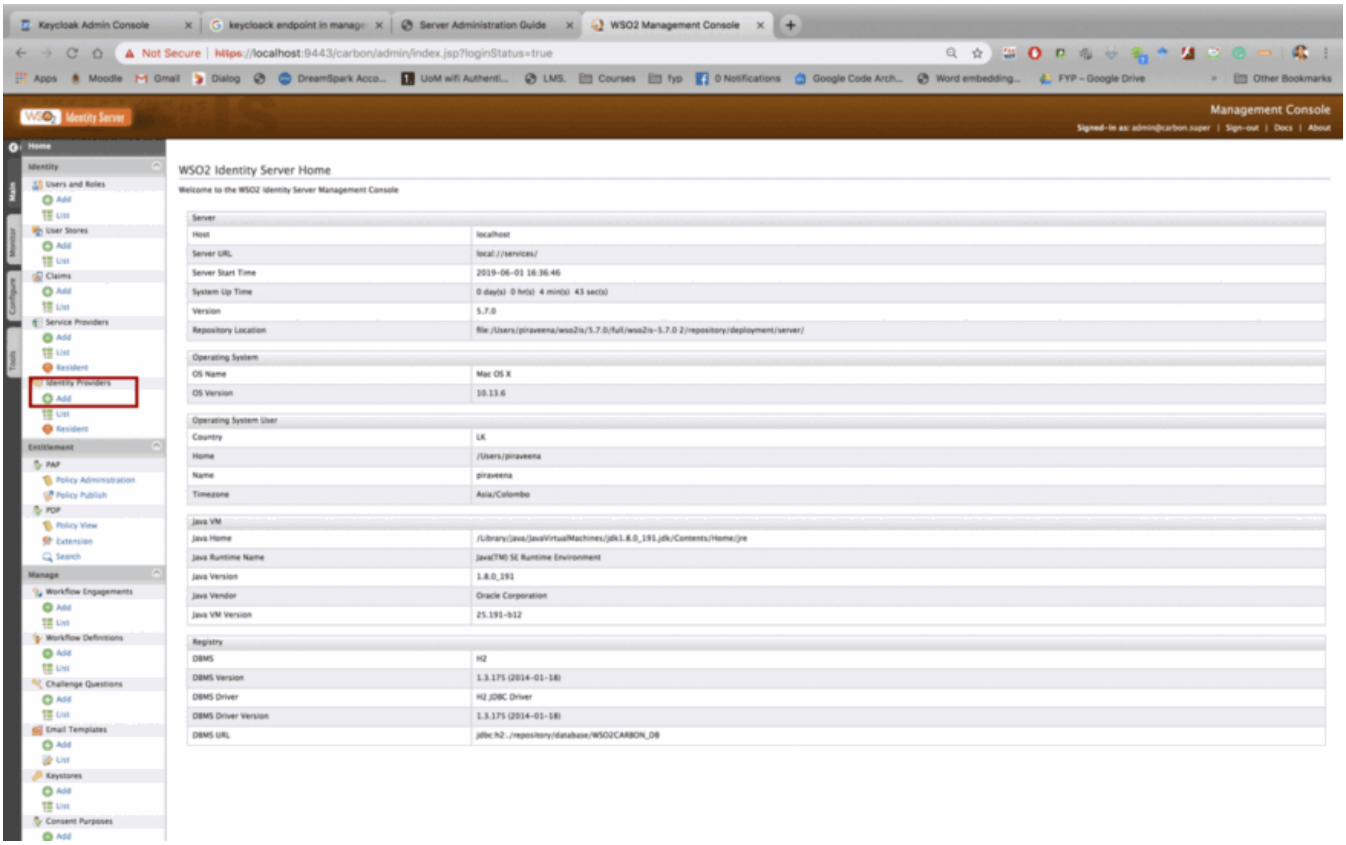


2. Configure Keycloak as a Federated Identity Server in WSO2 Identity Server.

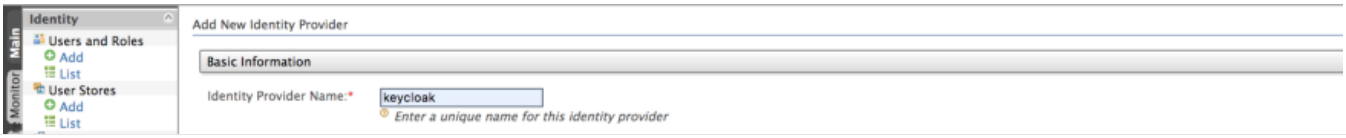
- Run WSO2 Identity server.

