**KeyClock**

# KeyClock Configuration:-

1. Configuring Java in KeyClock.

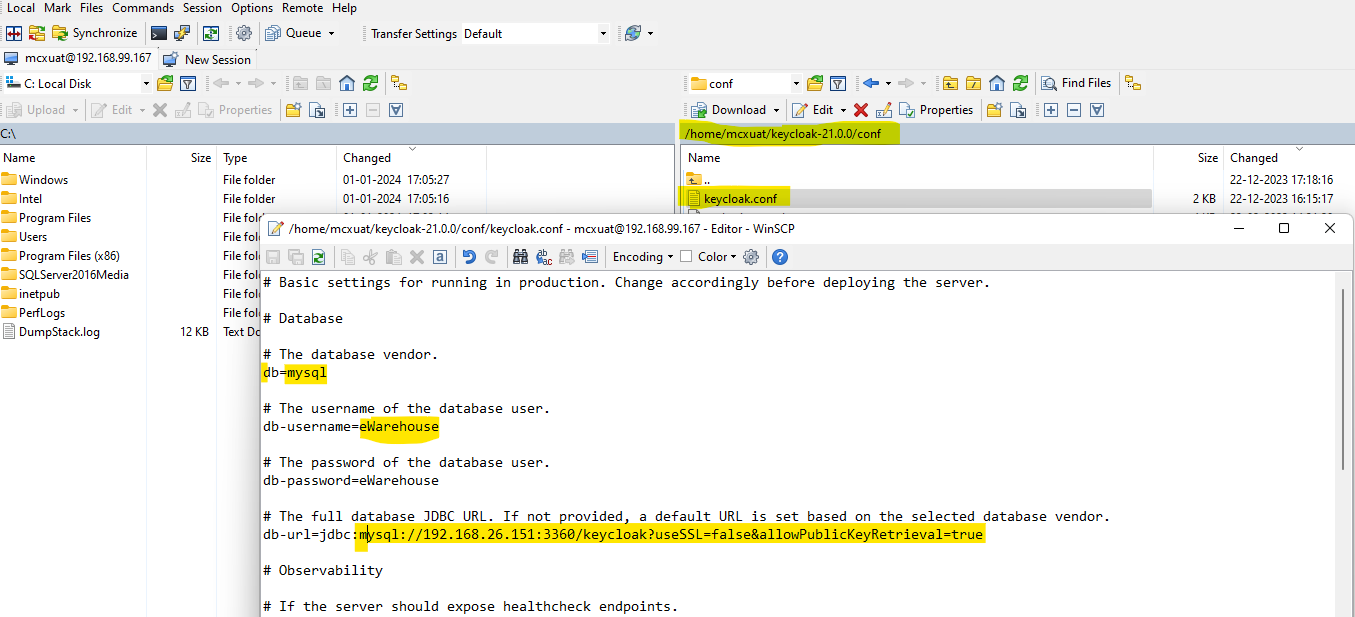
Paste the JAVA\_HOME="/home/mcxuat/jdk-11.0.20" in the Kc.sh file in /home/mcxuat/keycloak-21.0.0/bin/Kc.sh as shown below.

A screenshot of a computer

Description automatically generated

1. Configuring MySQL database in KeyClock:

Mention the db, db username and password, d burl as shown below.



1. KeyClock Database creation in MySQL.

Create schema with name KeyClock. All the related database table will be created at the start of KeyClock server 1st time.

A screenshot of a computer

Description automatically generated

1. Port Configuration in KeyClock.

A screenshot of a computer

Description automatically generated

1. Starting KeyClock service

Go path: /home/mcxuat/keycloak-21.0.0/bin/

Paste the command : KEYCLOAK\_ADMIN=admin KEYCLOAK\_ADMIN\_PASSWORD=admin ./kc.sh start-dev

To run the service in background, use the same command with “&” in the end.

KEYCLOAK\_ADMIN=admin KEYCLOAK\_ADMIN\_PASSWORD=admin ./kc.sh start-dev &

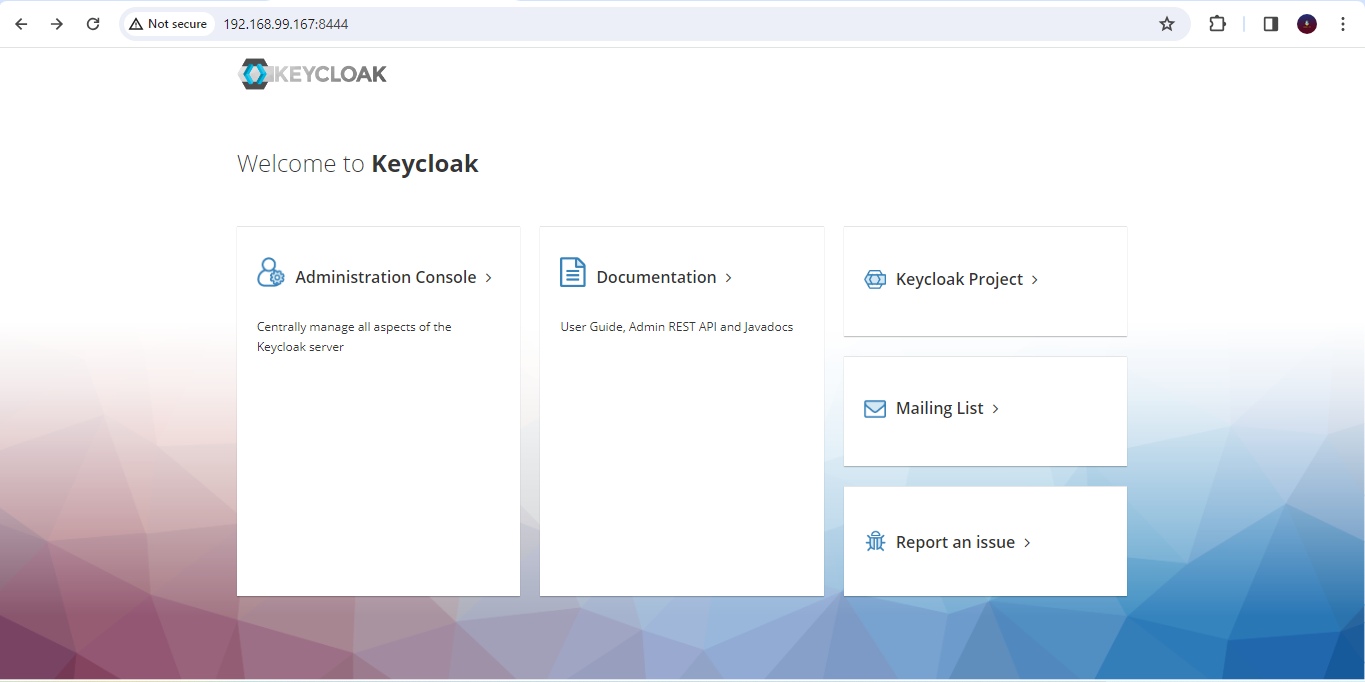
# User registration

1. Details required for User creation.

MCX members will share member/User details on email to MCX administrator to register the member in KeyClock server. Following member details would be shared on email.

