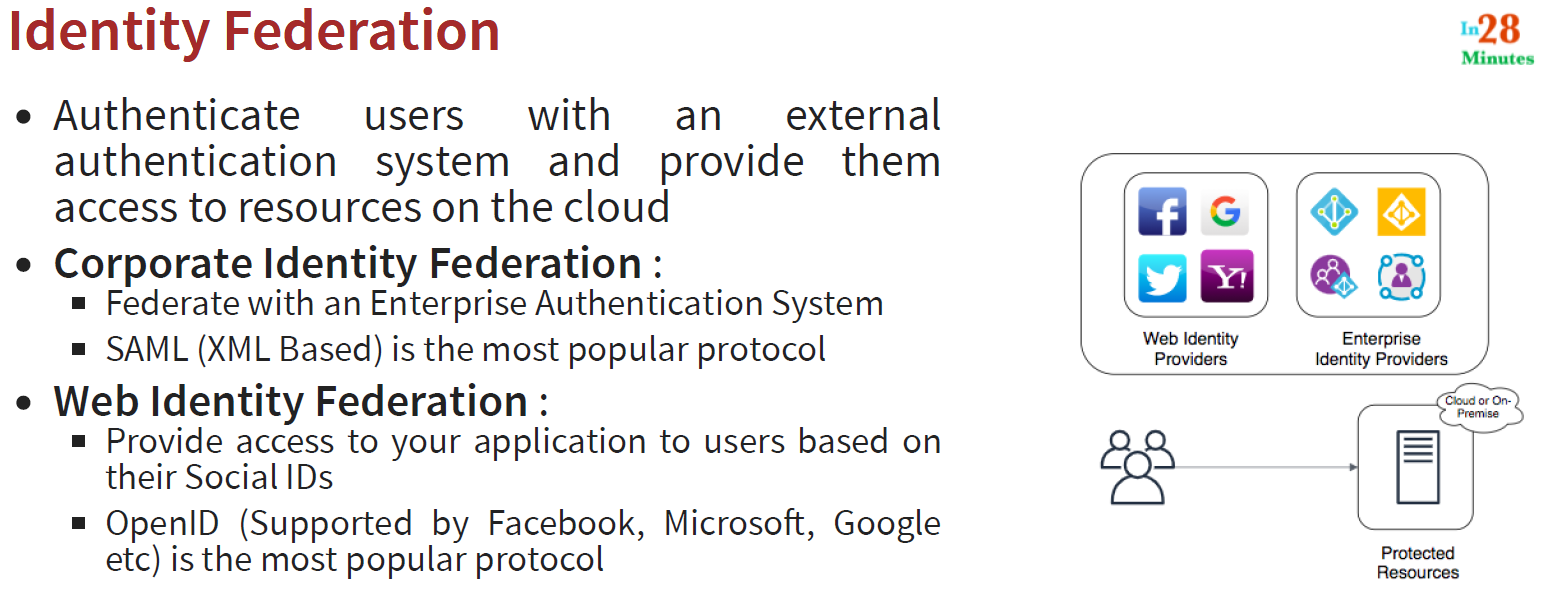
**Section-10 AMAZON Cognito:**

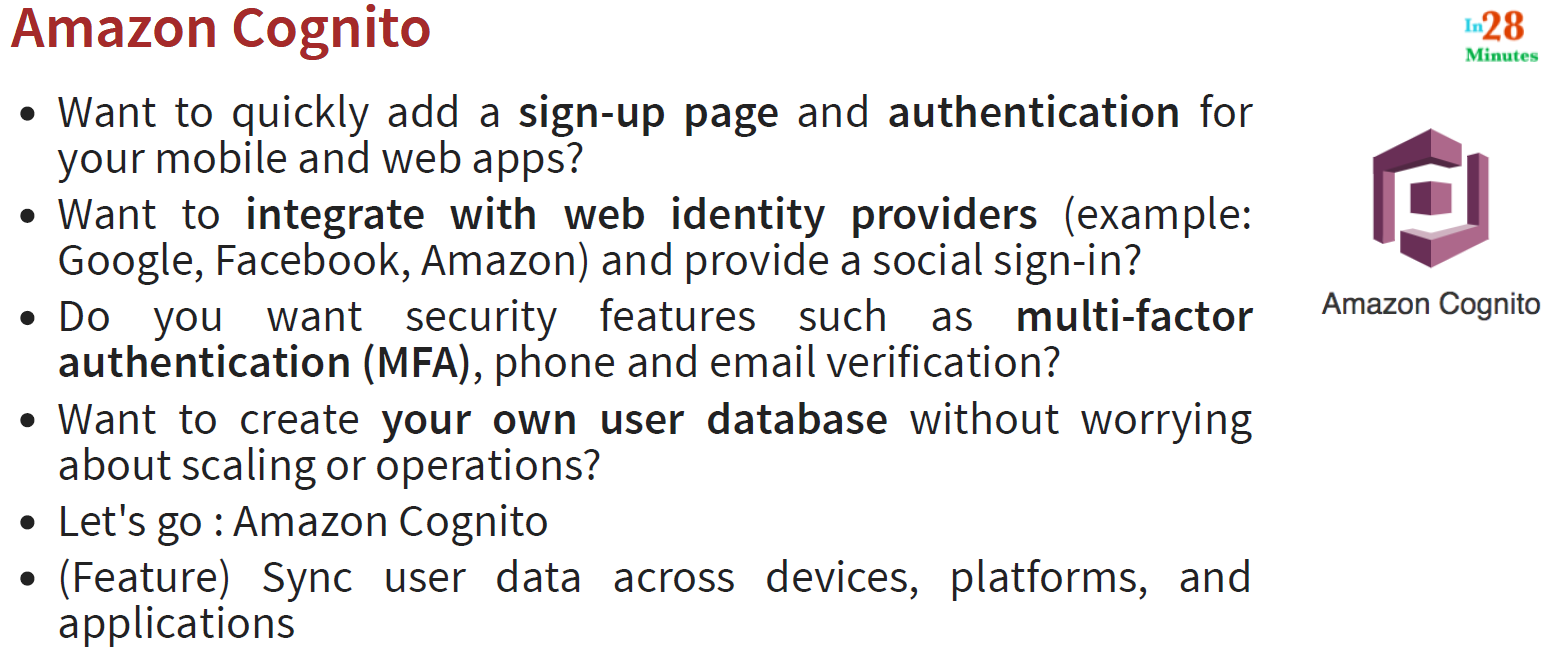
**107. Step 00 - 01 - Introduction to Identity Federation**

****

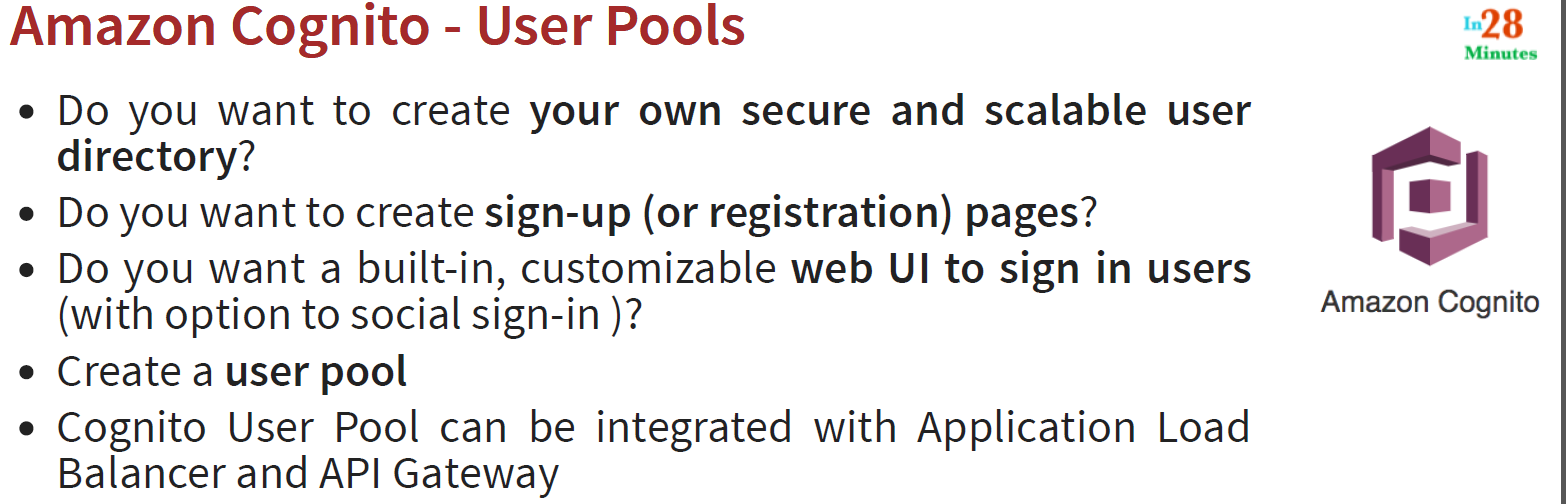
Identity federation is nothing but giving the access to some resources which are protected based on external authentication system. The authentication system can be a web identity provider or a enterprise identity providers.