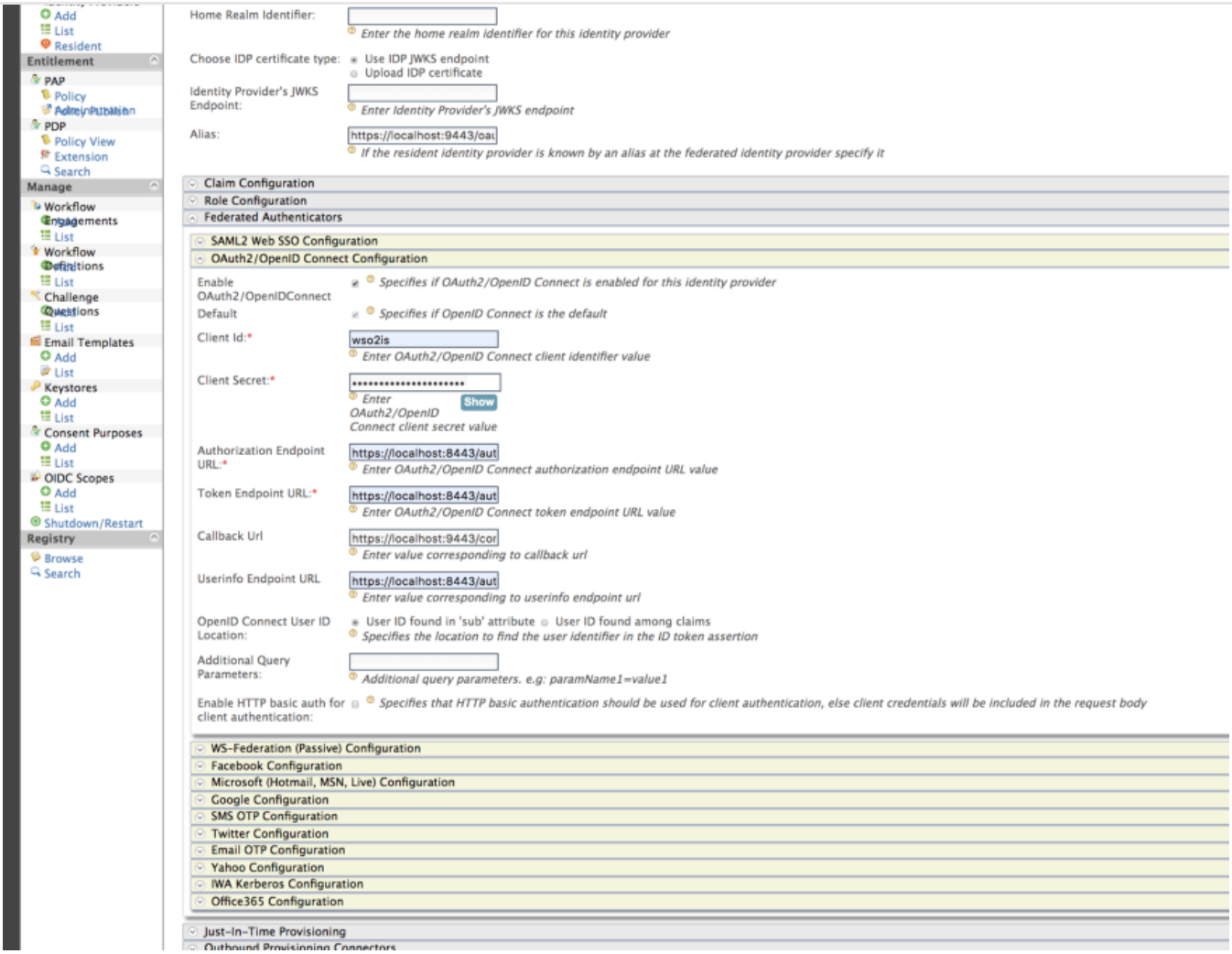
```
sh wso2server.sh
```

- Go to management console (https://localhost:9443/carbon)
- Navigate to Main > Identity> **Identity Providers** and click on **Add**.



- Now click on Add Identity provider. Add details of Identity Provider.





Authorization endpoint:
https://localhost:8443/auth/realms/master/protocol/openid-connect/auth

Token endpoint:
https://localhost:8443/auth/realms/master/protocol/openid-connect/token

Callback Url : https://localhost:9443/commonauth

UserInfo endpoint:
https://localhost:8443/auth/realms/master/protocol/openid-connect/userinfo?schema=openid

- You can check oidc enpoints of keycloak from here [1]

3. Import Keycloak certificate in Identity Server's truststore

To ensure the trust relationship, the public certificate of Keycloak need to be imported in to IS truststore.