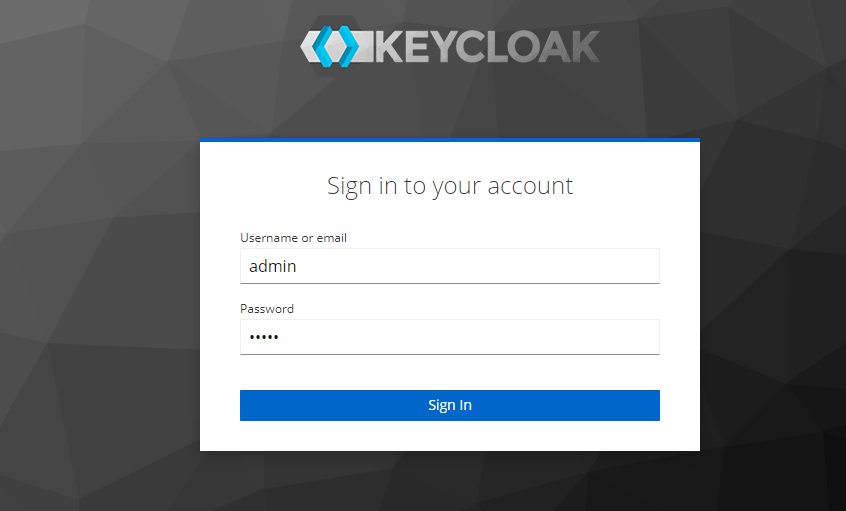
|  |  |
| --- | --- |
| **Particulars** | **Details** |
| Contact Number | 8802766277 |
| Email id | [srikrishan@globecapital.com](mailto:srikrishan@globecapital.com) |
| Static IP | 14.143.36.10 |
| CM ID  & Name | 8550 – AY Securities and Commodities ltd |

1. Registering User in KeyClock.
   1. Access KeyClock console using <http://192.168.99.167:8444/> in UAT. After clicking the given link you will see the following screen.



* 1. Login with admin user.

UserId : admin Password: admin



* 1. Now create a Realm with name “Collateral” for collateral API. Similarly one can create multiple realms as per requirement.

A screenshot of a computer

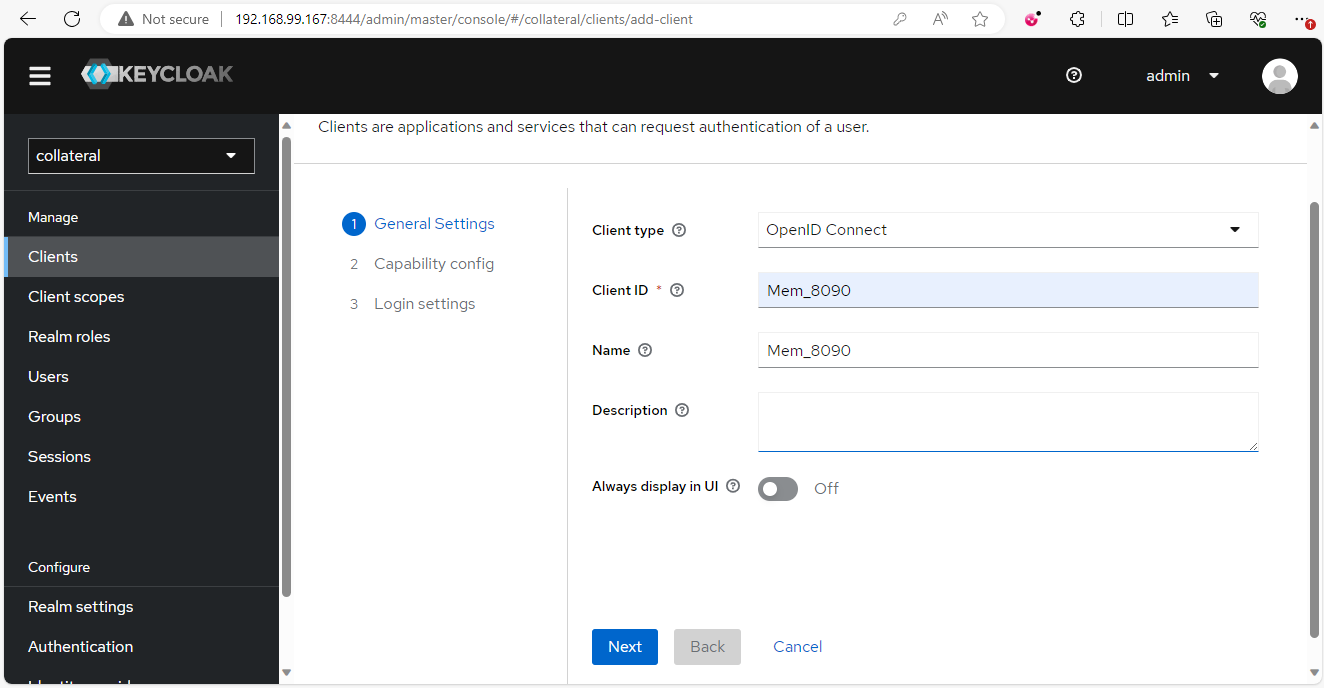
Description automatically generated

* 1. Now click on client menu, to create a new client.