**108. Step 00 - 02 - Introduction to Amazon Cognito**

1. It allows us to create our own user database
2. It provides the right page for sign up, sign in, password reset
3. It also integrate with a variety of web identity providers and enterprise identity provider



**109. Step 01 - Understanding Amazon Cognito User Pools**



**110. Step 02 - Understanding Amazon Cognito Identity Pools**



In last step we have talked about user pools, which is all about authentication i.e. creating your signup, sighIn pages, creating your own pool of users. And Identity pools all about authorization. In other words,



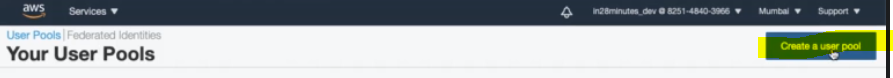
* We would connect our identity pool with Authentication (identity) providers. The Authentication provider could be
* Our own user pools (e.g. We are creating a Cognito user pool)
* OR it could be social IDs like Amazon, APPLE, Facebook, Google Twitter
* OR It could be any Open ID Connect provider
* OR we can also integrate with SAML identity provider (SAML 2.0)
* The good thing is we can configure multiple authentication (identity) providers for each identity pool. So for a single identity pool and for single application authentication we can any of the above identity providers

**111. Step 03 - 01 - Playing with Amazon Cognito User Pools**

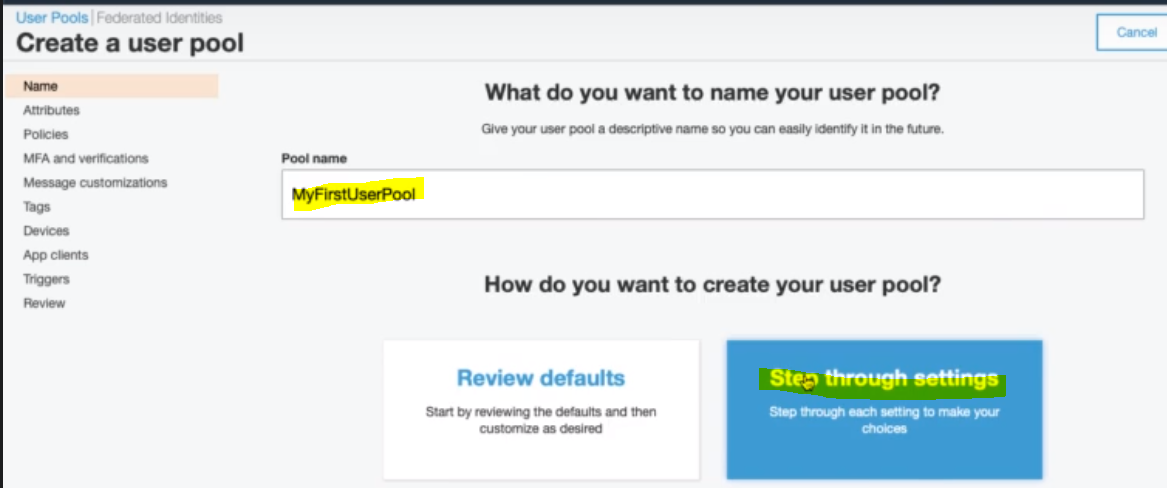
1- Go to ASW Management Console and search for Amazon Cognito

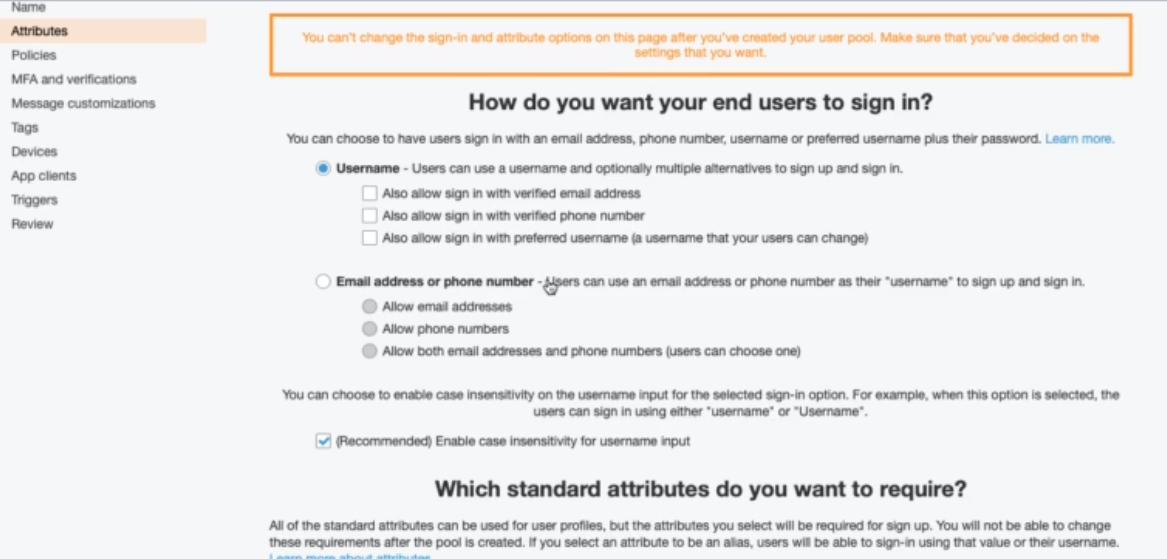


2- Click on Manage User Pools

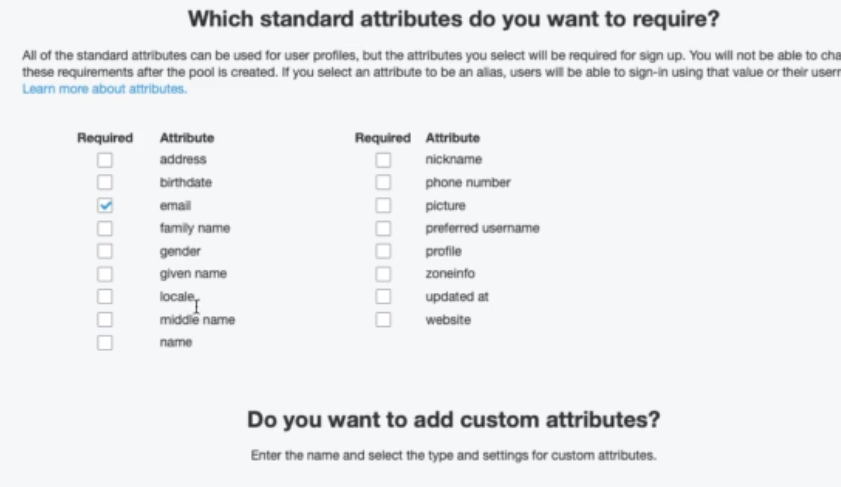


3-: Click on Create a user pool: > Give the Pool name > Click on Step through settings



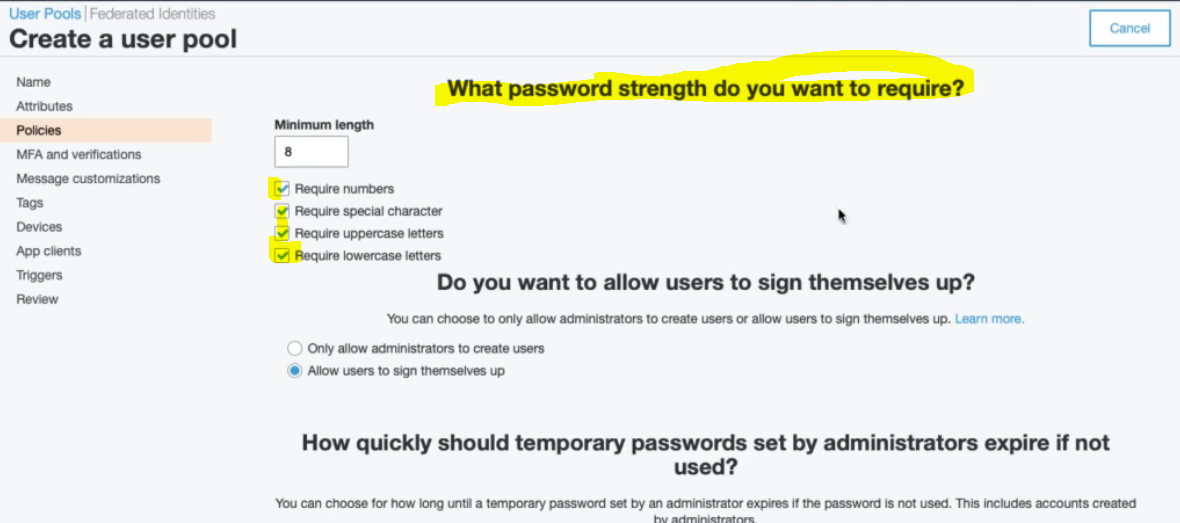


So as here we can see that we can create the users with different type of sing in options e.g. with email, phone number. If we scroll down then it asks to add standard attributes with the user sign in: e.g. address, birthdate, email etc.

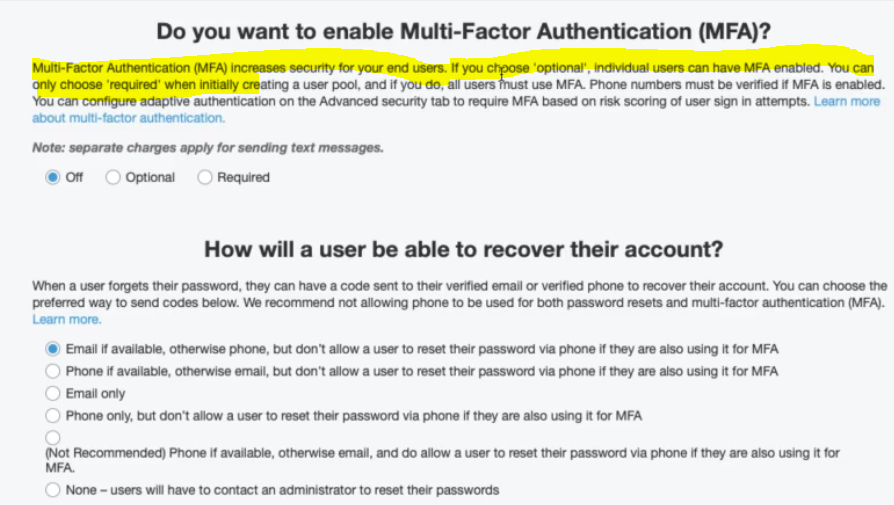


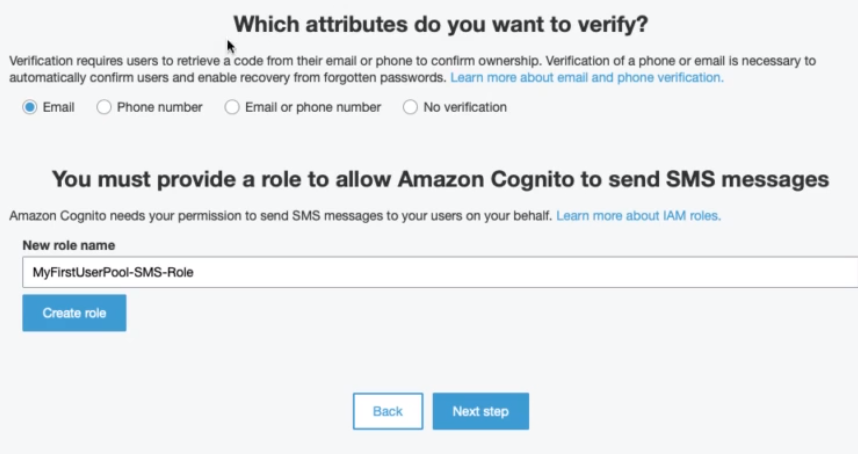
Click Next:

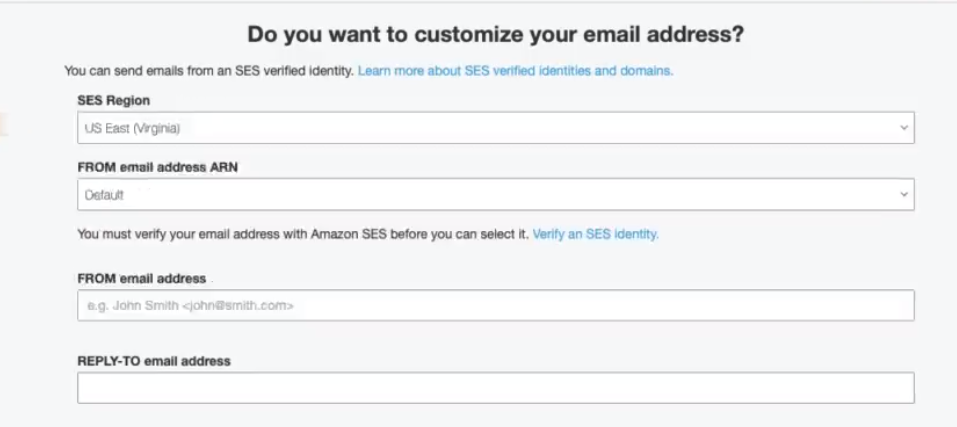
So in the first step we have gathered the info required to sign in user and now in the next step we will setup password with require?

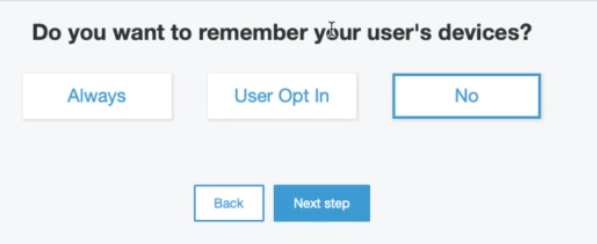


Click Next:

In this step it is saying how we can verify the security, like using email or sms etc. If we go further then we can configure to recover the account using one of the option given below.



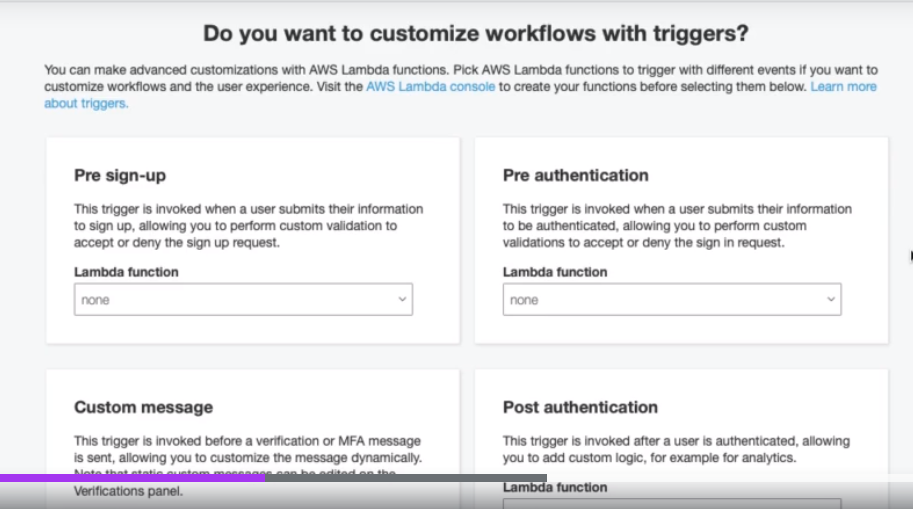




We can choose the option to remember your user’s devices?

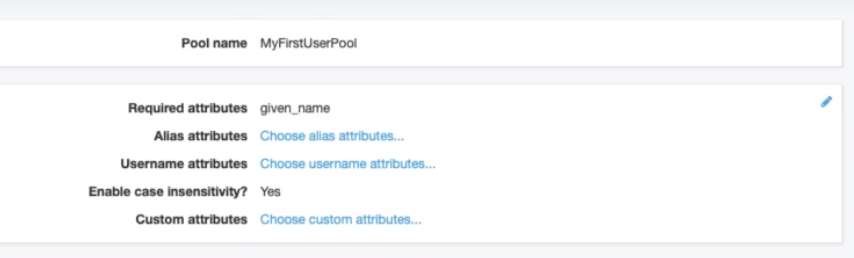


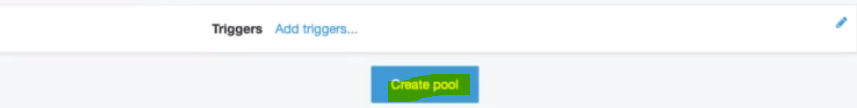
Here we can add the client application for which user pool would have the access. Click next step



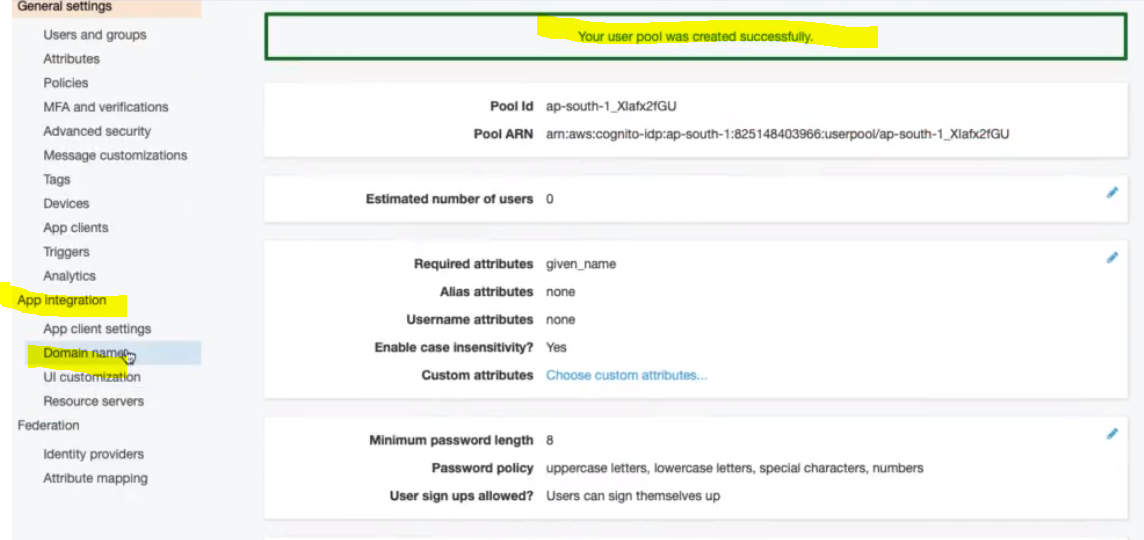
Now here we can configure the lambda function for each steps like when user will sign-up, authentication, password reset etc and accordingly lambda function will be triggered.

Finally : Review and Create pool

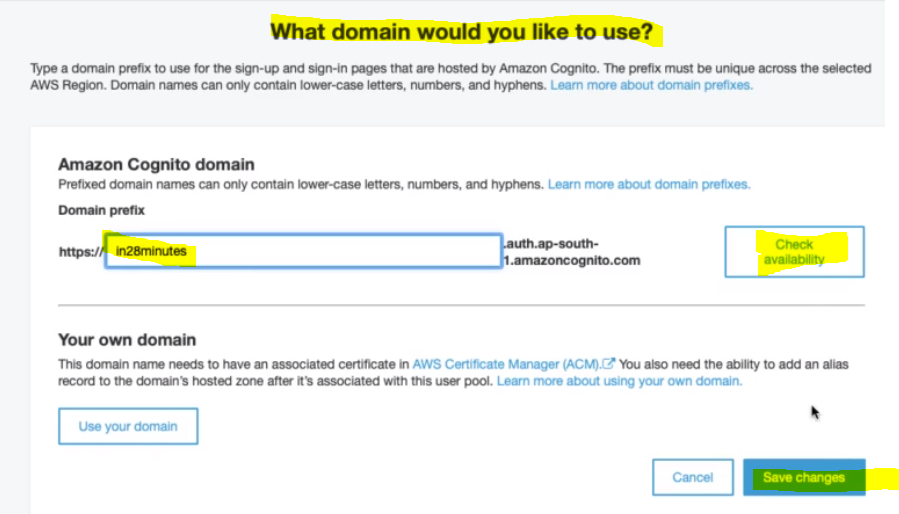




Click On Create pool:

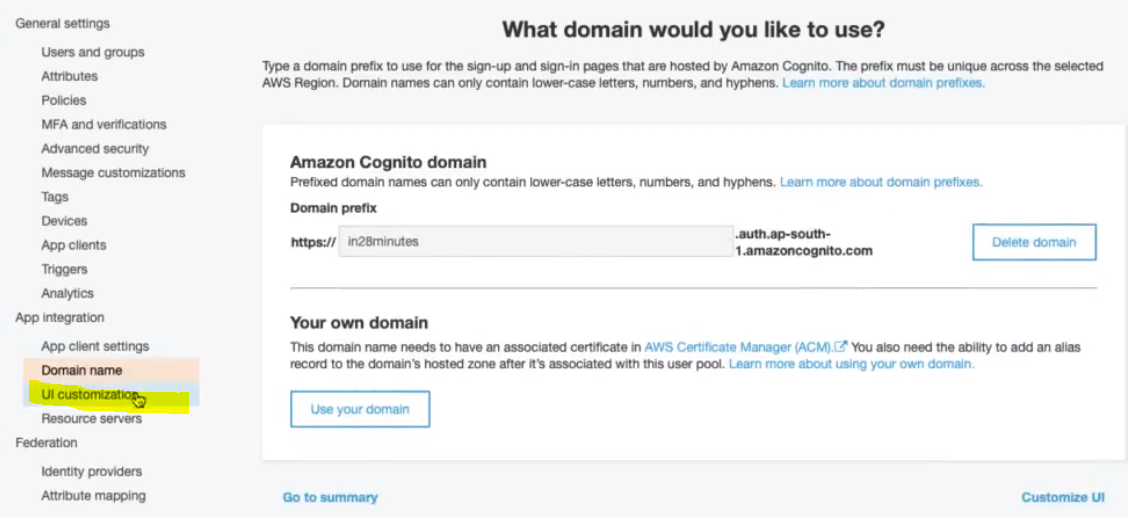


Now go to Domain Name present inside the App Integration:

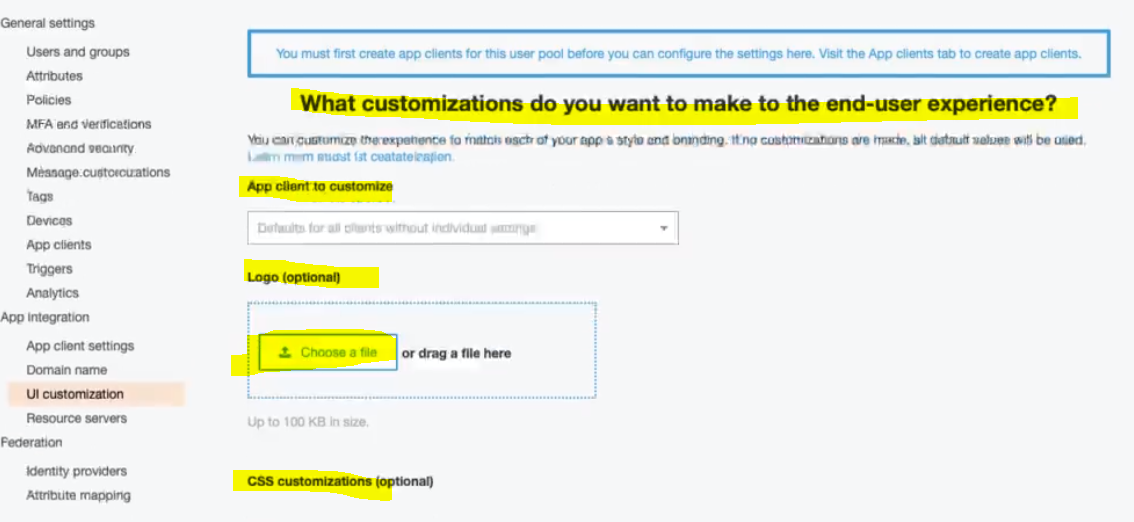


Here we can provide the domain based on choice and its availability > Save changes

After configuring the above domain name we can go for UI Customization.

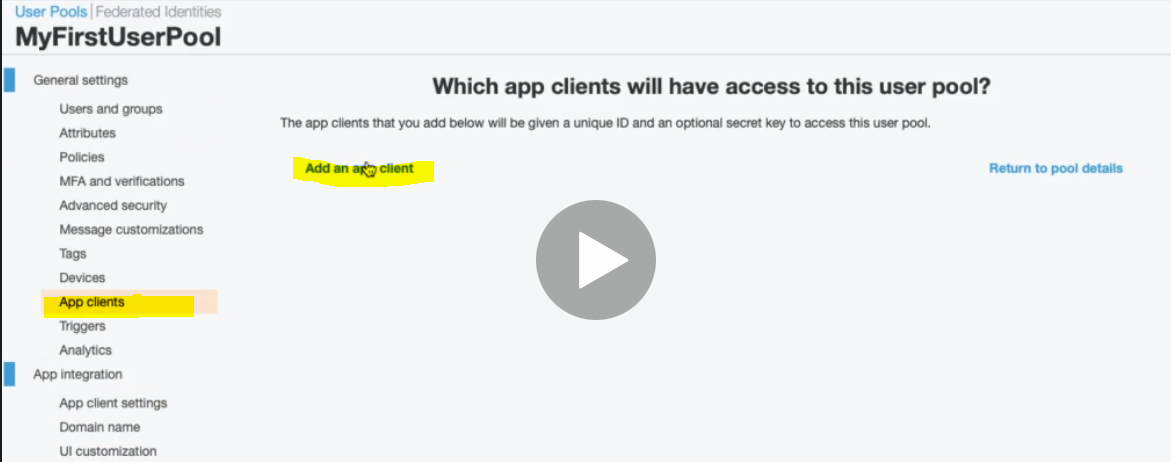


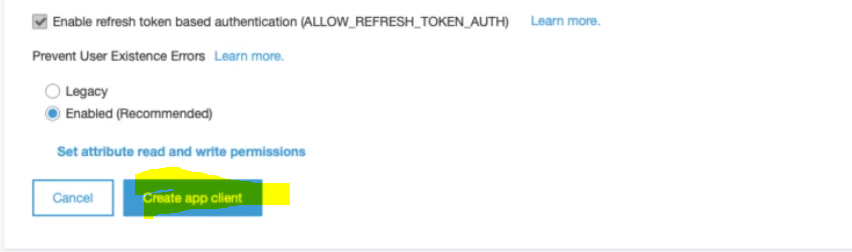
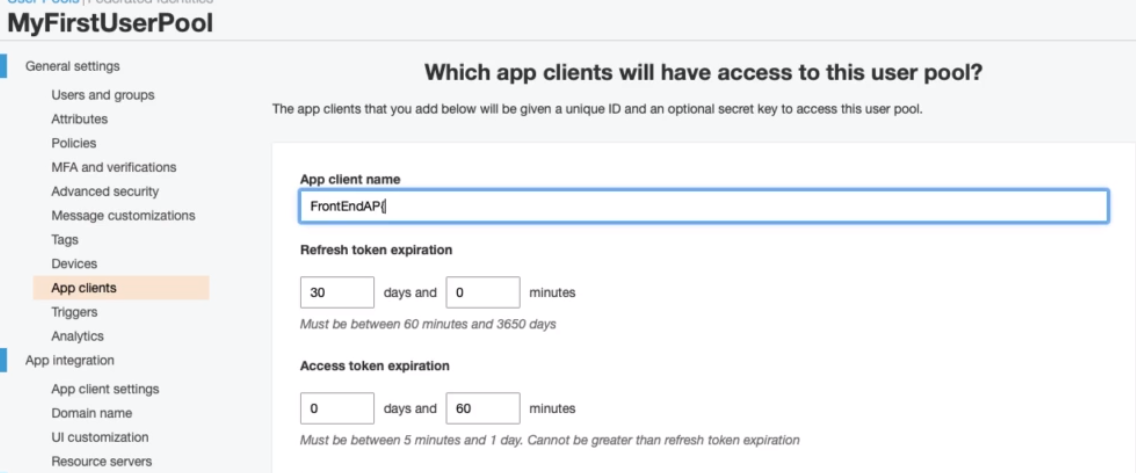
Click on UI Customizations:

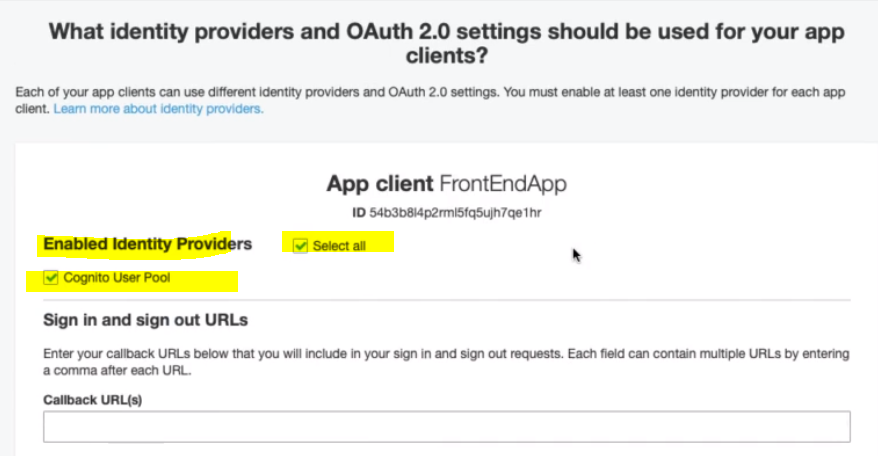


So as above we can see that we can customize the logo, CSS etc of the application.

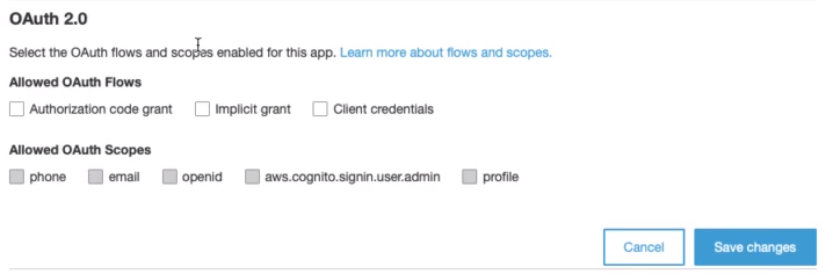
Once we create the Domain Name and Customized UI, let’s create the App Client:



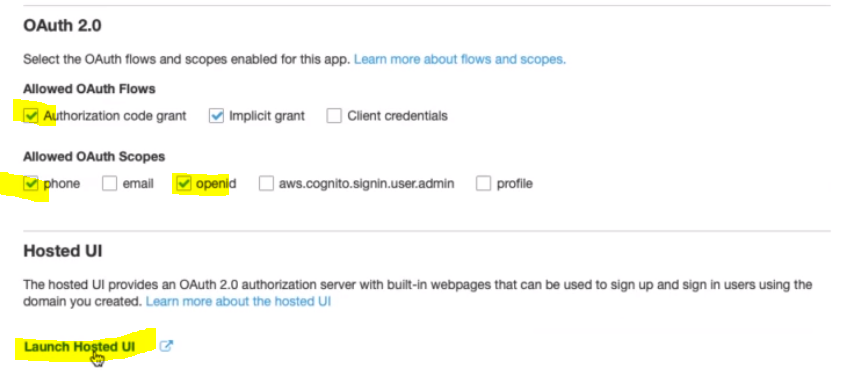




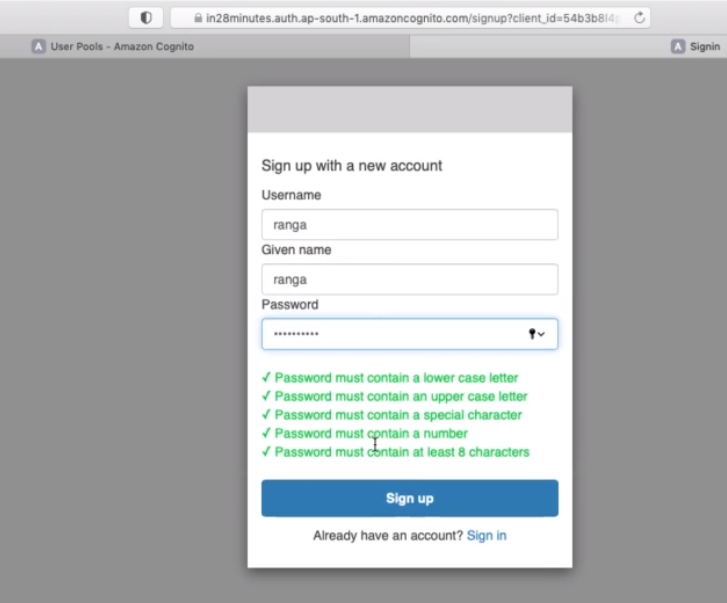
Callback URL cannot empty So let’s give the callback URL(s) <http://localhost>



We can enable OAuth 2.0 also > Save Changes:

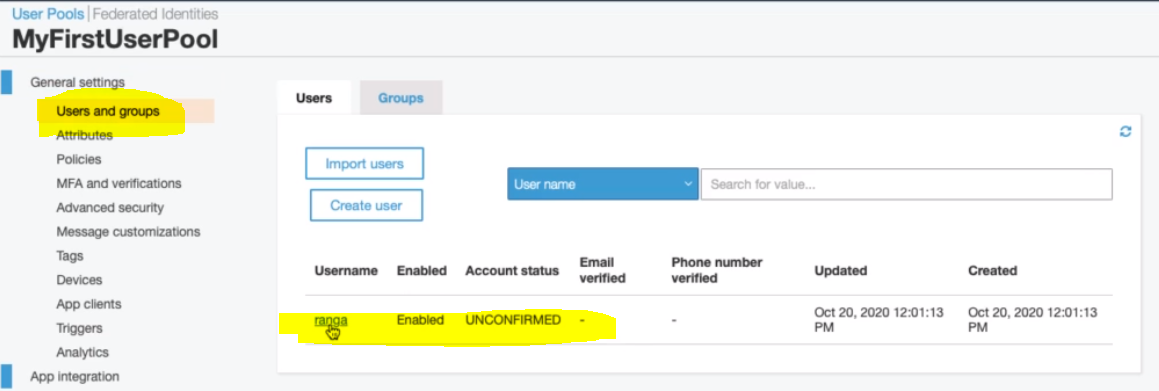


Now finally we can launch the Hosted UI : Click Launch Hosted UI:

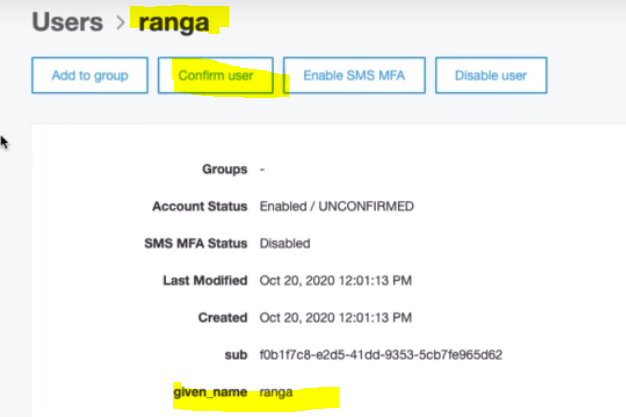


And now we will get the sign up page: Let’s provide the Username, name, password:

Click on sign Up button:



Now let’s go the Users and group and finally we will see the created user. Click on the username and confirm it:



So if we would have provided the email to confirm then it would be confirmed by email.

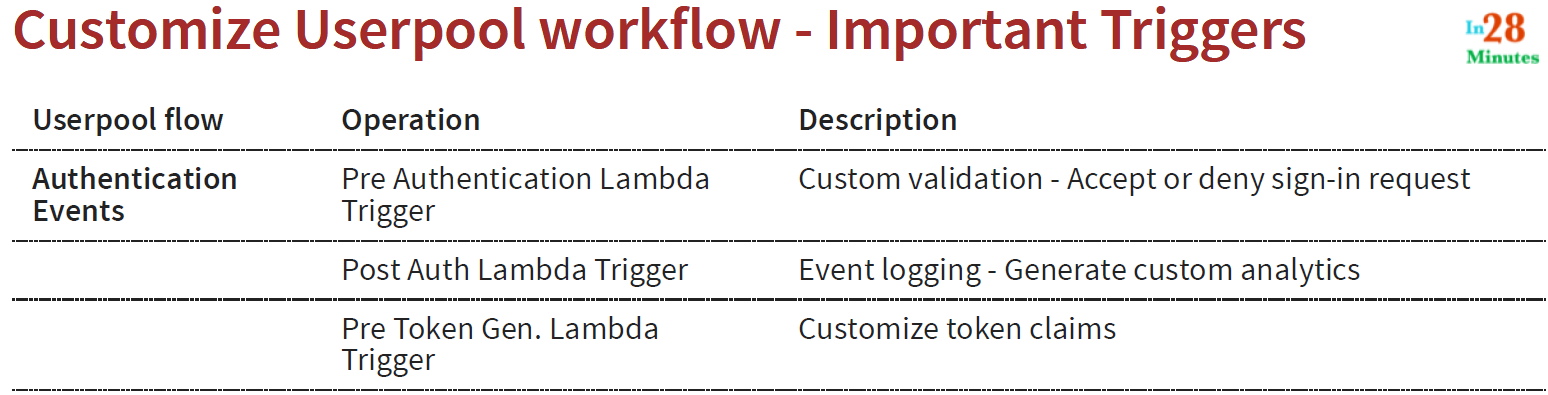
So in this way we can create the user pool. Now let’s go sign in with this created user.

|  |  |
| --- | --- |
|  | Once we sign in we will get a generated code which we can use to re-direct to our application by passing the code. The application can this code and authenticate the user and provide the access of the application.  The important thing to remember here is we can configure the below list as the part of User pool   1. We can create our own set of users 2. We can create our own UI 3. We can customize our sign in and sign up pages 4. We can customize the logo for the sign up and sign in pages   The above point is important for exam point of view. |

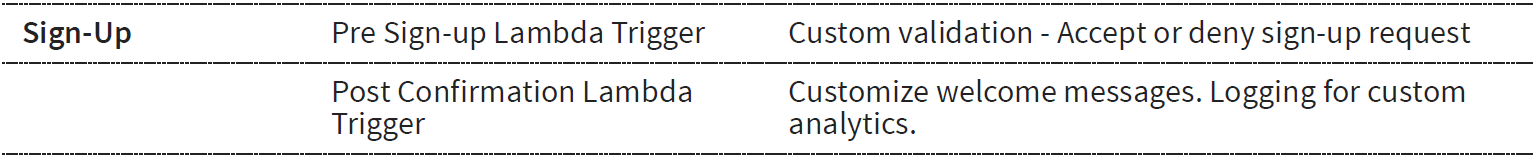
**112. Step 03 - 02 - Customize UserPool Workflow With Triggers**

When we are creating Cognito User Pool then there are lot of places where actually trigger events (we can create lambda function and trigger those lambda function on specific event) in the user pool workflow.

Let’s looks some of the important triggers that we can trigger, let’s look some specific flow, what operation we can trigger and little bit description.

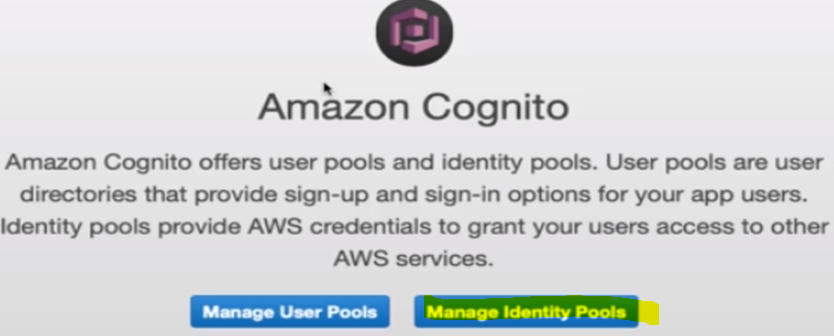


1. When we want to do some custom validation(Accept or deny sign-in request) just before the user sign-in or just before the user is authenticated then we can trigger [Pre Authentication Lambda Trigger]
2. Once the user is authenticated if we want to do our own event logging – Generate custom analytics then in this case we can trigger Post Auth Lambda Trigger (Lambda Function)



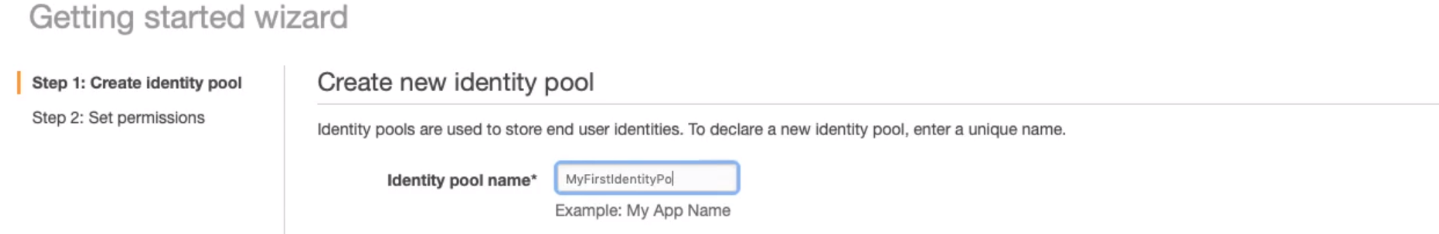


**113. Step 04 - Exploring Amazon Cognito Identity Pools**

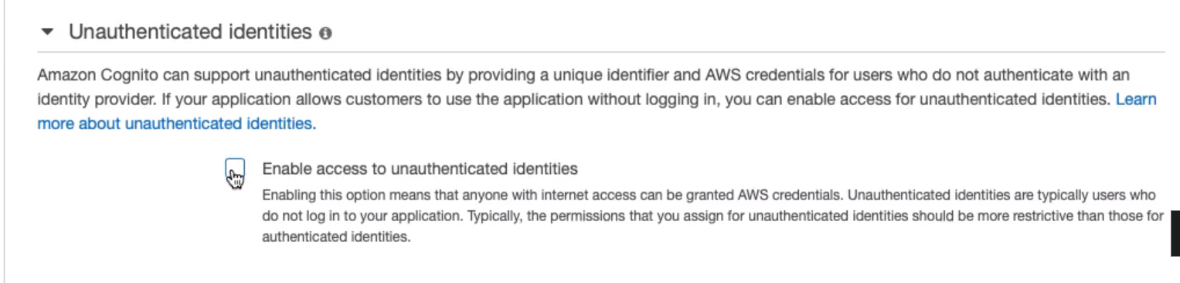


So far we have created User pools using Cognito. Now let’s see the step for Managing Identity Pools.