- Shutdown keycloak server and Identity Server
- Go to **<KEYCLOAK_HOME>/standalone/configuration**
- Remove existing application.keystore file and create new keystore. Here the **CN name** and the **host name** of keycloak should match.
- In my example, both are localhost.

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -validity
3650 -keystore application.keystore -dname
"CN=localhost,OU=Support,O=WSO2,L=Colombo,S=Western,C=LK" -storepass
password -keypass password -noprompt

keytool -export -alias server -file keycloak.crt -keystore
application.keystore -storepass password -noprompt
```

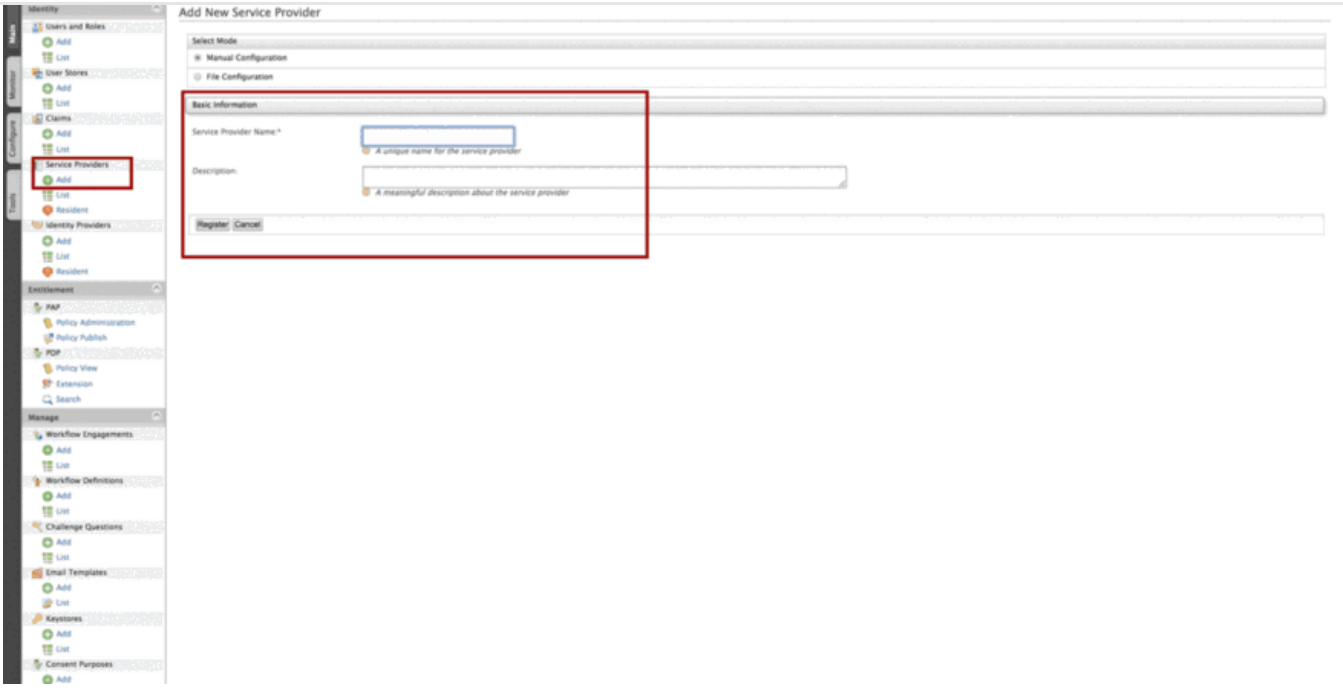
- Now you can see keycloak.crt file in the folder <KEYCLOAK_HOME>/standalone/configuration. Now you can export the public certificate into IS truststore.
- Copy the server.crt file into the folder certificate and Go to <IS_HOME>/repository/resources/security and paste there. Now execute the following command and Import the server.crt to client-truststore.jks