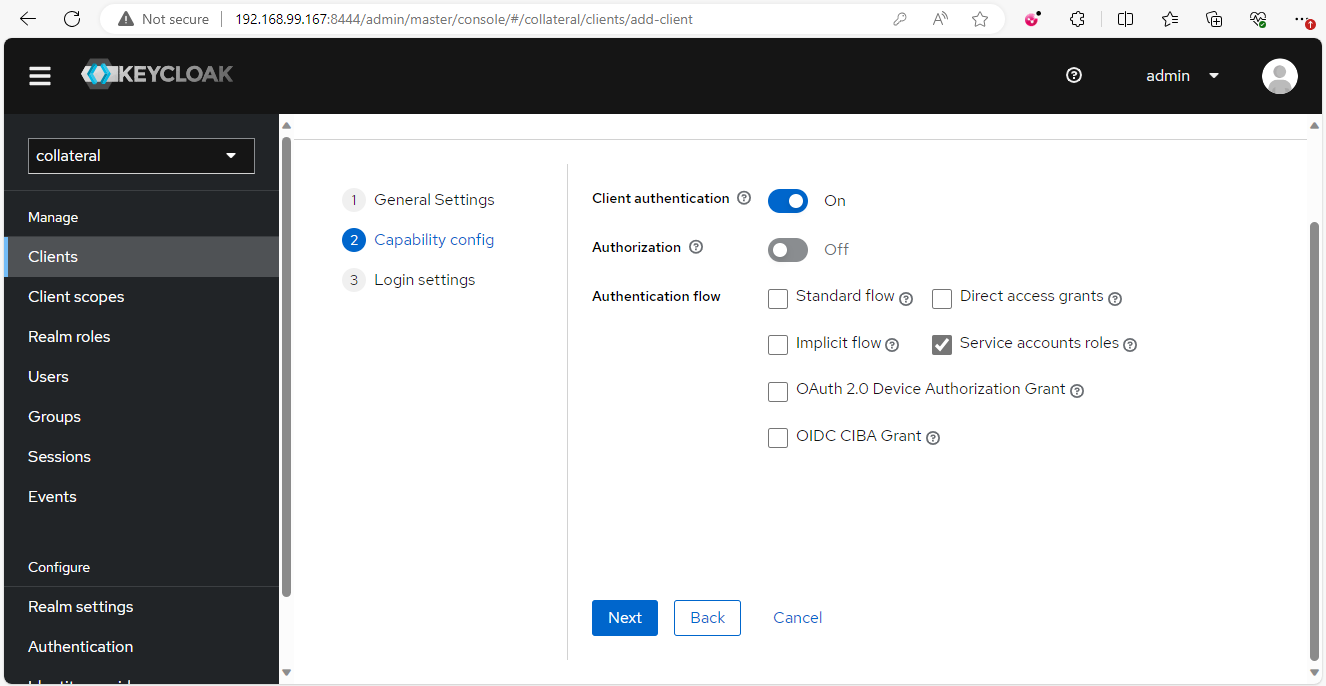
A screenshot of a computer

Description automatically generated

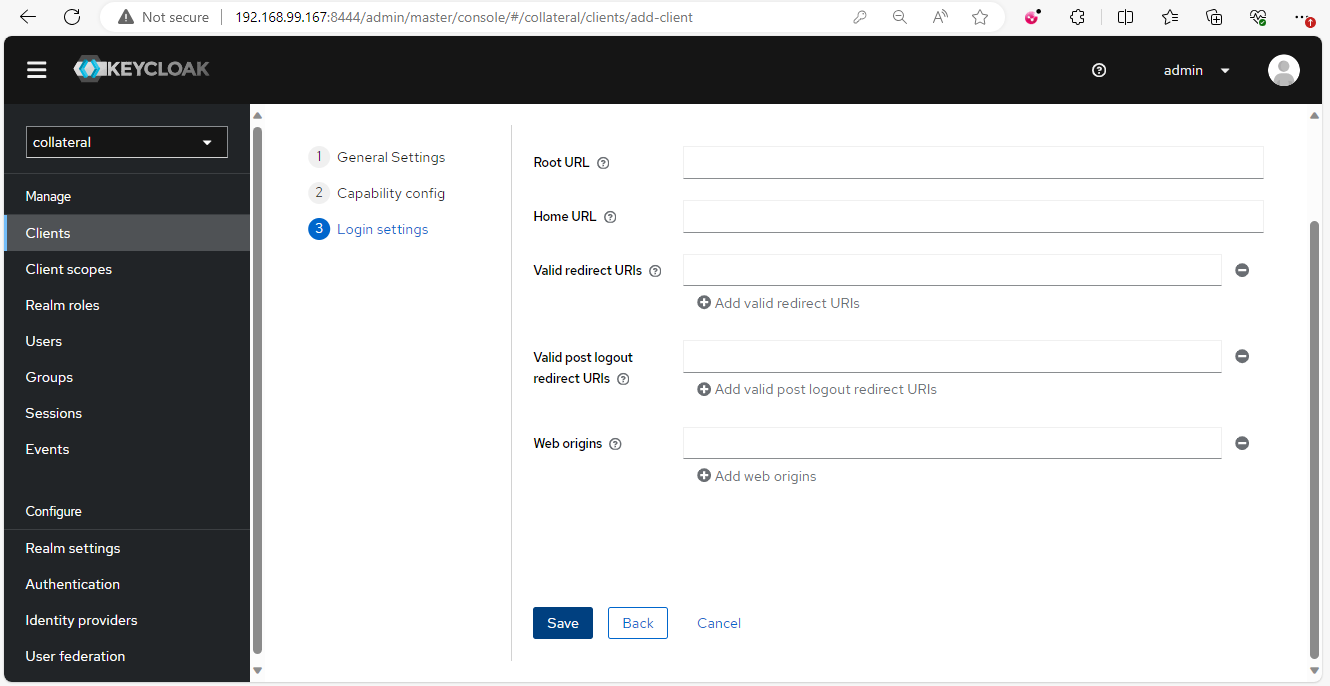
* 1. Go to Create client. After clicking on create client you will see the following screen.



* 1. Now mention ClientID (format for creating client should be “Mem\_memberid”) and client name(Same as ClientId) and click next. After clicking on next you will have to select the capability config as follows.



After choosing the client authentication and service accounts roles click next. After clicking you will see the login settings page.

