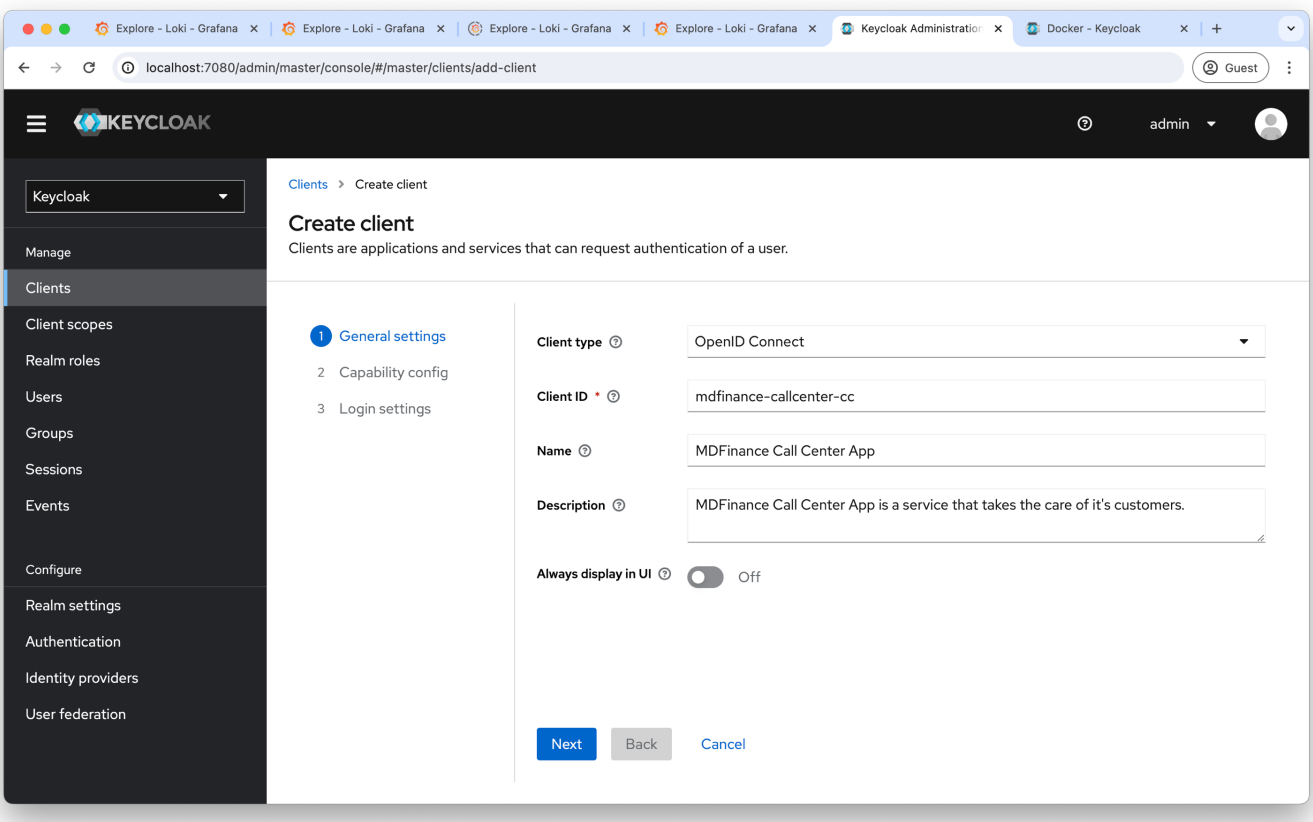