```
keytool -import -trustcacerts -alias keycloak -file keycloak.crt -
keystore client-truststore.jks -storepass wso2carbon -noprompt
```

- Restart both servers.

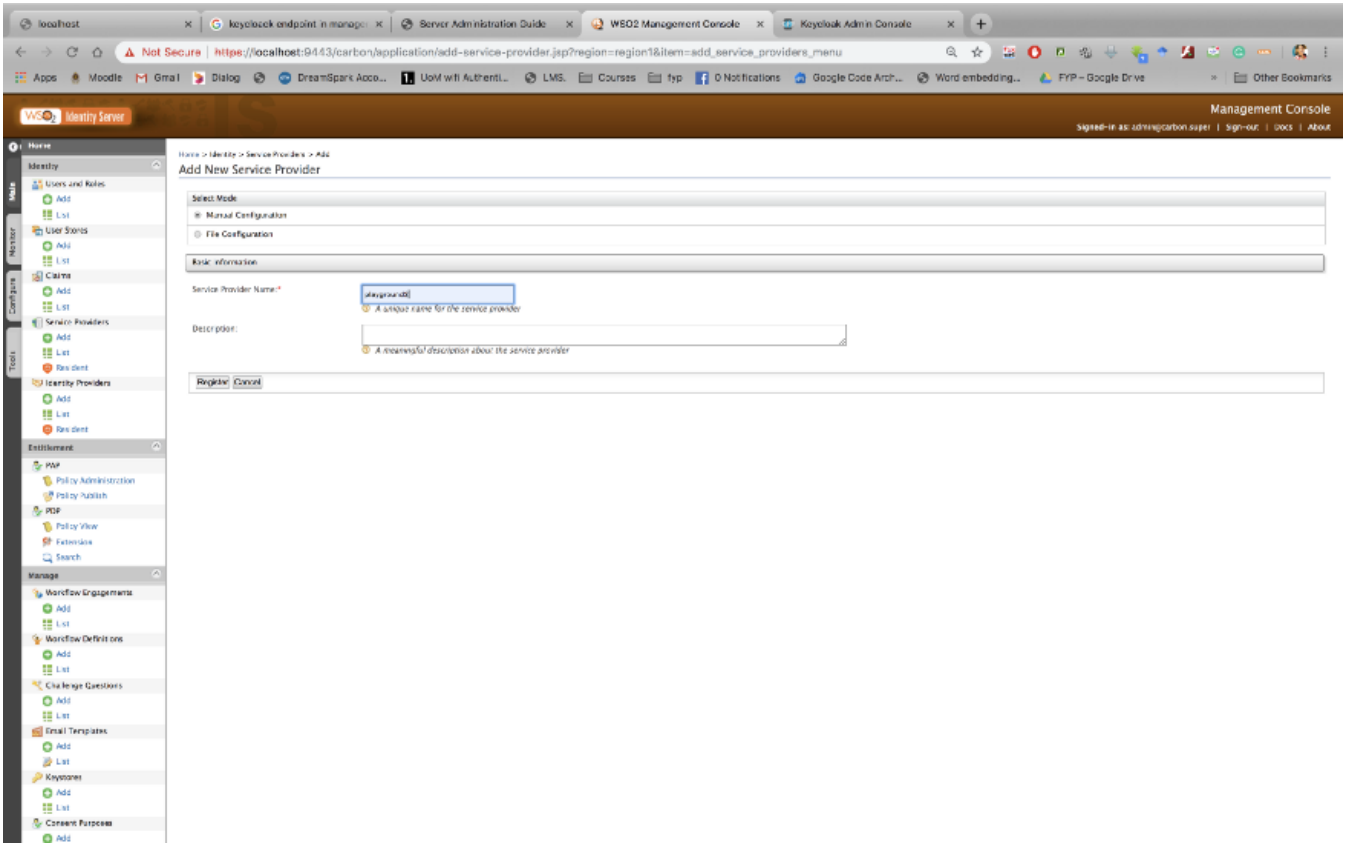
4. Configure a Service provider in WSO2 Identity Server

- Navigate to Menu> Identity> **Service Providers** and click on **Add**

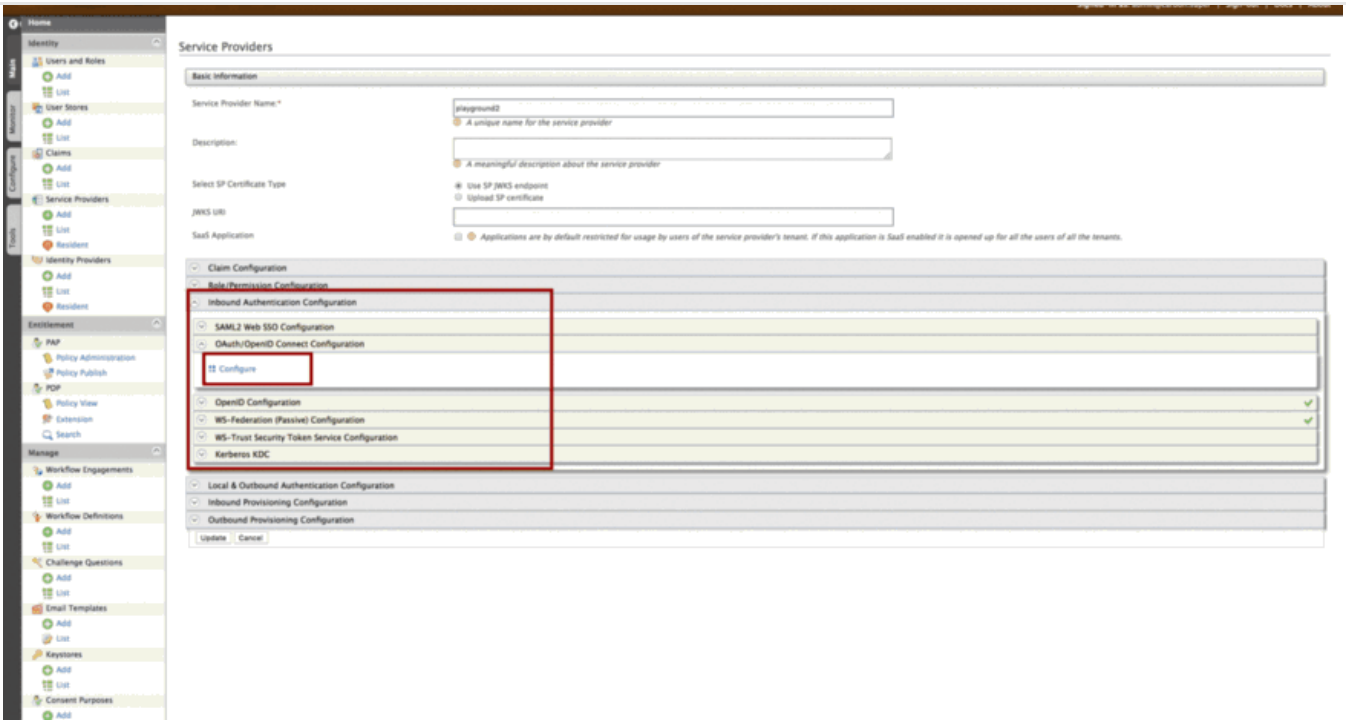