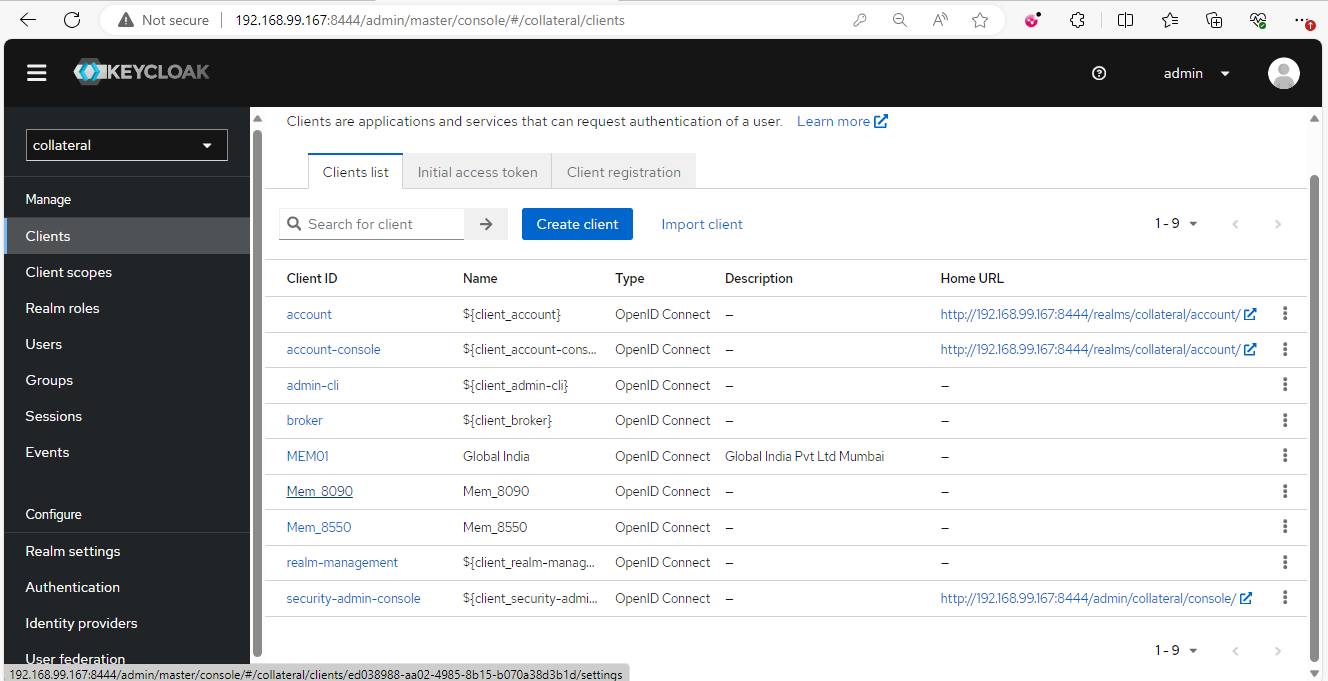


On this page we don’t have mention anything and just click on save. We have successfully created a client. With Client, a service account user is also created as below ( e.g., service-account-mem\_8090) for grant\_type client\_credentials.