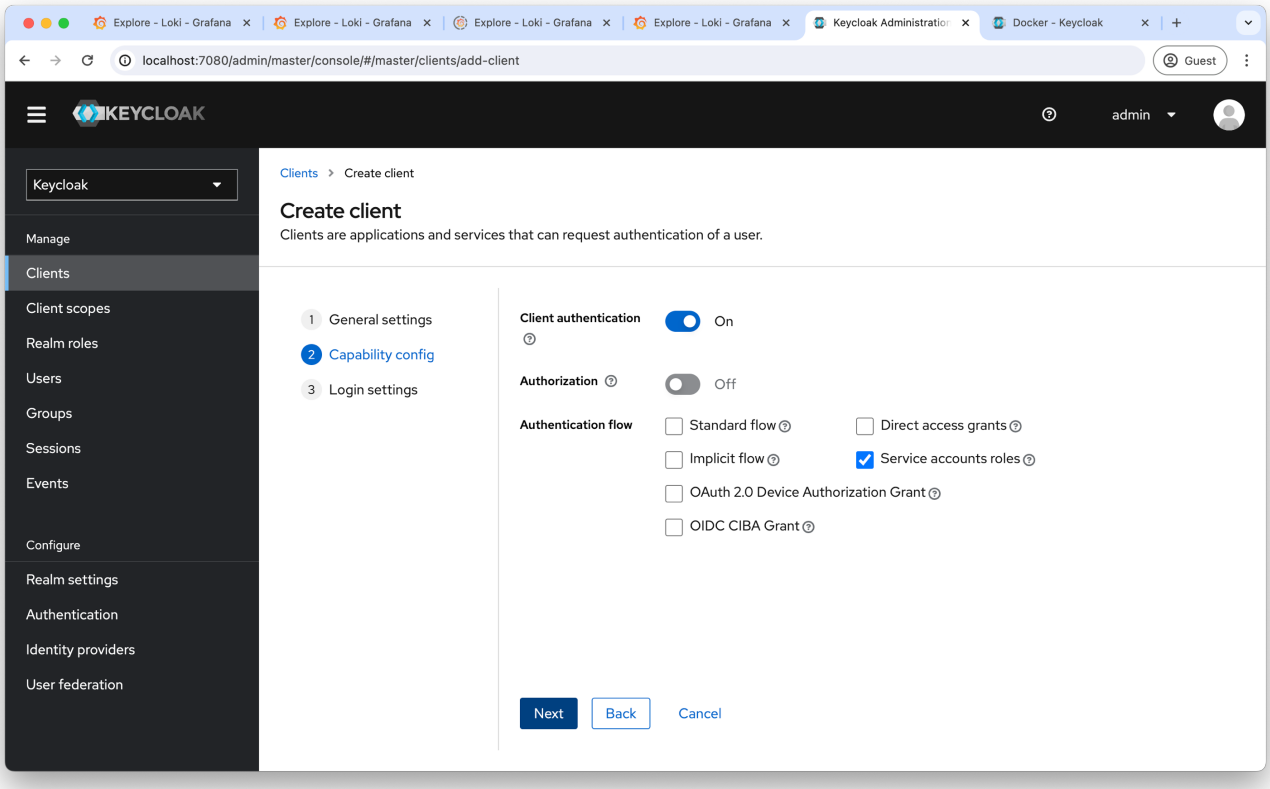
OAUTH2

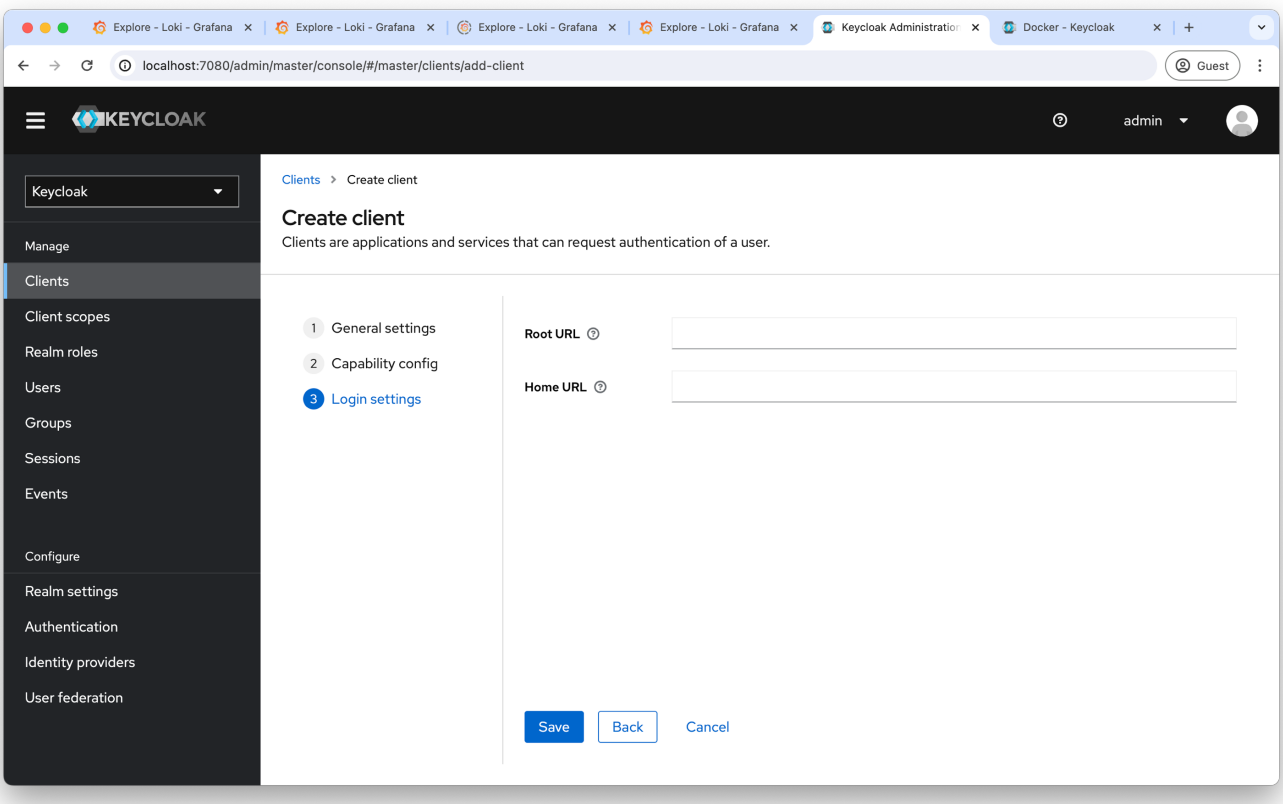
- Back in the early days of web invention, all websites they usually ask for credentials of an end user inside an HTML form. So the end user will enter his credentials.
- The same will be sent over to the backend server inside the backend server using the credentials provided by the end user, the authentication will be completed and after the successful authentication, the backend server is going to generate a session value and the same it is going to store inside a cookie of the browser.
- So as long as the session is active, the user can access the any protected resources and URLs. So this is how the basic authentication used to work. The drawbacks of this approach is backend server will have both business logic and authentication logic tightly coupled.
- So if there is a change that you need to make inside the authentication logic, then definitely you need to make sure that it is not going to impact your business logic.
- So there has to be enough regression has to be done. Because both the business logic and the authentication logic is deployed into a single server.
- Basic authentication flow does not accommodate well the use case where users of one product or service would like to grant third-party clients access to their information on the platform.

Know the difference between OpenID and OAUTH2

- Review all the slides and diagrams for "Client Credentials Grant Type Flow in OAUTH2"
- In Lecture 185, we are registering client details using keyClock
  - Assuming admins of keyClock and MDFinance has approved some clients coming to the application
  - Next step is to register their details using keyClock console. (Below screenshots are the sample)







Please note that the "credentials" will be be generated by "keyClock". Any client that want to access the resources from MDFinance has to first get the access token from Auth Server in our case they have to authenticate through keyClock by providing client-id and client-secret. As we can see in below screenshot.

client-id: mdfinance-callcenter-cc
client-secret: S8ez9SRi6Jnam2SWo0vWhP7vm6s4yFCV

Clients > Client details

mdfinance-callcenter-cc OpenID Connect

Enabled Action

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

Settings | Keys | Credentials | Roles | Client scopes | Service accounts roles | Sessions | Advanced

Client Authenticator Client Id and Secret

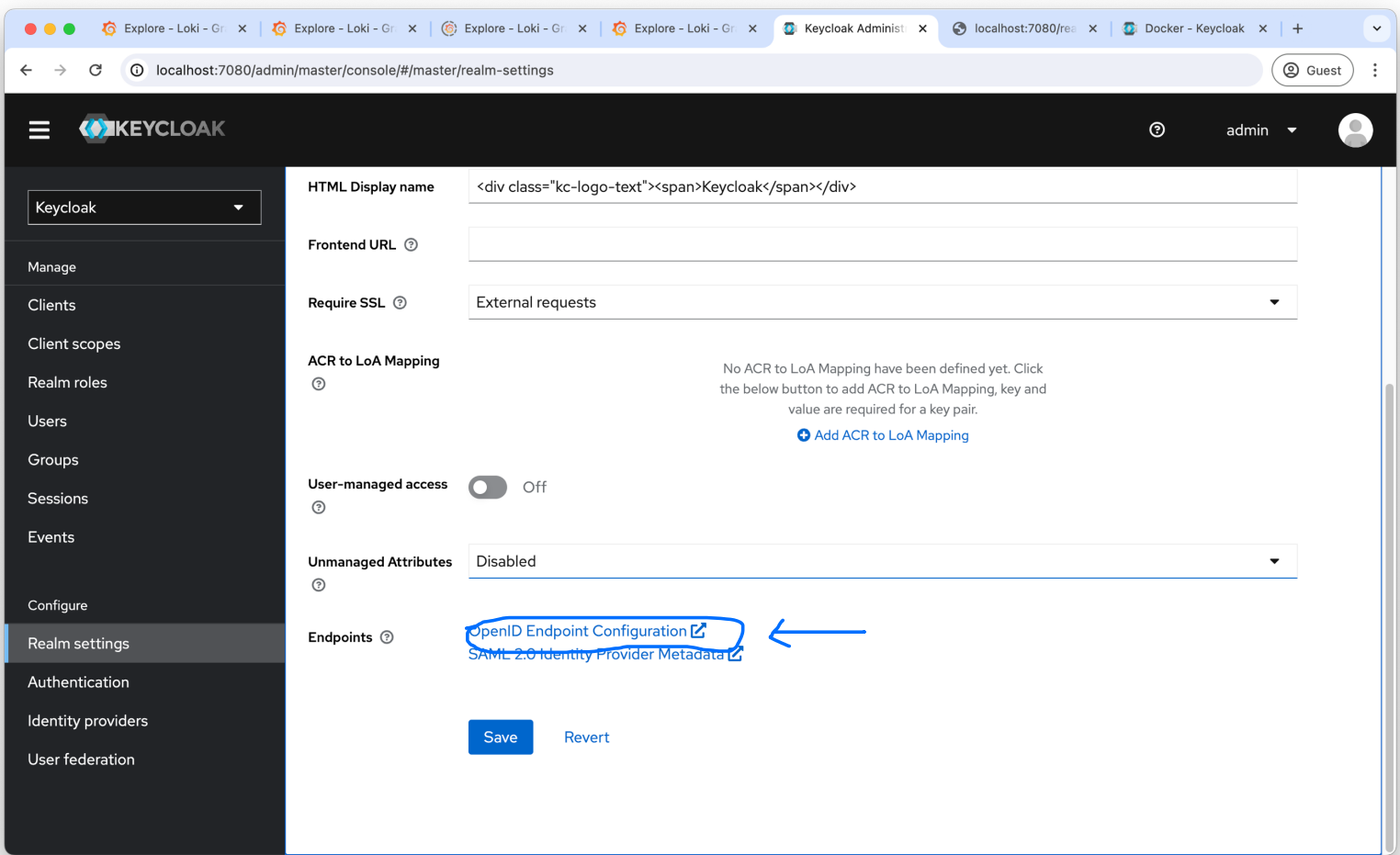
Save

Client Secret S8ez9SRi6Jnam2SWo0vWhP7vm6s4yFCV Regenerate

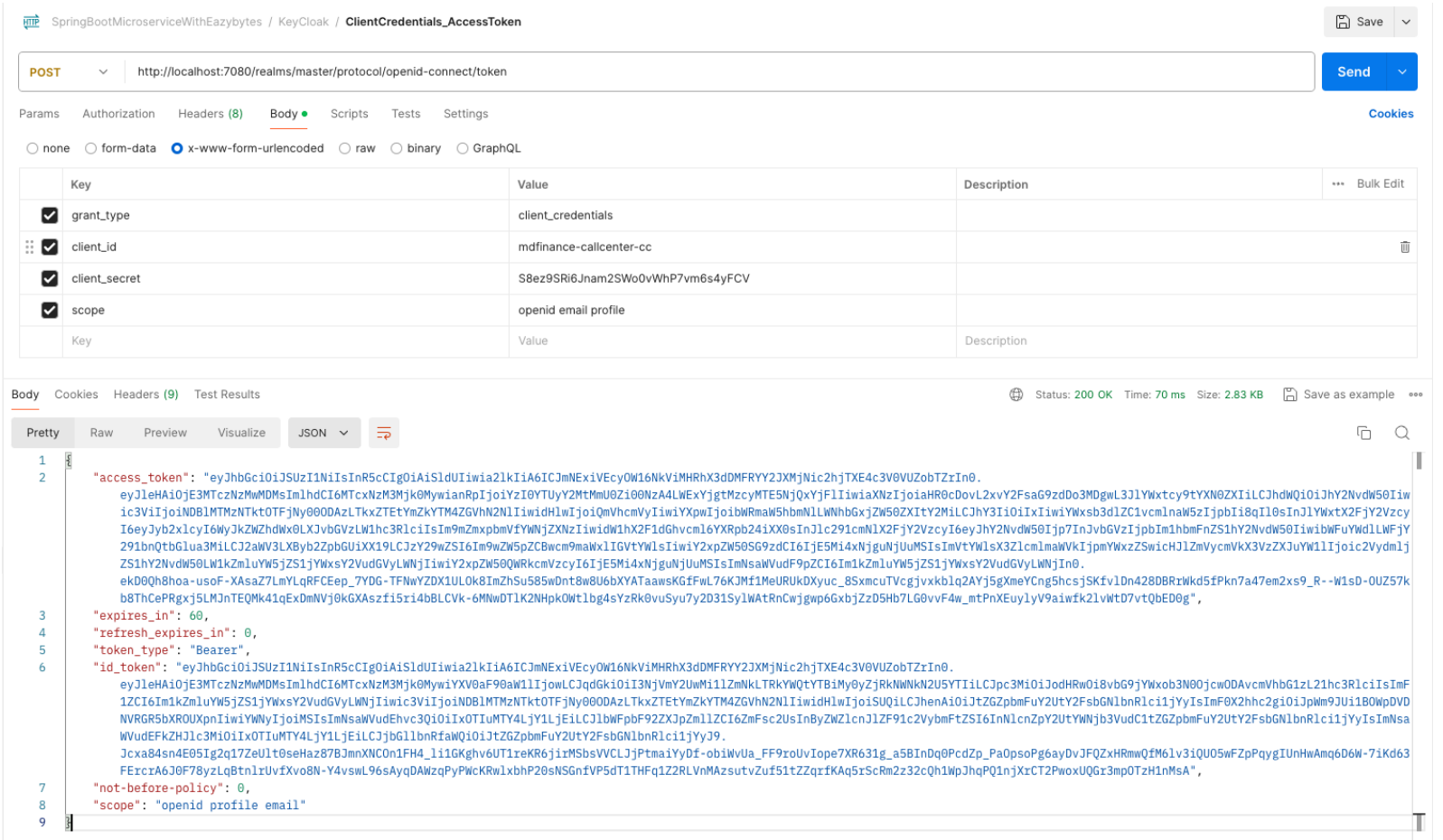
Registration access token Regenerate

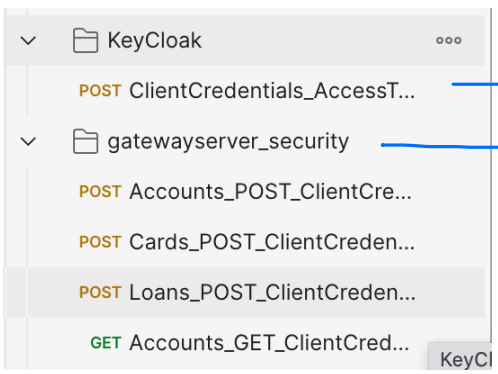
Now follow below steps to get the "token_endpoint url".

- Client has to pass this "token_endpoint url" in order to get the access token



We can test the flow using postman to see if we can get the access token from Auth Server



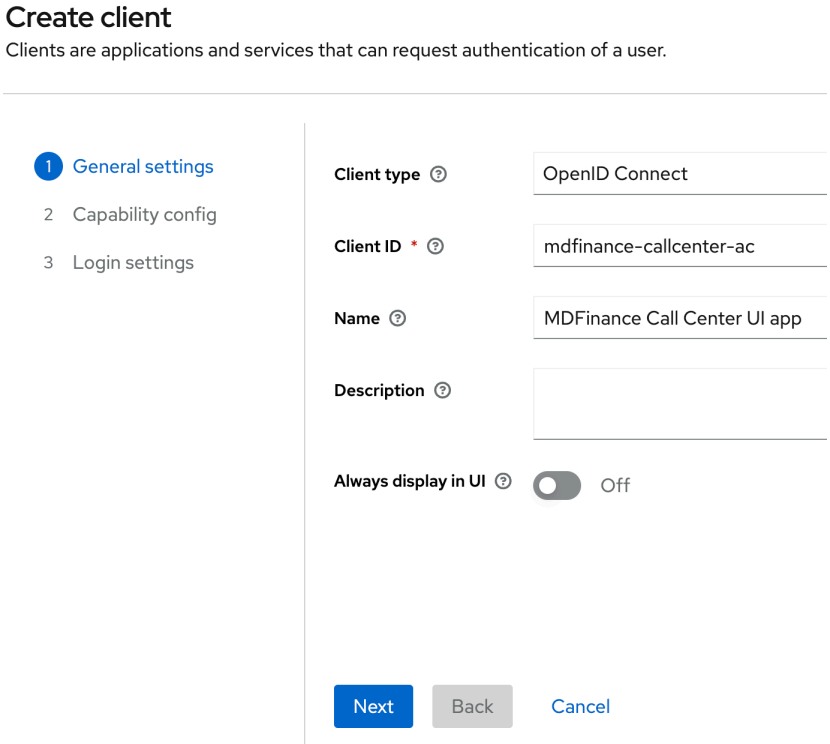


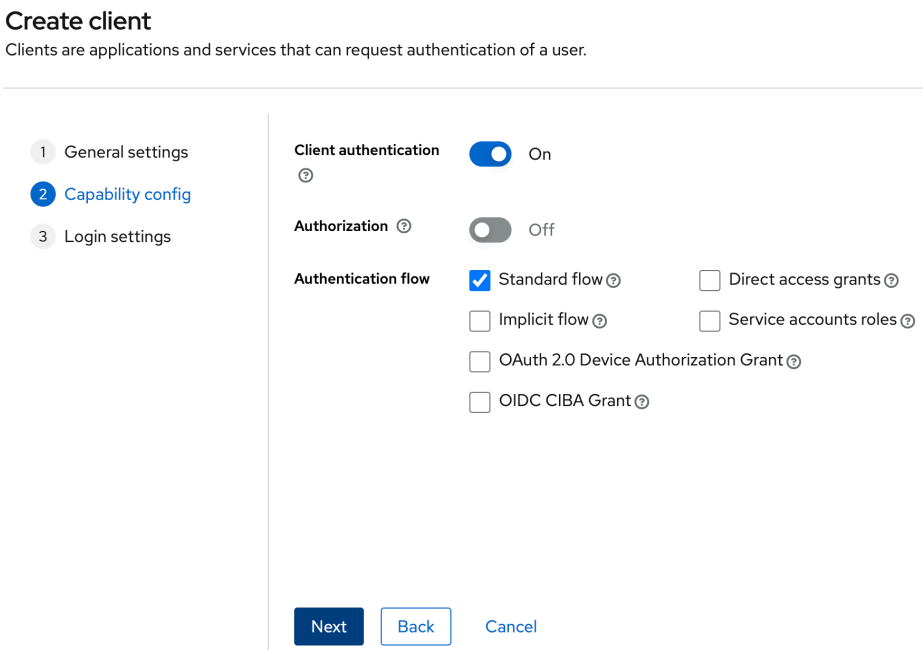
use this request to get the token

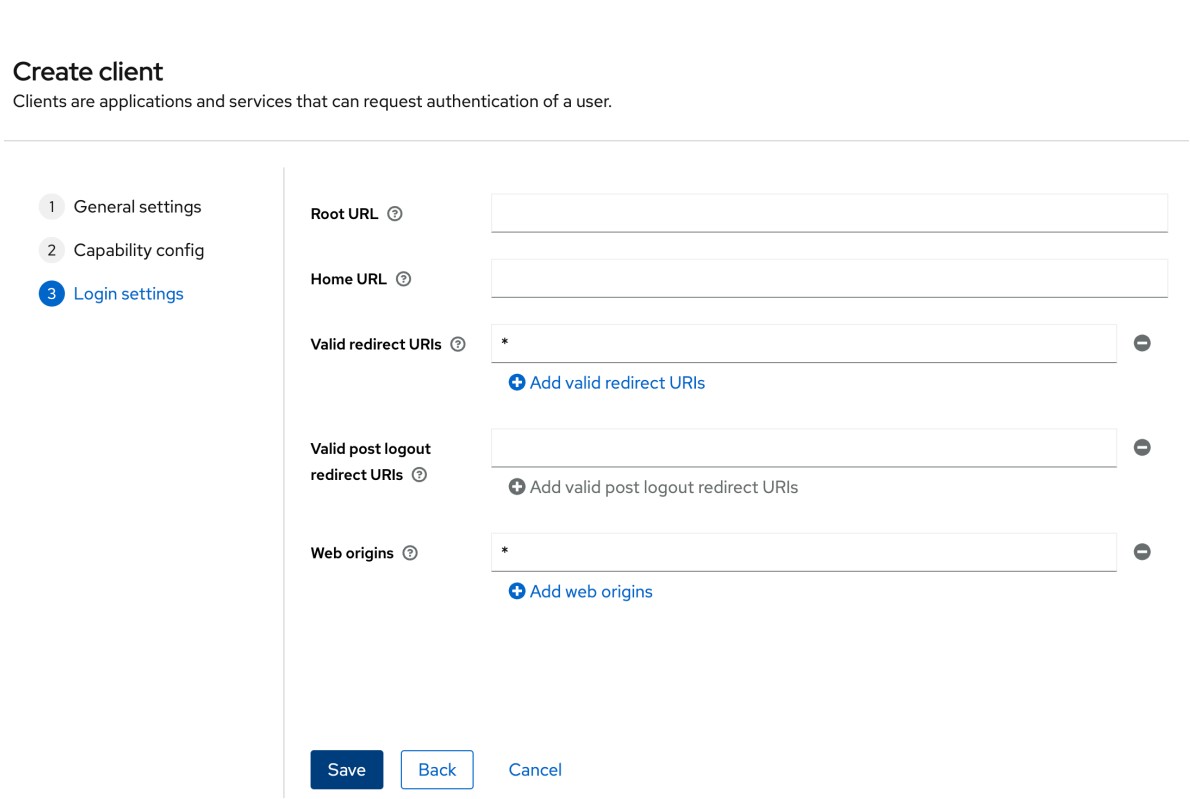
we can use any of these request. First we need to get the access token and then use the token to hit the request. Explore the "Authorization" tab within the Postman.

Authorization Code Grant Type Flow in OAUTH2

- Understand different diagrams presented in the pdf by eazy-bytes.
- To test the demo navigate to this website: https://oauth.com/playground/







- Next we must create a user within KeyCloak server (set the email, username, password (temporary))
- Please note that in the latest build of the section 12 we have removed ports mapping for "accounts", "cards", "loans" services as we don't want to expose the port rather we want user/application to communicate with the gateway server/ resource server in order to get access to services.
- To test the functionality, pull the latest image (12) from the docker hub and after all the containers are up and running we need to navigate to "localhost:7080" and login with admin credentials, after that we need to set up clients, realm roles, user as we can see in above snippets. Please go through postman - "gatewayserver_secruity" folder which has all the information about generating token (all we have to do is update the client_credentials and hit the POST request)
- For more info, please re-watch the videos.