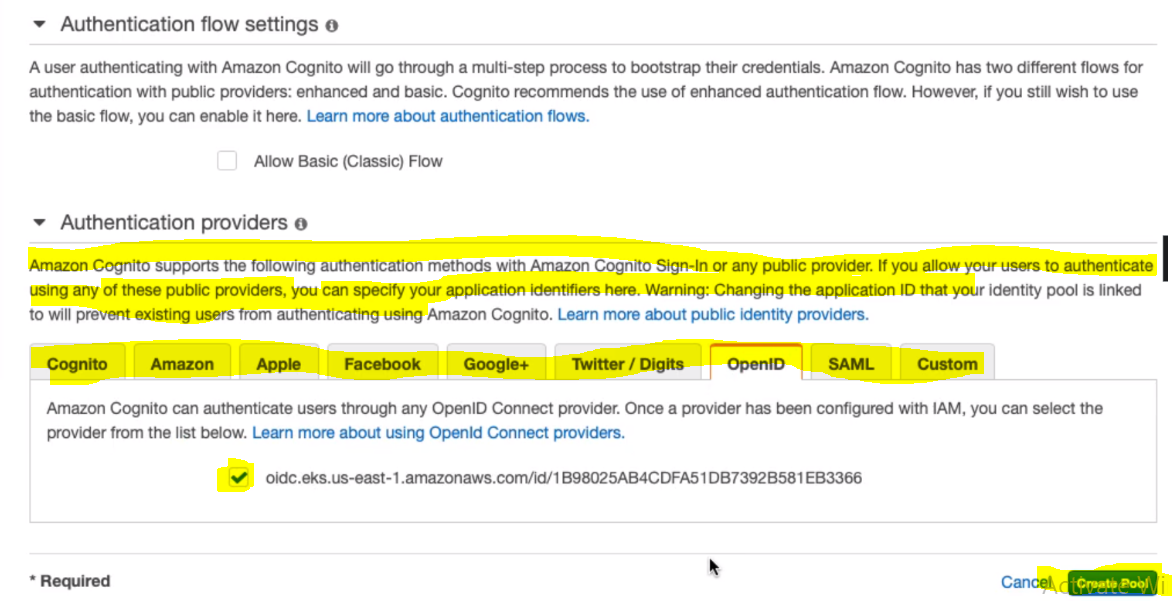
Click on Manage Identity Pools.



**Provide the Name of the Identity Pool.**

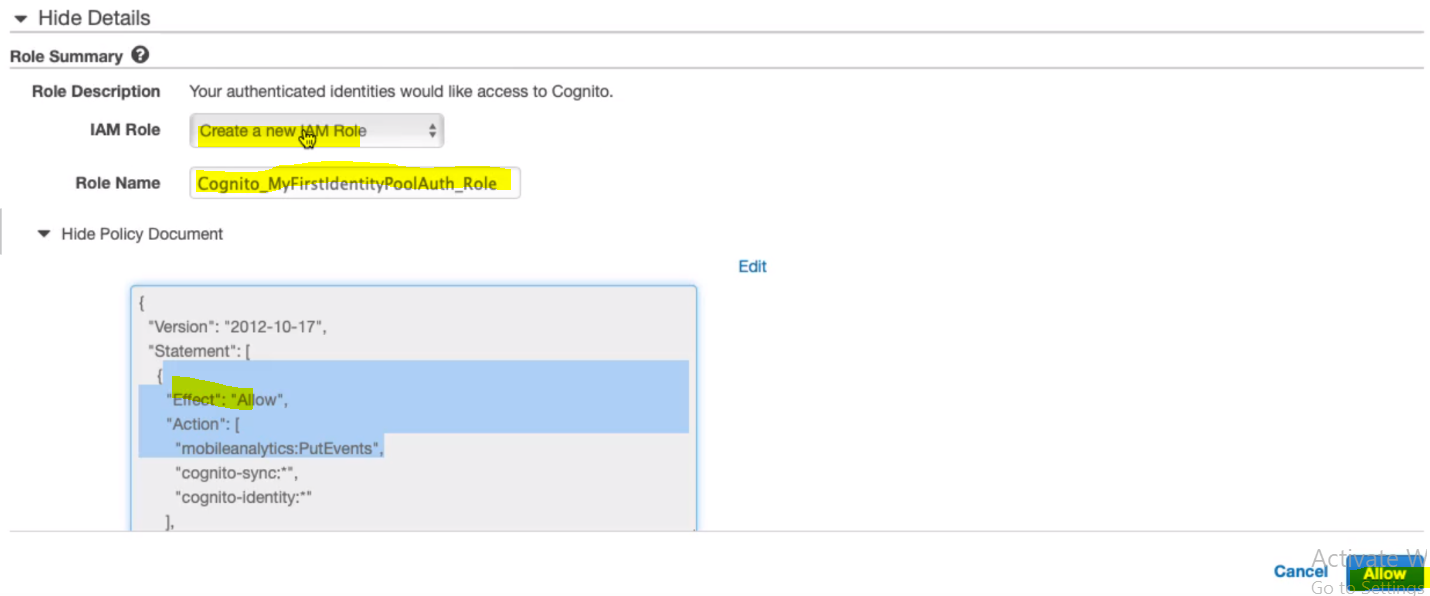


**Check for enabling assess to unauthenticated identities.**

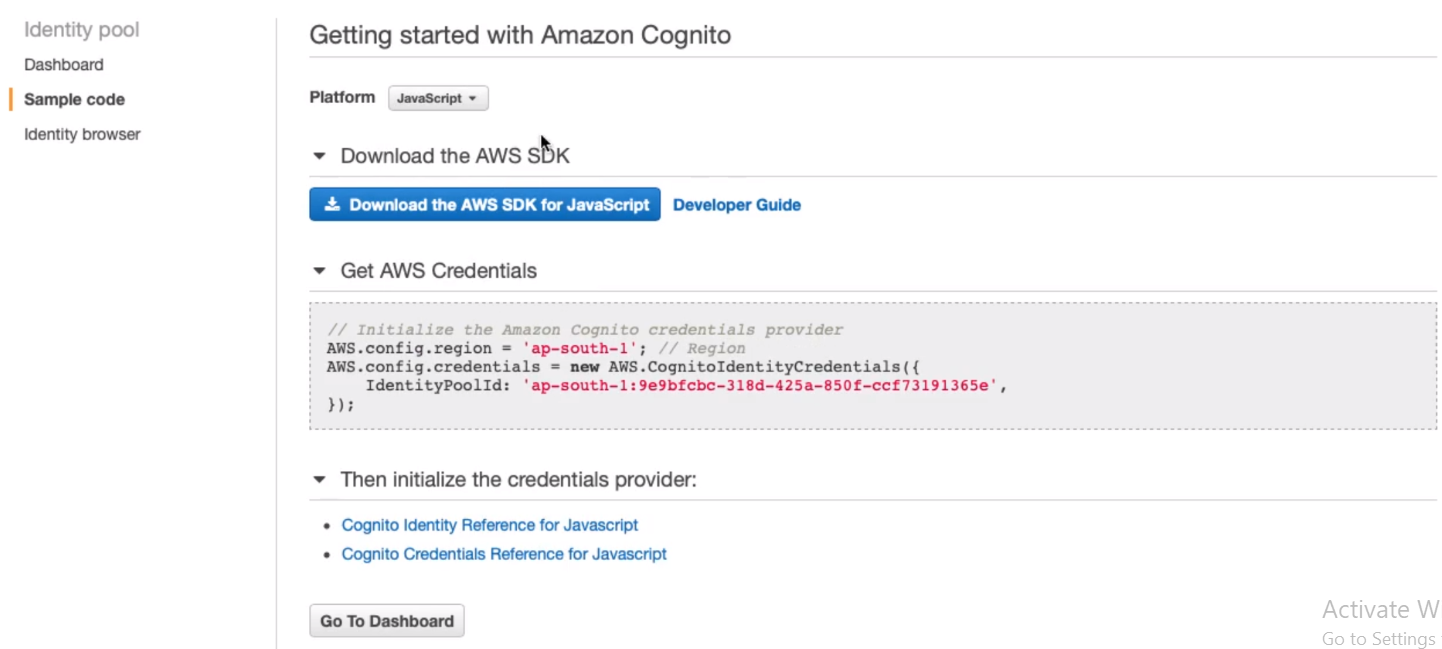


So here we can see that Amazon Cognito supports the above public providers for authentication. Click on [**Create Pool**]

Once create the pool then we can decide what kind of access you want to provide to AWS resources.