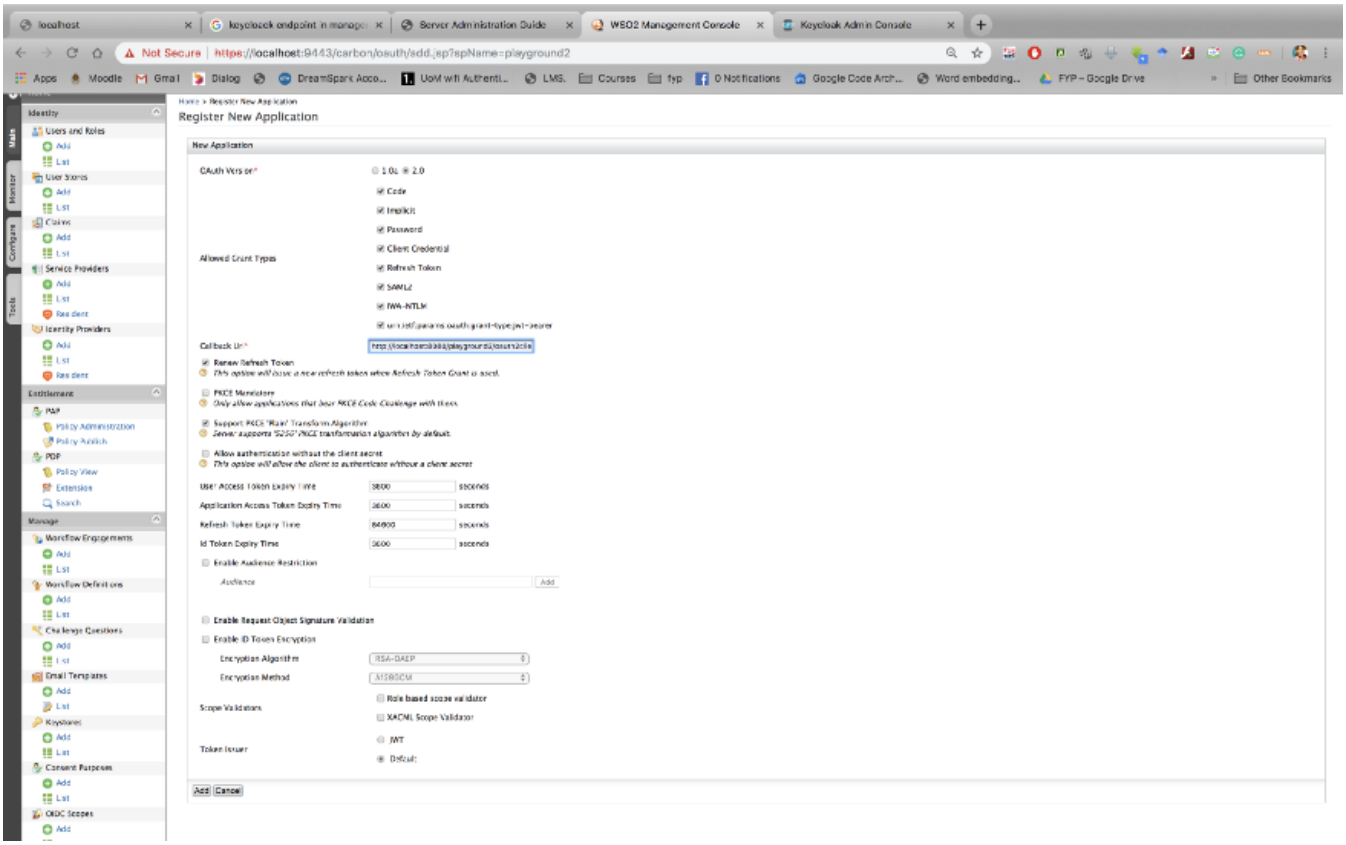
- Provide service provider's **name** and **description**. Click on **Register.**

Here I'm going to register playground as a service provider.



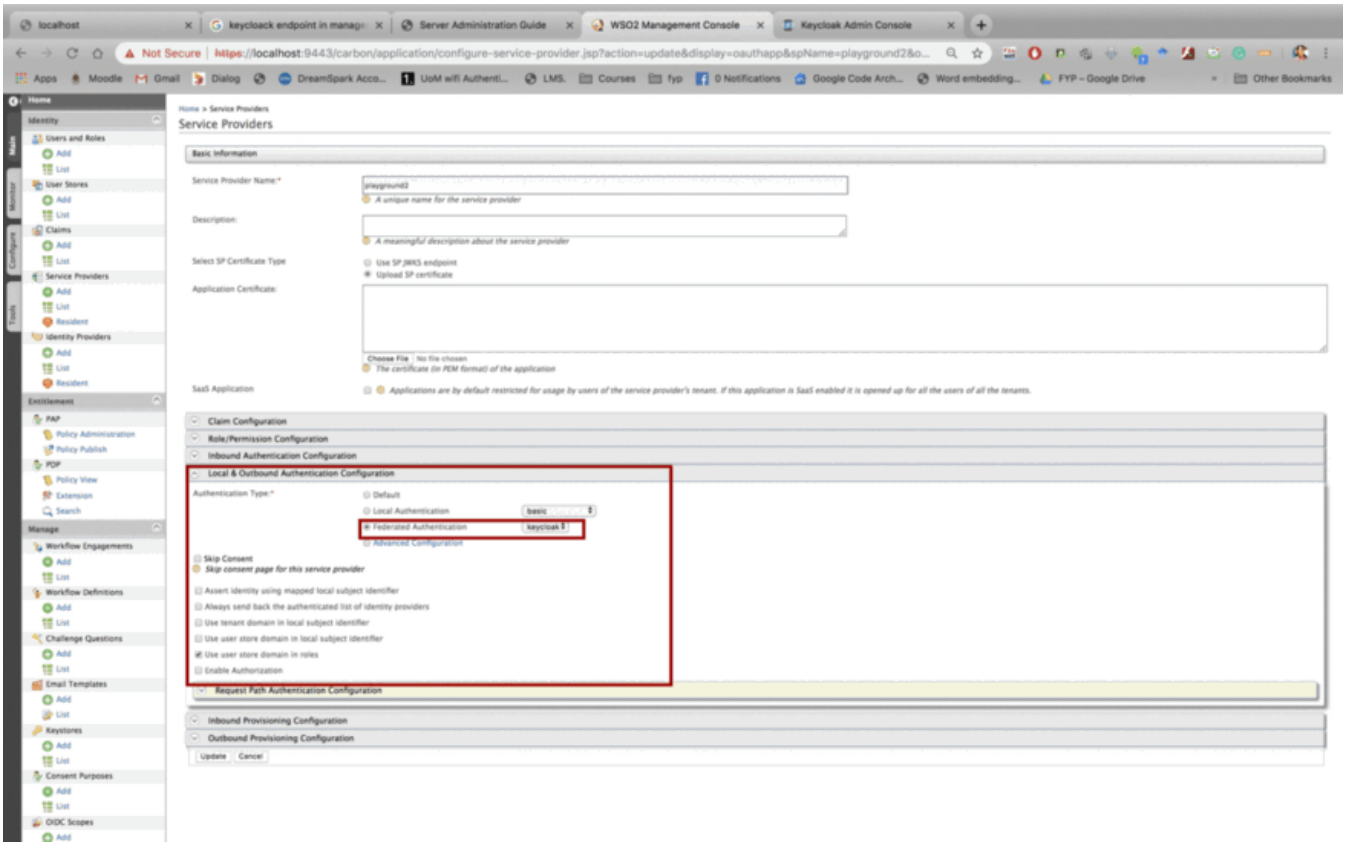
- Navigate to **Inbound Authentication Configuration > OAuth/OpenID Connect Configuration.** Click on **Configure.**





Callback Url of Playground app : http://localhost:8080/playground2/oauth2client