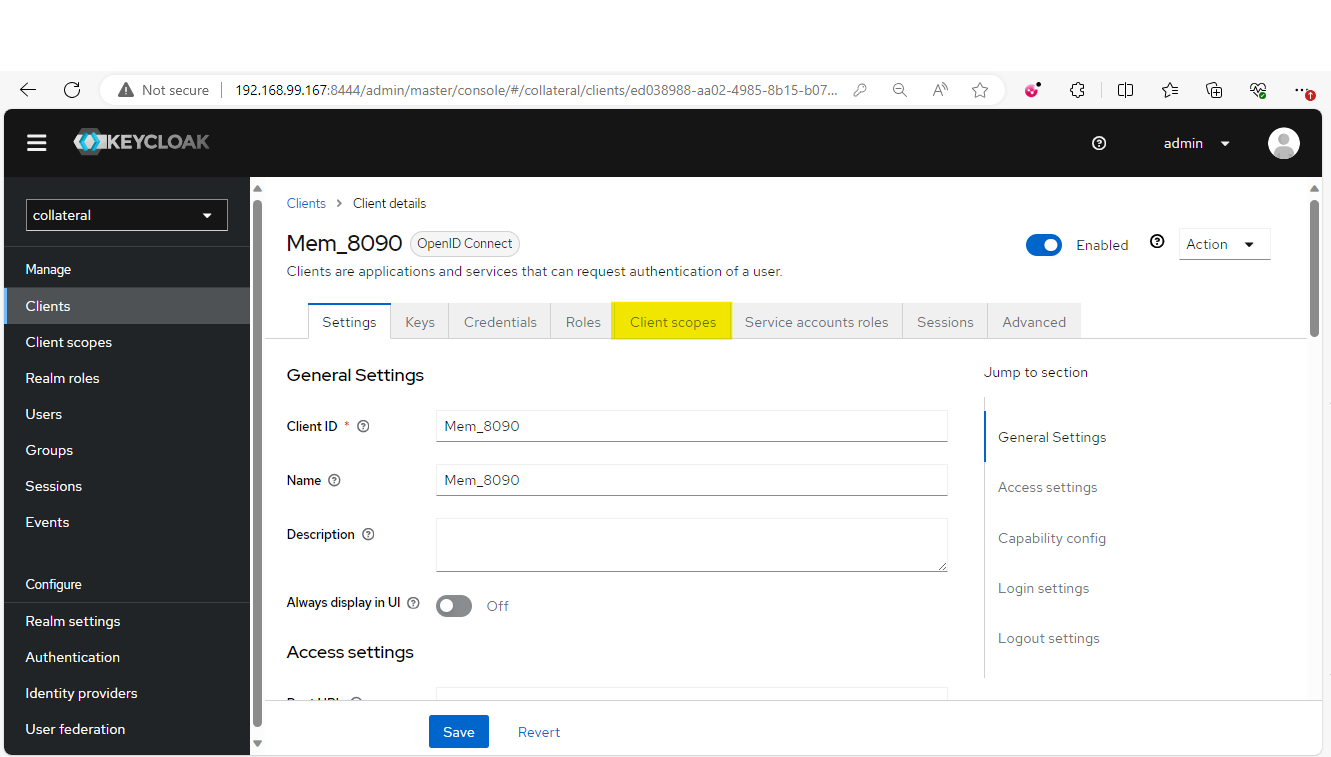
A screenshot of a computer

Description automatically generated

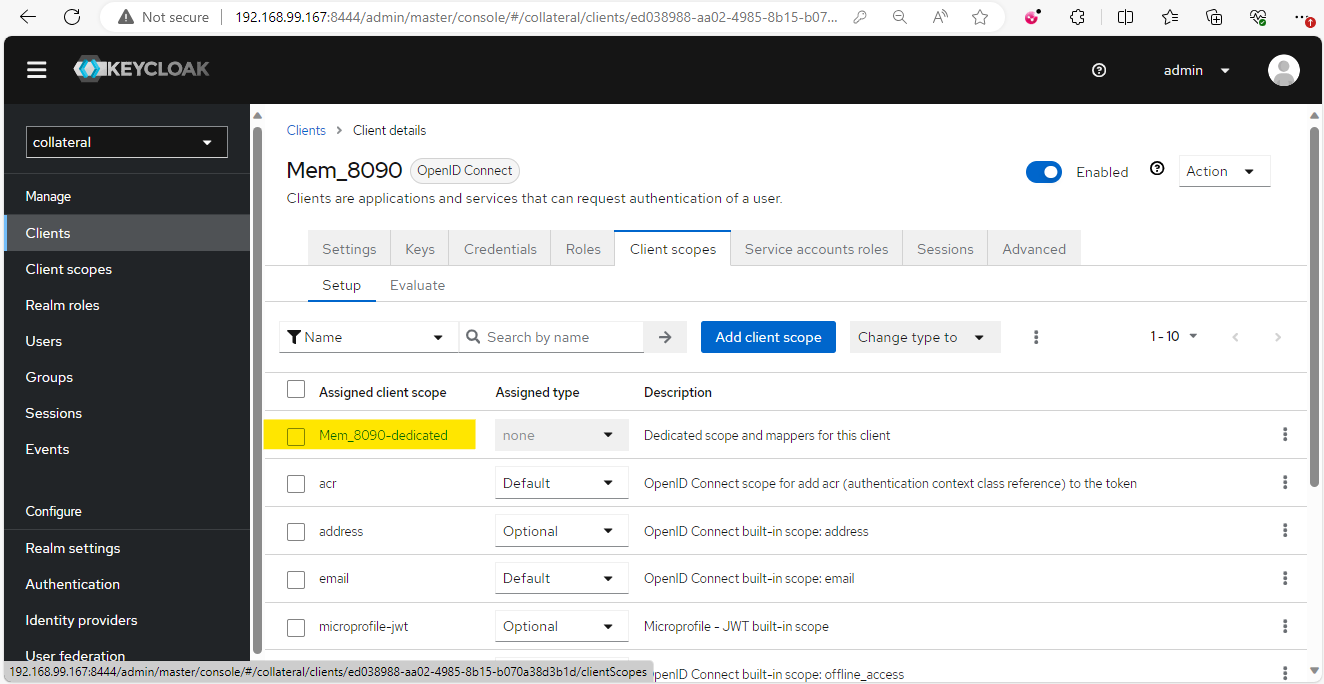
* 1. Now, after creating a client we will add details of the following client in client scope tab. In client menu, click on the new client you created (e.g., Mem\_8090)



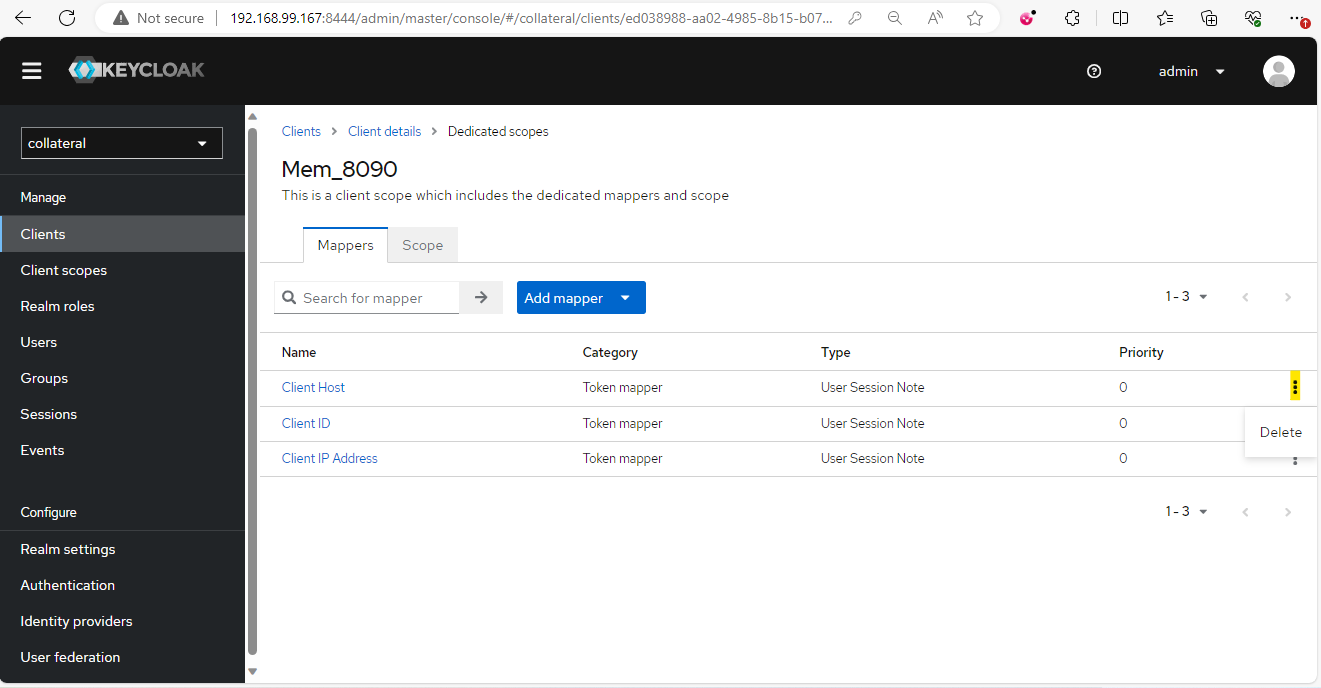
After clicking on the new client you created, you will see the following page.



