Setup AWS Cognito User Pools for User Authentication and Authorization of AppSync APIs

AWS Cognito Service

A user pool is a user directory in Amazon Cognito. With a user pool, your users can sign in to your web or mobile app through Amazon Cognito. Your users can also sign in through social identity providers like Google, Facebook, Amazon, or Apple, and through SAML identity providers. Whether your users sign in directly or through a third party, all members of the user pool have a directory profile that you can access through a Software Development Kit (SDK).

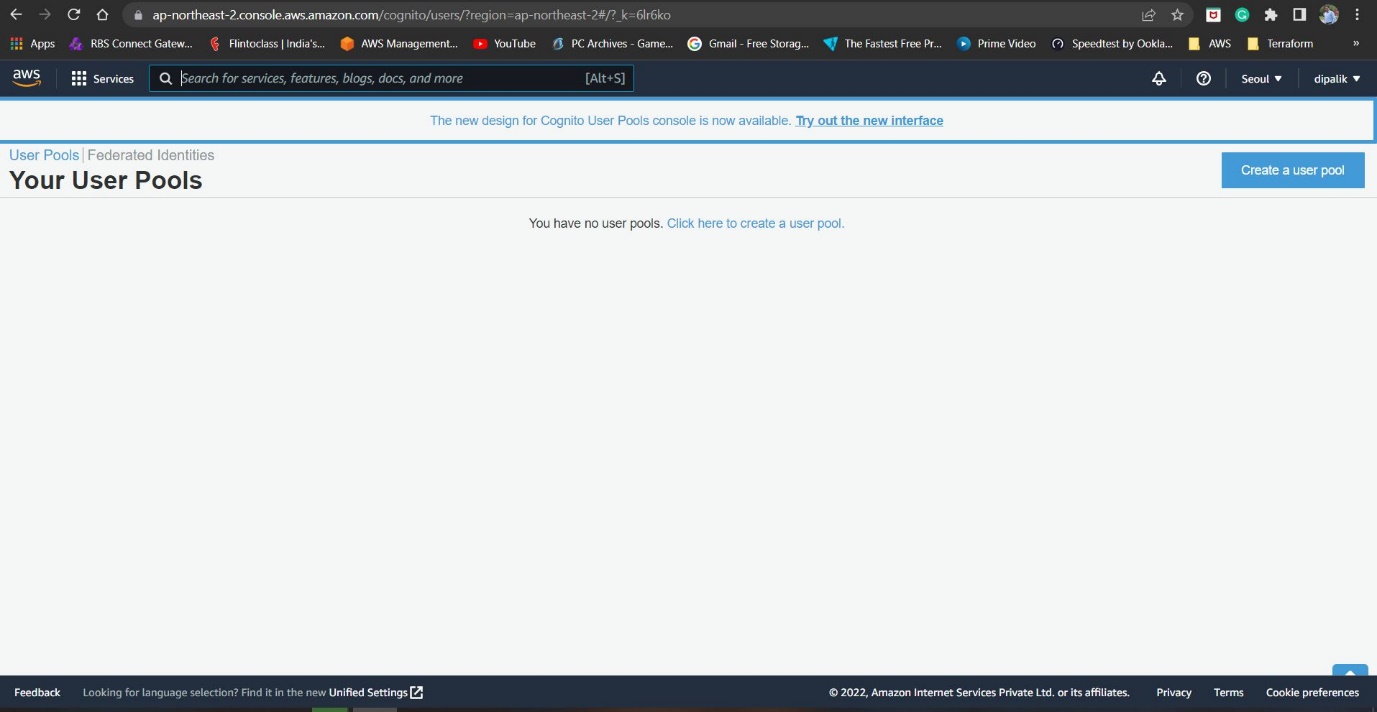
User pools provide:

* Sign-up and sign-in services.
* A built-in, customizable web UI to sign in users.
* Social sign-in with Facebook, Google, Login with Amazon, and Sign in with Apple, as well as sign-in with SAML identity providers from your user pool.
* User directory management and user profiles.
* Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
* Customized workflows and user migration through AWS Lambda triggers.

After successfully authenticating a user, Amazon Cognito issues JSON web tokens (JWT) that you can use to secure and authorize access to your own APIs, or exchange for AWS credentials.

Now lets learn how to setup a AWS Cognito Users pool to implement Role based access the GraphQL APIs

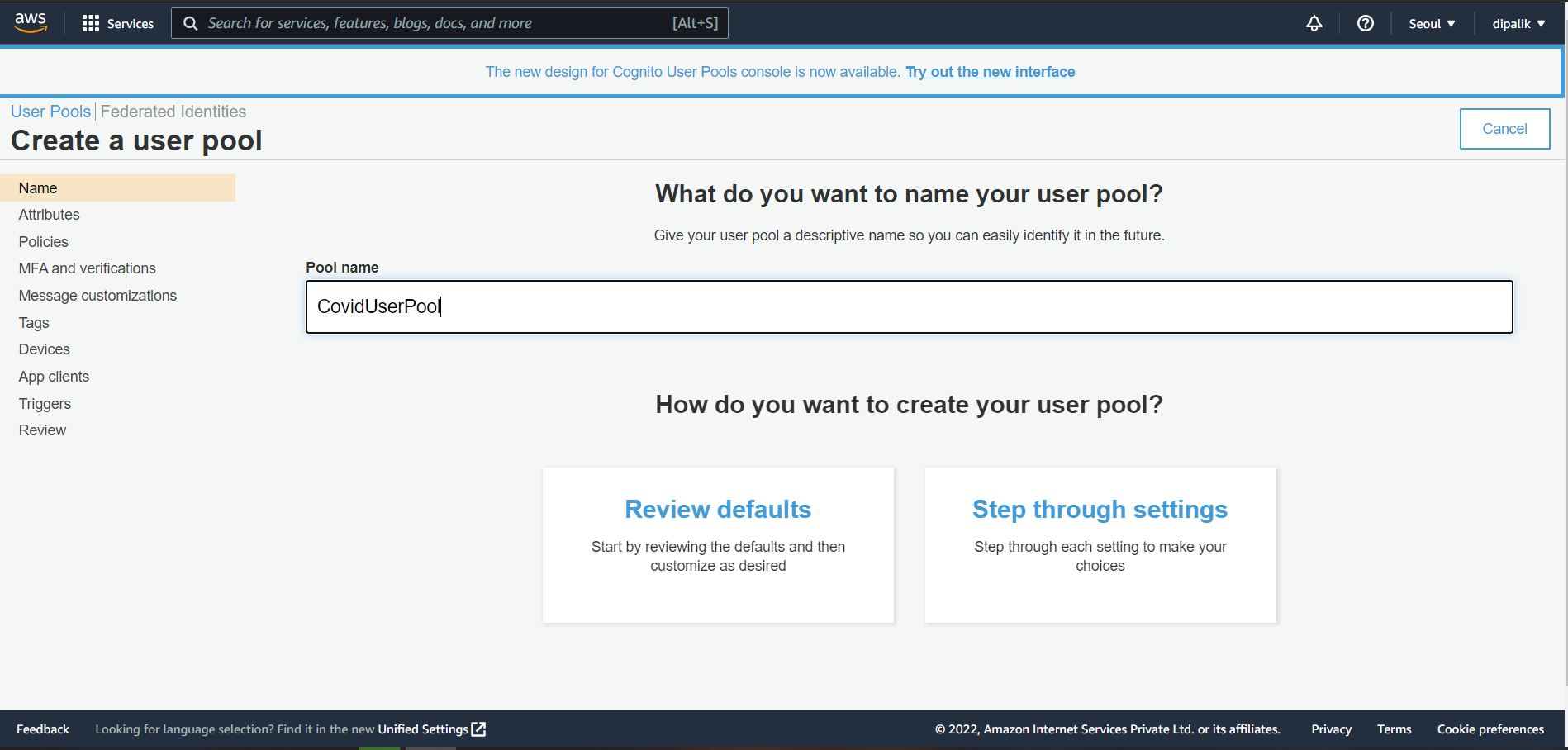
Step 1 – Open the AWS Cognito Users Pool dashboard and Create User pool.



Step 2 – Create user pool

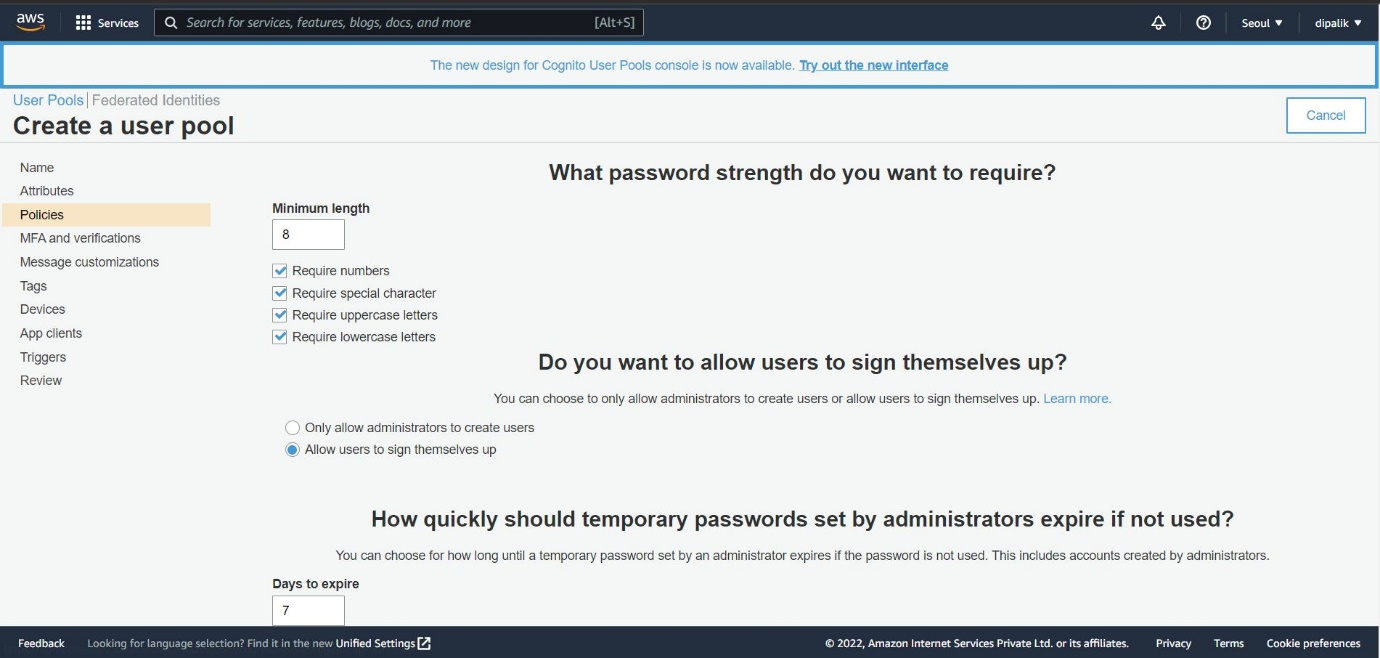
Click on “Create a User Pool” Button to create a pool.

Then provide a unique Pool Name, User can directly click on Review Defaults to review the settings or you can choose to Step Through Settings to view the different settings. We prefer to use Review Defaults in this case.



Step 3 – Review Pool Settings

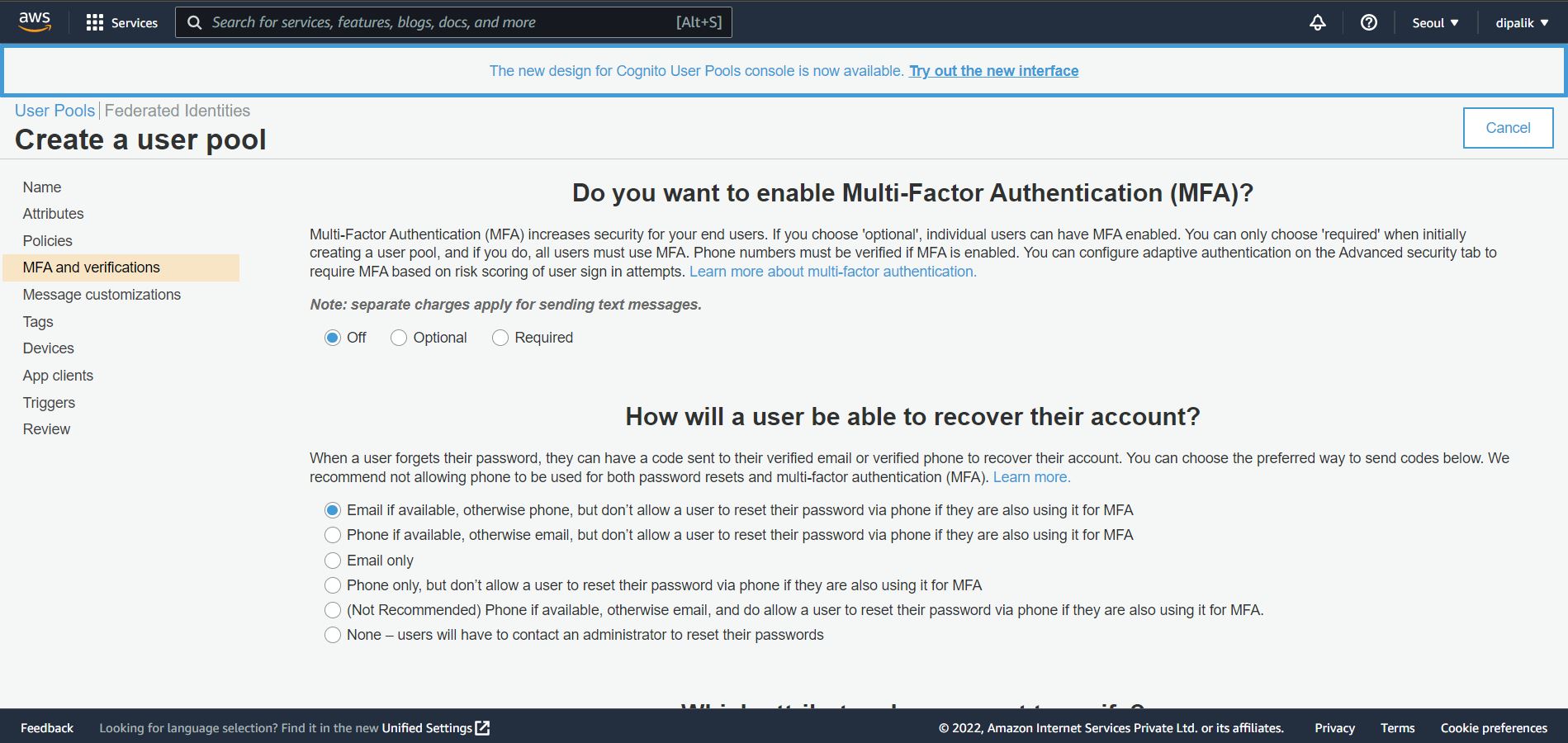
Now you can review different settings, click on Policies to review the user policy.



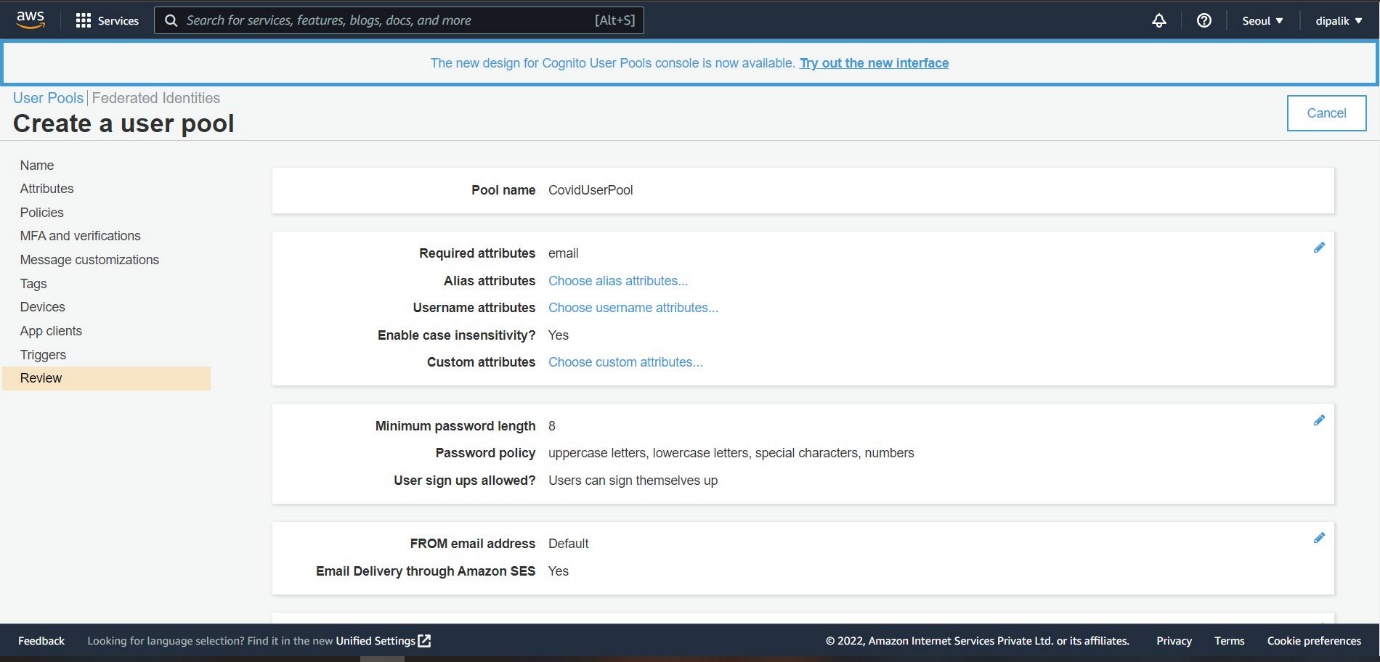
Here you can specify the password policy for users in your pool i.e. password length, use of numbers, lowercase etc, you can also force users to set new password after login.

Enable MFA Authentication

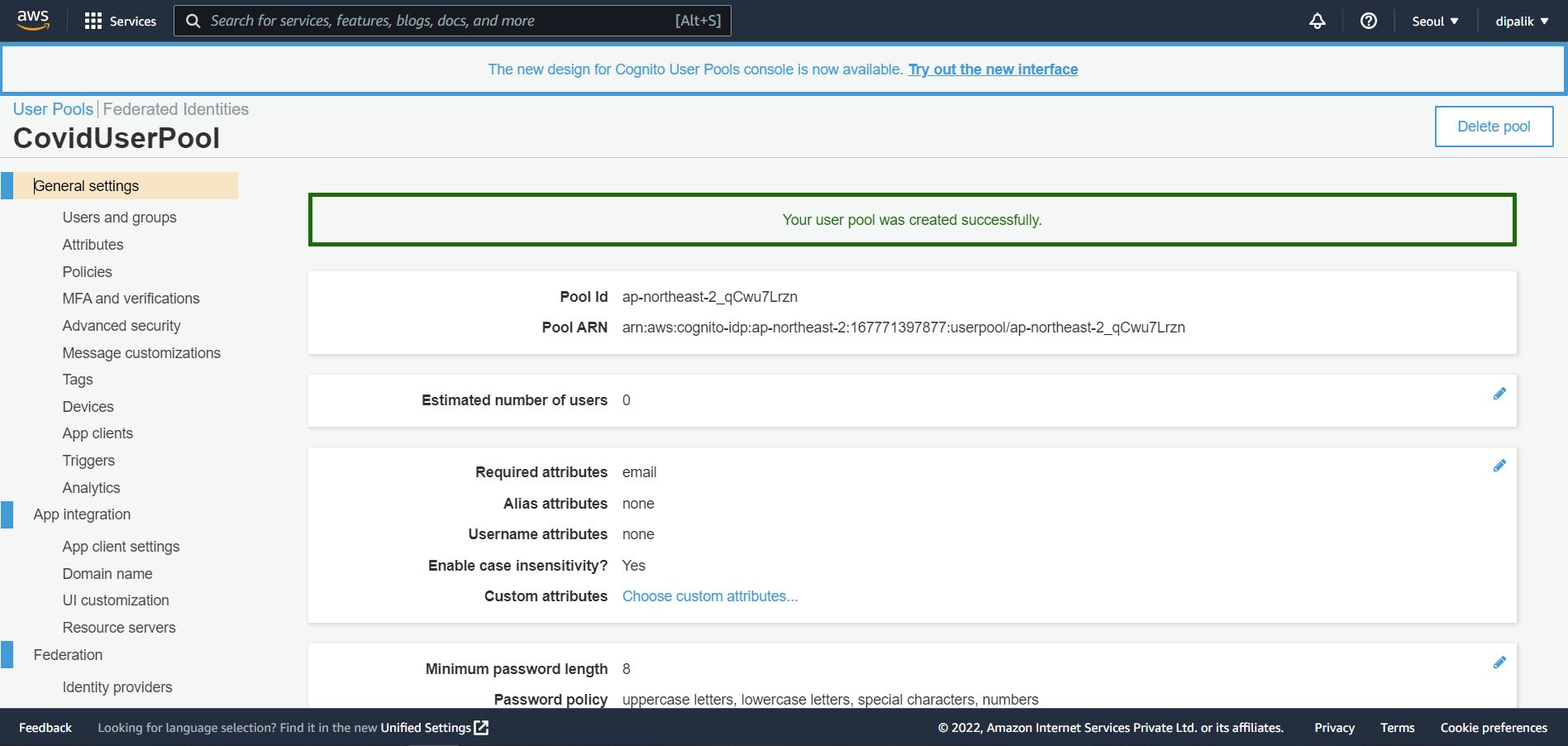
You can go to MFA and verifications link and enable MFA authentication for you require additional security for your users.



Click on the Review link and review the final settings



If you find all the settings are as per your requirement click on Create Pool to create your user pool.

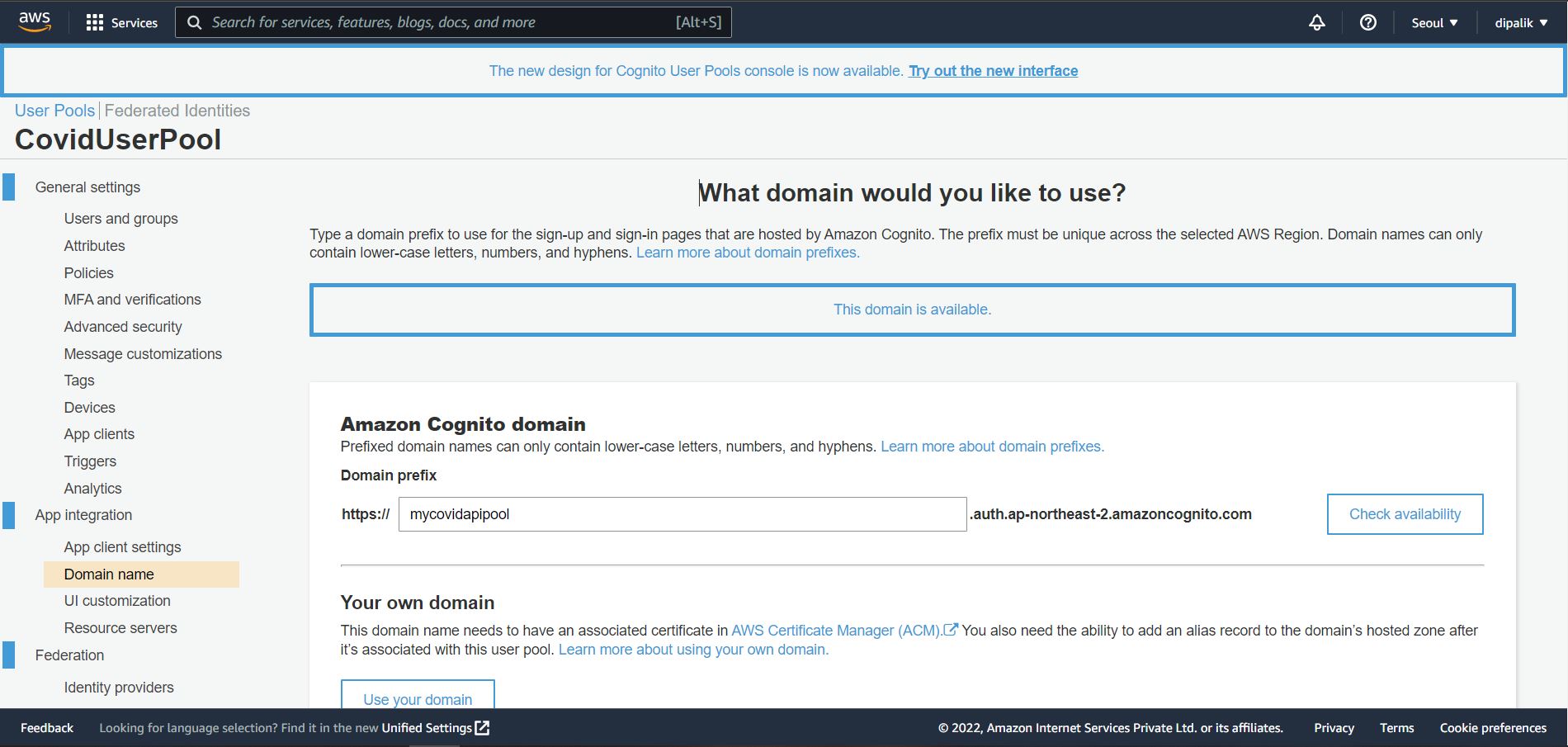


After clicking on the Create Pool you can see a unique Pool ID is generated for your User pools, now we will learn how to configure other important elements for User Authorizations.

Step 4 – Setup Domain for User Registration

After creating Cognito User pool its very important to setup a public domain name for your pool, so that your users can register themselves using the public url.

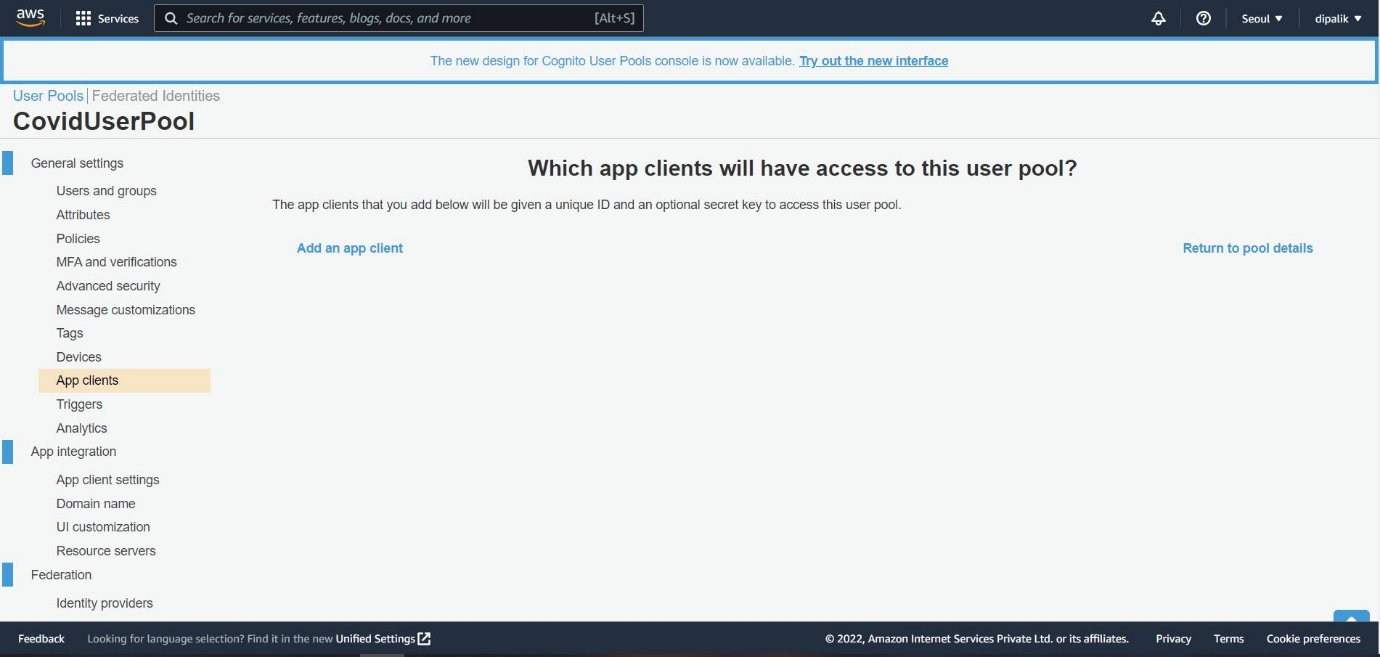
For creating Domain, go to the Domain Name under App Integration settings.



Now provide a unique domain prefix for your public domain and check if its available for the free hosting. This domain will be provided by AWS without any additional cost. If your domain is available click on Save settings button to register your domain.

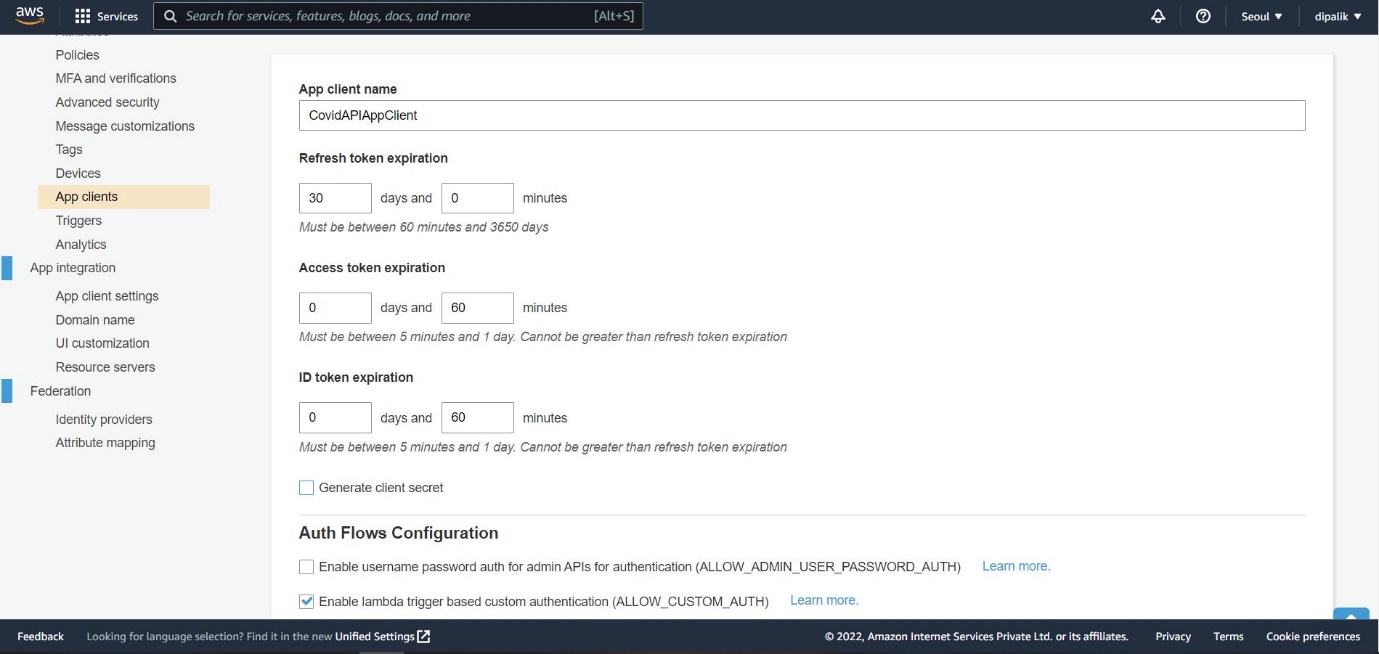
Step 5 – Setup AppClient for Authenticating users.

Go to App Clients under General Settings and click on “Add an app Client”



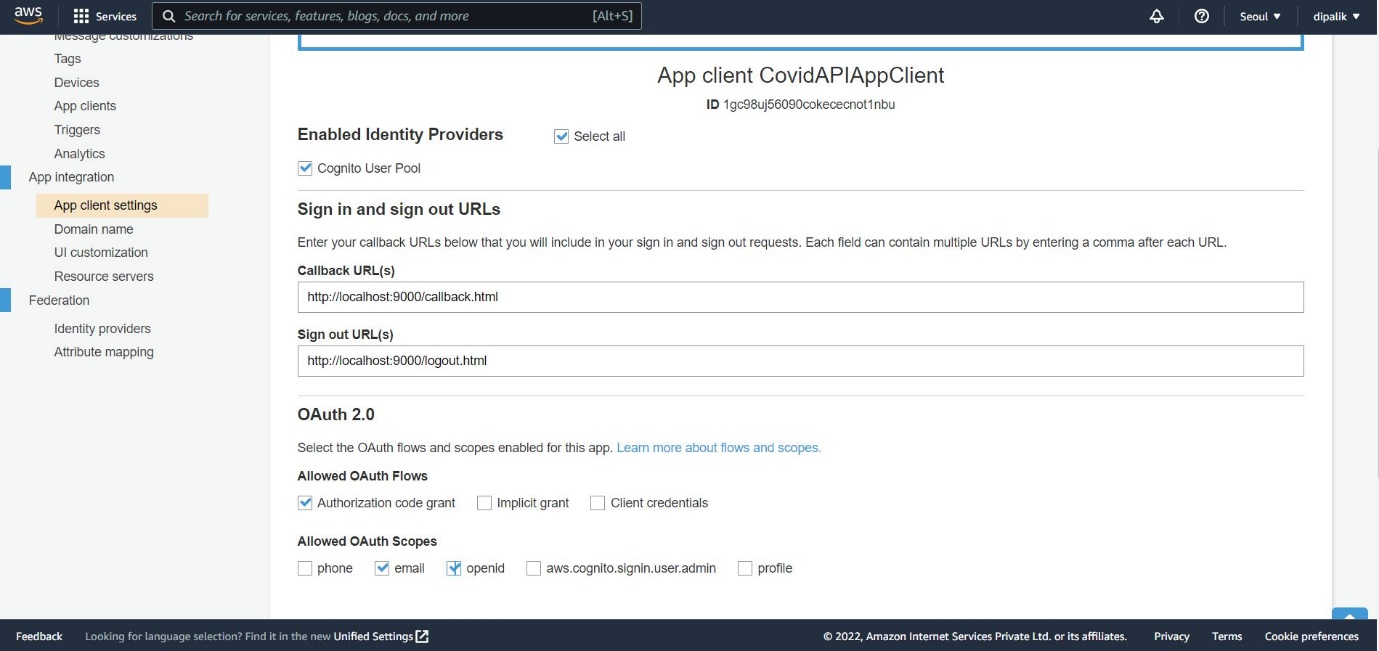
Review the App Client Settings and remember to uncheck “Generate client secret”

Note : As we want to use this Pool for Authentication and Authorization with GraphQL APIs hence its very important to uncheck “Generate client secret” else you will not be able to use this pool in your AppSync Dashboard.



Step 6 – Configure App Client Settings

After successfully creating the App client next steps is to configure the AppClient settings, you can go to “App client settings” under App Integration.

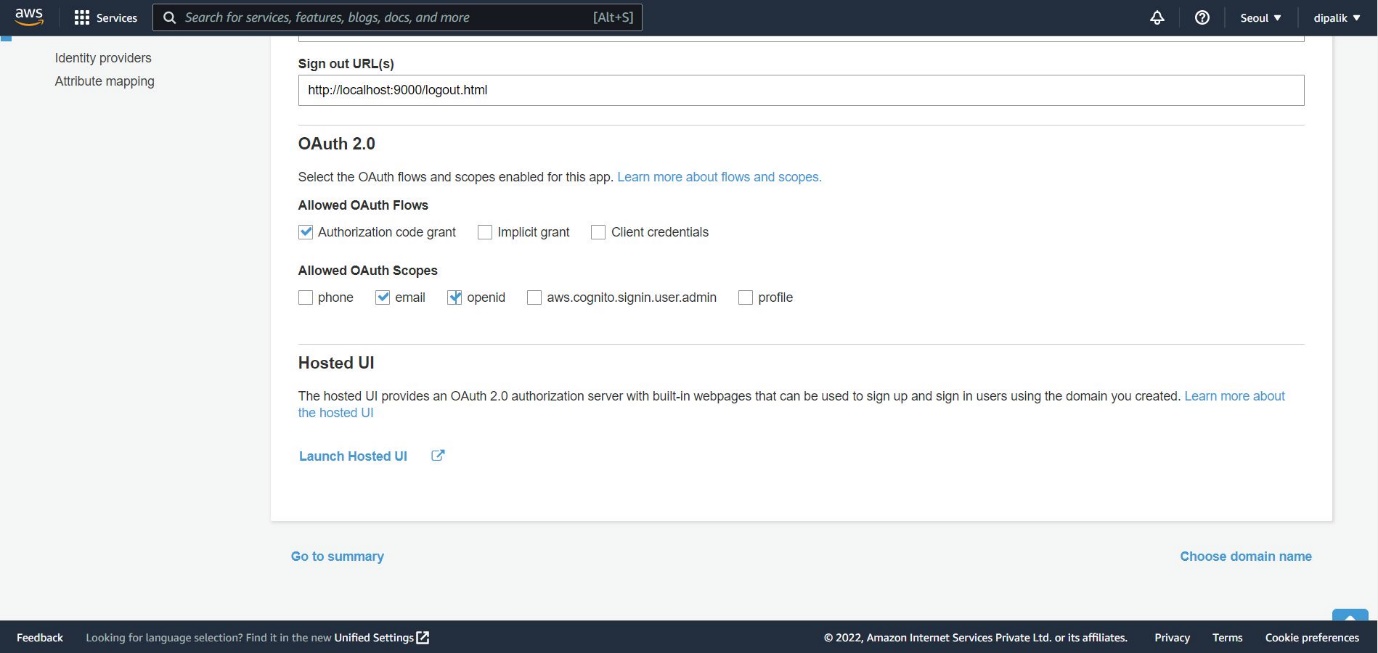


Select Cognito user pool settings checkbox and provide callback URL and signout URL for your users registrations, if you want to link to your existing UI application.

Enable OAuth flows as Authorization code grant and select email and open id as valid allowed OAuth Scopes, its important to select open id if you are using email for your user verification else you will not be able to save settings.

Here you can also enable Third party authentication using your Social identify providers such as Google, Facebook etc.

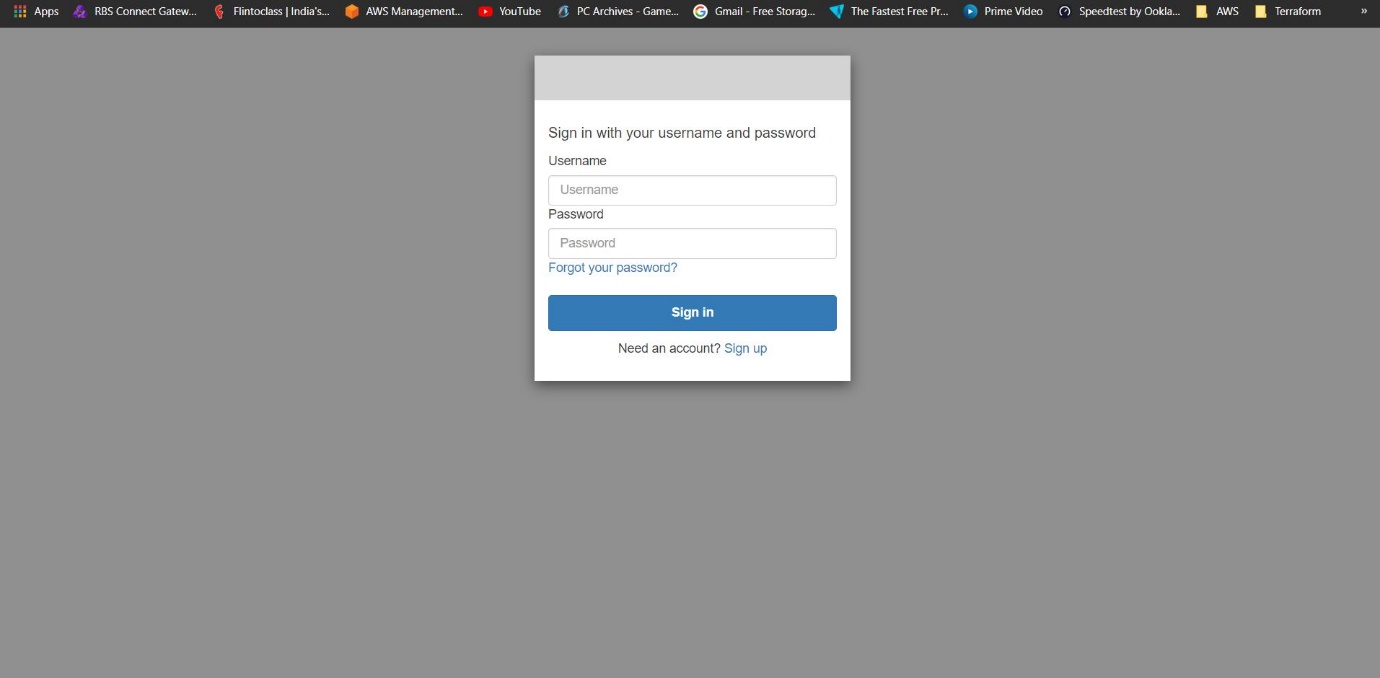
Once you save the settings, AWS will host the user registration UI on the domain you created in previous steps, it will be an interactive UI using which your users can signup on your user pool.



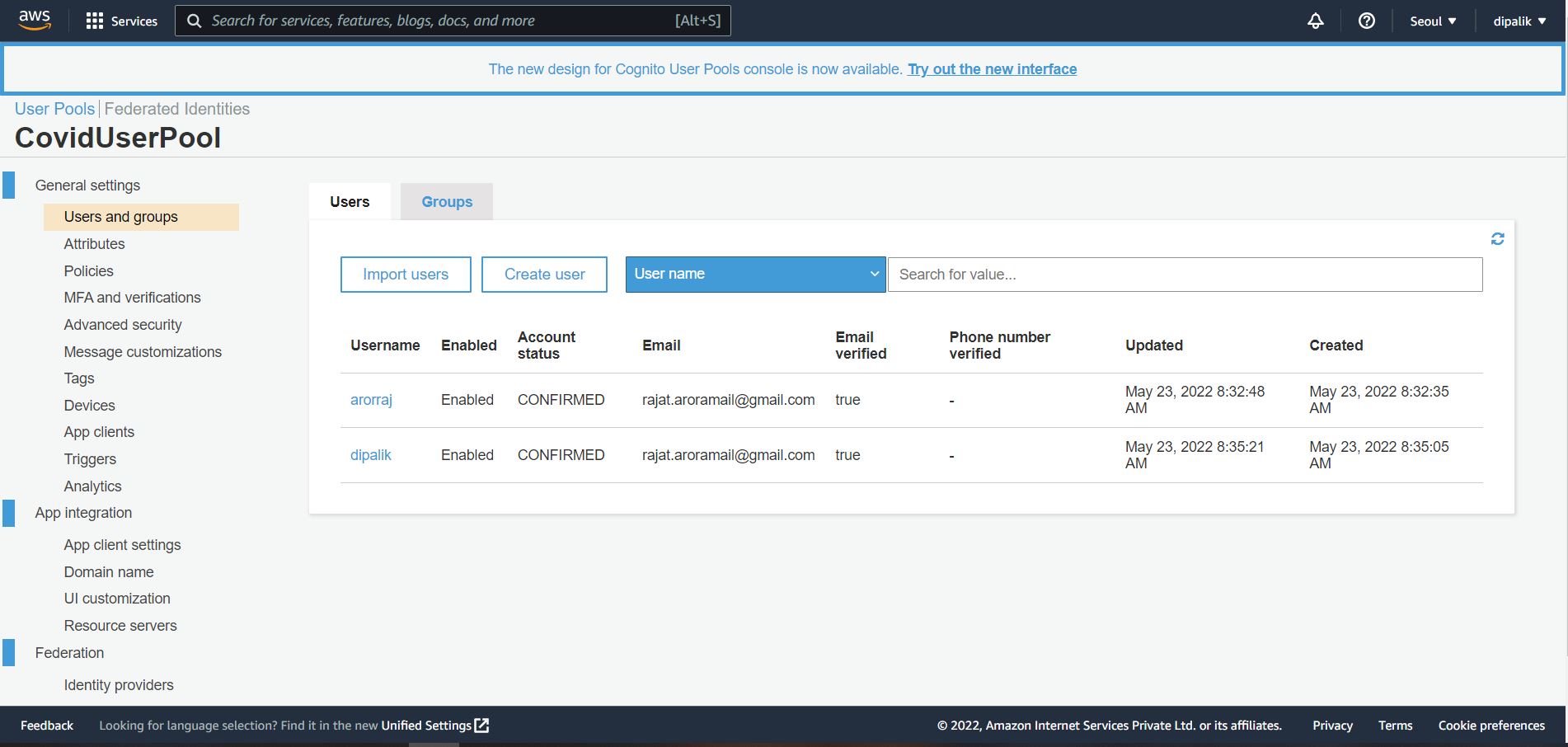
Click on Launch Hosted UI to open your users registration portal.

Step 7 – Signup Users using Hosted UI

Your users can use this URL and click on Sign up link to register themselves, it will ask for username, email and password. Once registered it will send verification code to the email id, users have to provide the verification code to complete the registration process.



You can go to Users and Groups in your Cognito User pool to see the list of verified and registered users.



Step 8 – Add Role/User Groups and add users to roles

If you want to enable Role based access you can create Groups and assign users to Groups based of their access level so that based on this role they will get access to the GraphQL APIs.