- Navigate to **Local & Outbound Configuration** and open the menu. Make the **Authentication Type** as **Federated Authentication** and the IDP as **Keycloak**



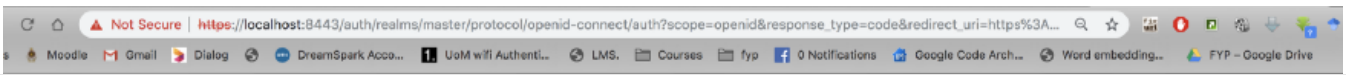
- Click on Update.
- Now you have configured Playground service provider with federated IDP as Keycloak.

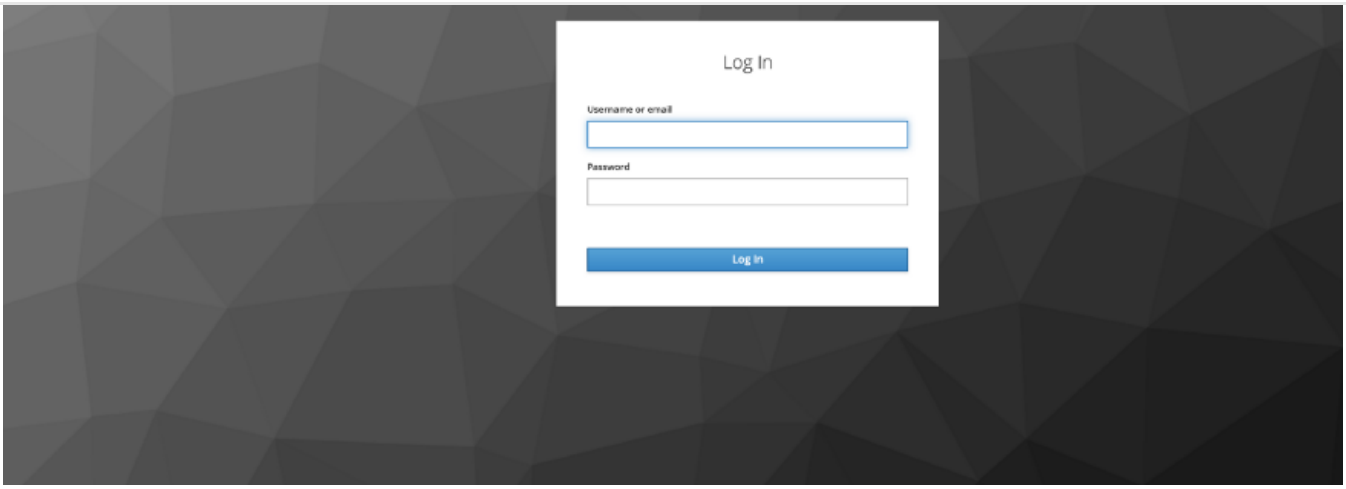