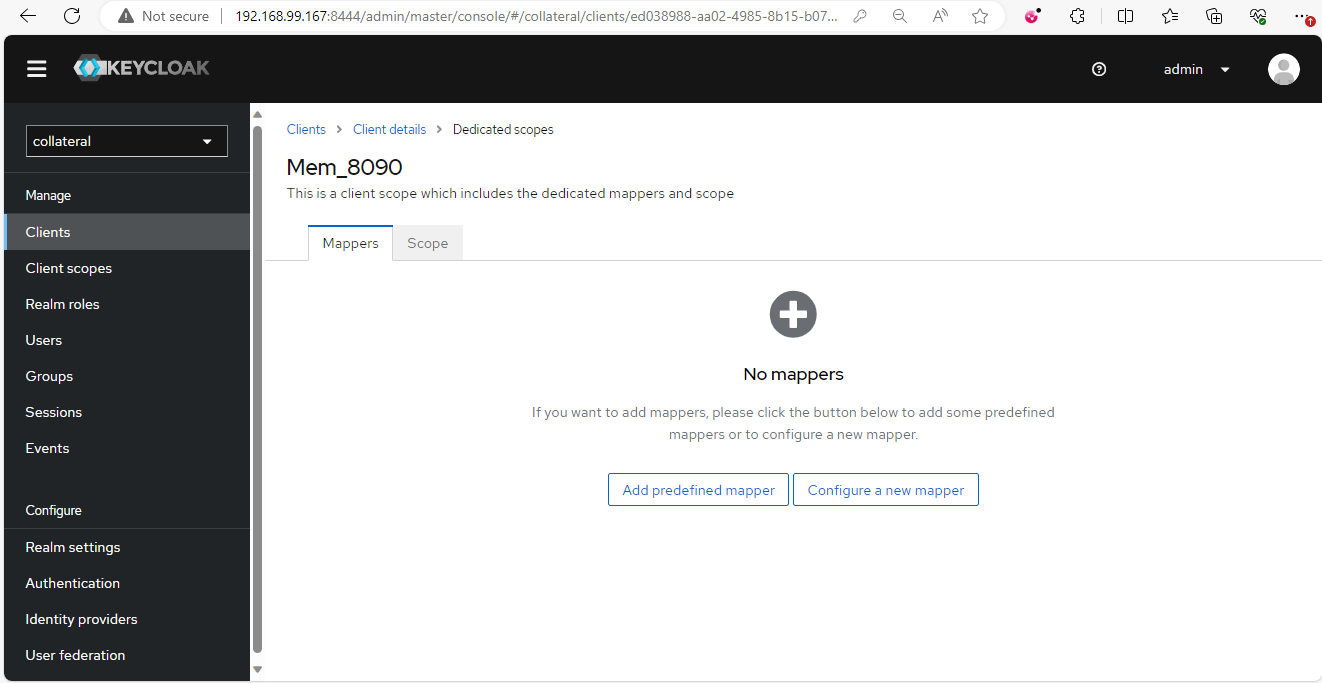
Now click on Client scopes as highlighted in the above screen. After clicking on Client scopes, you will see the following screen.



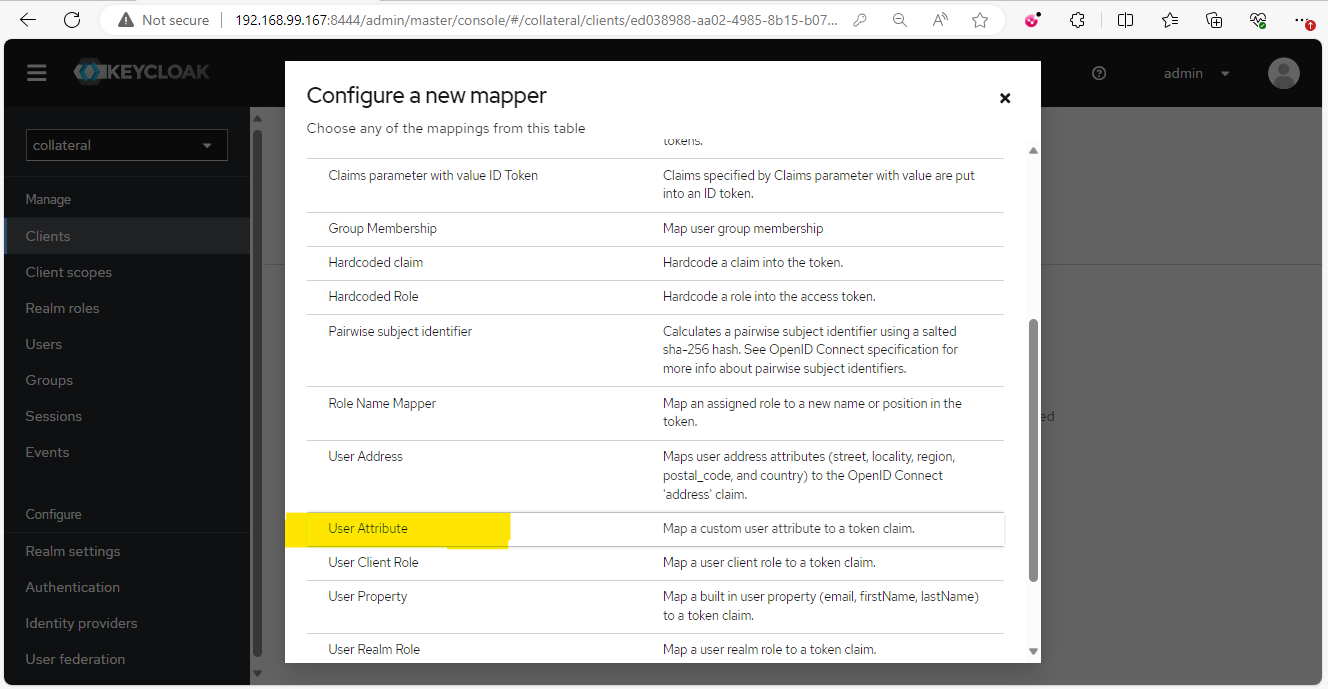
Now for adding mapper click on the Dedicated scope and mappers option as highlighted in above image (e.g., Mem\_8090-dedicated). After clicking on the above option, you will see the following screen.



* 1. Here, first we will delete the existing Client mappers by clicking on the 3 dots on the right corner. After deleting the mappers, the screen will look like below.



Now click on Configure a new mapper, after clicking on configure a new mapper you will get a pop-up page.



Click on User Attribute as shown in above screen. After clicking on User Attribute, you will get following screen. To customize the access token, we need to add following attributes as user attributes.

