Module 2: Security Management in AWS

Demo Document 5

Title: Configuring Strong and Secure Authentication Access Mechanism using Amazon Cognito

Use Case

A MNC company wants to migrate their popular web community application from on premises to AWS cloud. First thing they want is to develop a strong and secure authentication access mechanism. The Chief Architect of the company recommend tech team to use Amazon Cognito for it.

He expects for the following requirements to be covered:

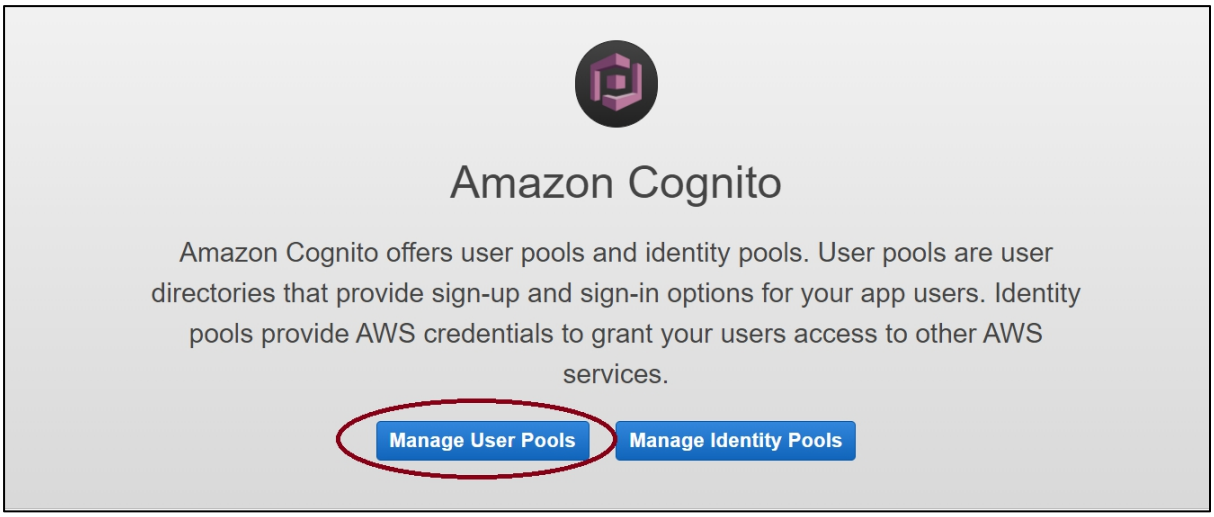
1. Users should be able to Login to application using one of social media credential (Facebook or Google or Amazon)
2. Users should be able to create their own login credentials and login with same
3. Enable email communication through SES service
4. Users should not find any credentials related data on the application layer or the database layer

As a part of the team, please demonstrate how would you implement a solution that incorporates all these requirements.

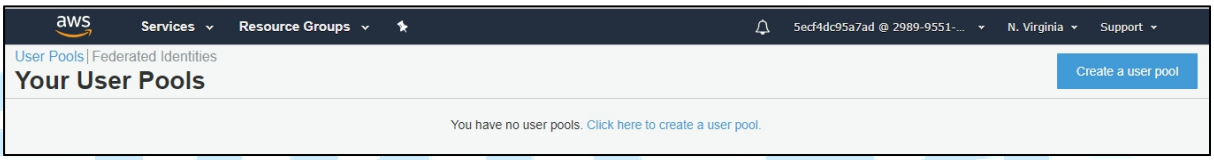
Services Covered: AWS Cognito, AWS SES

Solution Steps

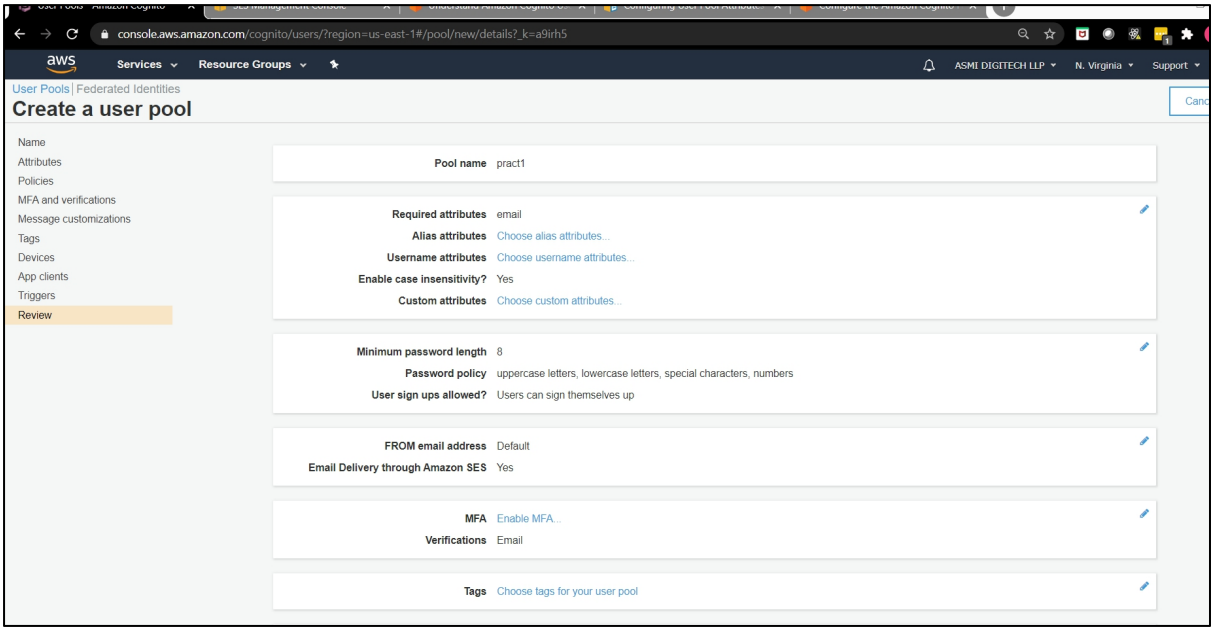
- Login to AWS account and select **Cognito** service.
- In the Amazon Cognito console, choose **Manage User Pools**, and then choose your user pool.



- Select "**Create a User Pool**"



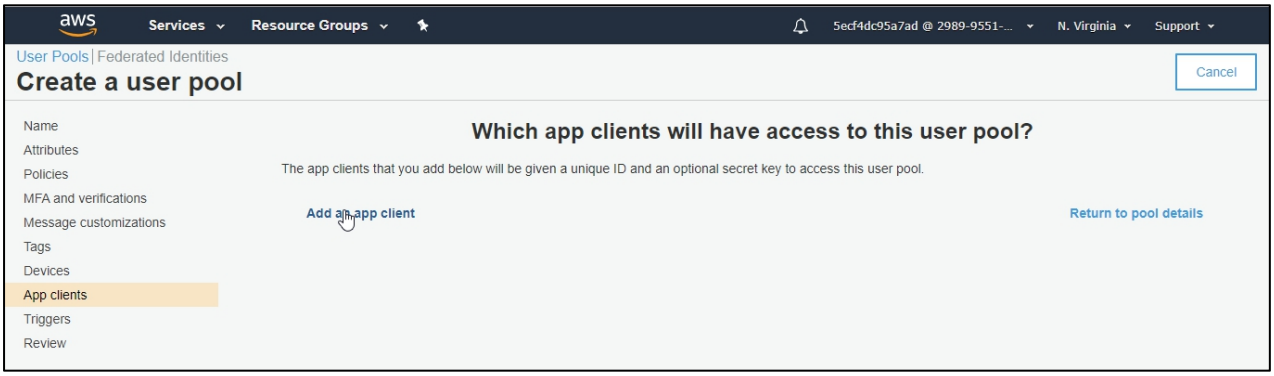
- Enter **Pool name** as "pract1" and click on "**Review Default**" option below.



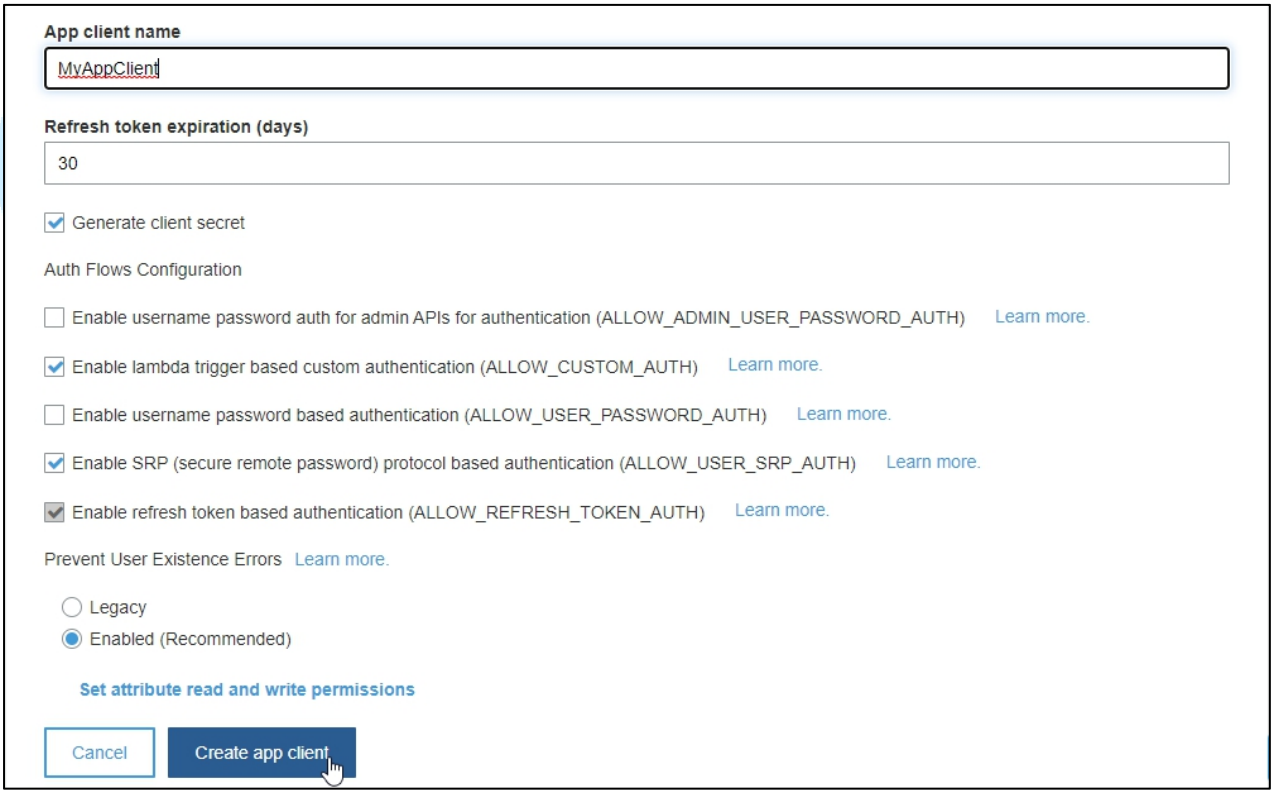
- There are 2 parallel services users need to create before creating user pool.

Task1: Create App client ID

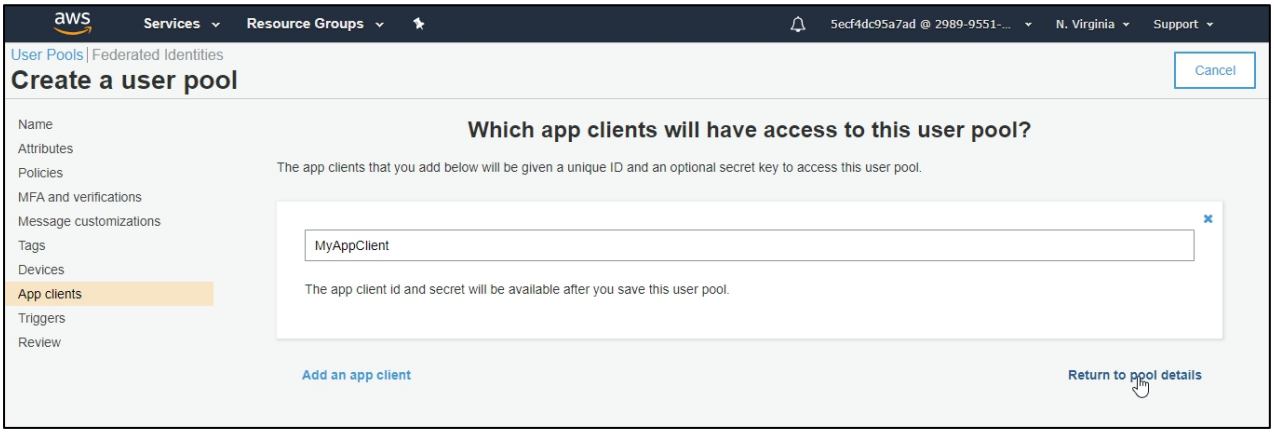
- On left panel click on **App Clients** link. Select **Add an app client** link



- Enter app client name as "MyAppClient". Keep all default options as it is and click on "**Create app client**" link.

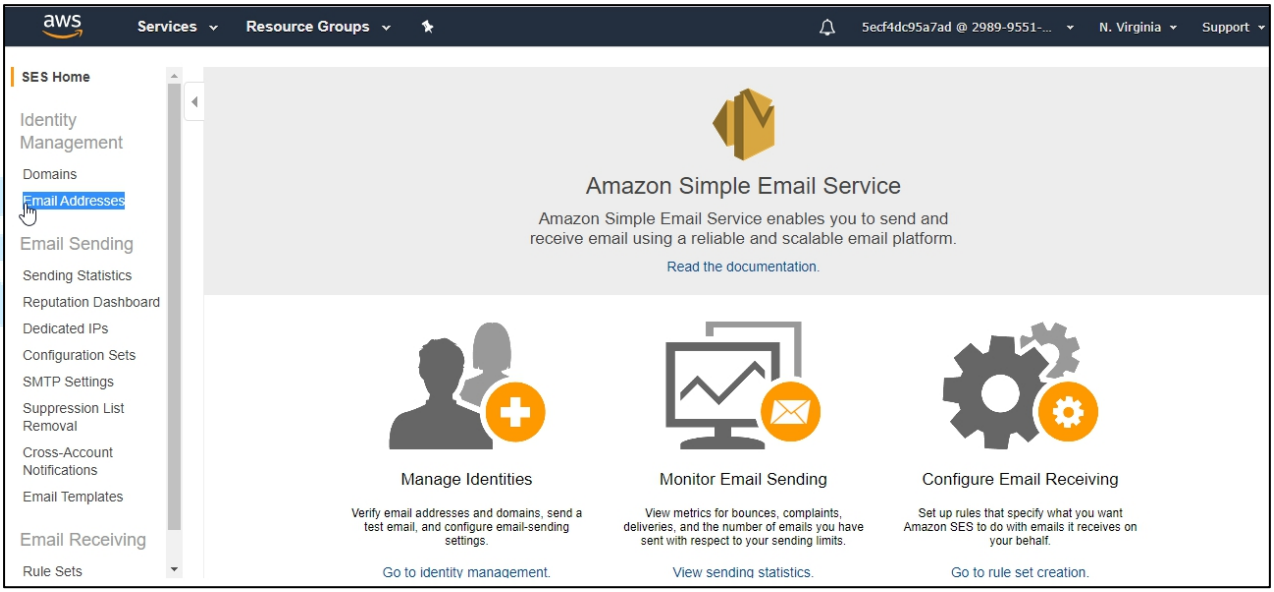


- Click on "**Return to pool details**" link

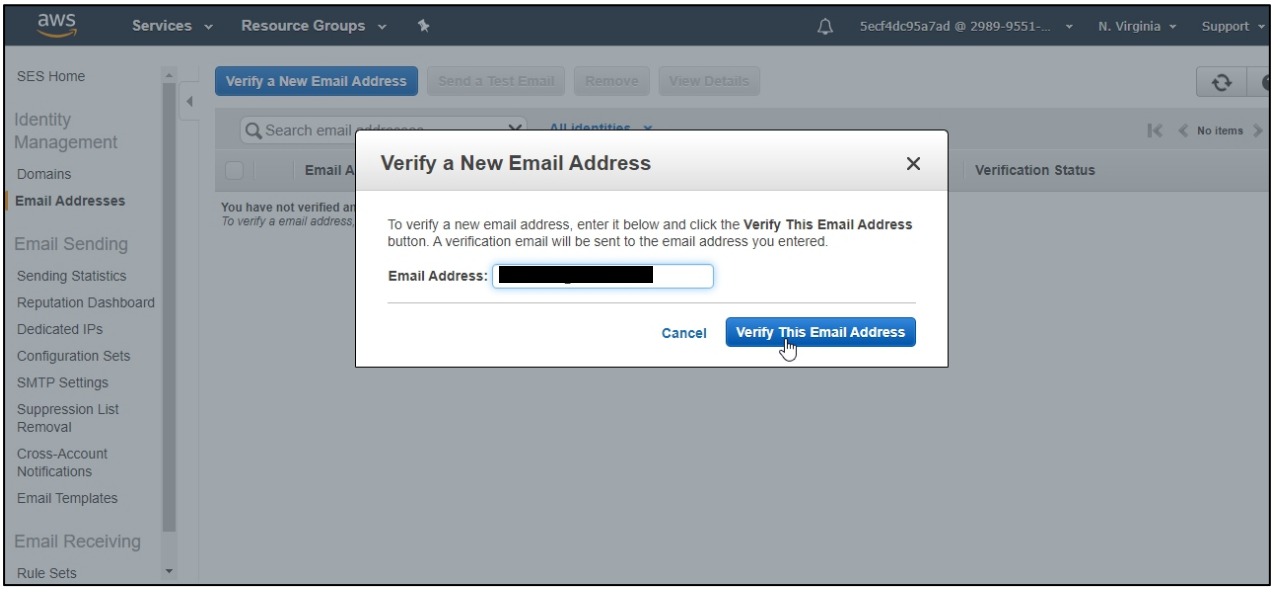


Task2: Create SES (Simple Email Service) client ID

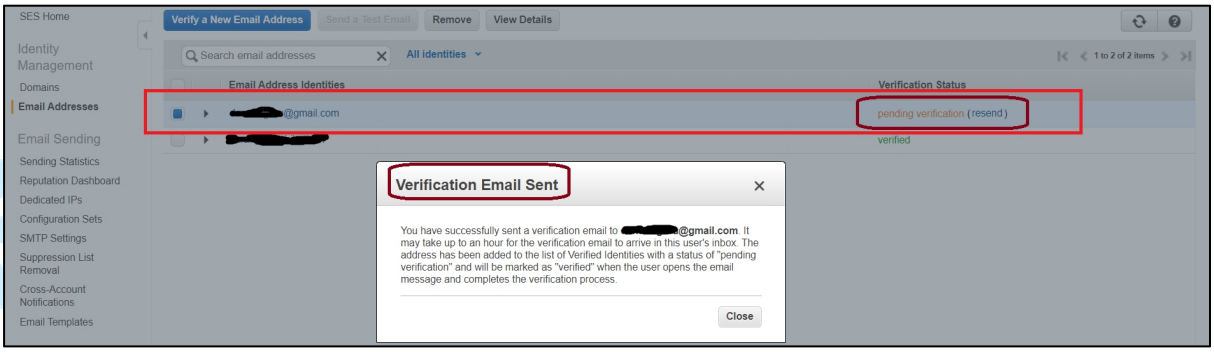
- Go to AWS services and Select **SES (Simple Email Services)** on different browser window. On SES Home page, on left panel, select "**Email Addresses".**



- Select "**Verify a New Email Address**". Enter a valid email ID for which you have access. Click on "**Verify This Email Address".**

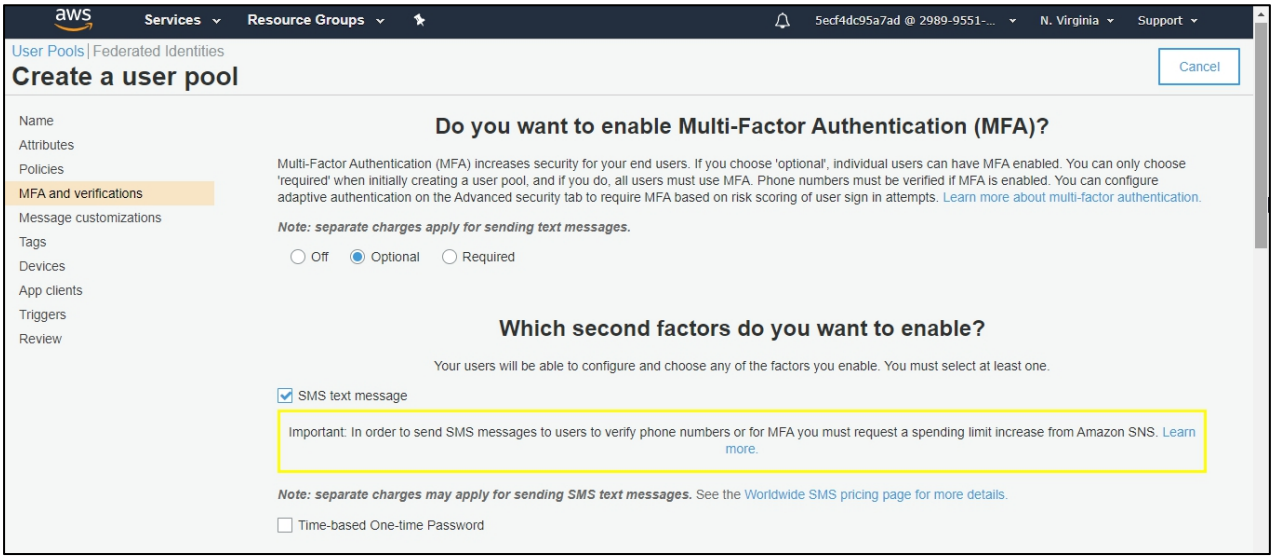


- By this point, you would have got an email to the mail address that you have specified. Open the mail and click on verify link. Make sure that your status change to **Verified** on SES home page.

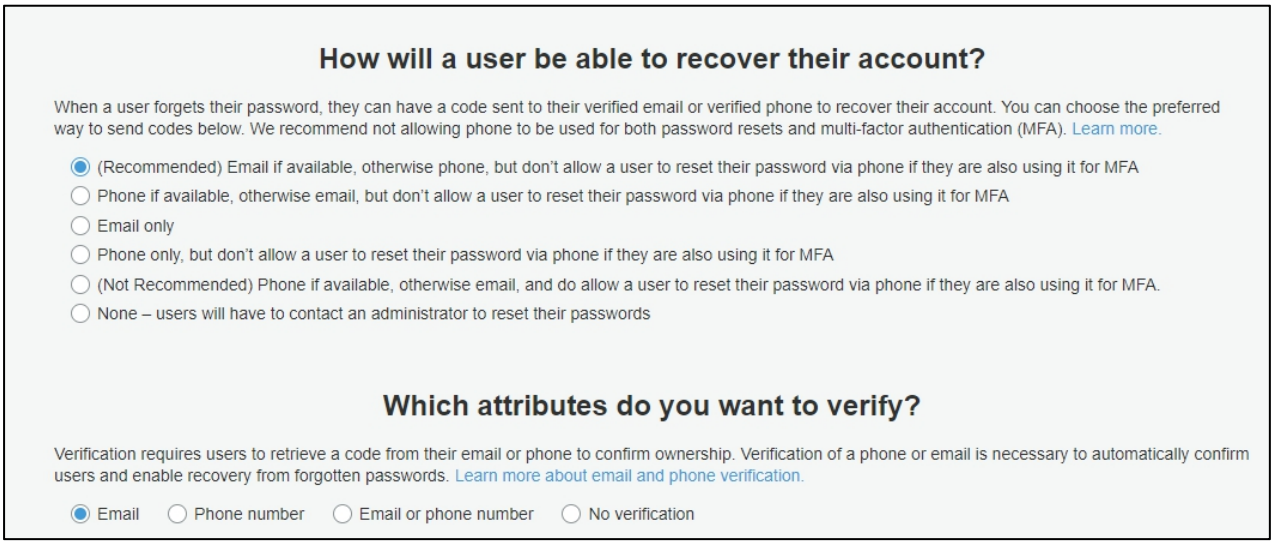


Come back to Create a user pool review page

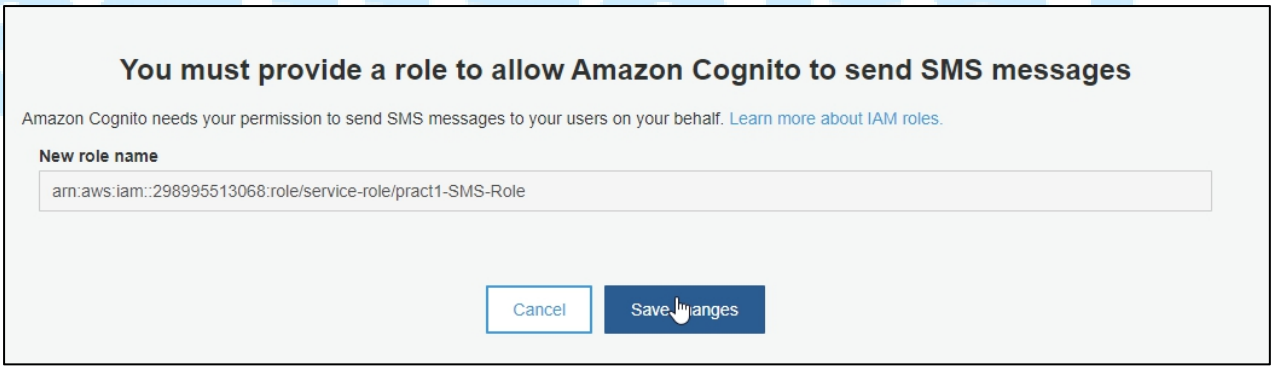
- Click on **"MFA and verifications".** Select **"Optional"** radio button on right hand side for MFA**.** Under "**Which second factors do you want to enable?",** select "**SMS Text message**" check box.



- For **"How will a user be able to recover their account?",** select first radio button which is a recommended option**.** For **"Which attributes do you want to verify?",** select email option if not selected.

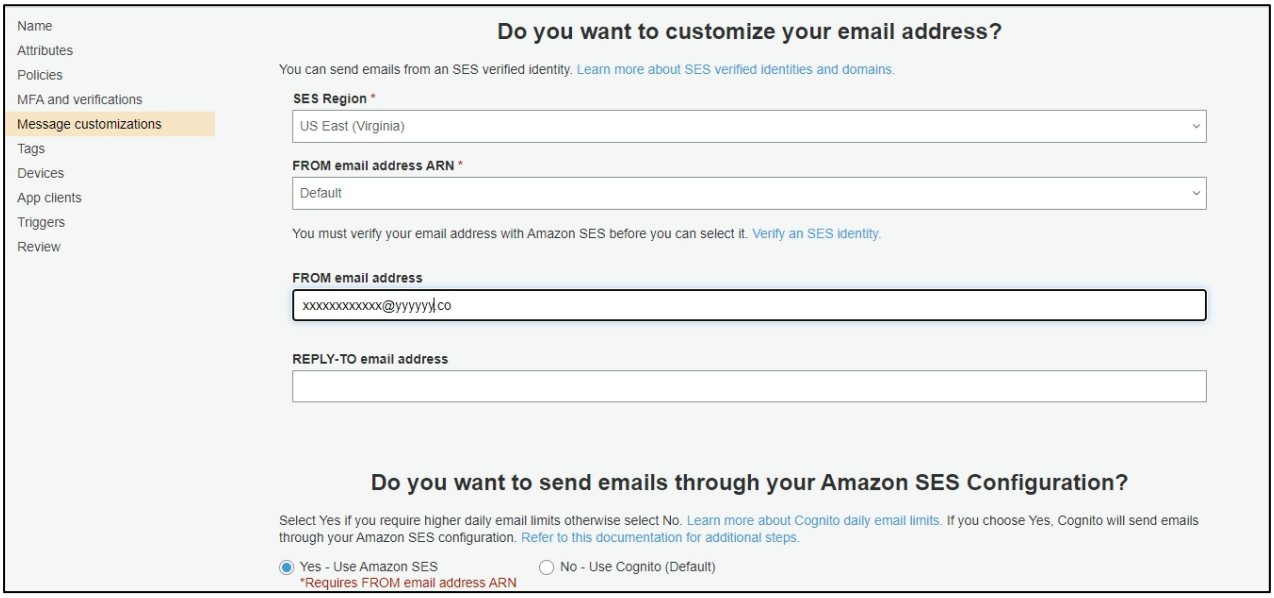


- For "**You must provide a role to allow Amazon Cognito to send SMS messages**", click on **Create Role** button with default name selected by AWS Cognito. Note down the ARN of the new role created. Click on **Save changes**.

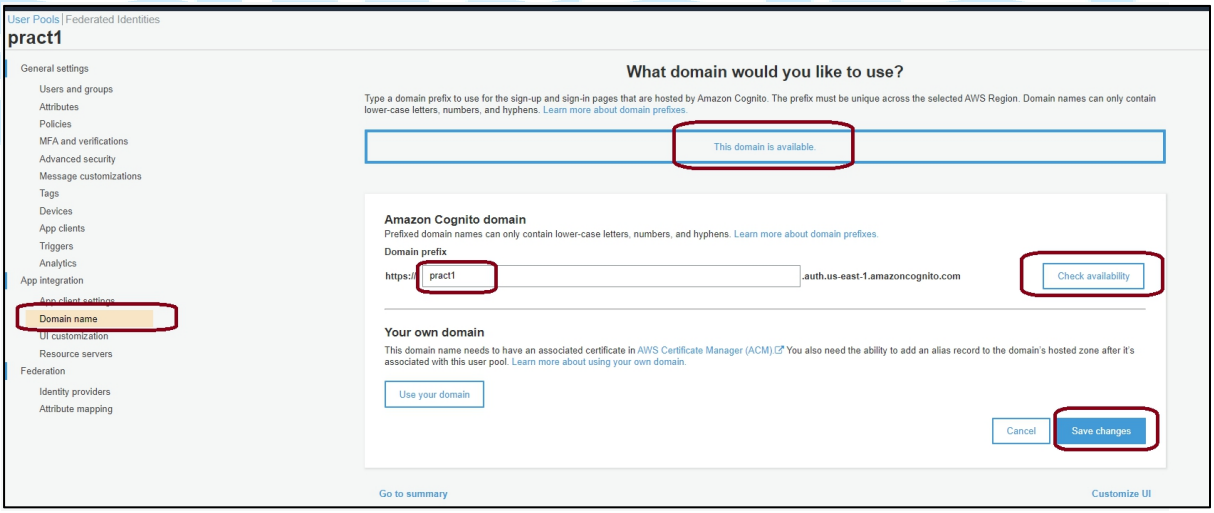


Page will navigate to next section, which is "message customization".

- For option **"FROM email address ARN *",** select the email which you verified in SES service**.** Next, for **"Do you want to send emails through your Amazon SES Configuration?",** select **"Yes – Use Amazon SES"** option.



- Keep all other options default and click on **Next** step which goes to next section. In the left panel, click on **Review** and click "**Create pool**" button. For confirmation, user will see the message as "Your user pool was created successfully."
- In the left navigation pane, under **App integration**, choose **Domain name**. Under "**Amazon Cognito domain**", enter unique name and check domain availability. Once you see the display confirmation as "**This domain is available**.", click on **Save**.

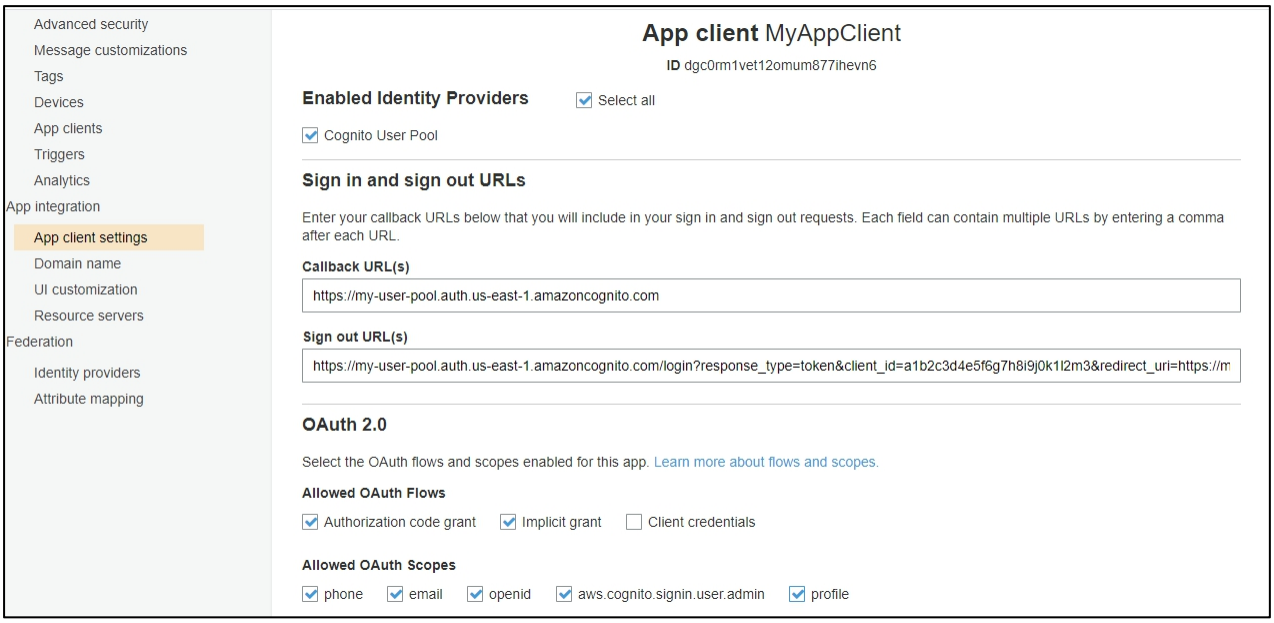


Select "App client settings" in the left navigation pane

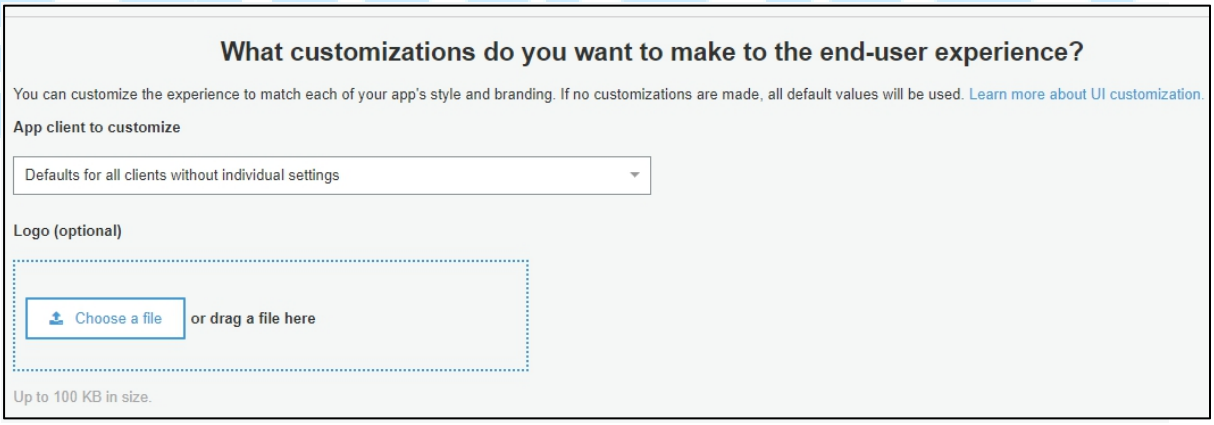
- Select "**Select All**" option. Select "**Cognito User Pool**".
- Enter **Callback URL**. A callback URL indicates where the user is to be redirected after a successful sign-in. Construct the URL for the hosted web UI. For example: https://my-user-pool.auth.us-east-1.amazoncognito.com
- Similarly, for Sign out URL, you can use URL:

  https://my-user-pool.auth.us-east-1.amazoncognito.com/login?response_type=token&client_id=a1b2c3d4e5f6g7h8i9j0k1l2m3&redirect_uri=https://my-website.com

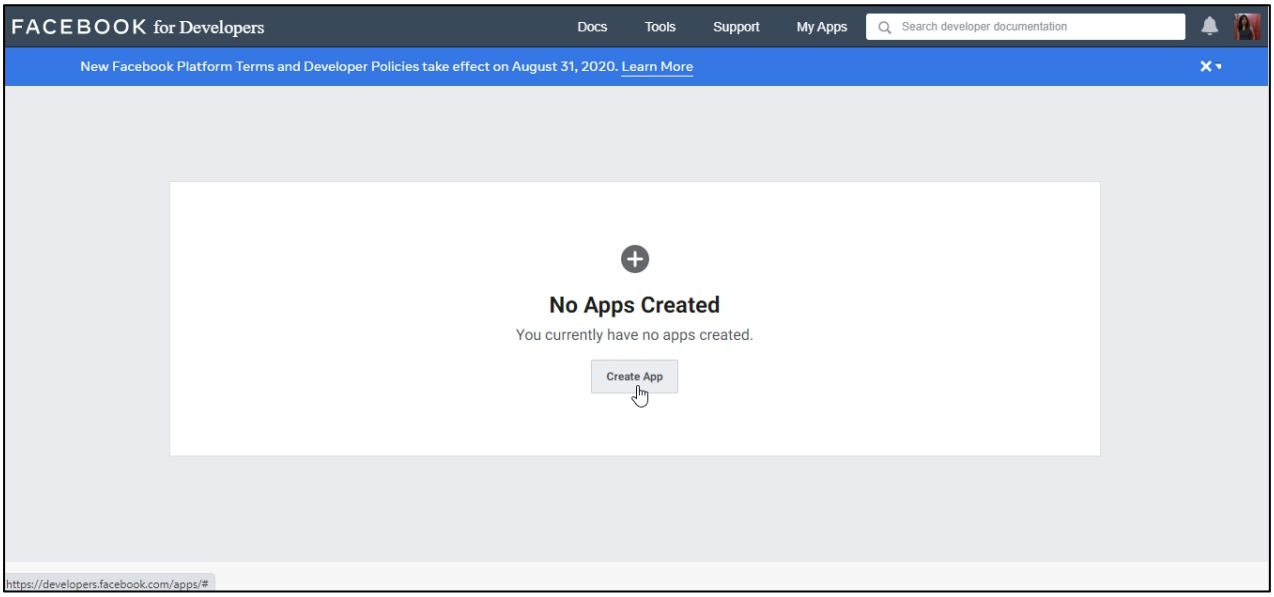
- Under OAuth 2.0 and Allowed OAuth flows, select "**Authorized code grant**" and "**Implicit grant**". Select all options under "**Allowed OAuth Scopes**". Click on Save changes

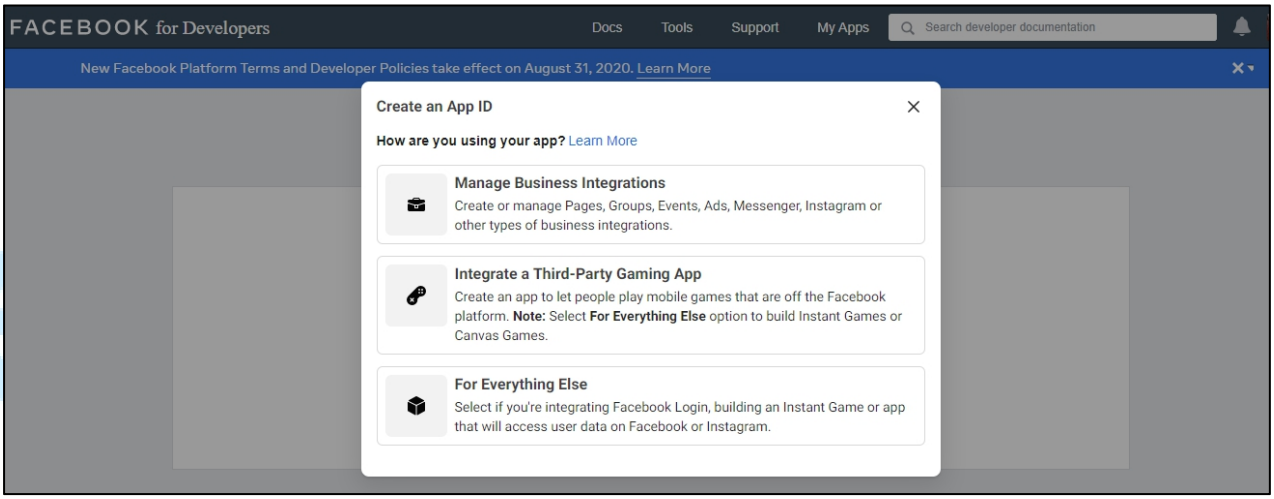


- Go to **UI Customization** section and under "**What customizations do you want to make to the end-user experience?"**, choose a logo section upload relevant logo file. Do not forget to click om "**Save Changes**" at the end of the page.

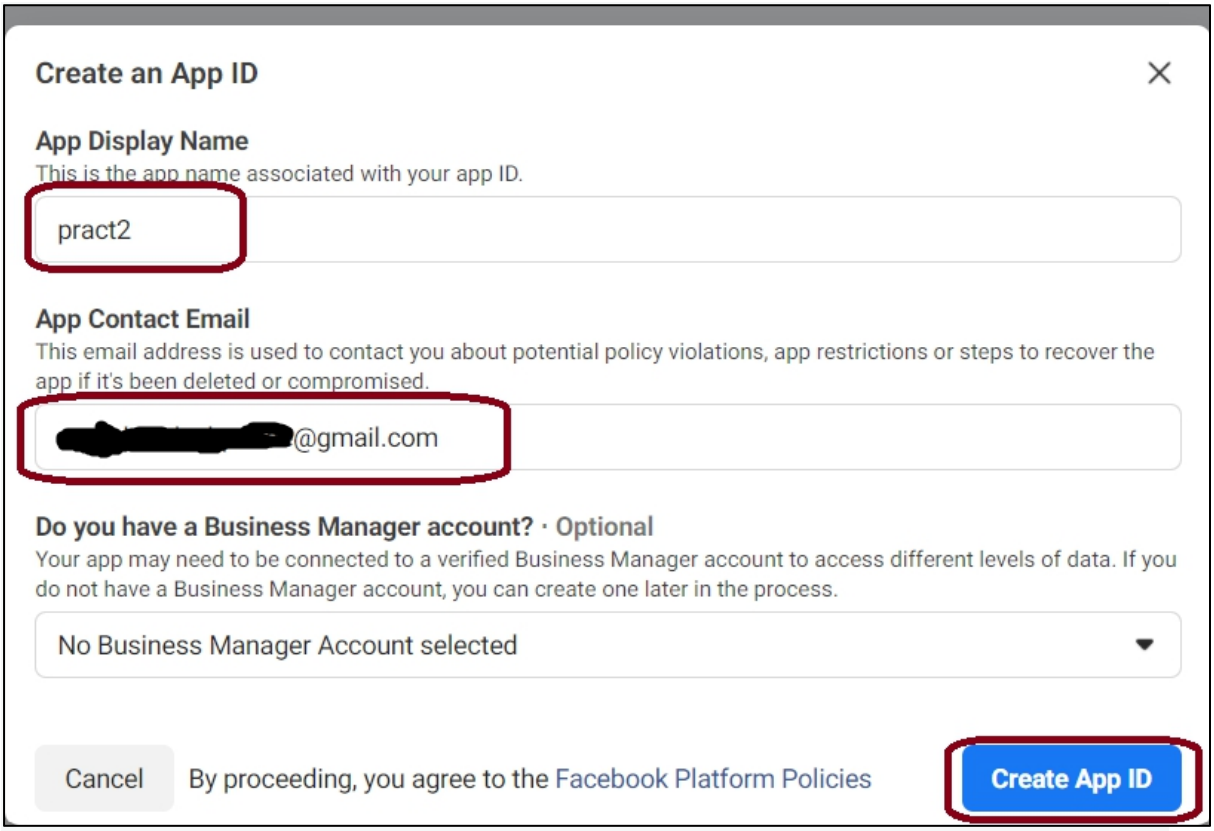


- Go to Identify Providers. Select either Amazon/Google/Facebook/Apple/SAML/OPENID connect. In this demo, we will select Facebook.
- Login with valid credentials at https://developers.facebook.com/. Go to **My Apps**. Select "**Add a new App**" and select option as "**For everything Else**".