Try it out !

- Call the authorize endpoint of WSO2 Identity Server with oidc implicit flow.

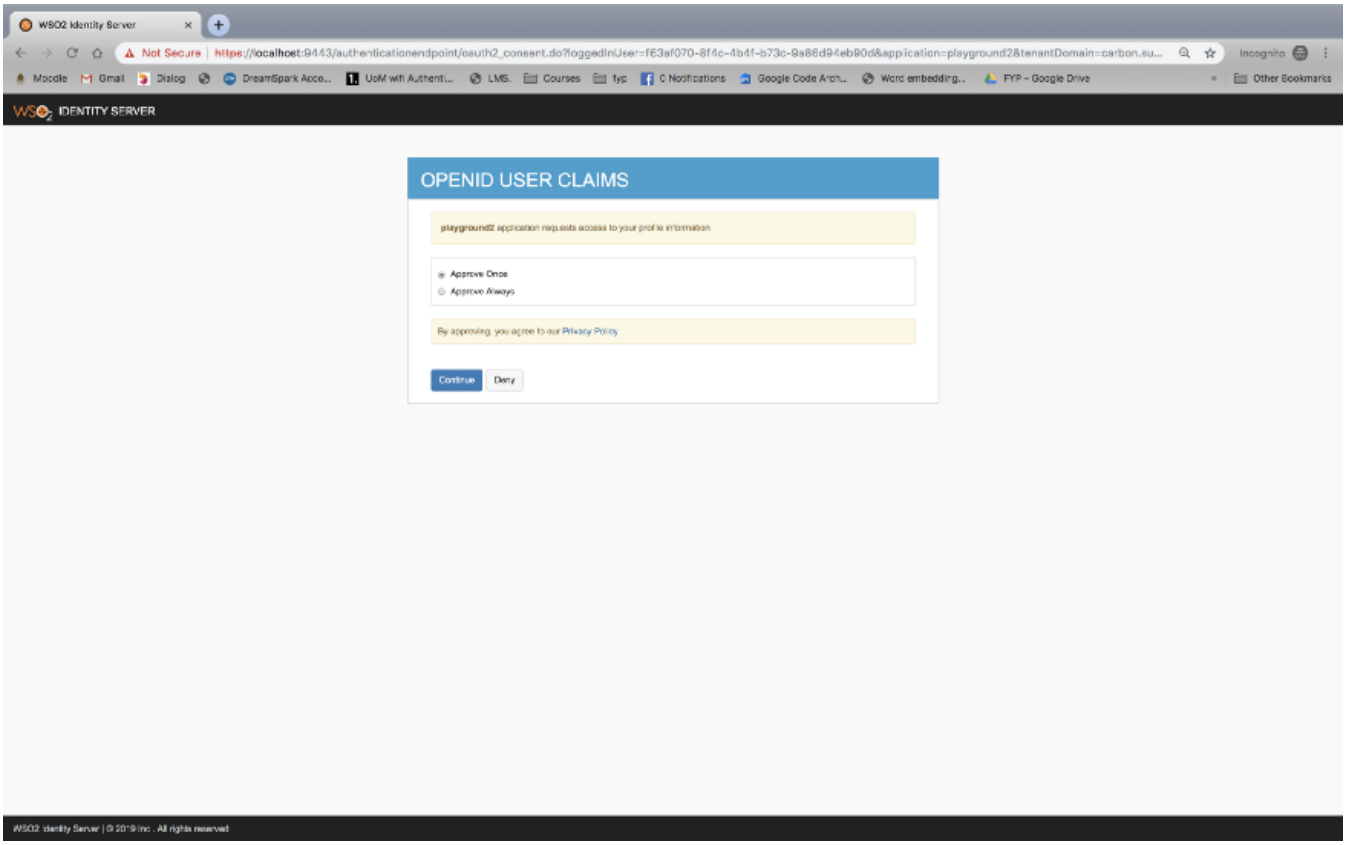
```
https://localhost:9443/oauth2/authorize?
response_type=id_token%20token&scope=openid&redirect_uri=http%3A%2F%
2Flocalhost%3A8080%2Fplayground2%2Foauth2client&client_id=
<client_id>&nonce=n-0S6_WzA2Mj
```

- You will be redirected to key cloak login page.





- Provide the user credentials and login.
- You will be redirected to the consent page of Identity Server.



- Once you approve this you can get the access token and idtoken.

[1]https://www.keycloak.org/docs/latest/server_admin/index.html#keycloak-

[2]https://docs.wso2.com/display/IS570/Configuring+Federated+Authentication

Wso2 Wso2is Identity Management Keycloak