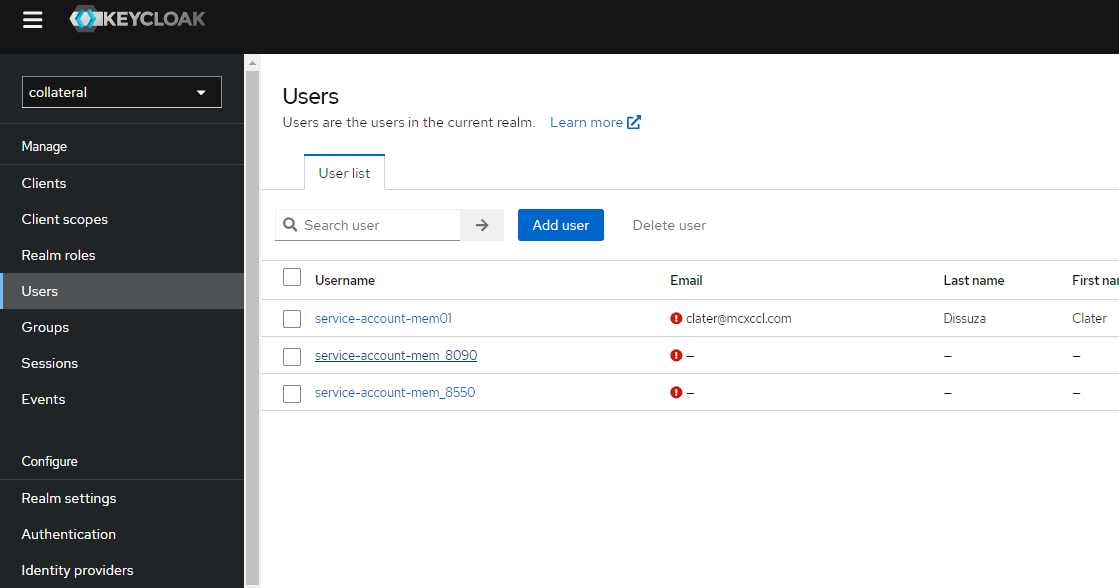
|  |  |
| --- | --- |
| **Sr. no.** | **Attributes** |
| 1 | userId |
| 2 | ipAddress |
| 3 | phone |
| 4 | fullName |
| 5 | email |

Configure attribute “userId” as shown below.

A screenshot of a computer

Description automatically generated

* 1. Go to User menu and select service\_account\_(created\_user)

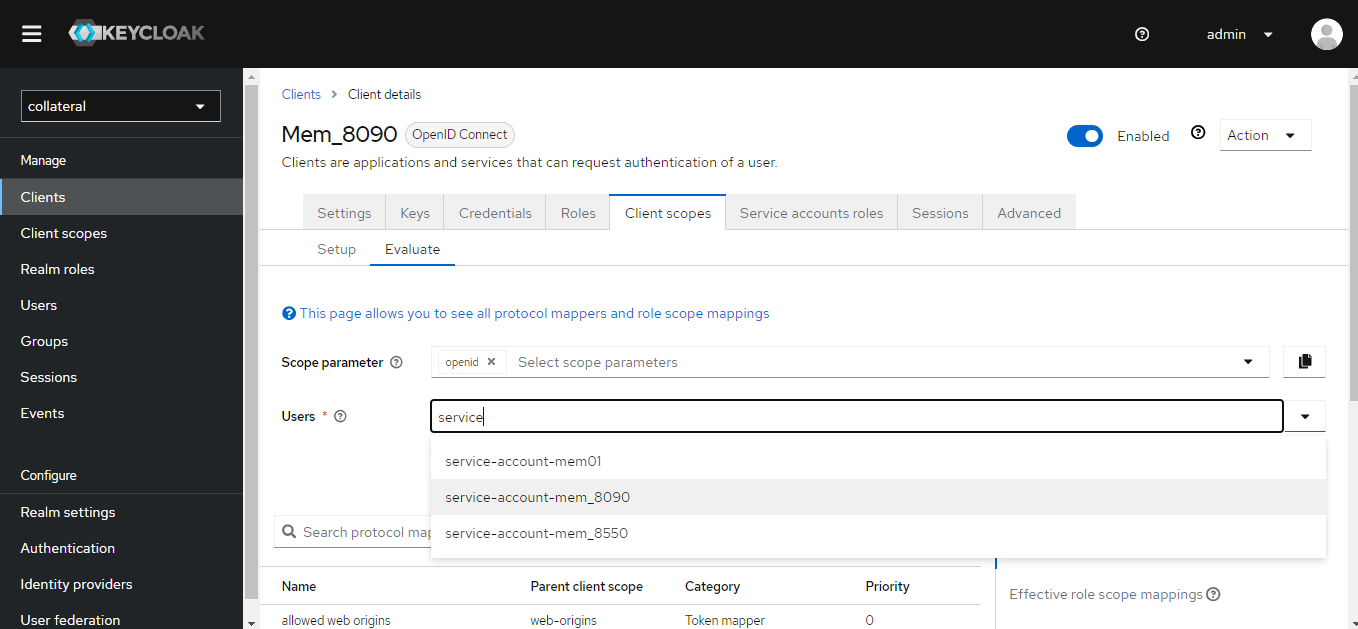


Here we will add attributes.