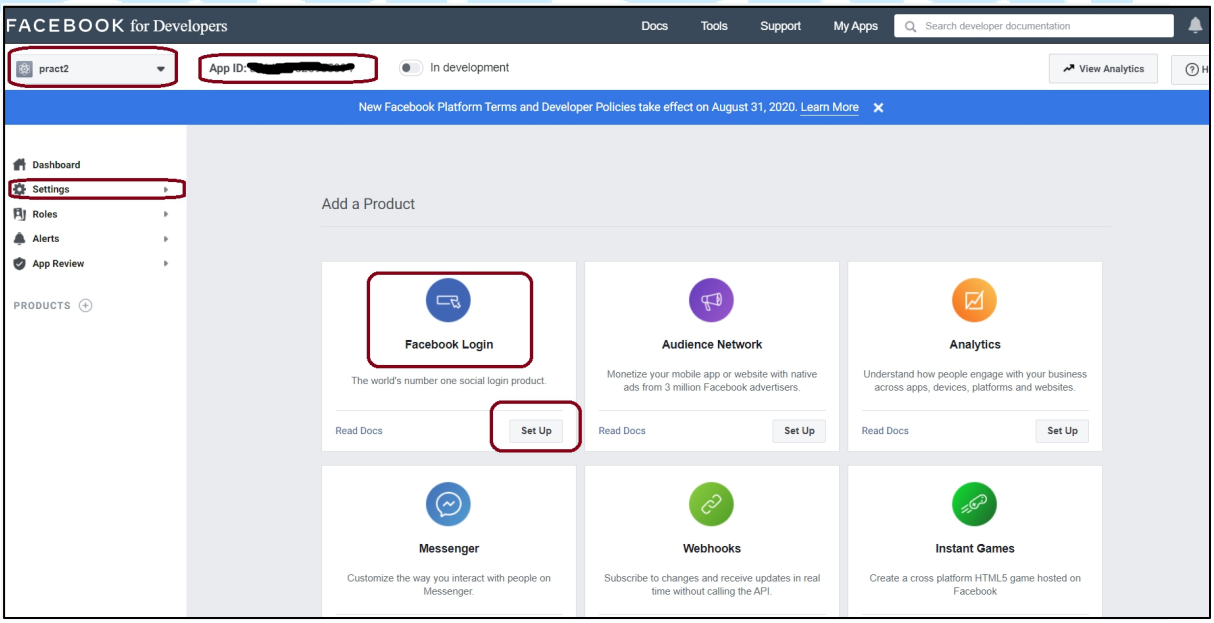




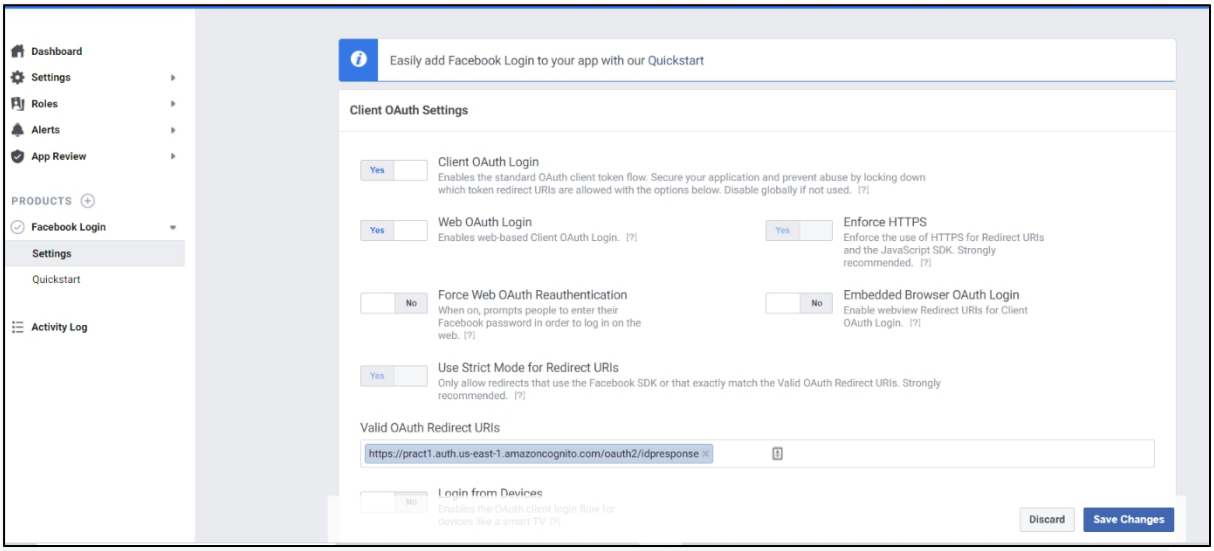
- In the dialog box that opens, enter details like App Display Name and App Contact Email (which is already displayed same as logged in ID)



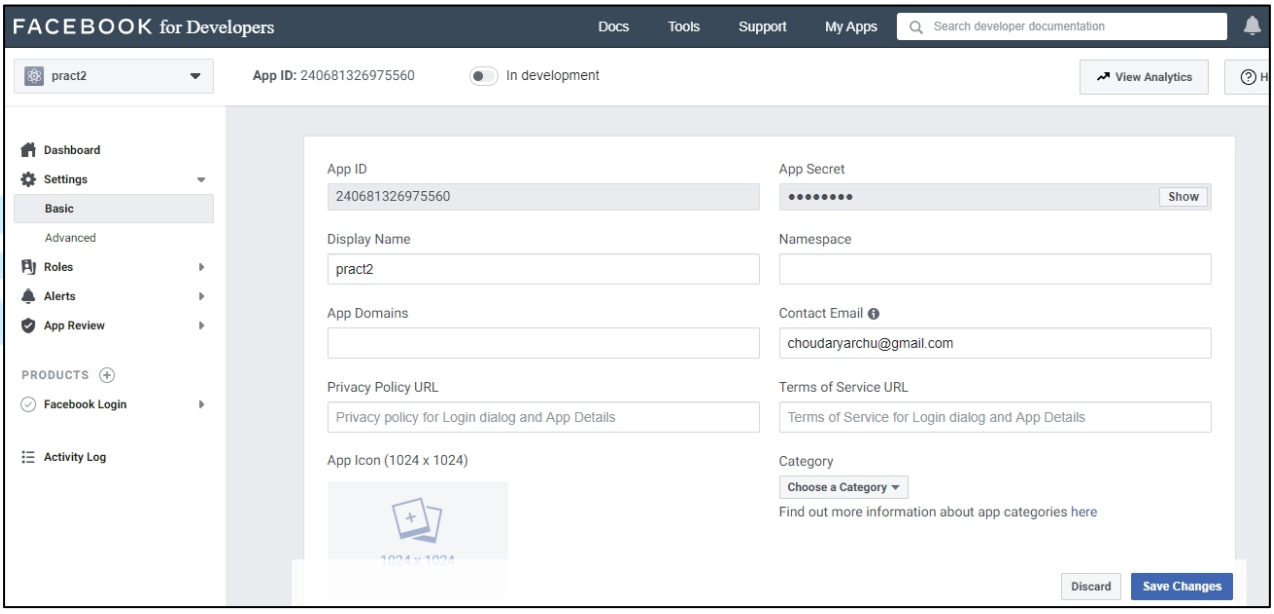
- Click on "**Create App ID**". This will navigate to a page with App ID displayed at the top. Select "**Facebook Login**".



- On the login page, go to setting link. Enter URL in section "Valid OAuth Redirect URIs" as ***https://<your-user-pool-domain>/oauth2/idpresponse.*** Here in our case, enter URL as https://pract1.auth.us-east-1.amazoncognito.com/oauth2/idpresponse
- Click on save changes.

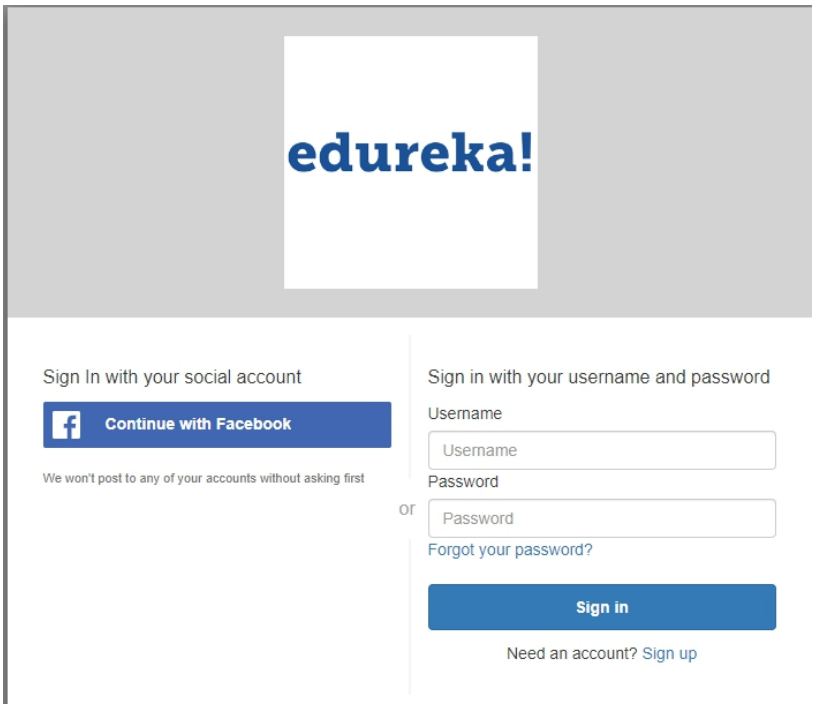


- Go to Settings and under that **Basic**. Observe that at right side of the page display App ID and App secret ID are available.



- Come back to User pool page and click on **Identify Providers**, enter **Facebook app ID** as above displayed App ID and **App secret** as App secret ID and **Authorized Scope** as Facebook logged in email id.
- Click on "Enable Facebook".
- Go to "**App client settings**", click on **Launch Hosted UI**.

- Login page will be displayed with logo on top and **Login** and **Password** on the right. On the left side, Facebook login will be displayed.



- Try sign up with a new account and validate email id by opening email and validate it.

----End of the Demo---