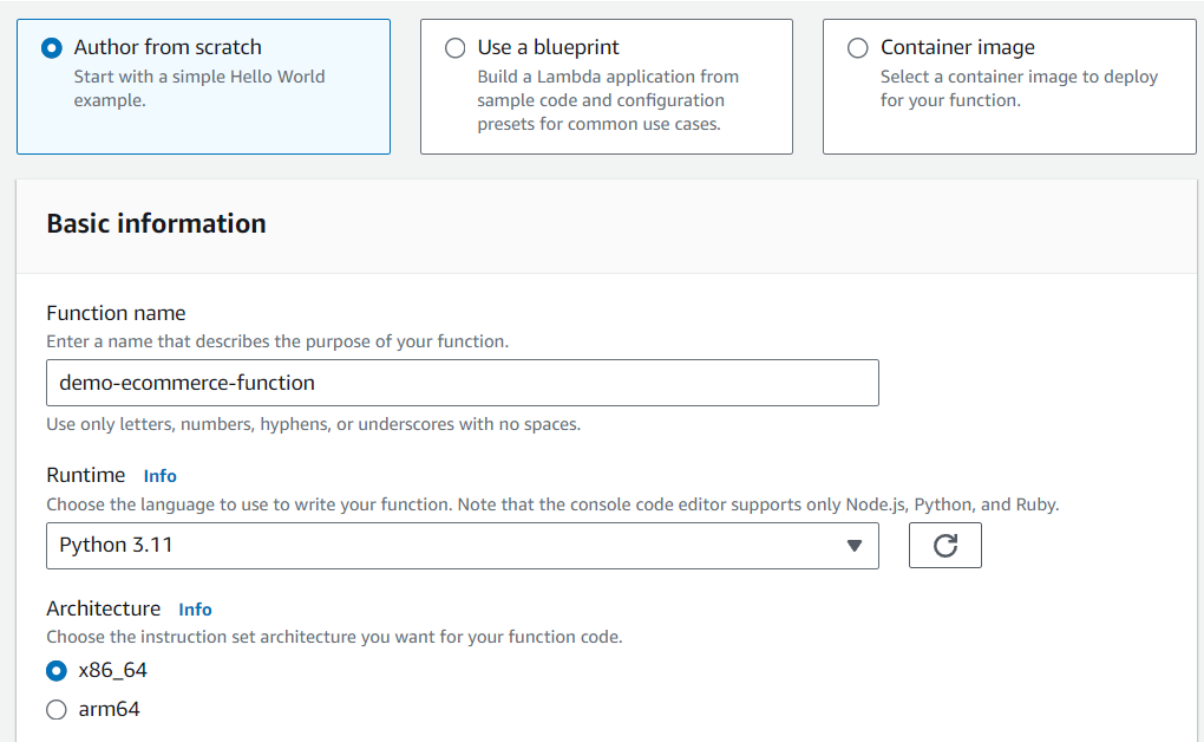
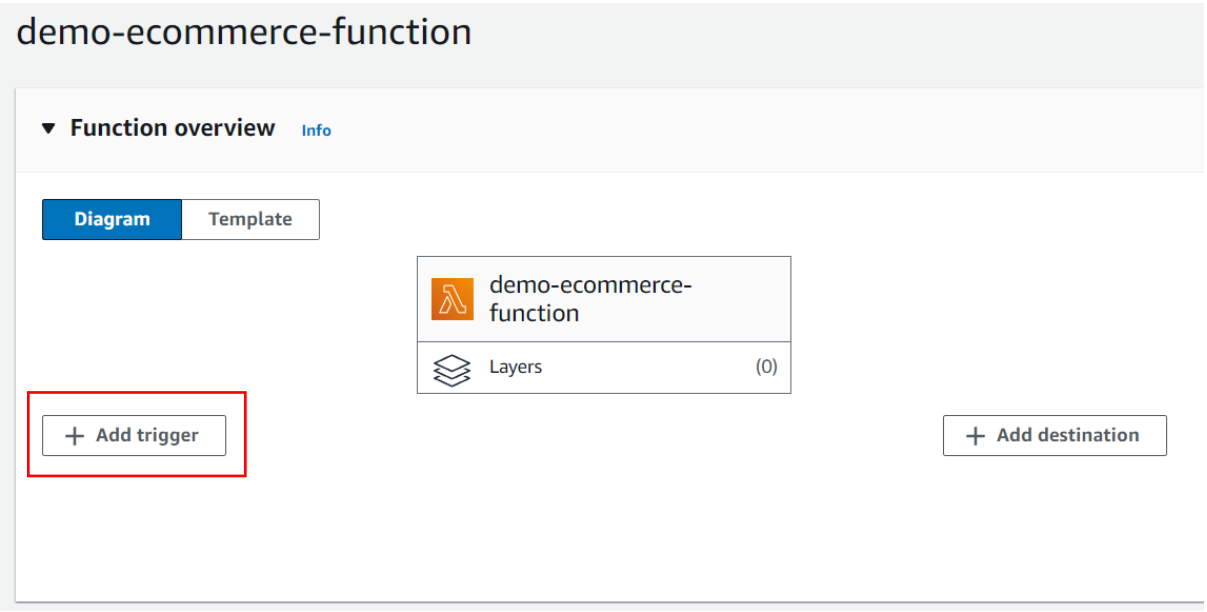
😊 Secure your API Gateway with Amazon Cognito User Pools

😄 Step1: Create Lambda Function and API Gateway

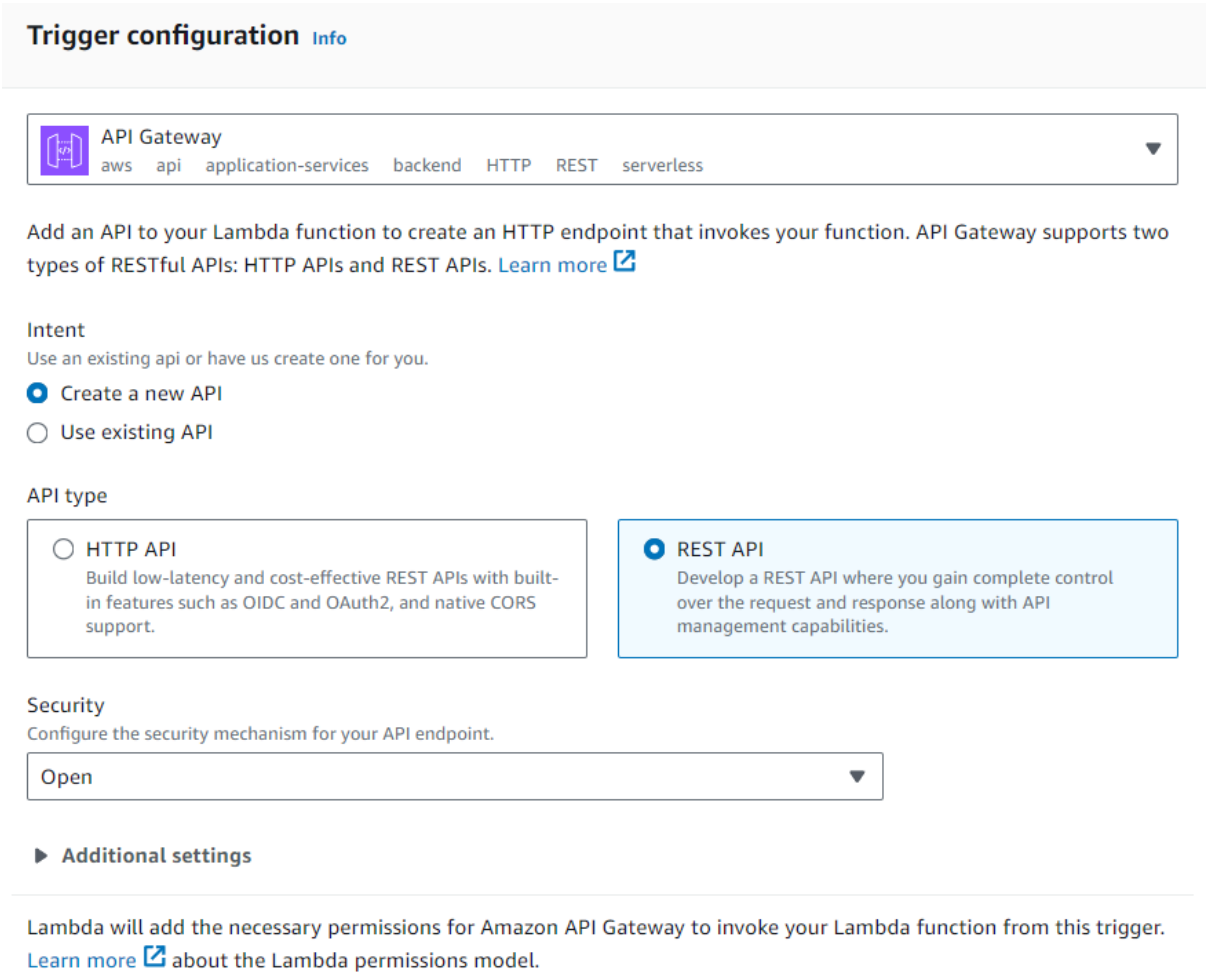
1. Now go to Lambda and click on the Create function. Now you have to give your function a name choose runtime as Python 3.11 and create your function.



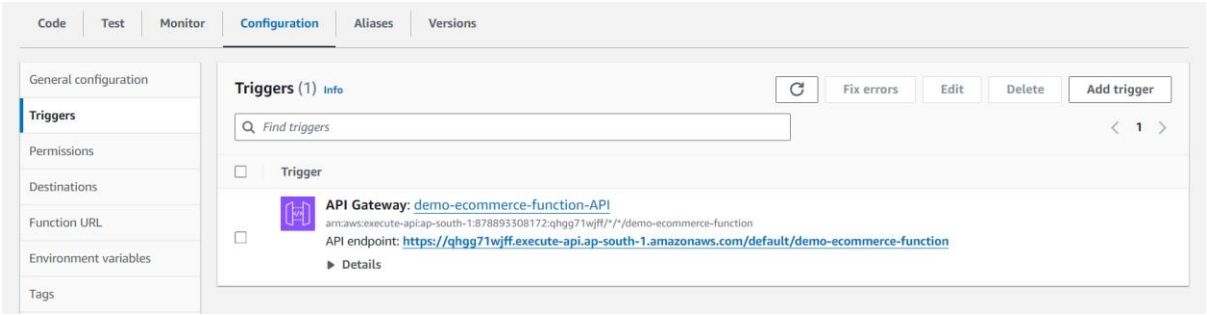
2. Then come inside of your function and click on the Add trigger.



3. Now in the trigger configuration you have to choose API gateway, then choose to create a new API, choose Rest API and keep security to Open. Then click on Add.



4. In the configuration tab you can see that our API gateway has been created and added as a trigger to our lambda function. Now if you click on the API endpoint then you will get a hello from lambda.

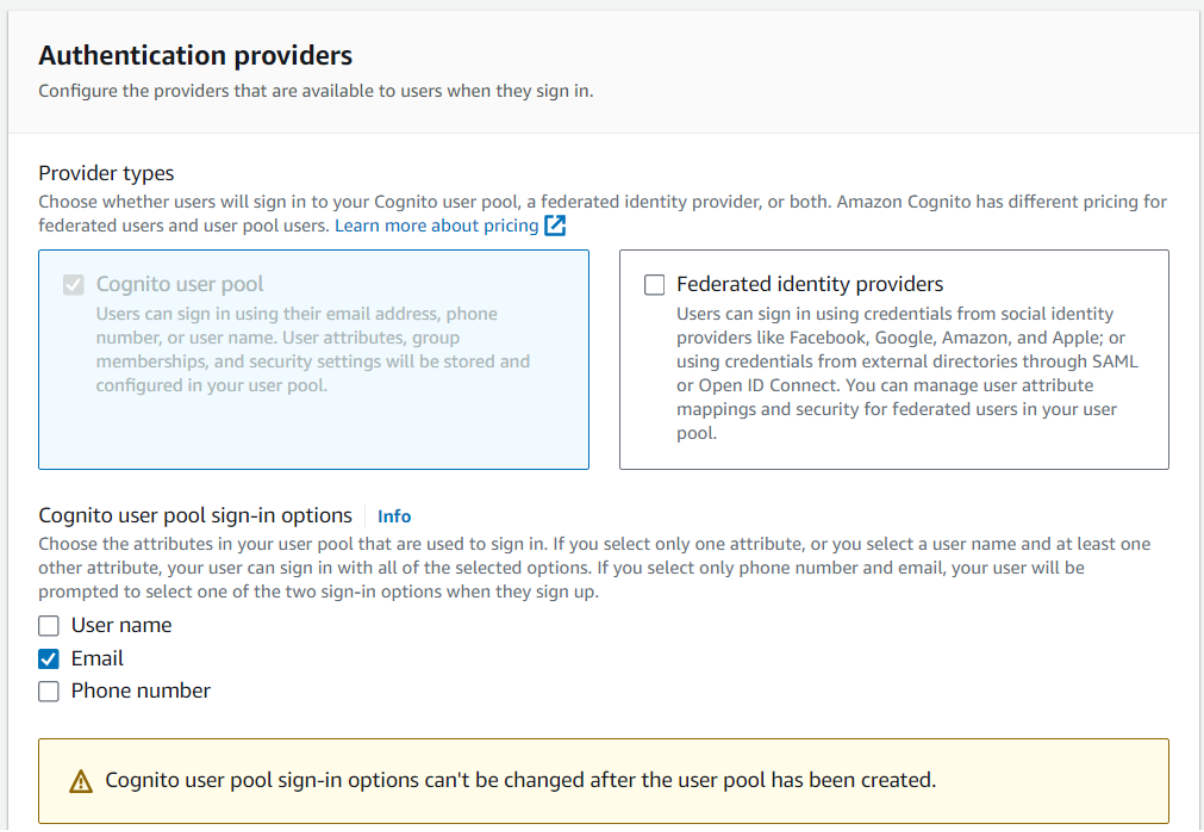


Pretty-print ☑

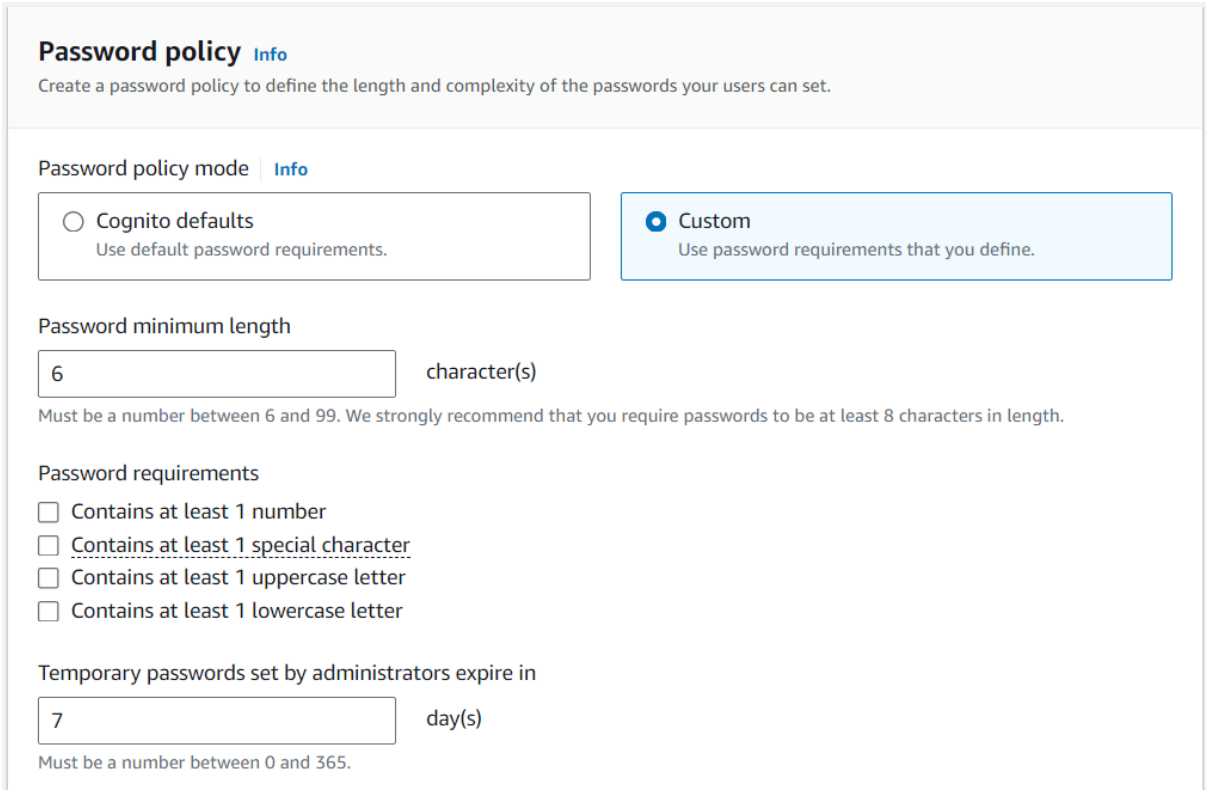
"Hello from Lambda!"

😄 Step 2: Create Cognito User Pool

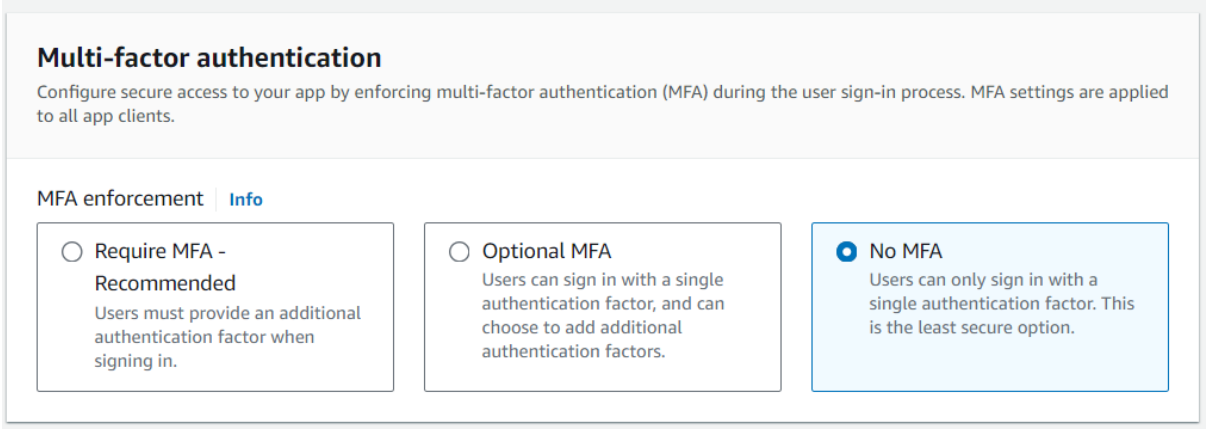
1. Now navigate to Cognito and click on Create User Pool. In the step 1 choose Email as your sign-in option.

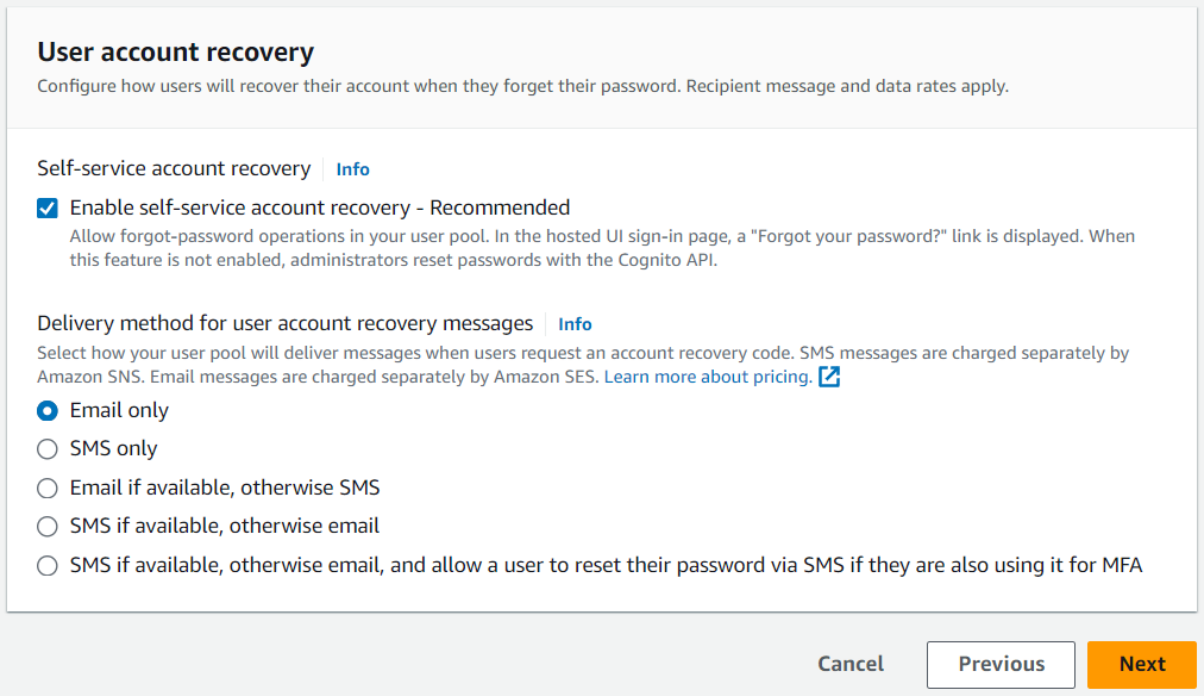


2. Then in step 2 you have to choose custom for password policy mode and set the password minimum length to 6 characters. After that disable all password requirements and scroll down.

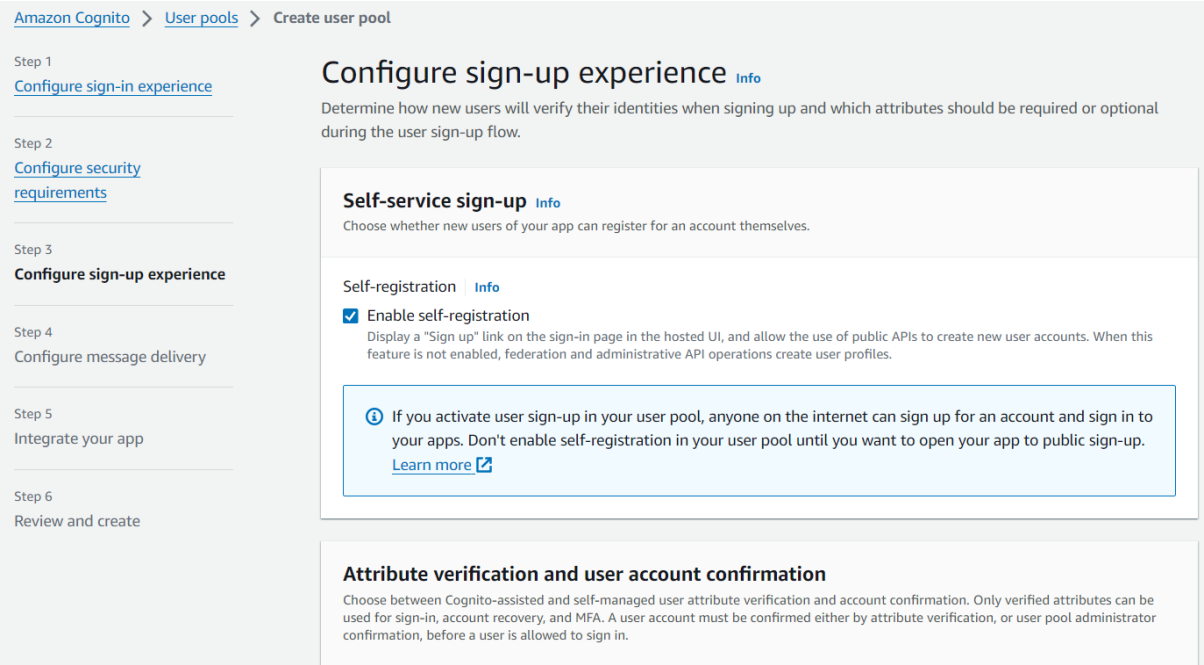


3. Now say no to multi-factor authentication but enable user account recovery as shown below and click on next.

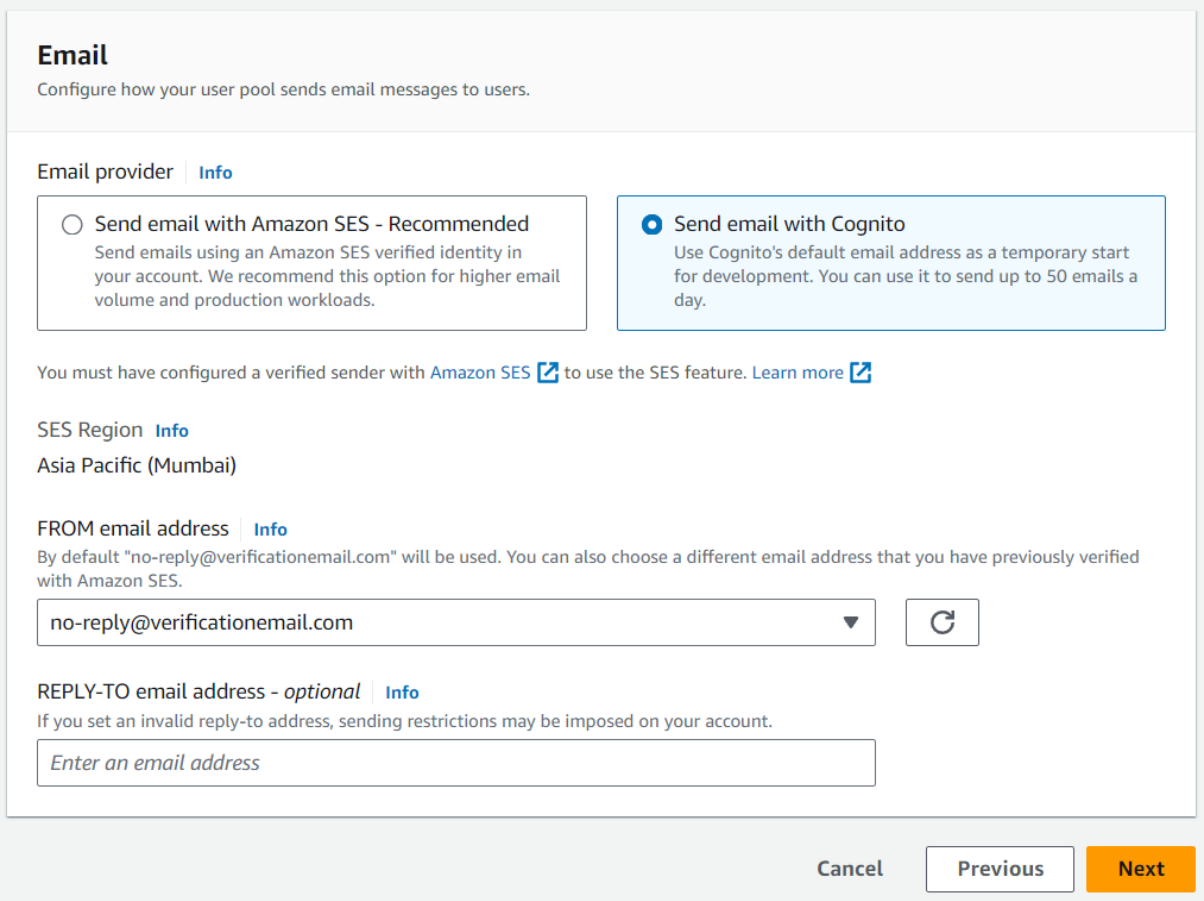




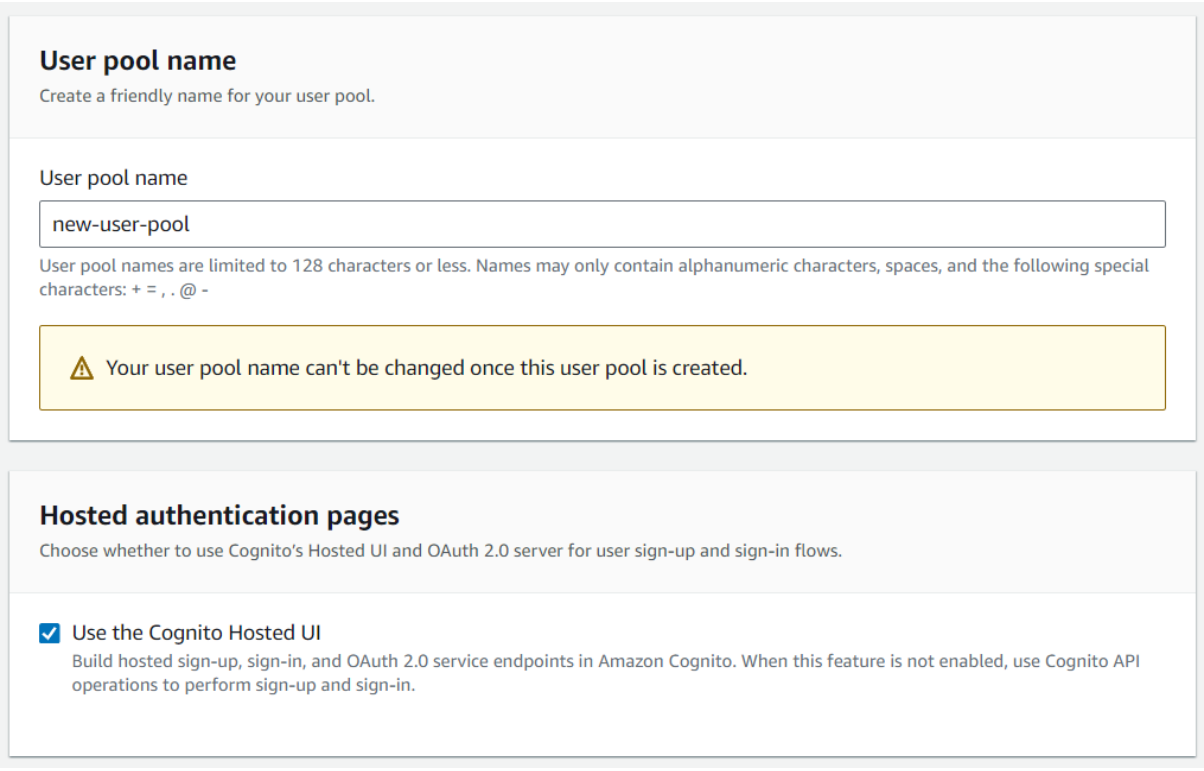
4. So, for step 3 you have to keep this step to default settings and move to the next step.



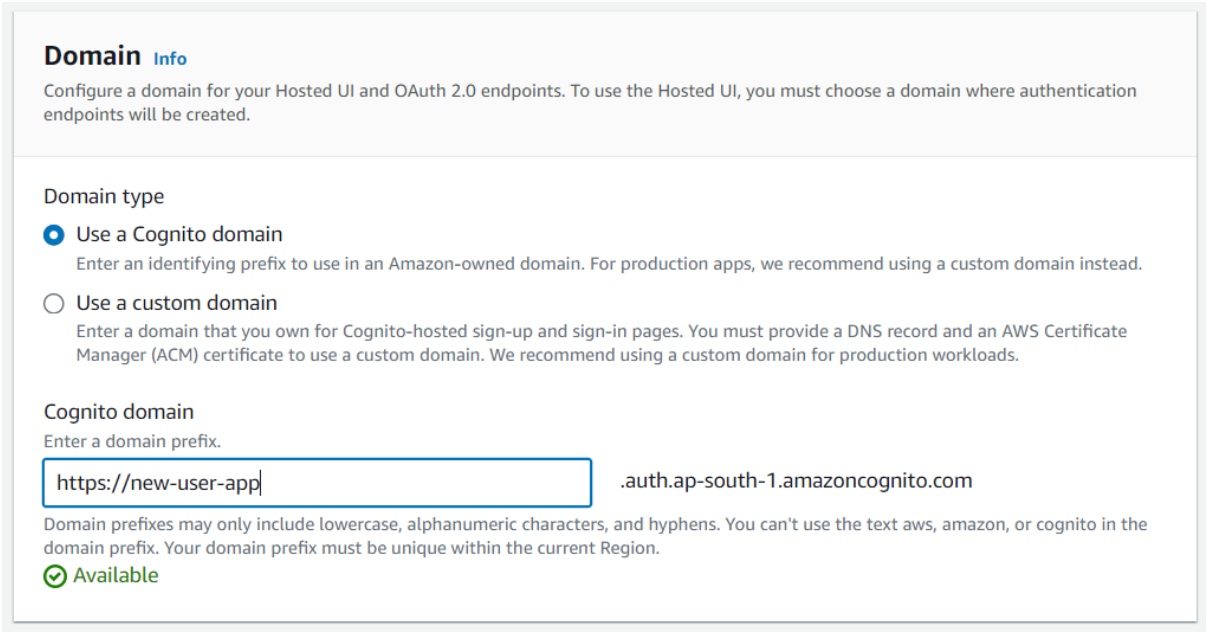
5. Now for step 4 choose Send email with Cognito and click on next.



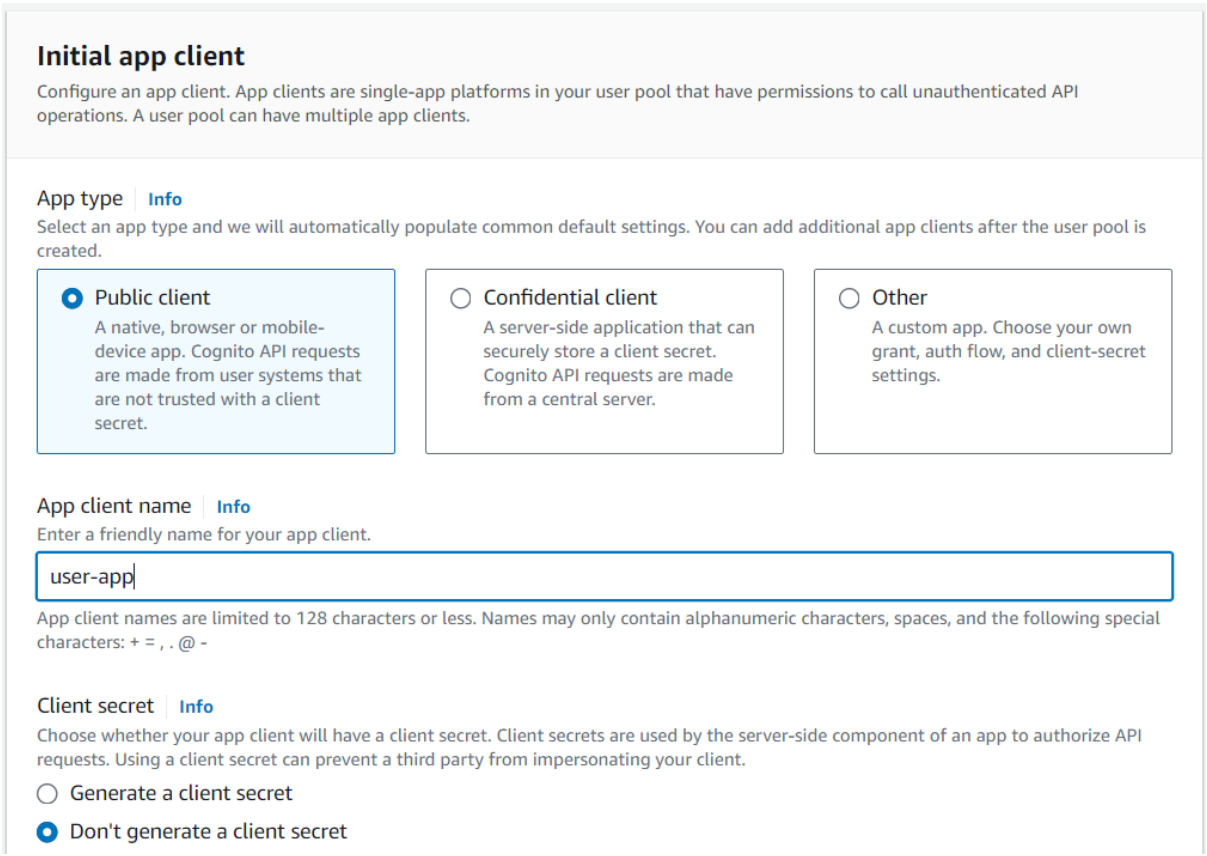
6. Now on step 5, first you should give a user pool name and enable the Cognito Hosted UI.



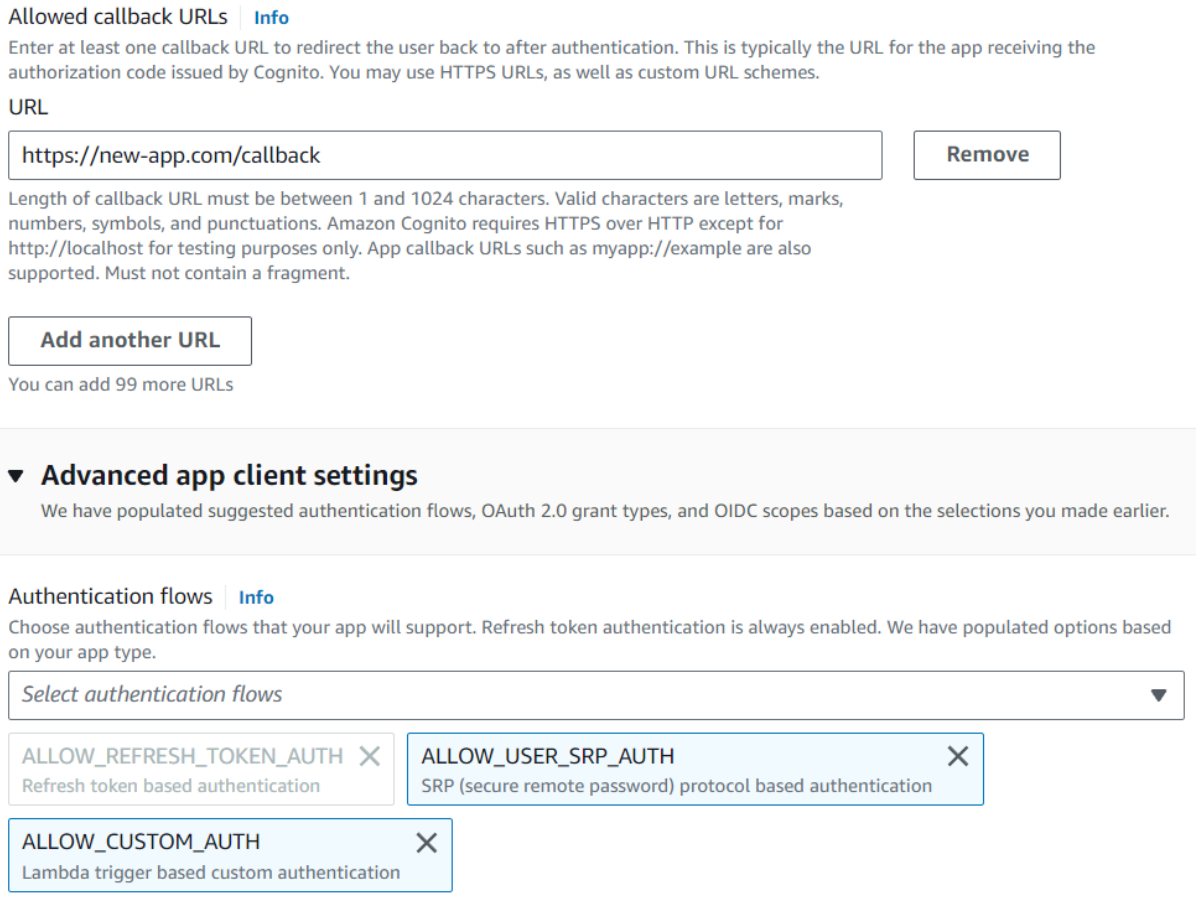
7. Then for the domain choose use a Cognito Domain and give a unique domain name.



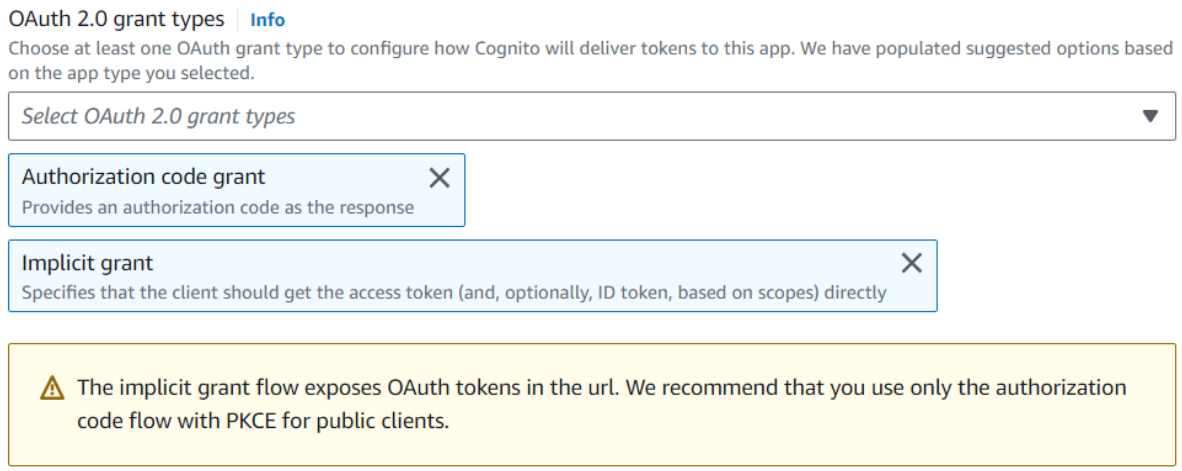
8. Now in the app type choose public client and give an app client name. Then disable client's secret.



9. Then in the allowed callback URLs give a URL and then expand the advanced app client settings and check in the authentication flows, these option must be selected.

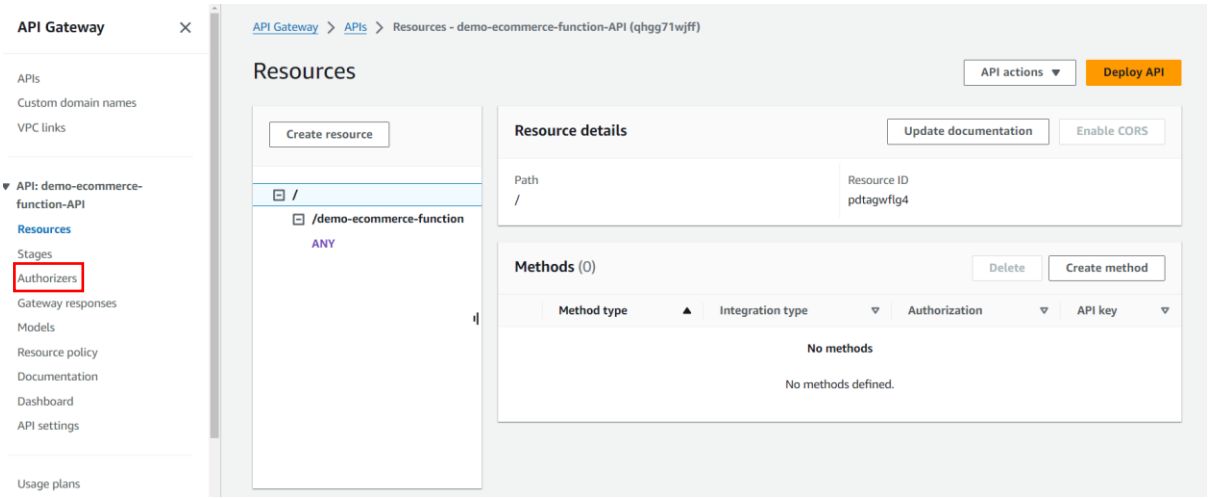


10. After that scroll down to OAuth 2.0 grant types and here you have to add implicit grant.
11. Then just go ahead to the review page and create your user pool.

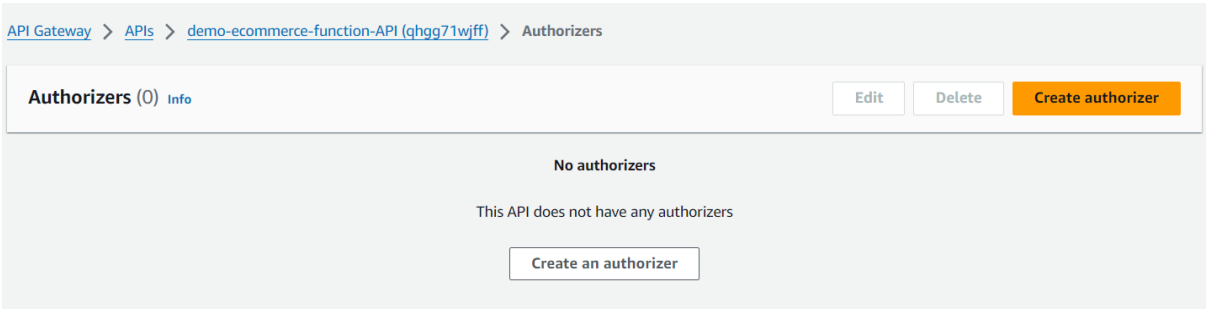


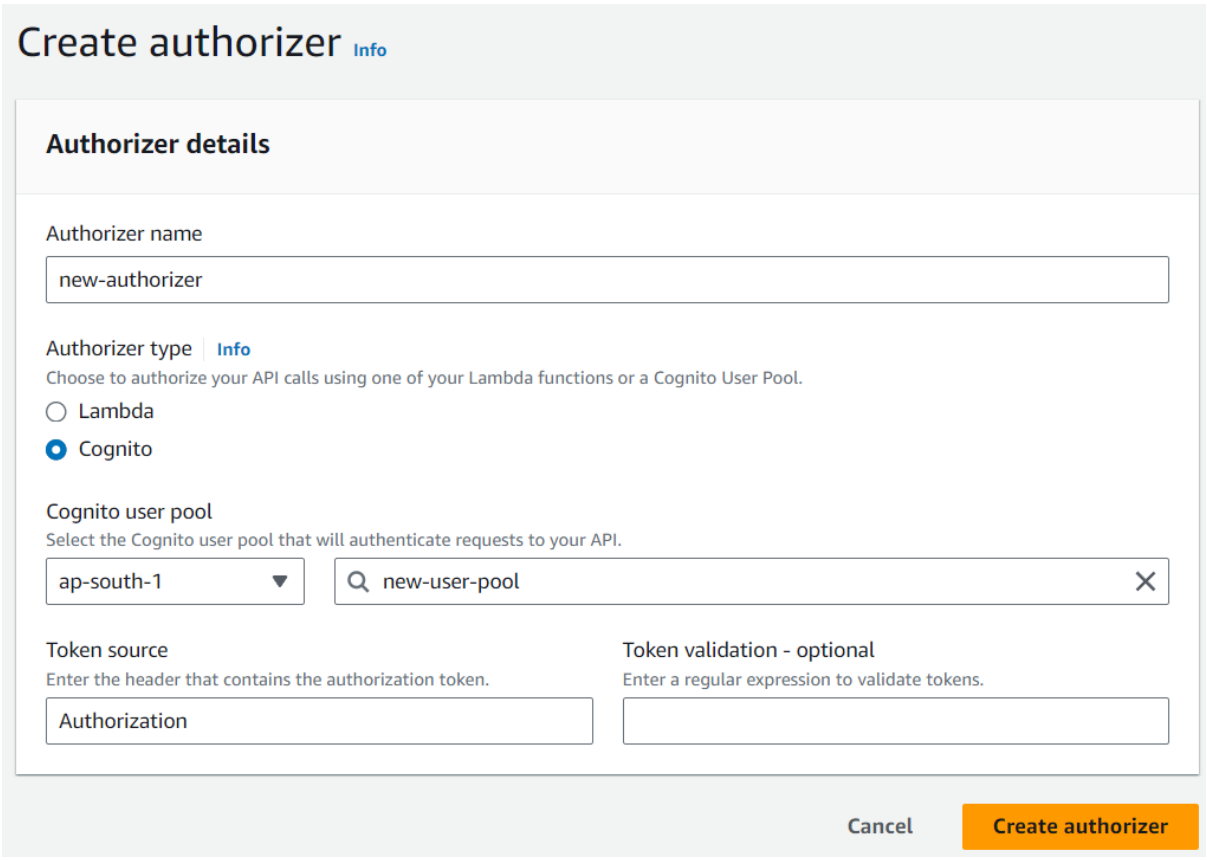
Step 3: Create Authorizer in API Gateway

1. Now go to API gateway, open your API which was created using lambda and go to authorizer from the left pane.

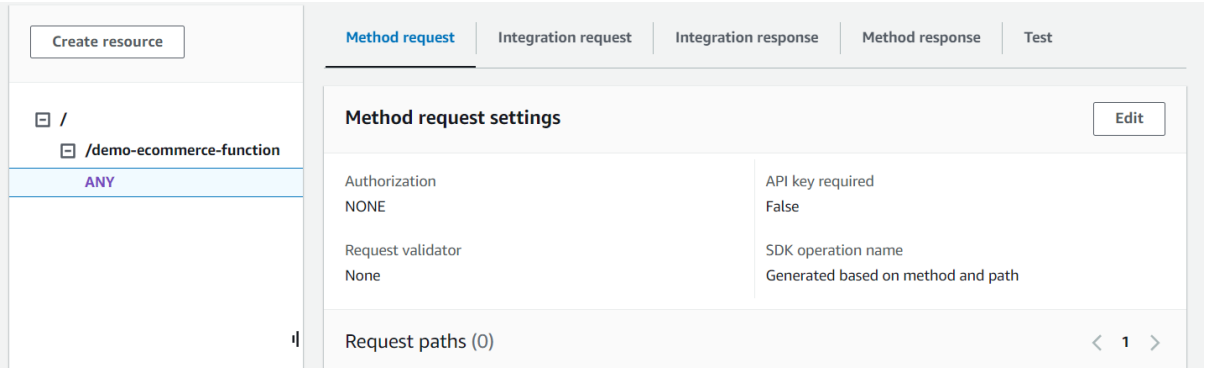


2. Now click on Create Authorizer. Then you have to give it a name and in the authorizer type choose Cognito, choose your user pool and in the token source write Authorization.

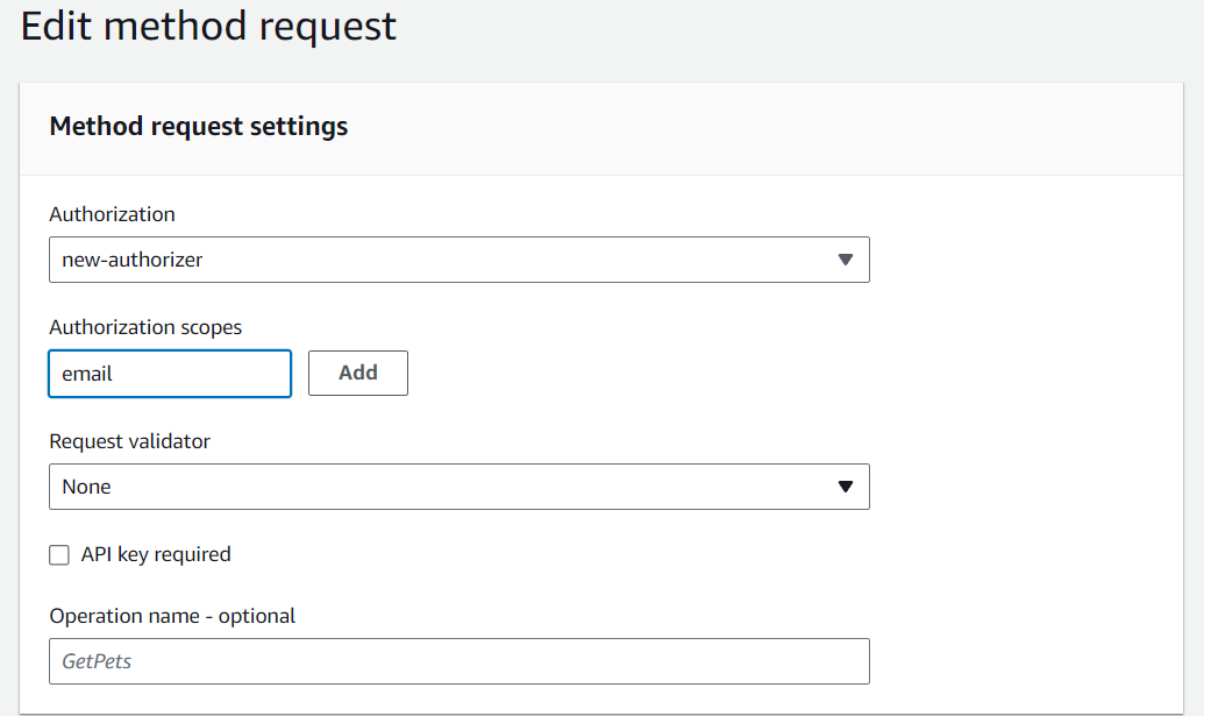




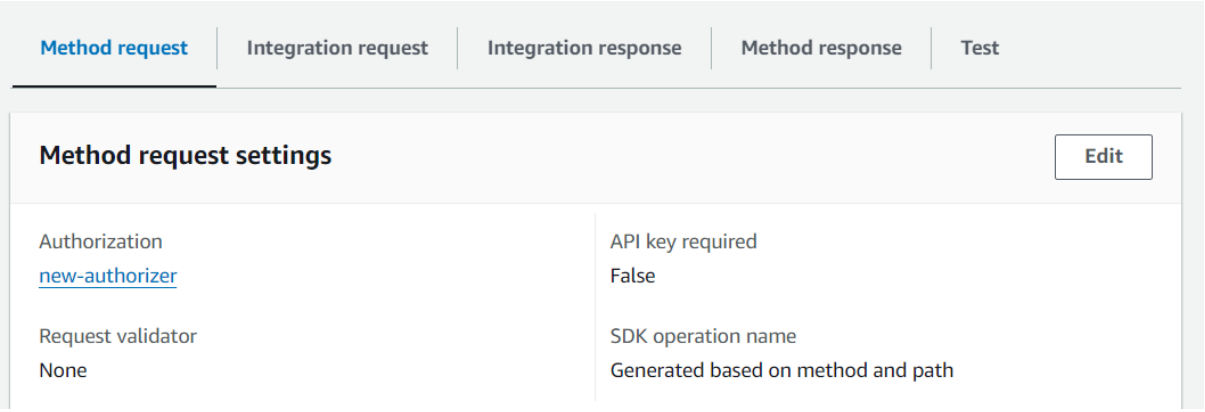
3. Now from the left pane choose Resources come to this ANY Method and go to method request here you can see that the authorization is set to none. So, now we need to click on edit.



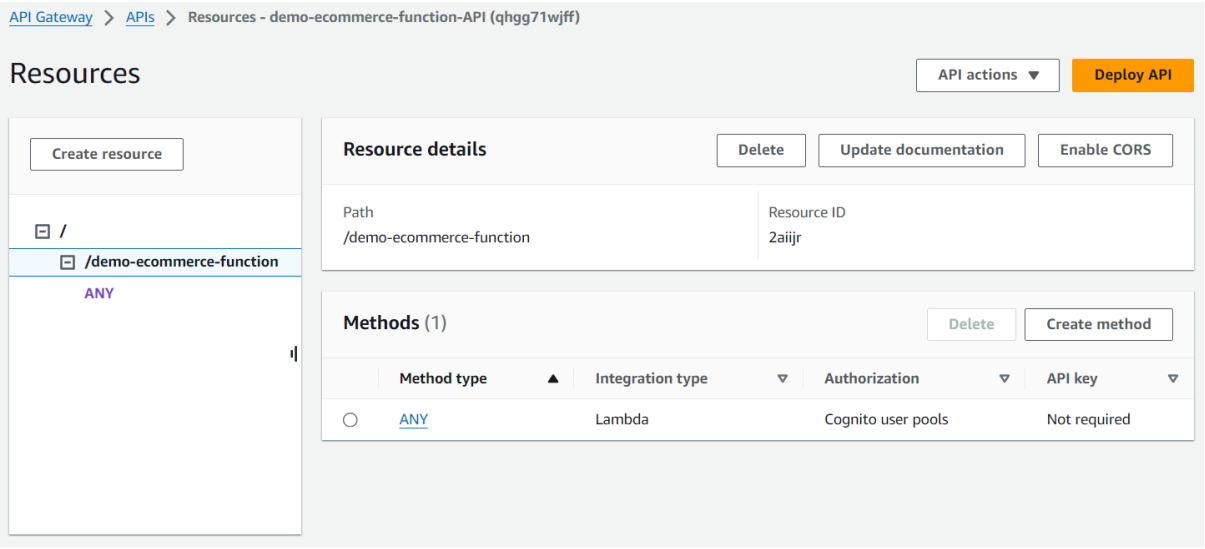
4. Then in the authorization choose your authorizer and in the authorization, scopes write email and click on add. Then just save your settings.



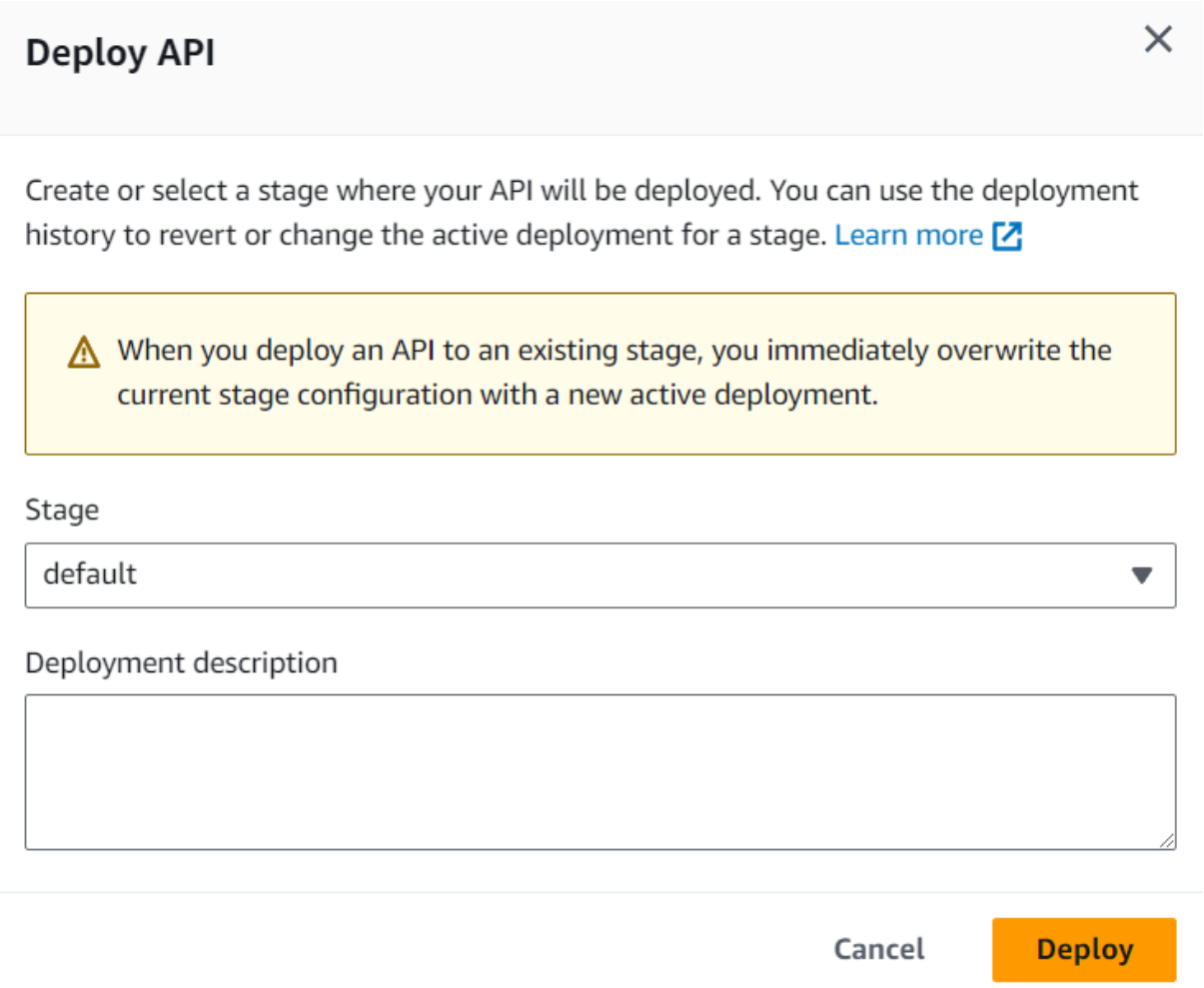
5. Now you can see that in the method request your authorizer has been added.



6. Now come back to your resource and click on Deploy API.

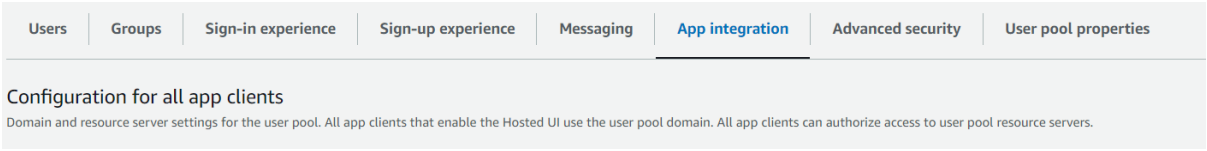


7. Here choose default as your deploy stage and click on deploy.

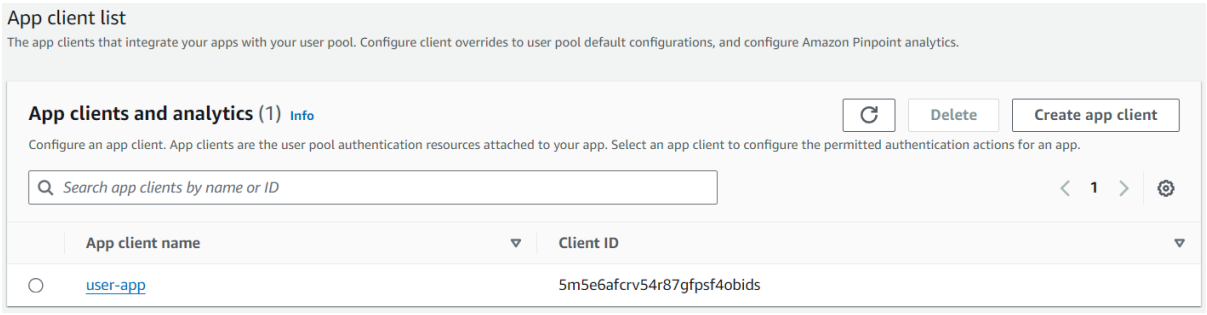


Step 4:

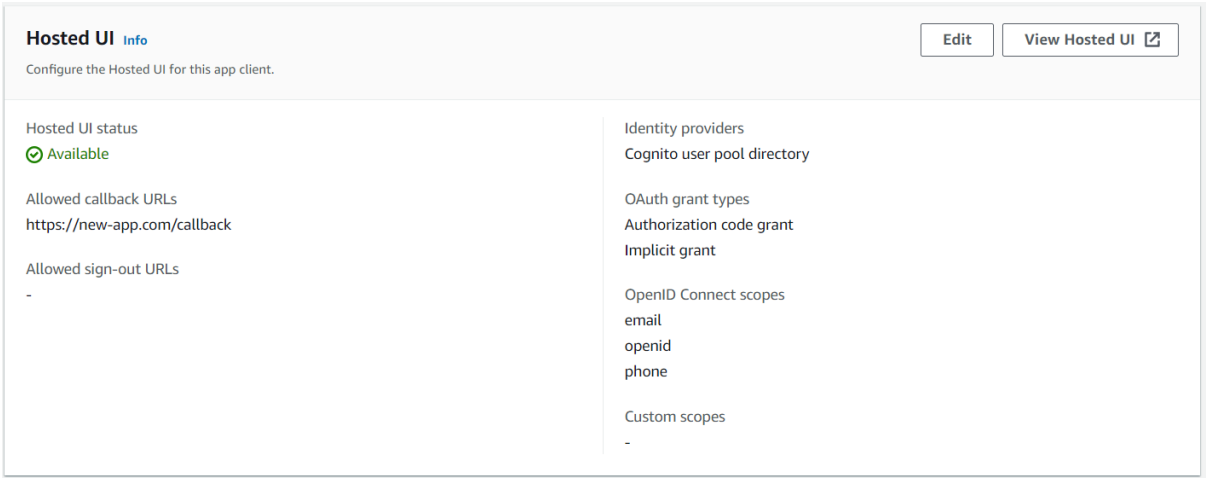
1. Now go to Cognito and open your user pool then go to App Integration.



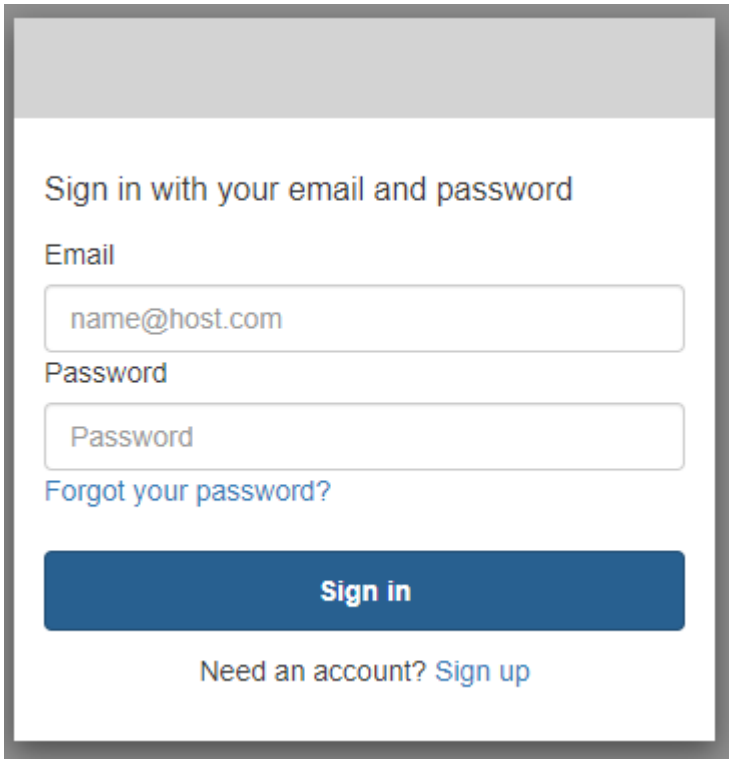
2. Scroll down to app clients and analytics and open your user-app.



3. Here you will see a hosted UI, click on view hosted UI.

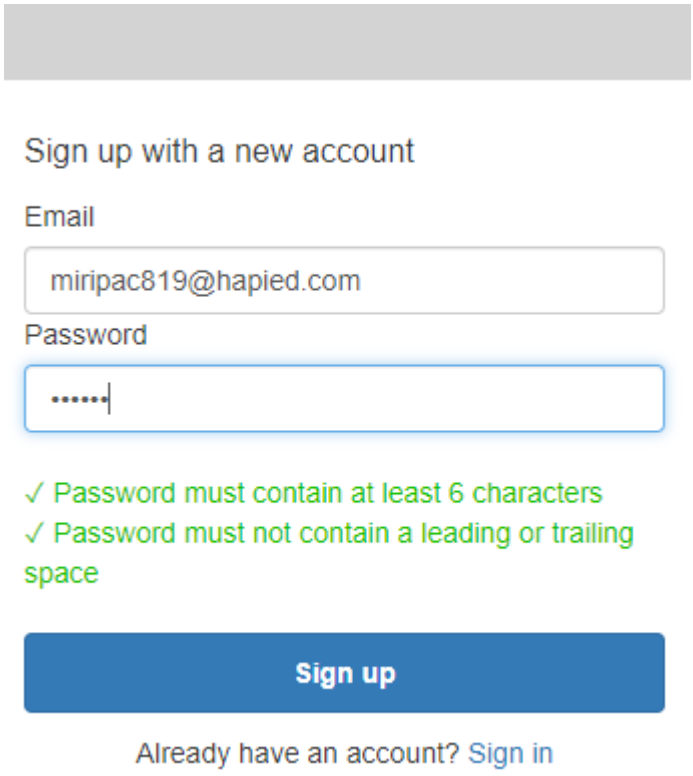


5. Then you will see that it is asking you to sign in.

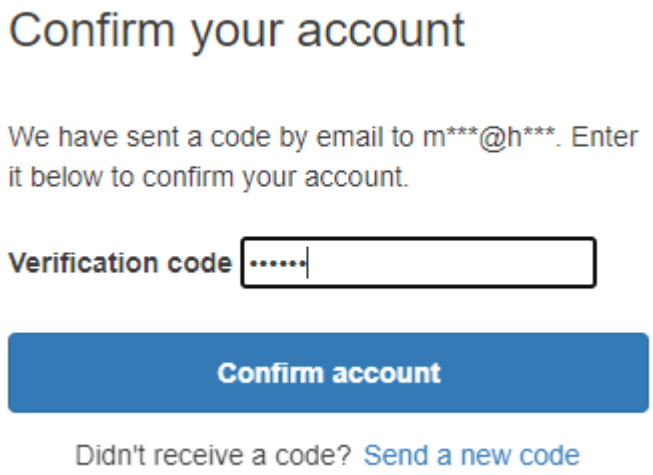


6. But you need to copy the URL of this sign-in page you will see that in the type you will be having code, so you need to change it to the token and then again the sign-in page will be opened.
7. So, now you need to choose Sign up and create a new user.

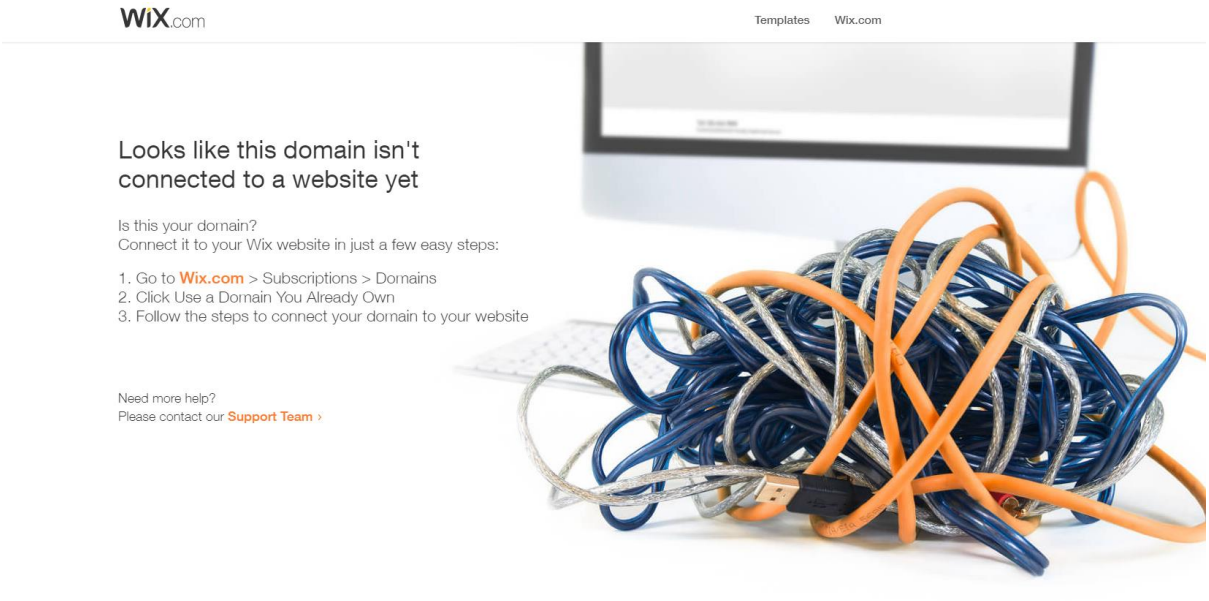
```
https://new-user-app.auth.ap-south-1.amazoncognito.com/login?client_id=
5m5e6afcrv54r87gfpsf4obids&response_type=token&scope=email+openid+phone&red
irect_uri=https%3A%2F%2Fnew-app.com%2Fcallback
```



8. Then you need to give the verification code to it.

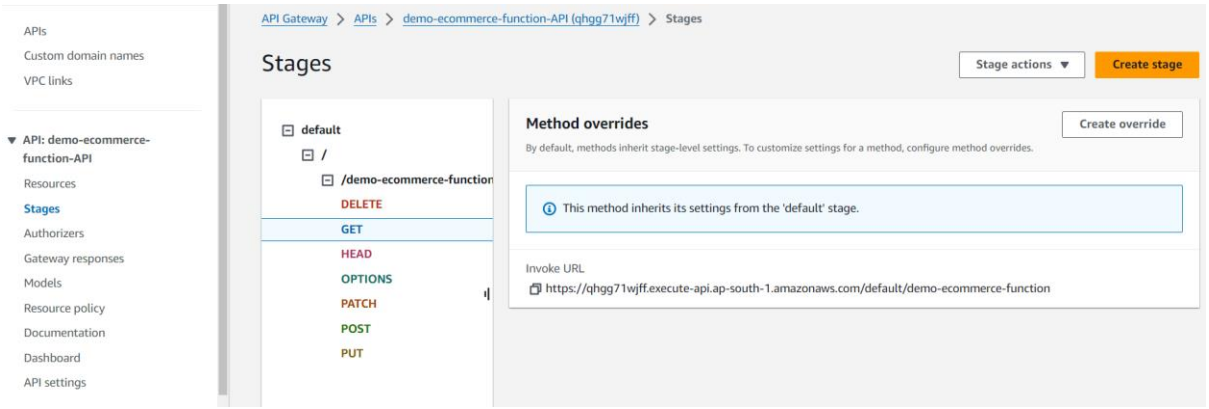


9. Below you can see that the error has occurred, but you need to copy the URL and paste it in a notepad.

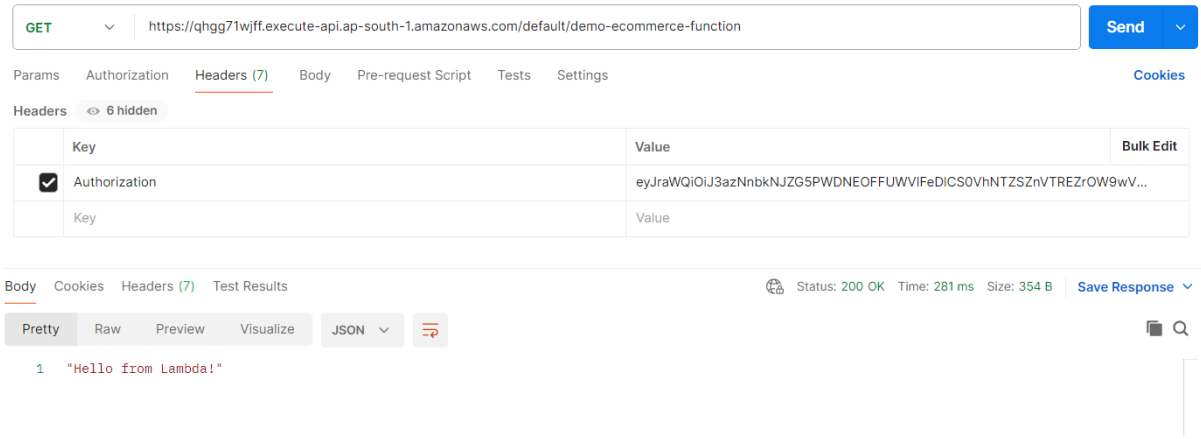


10. After pasting in the notepad, you will have two things Token ID and Access Token. So, you need to copy the Access Token.

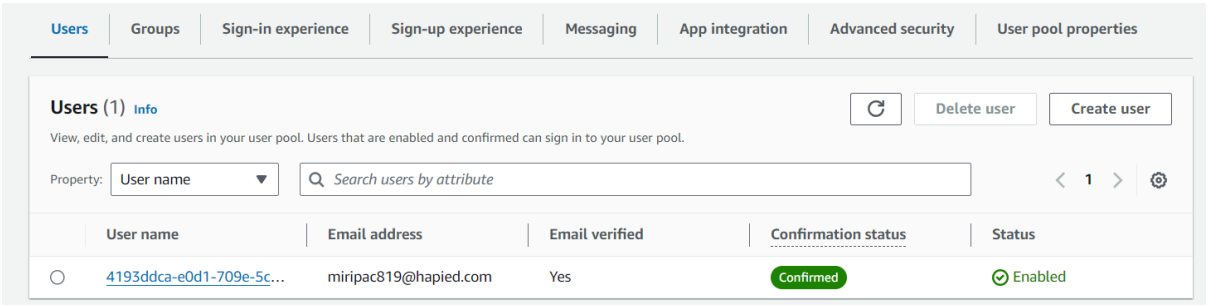
11. After that open Postman and choose GET, but you will need an invoke URL. So, come back to API gateway, go to stages expand default then come to GET Method, here you will find the invoke URL. Then copy it and paste it in the Postman GET method.



12. After that choose headers and, in the key, write authorization in the value paste the Access Token then click on Send. As you can see below you will get a hello from lambda.
13. This means that we have successfully secured our API gateway by choosing the Amazon Incognito User Pool.



14. Now if you go back to Cognito and go to users then you will see that we also have a new user.



15. Now clean up all the resources, so first delete your lambda function, API gateway then go to Cognito and delete your user pools.