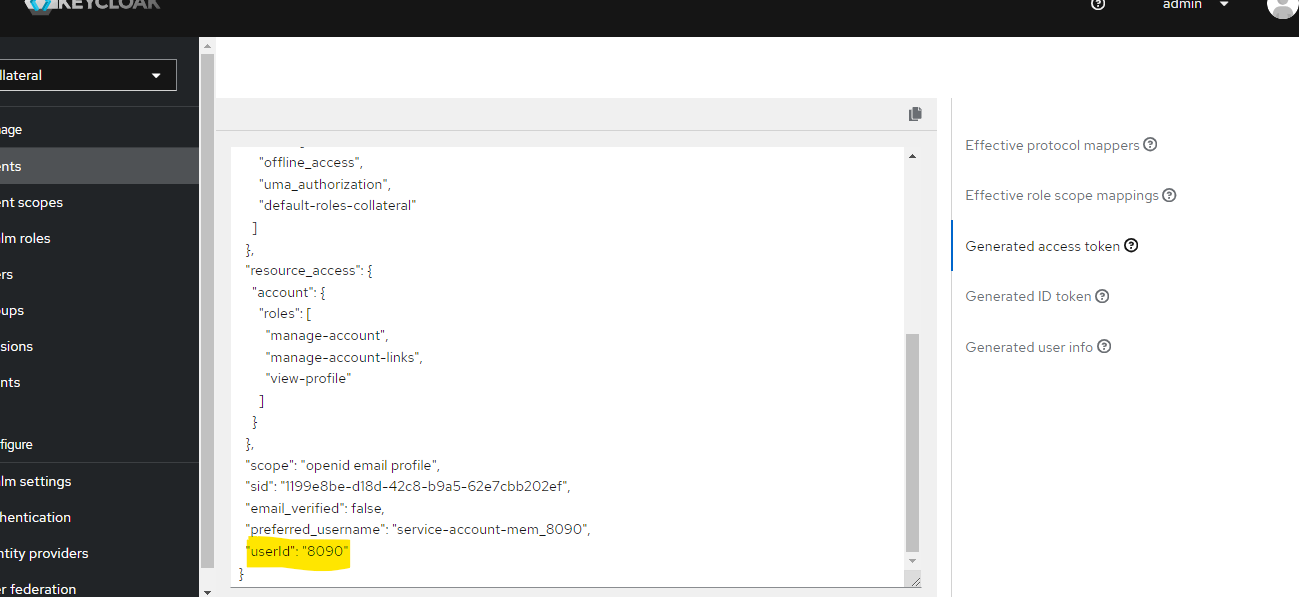
A screenshot of a computer

Description automatically generated

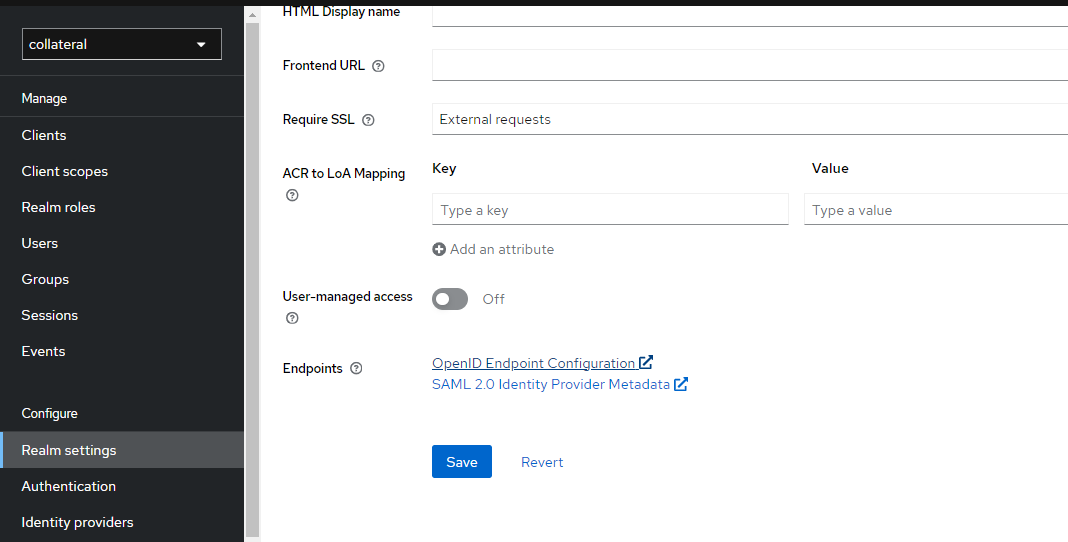
* 1. To verify that the attribute is reflected in token, go to Client menu > Client scopes > evaluate and search the user you created as follow.



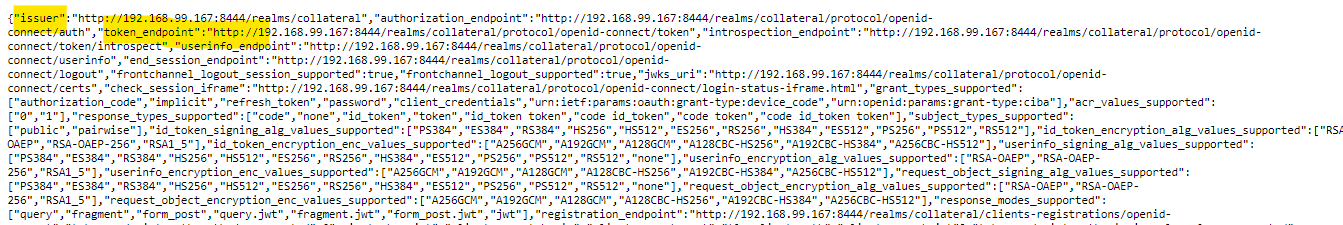
Now click on Generated access token and verify if the user id is available in token.



Similarly add other attributes ipAddress, phone, fullName, email to display in the token. To get the token and issuer URL go to Realm settings and click on “OpenID Endpoint Configuration”.

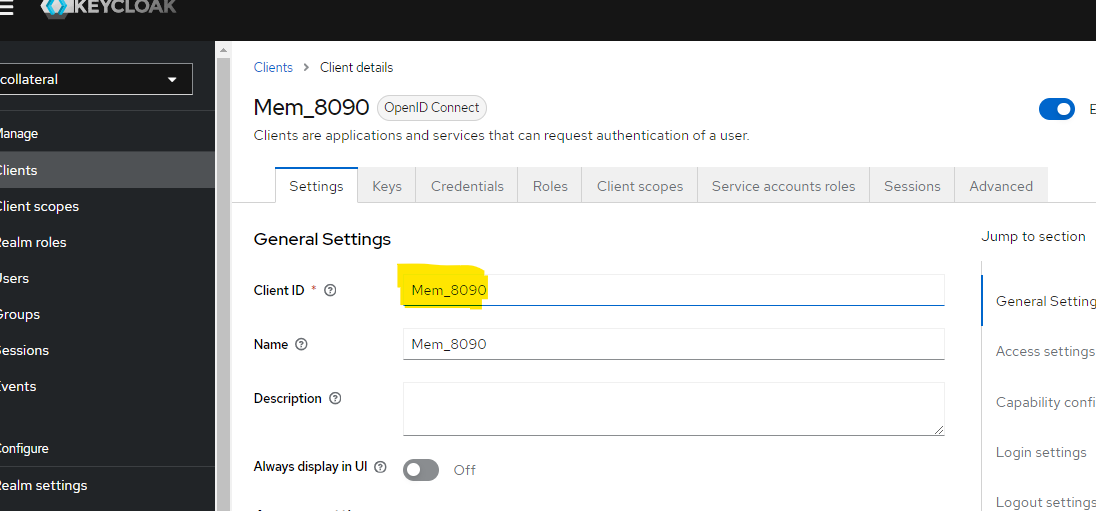


Here you can find the Issuer URL and token URL.



And after completing the registration process, we will share the Client\_ID and Client\_secret to member on email.

Cllient\_ID:



Client\_Secret:

A screenshot of a computer

Description automatically generated

1. Token generation by client application:

