

Module 2: Security Management in AWS

Demo Document 5

edureka!

edureka!

© Brain4ce Education Solutions Pvt. Ltd.

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

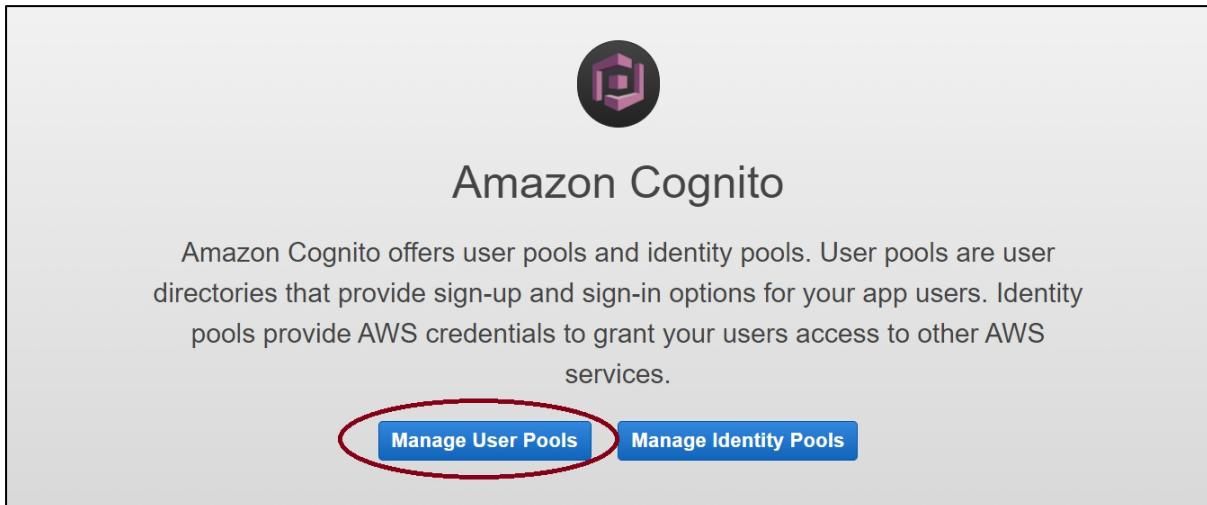
As a part of the team, please demonstrate how would you implement a solution that incorporates all these requirements.

Services Covered: AWS Cognito, AWS SES

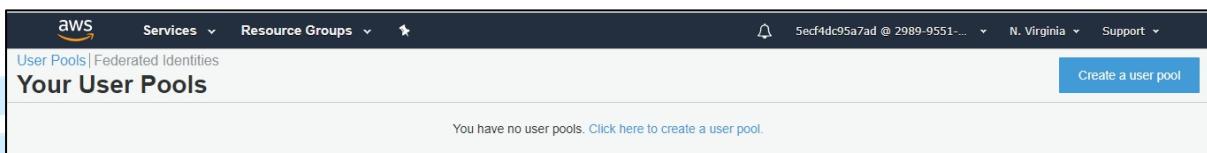
edureka!

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.

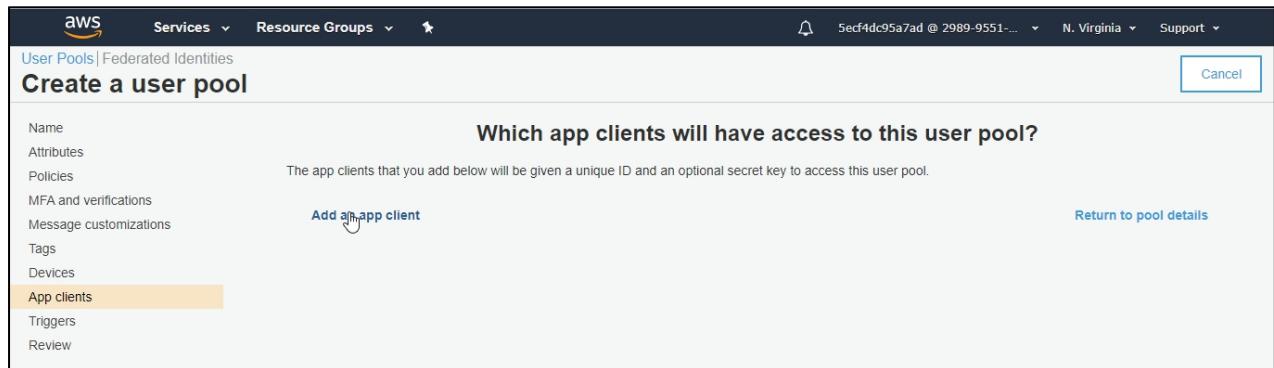
A screenshot of the "Create a user pool" configuration page in the AWS Cognito console. The left sidebar lists options: Name, Attributes, Policies, MFA and verifications, Message customizations, Tags, Devices, App clients, Triggers, and Review (which is selected). The main form has several sections:

- Name:** Pool name: pract1
- Attributes:** Required attributes: email; Alias attributes: Choose alias attributes...; Username attributes: Choose username attributes...; Enable case insensitivity? Yes; Custom attributes: Choose custom attributes...
- Sign-up:** Minimum password length: 8; Password policy: uppercase letters, lowercase letters, special characters, numbers; User sign ups allowed? Users can sign themselves up
- Email:** FROM email address: Default; Email Delivery through Amazon SES: Yes
- MFA:** MFA: Enable MFA...; Verifications: Email
- Tags:** Choose tags for your user pool

- 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

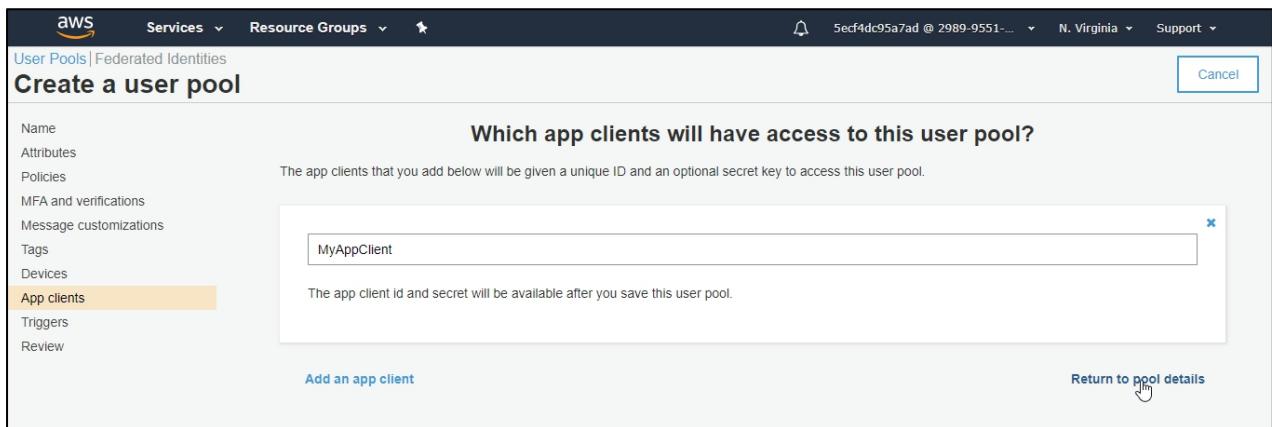


- Enter app client name as "MyAppClient". Keep all default options as it is and click on "**Create app client**" link.

The screenshot shows the 'Add an app client' configuration page. It includes fields for 'App client name' (set to 'MyAppClient'), 'Refresh token expiration (days)' (set to 30), and a checkbox for 'Generate client secret' which is checked. Under 'Auth Flows Configuration', several checkboxes are present: 'Enable username password auth for admin APIs for authentication (ALLOW_ADMIN_USER_PASSWORD_AUTH)', 'Enable lambda trigger based custom authentication (ALLOW_CUSTOM_AUTH)' (which is checked), 'Enable username password based authentication (ALLOW_USER_PASSWORD_AUTH)', 'Enable SRP (secure remote password) protocol based authentication (ALLOW_USER_SRP_AUTH)' (which is checked), and 'Enable refresh token based authentication (ALLOW_REFRESH_TOKEN_AUTH)' (which is checked). There's also a section for 'Prevent User Existence Errors' with options 'Legacy' and 'Enabled (Recommended)' (which is selected). At the bottom, there are 'Cancel' and 'Create app client' buttons, with the cursor hovering over the 'Create app client' button.

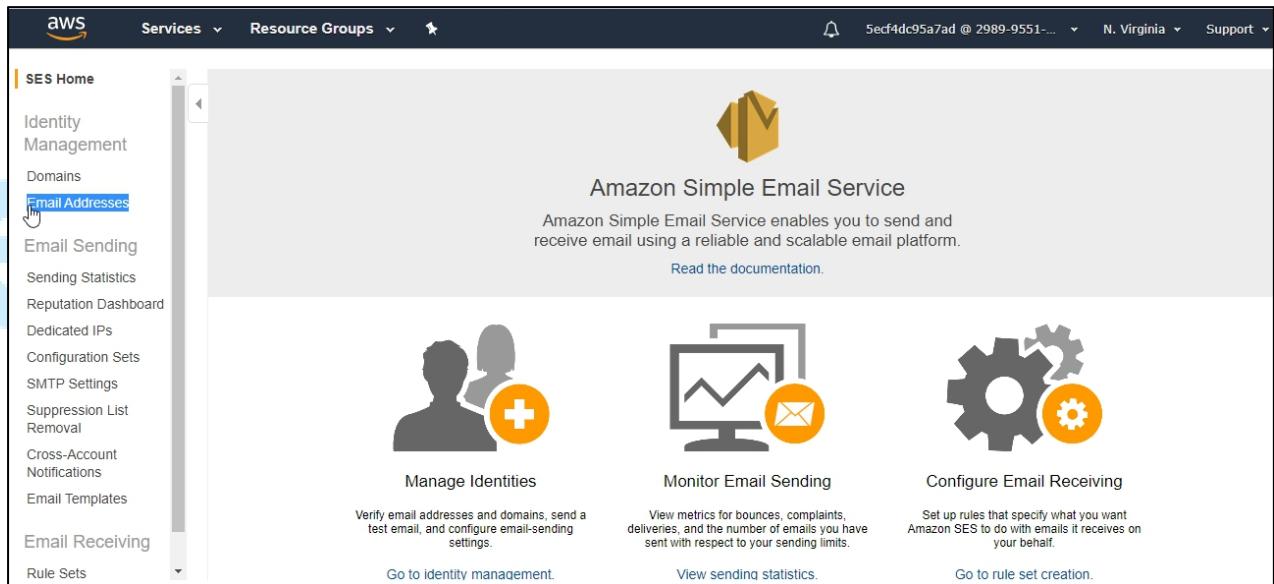
- Click on "**Return to pool details**" link

Security Management in AWS



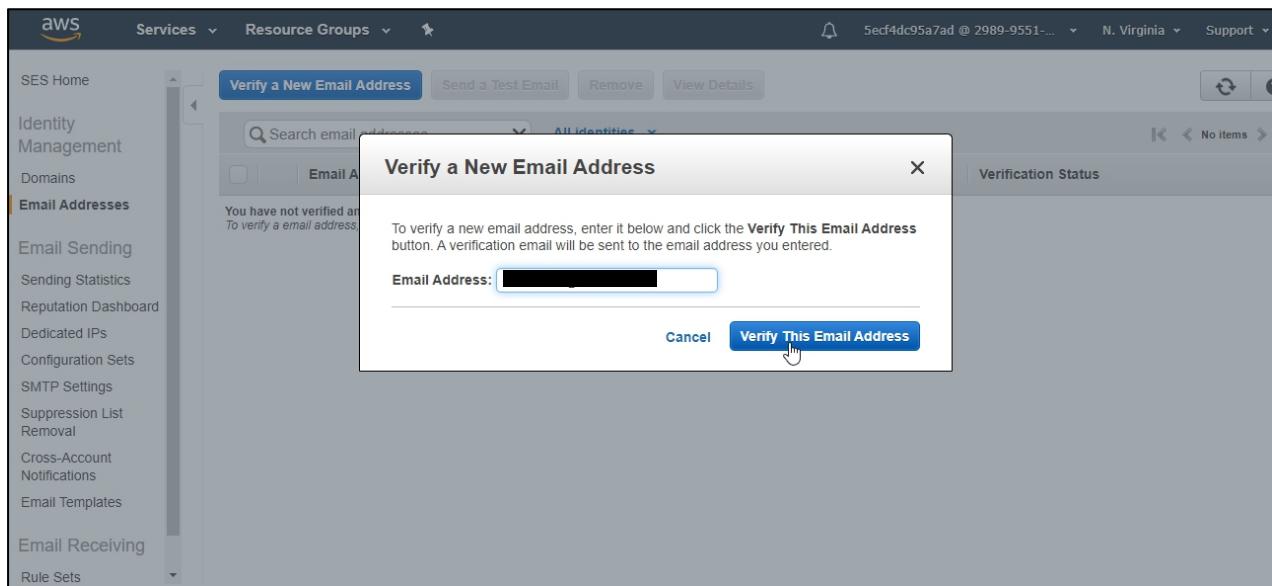
Task2: Create SES (Simple Email Service) client ID

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

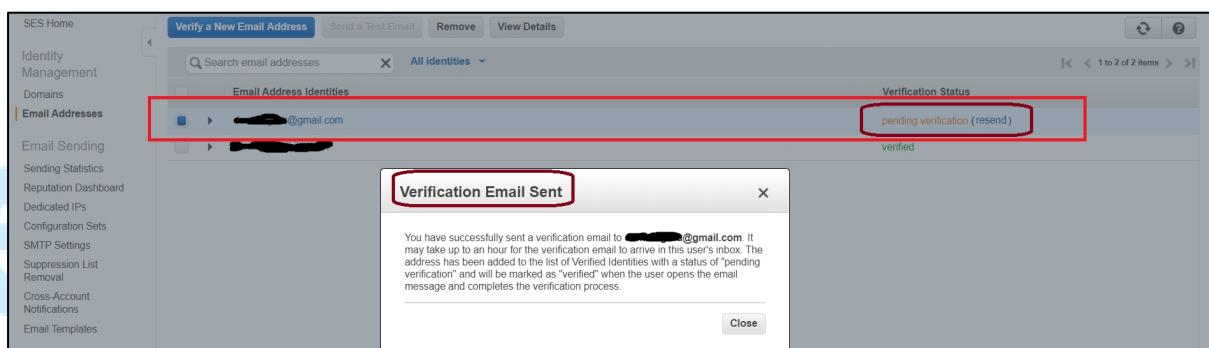


- Select “Verify a New Email Address”. Enter a valid email ID for which you have access. Click on “Verify This Email Address”.

Security Management in AWS

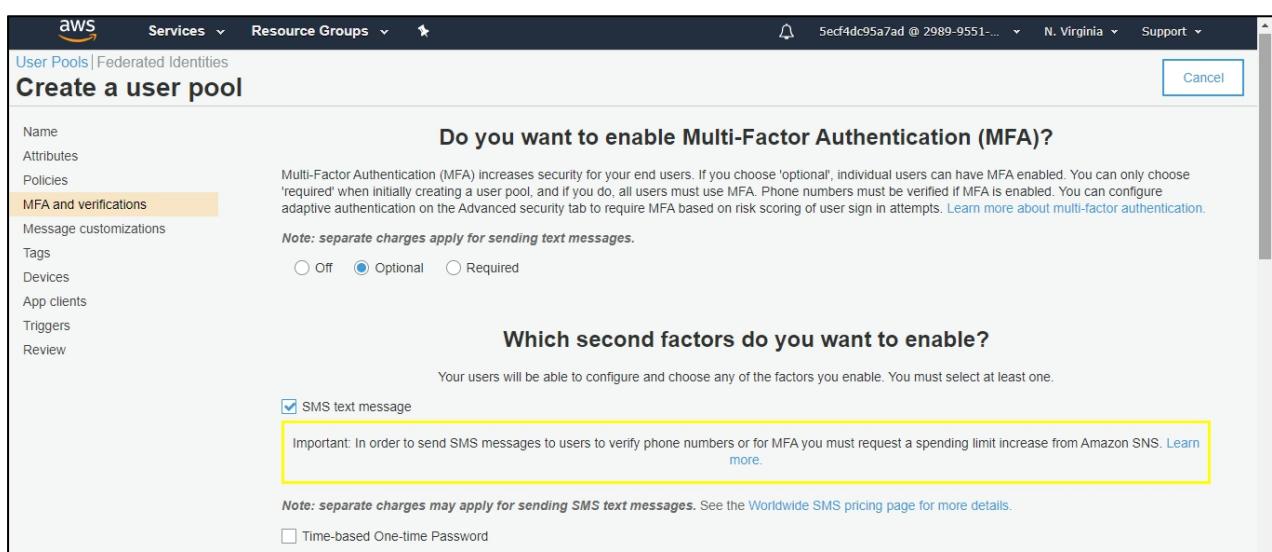


- By this point, you would have got an email to the mail address that you have specified. Open the mail and click on verify link. Make sure that your status change to **Verified** on SES home page.



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.

How will a user be able to recover their account?

When a user forgets their password, they can have a code sent to their verified email or verified phone to recover their account. You can choose the preferred way to send codes below. We recommend not allowing phone to be used for both password resets and multi-factor authentication (MFA). [Learn more](#).

(Recommended) Email if available, otherwise phone, but don't allow a user to reset their password via phone if they are also using it for MFA
 Phone if available, otherwise email, but don't allow a user to reset their password via phone if they are also using it for MFA
 Email only
 Phone only, but don't allow a user to reset their password via phone if they are also using it for MFA
 (Not Recommended) Phone if available, otherwise email, and do allow a user to reset their password via phone if they are also using it for MFA.
 None – users will have to contact an administrator to reset their passwords

Which attributes do you want to verify?

Verification requires users to retrieve a code from their email or phone to confirm ownership. Verification of a phone or email is necessary to automatically confirm users and enable recovery from forgotten passwords. [Learn more about email and phone verification](#).

Email Phone number Email or phone number No verification

- 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**.

You must provide a role to allow Amazon Cognito to send SMS messages

Amazon Cognito needs your permission to send SMS messages to your users on your behalf. [Learn more about IAM roles](#).

New role name
arn:aws:iam::298995513068:role/service-role/pract1-SMS-Role

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.

Security Management in AWS

Name
Attributes
Policies
MFA and verifications
Message customizations
Tags
Devices
App clients
Triggers
Review

Do you want to customize your email address?

You can send emails from an SES verified identity. Learn more about SES verified identities and domains.

SES Region *
US East (Virginia)

FROM email address ARN *
Default

You must verify your email address with Amazon SES before you can select it. Verify an SES identity.

FROM email address
xxxxxxxxxxxx@yyyyyy.co

REPLY-TO email address

Do you want to send emails through your Amazon SES Configuration?

Select Yes if you require higher daily email limits otherwise select No. Learn more about Cognito daily email limits. If you choose Yes, Cognito will send emails through your Amazon SES configuration. Refer to this documentation for additional steps.

Yes - Use Amazon SES
*Requires FROM email address ARN

No - Use Cognito (Default)

- 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**.

User Pools | Federated Identities
pract1

General settings
Users and groups
Attributes
Policies
MFA and verifications
Advanced security
Message customizations
Tags
Devices
App clients
Triggers
Analytics
App integration
Domain name
UI customization
Resource servers
Federation
Identity providers
Attribute mapping

What domain would you like to use?

Type a domain prefix to use for the sign-up and sign-in pages that are hosted by Amazon Cognito. The prefix must be unique across the selected AWS Region. Domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes.

This domain is available.

Amazon Cognito domain
Prefixed domain names can only contain lower-case letters, numbers, and hyphens. Learn more about domain prefixes.
Domain prefix
https://pract1 .auth.us-east-1.amazoncognito.com

Check availability

Your own domain
This domain name needs to have an associated certificate in AWS Certificate Manager (ACM). You also need the ability to add an alias record to the domain's hosted zone after it's associated with this user pool. Learn more about using your own domain.
Use your domain

Cancel **Save changes**

Go to summary Customize UI

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

Security Management in AWS

- 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

Advanced security
Message customizations
Tags
Devices
App clients
Triggers
Analytics
App integration
App client settings
Domain name
UI customization
Resource servers
Federation
Identity providers
Attribute mapping

App client MyAppClient
ID dgc0rm1vet12omum877hevn6

Enabled Identity Providers Select all
 Cognito User Pool

Sign in and sign out URLs
Enter your callback URLs below that you will include in your sign in and sign out requests. Each field can contain multiple URLs by entering a comma after each URL.
Callback URL(s) https://my-user-pool.auth.us-east-1.amazoncognito.com
Sign out URL(s) https://my-user-pool.auth.us-east-1.amazoncognito.com/login?response_type=token&client_id=a1b2c3d4e5f6g7h8i9j0k1l2m3&redirect_uri=https://m...

OAuth 2.0
Select the OAuth flows and scopes enabled for this app. [Learn more about flows and scopes.](#)

Allowed OAuth Flows
 Authorization code grant Implicit grant Client credentials

Allowed OAuth Scopes
 phone email openid aws.cognito.signin.user.admin profile

- 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 on “**Save Changes**” at the end of the page.

What customizations do you want to make to the end-user experience?

You can customize the experience to match each of your app's style and branding. If no customizations are made, all default values will be used. [Learn more about UI customization.](#)

App client to customize

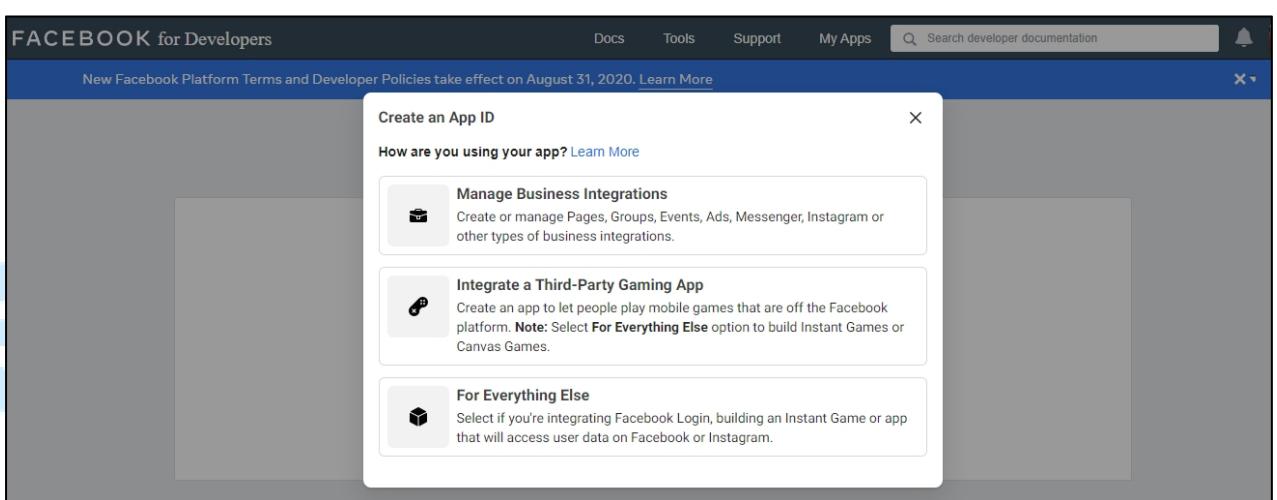
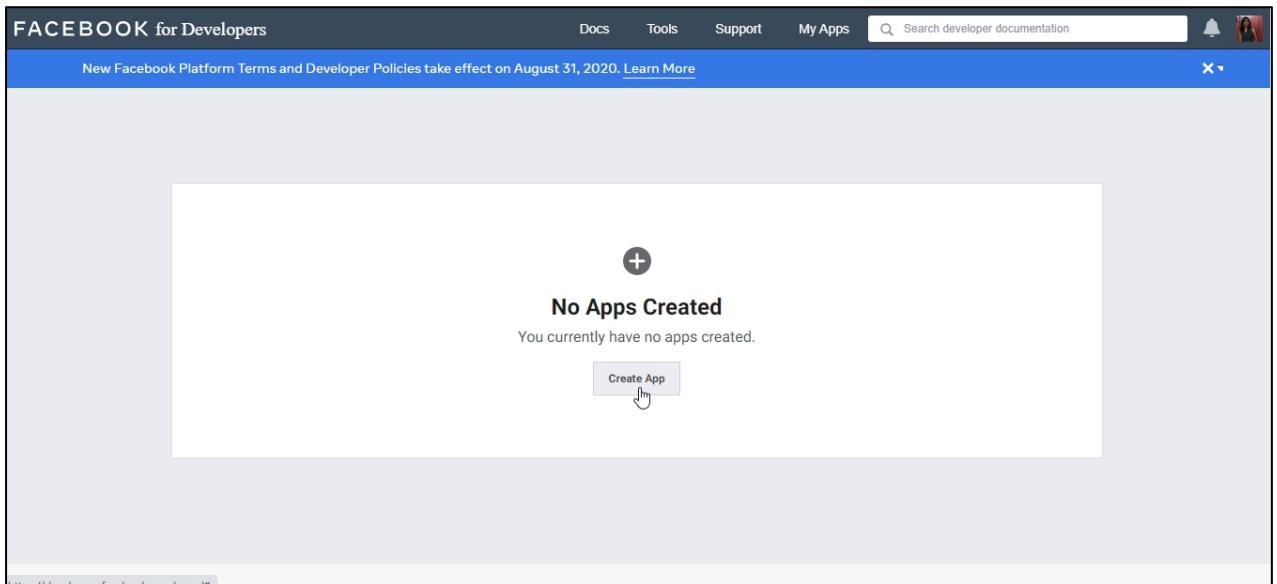
Defaults for all clients without individual settings

Logo (optional)

Choose a file or drag a file here
Up to 100 KB in size.

- 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**”.

Security Management in AWS



- 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)

Create an App ID

App Display Name
This is the app name associated with your app ID.

pract2

App Contact Email
This email address is used to contact you about potential policy violations, app restrictions or steps to recover the app if it's been deleted or compromised.

[REDACTED]@gmail.com

Do you have a Business Manager account? · Optional
Your app may need to be connected to a verified Business Manager account to access different levels of data. If you do not have a Business Manager account, you can create one later in the process.

No Business Manager Account selected

Cancel By proceeding, you agree to the Facebook Platform Policies **Create App ID**

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

FACEBOOK for Developers

pract2 App ID: [REDACTED] In development

New Facebook Platform Terms and Developer Policies take effect on August 31, 2020. [Learn More](#) X

Dashboard

Settings

Products +

Add a Product

Facebook Login The world's number one social login product. Read Docs Set Up	Audience Network Monetize your mobile app or website with native ads from 3 million Facebook advertisers. Read Docs Set Up	Analytics Understand how people engage with your business across apps, devices, platforms and websites. Read Docs Set Up
Messenger Customize the way you interact with people on Messenger. Read Docs Set Up	Webhooks Subscribe to changes and receive updates in real time without calling the API! Read Docs Set Up	Instant Games Create a cross platform HTML5 game hosted on Facebook.

- 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.

Security Management in AWS

The screenshot shows the 'Client OAuth Settings' section of the AWS Cognito User Pools settings. It includes configuration for Client OAuth Login, Web OAuth Login, Enforce HTTPS, Force Web OAuth Reauthentication, Use Strict Mode for Redirect URIs, Valid OAuth Redirect URIs (with a text input field containing 'https://pract1.auth.us-east-1.amazoncognito.com/oauth2/idpresponse'), and Login from Devices. At the bottom are 'Discard' and 'Save Changes' buttons.

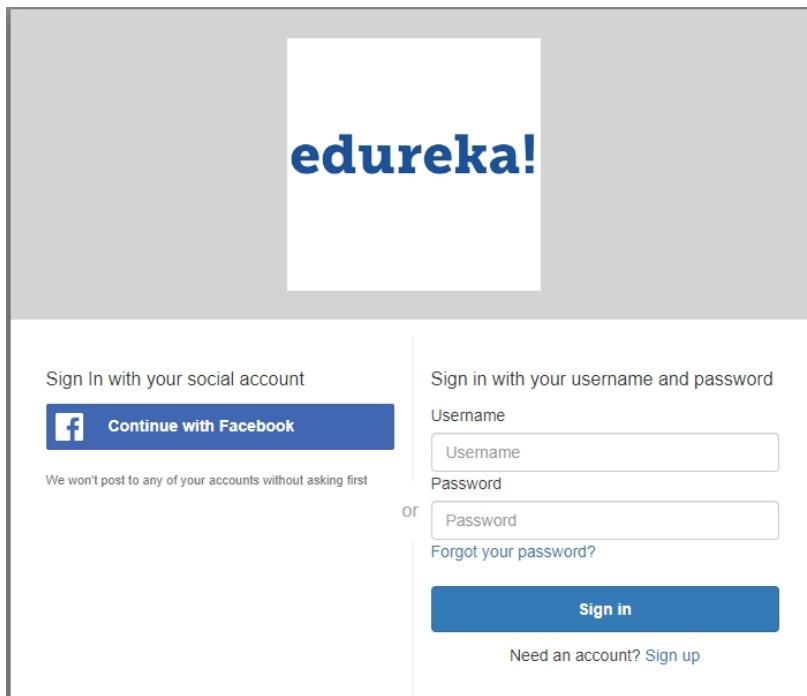
- Go to Settings and under that **Basic**. Observe that at right side of the page display App ID and App secret ID are available.

The screenshot shows the 'Basic' settings page for a Facebook app named 'pract2'. It displays the App ID (240681326975560), App Secret (redacted), Display Name (pract2), Namespace, Contact Email (choudaryarchu@gmail.com), Privacy Policy URL, Terms of Service URL, App Domains, and App Icon. A note says 'Find out more information about app categories here'. At the bottom are 'Discard' and 'Save Changes' buttons.

- 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**.

The screenshot shows the 'Hosted UI' configuration page. It has a 'Cancel' and 'Save changes' button at the top. Below is a section titled 'Hosted UI' with a note: 'The hosted UI provides an OAuth 2.0 authorization server with built-in webpages that can be used to sign up and sign in users using the domain you created. Learn more about the hosted UI'. At the bottom is a 'Launch Hosted UI' button with a cursor icon pointing to it.

- 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---