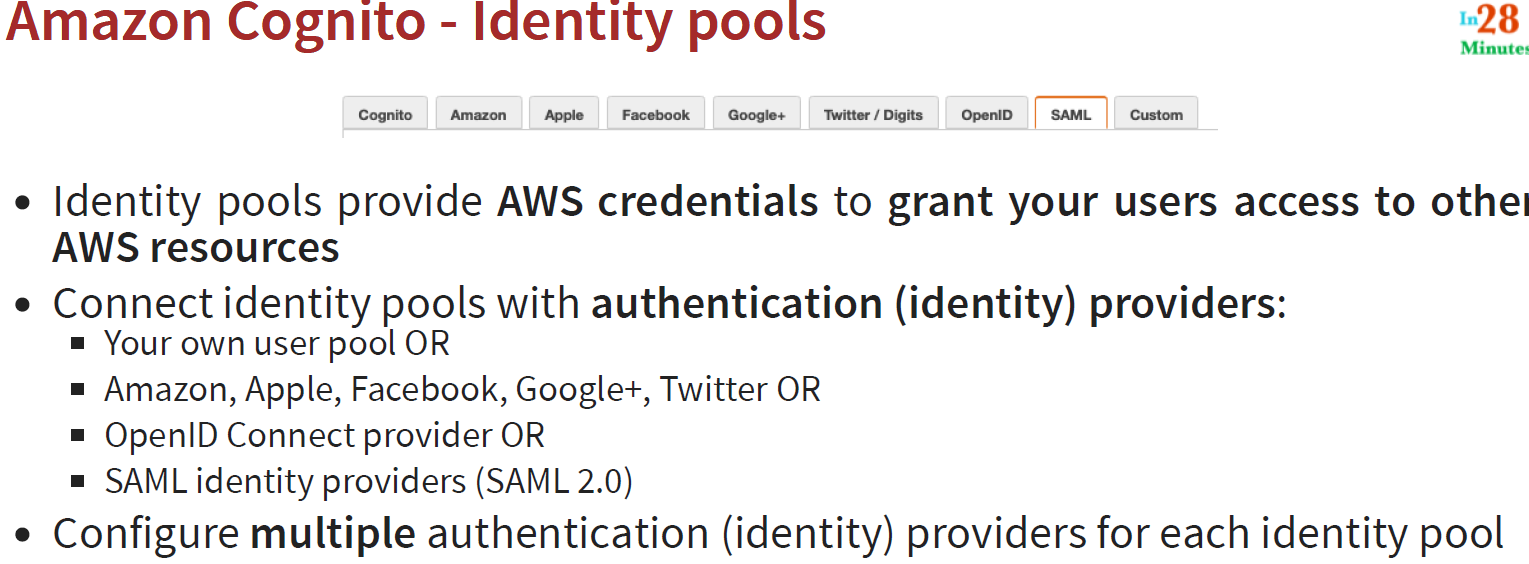


We can edit the access in the given Policy Document. Finally create Allow.



**Here we can choose the Platform and provide the credential to AWS resources.**

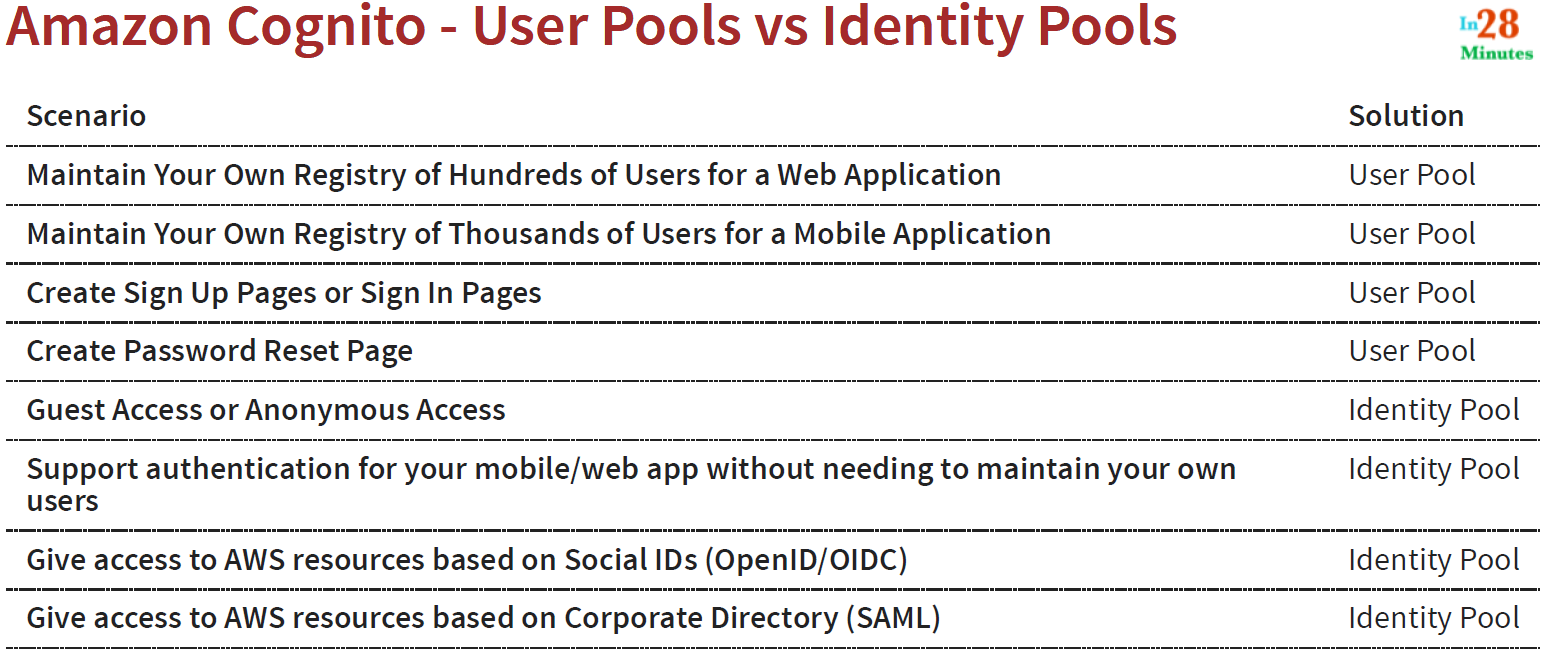
**So in this step we have seen AWS Identity Pool, which provides the blow points.**



**114. Step 05 - Exploring Amazon Cognito Use Cases - Identity vs User Pools**

In this step let’s see the different scenario and find out where we can see the User pools and Identity pools.

Note: Just add one word “When we want to” in the beginning for every point.



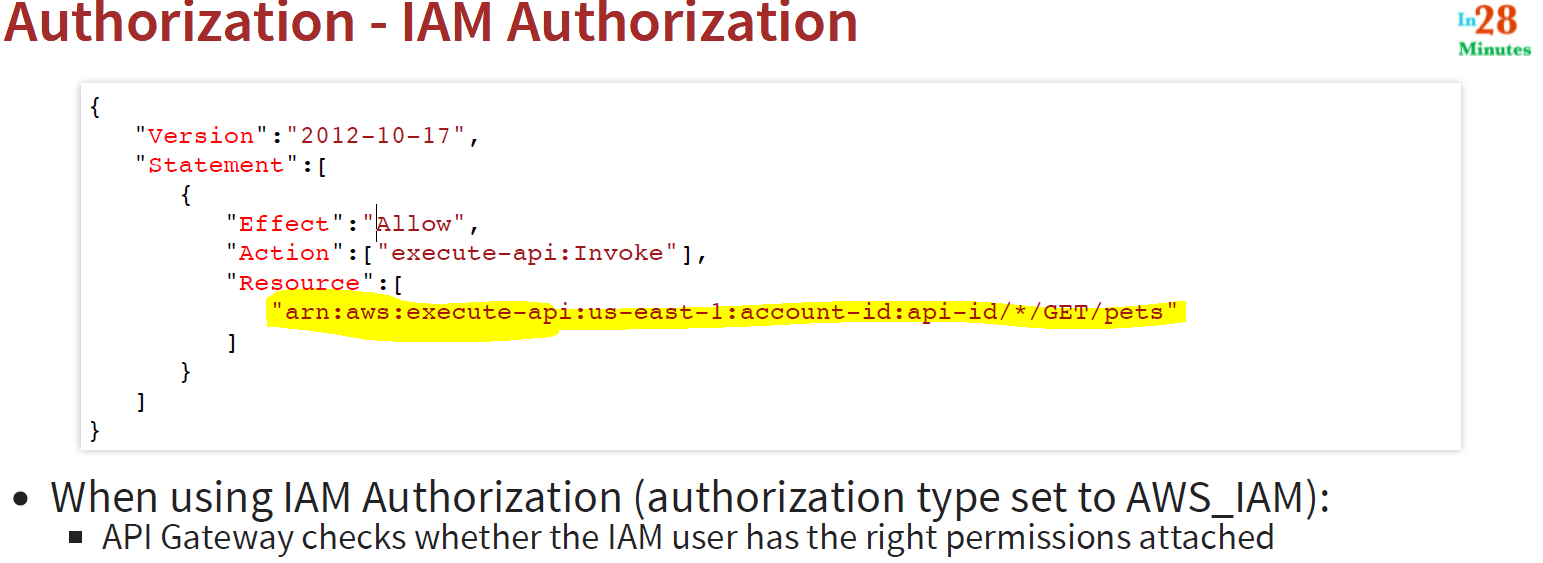
**115. Step 06 - Integrating Authorization with API Gateway**

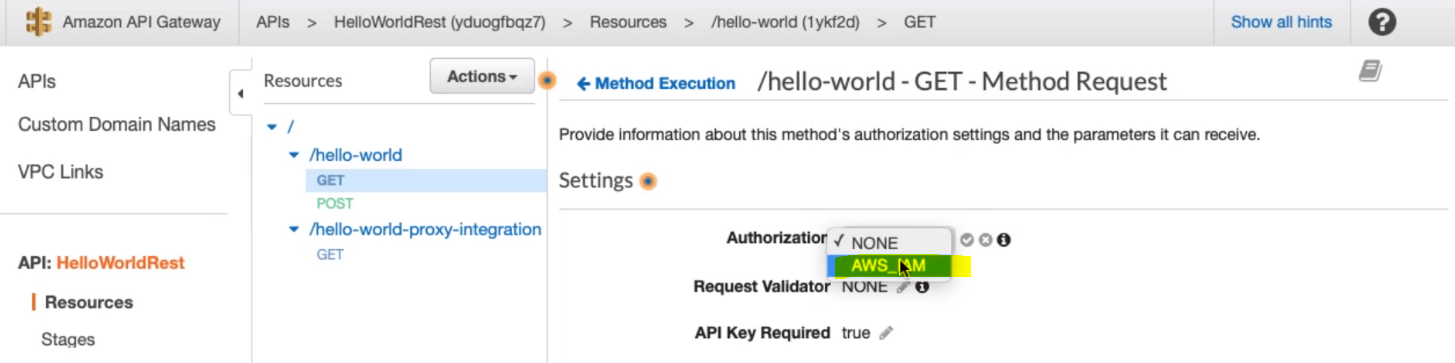
Here let’s discuss about the Authorization, how we integrate Authorization with API Gateway?

Ans: We have several options for integrating Authorization.

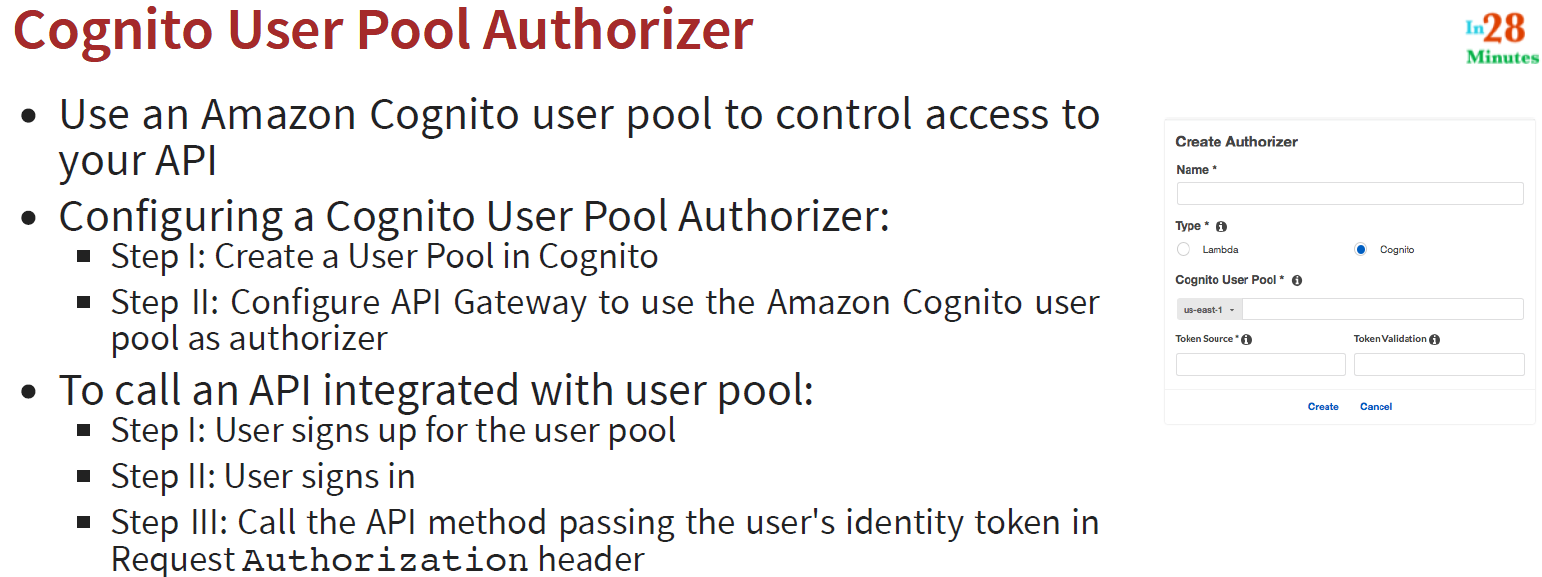
**Open** – When we want to have No authentication or authorization. Nothing to do here.

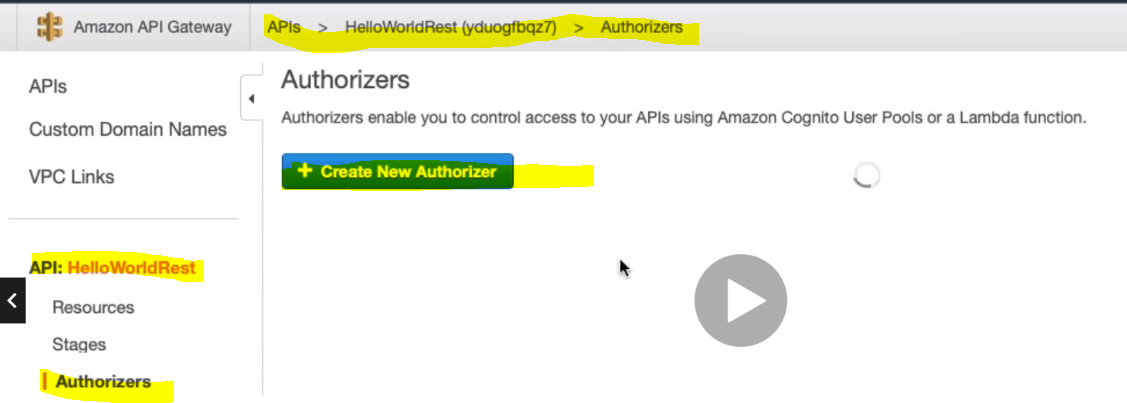
**IAM Permissions** - Use IAM Policies and AWS credentials to grant access. We can enable this using below

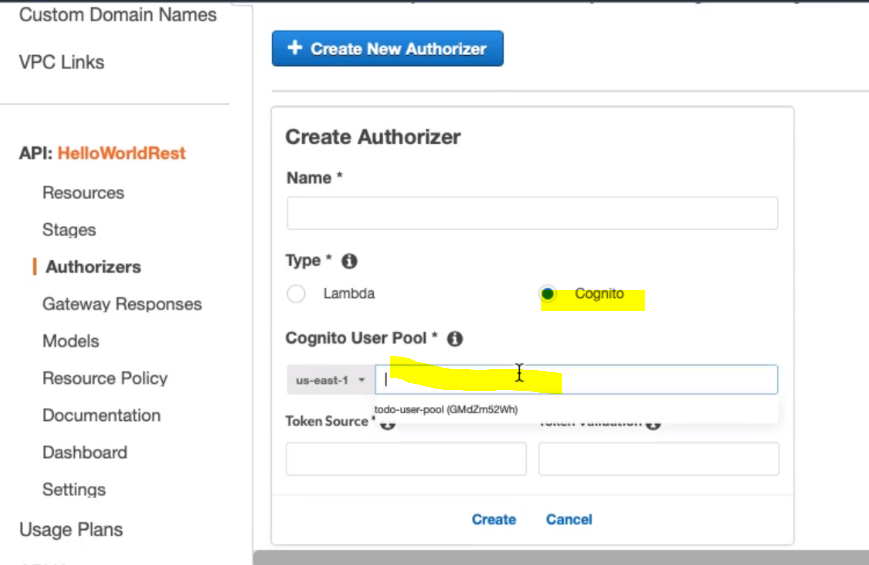




**Amazon Cognito authorizer** - Connect to Amazon Cognito User Pool (possible to use OAuth authorization)

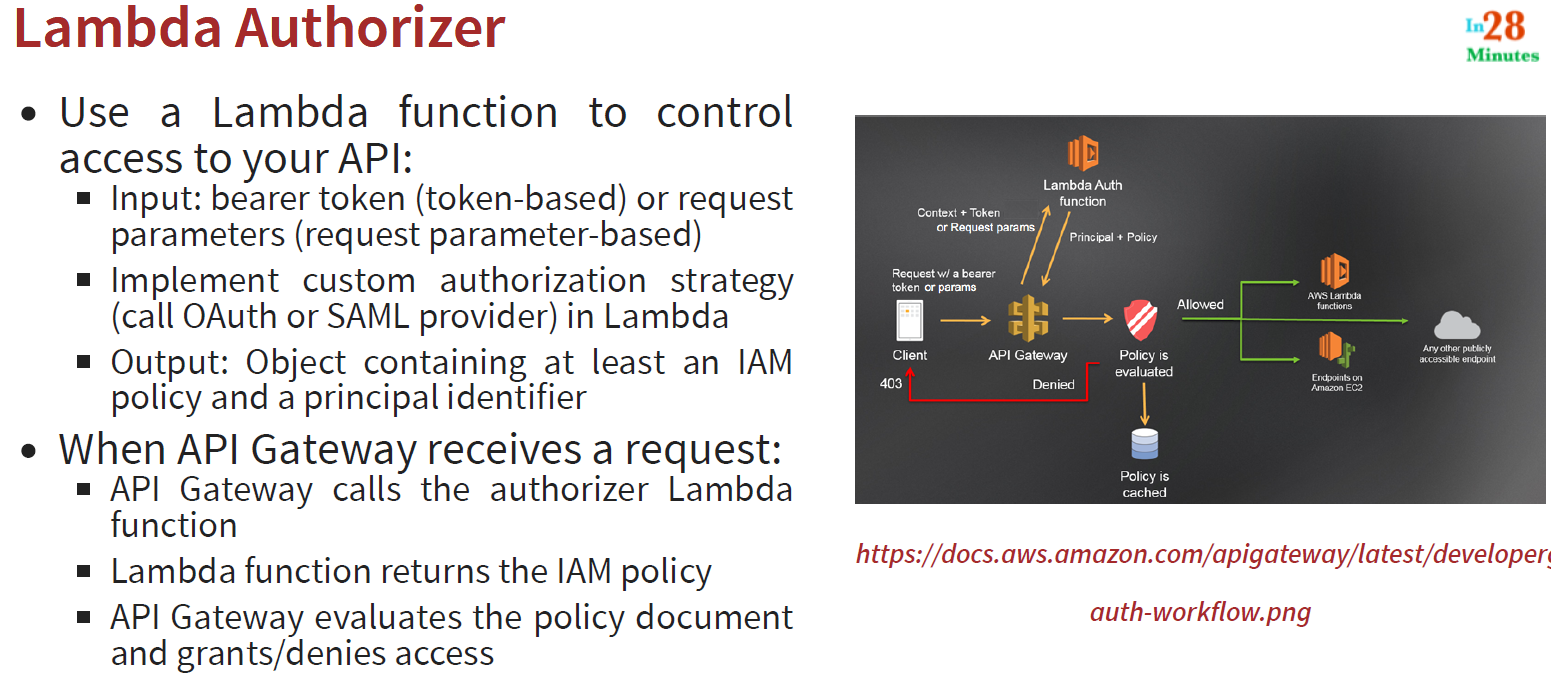


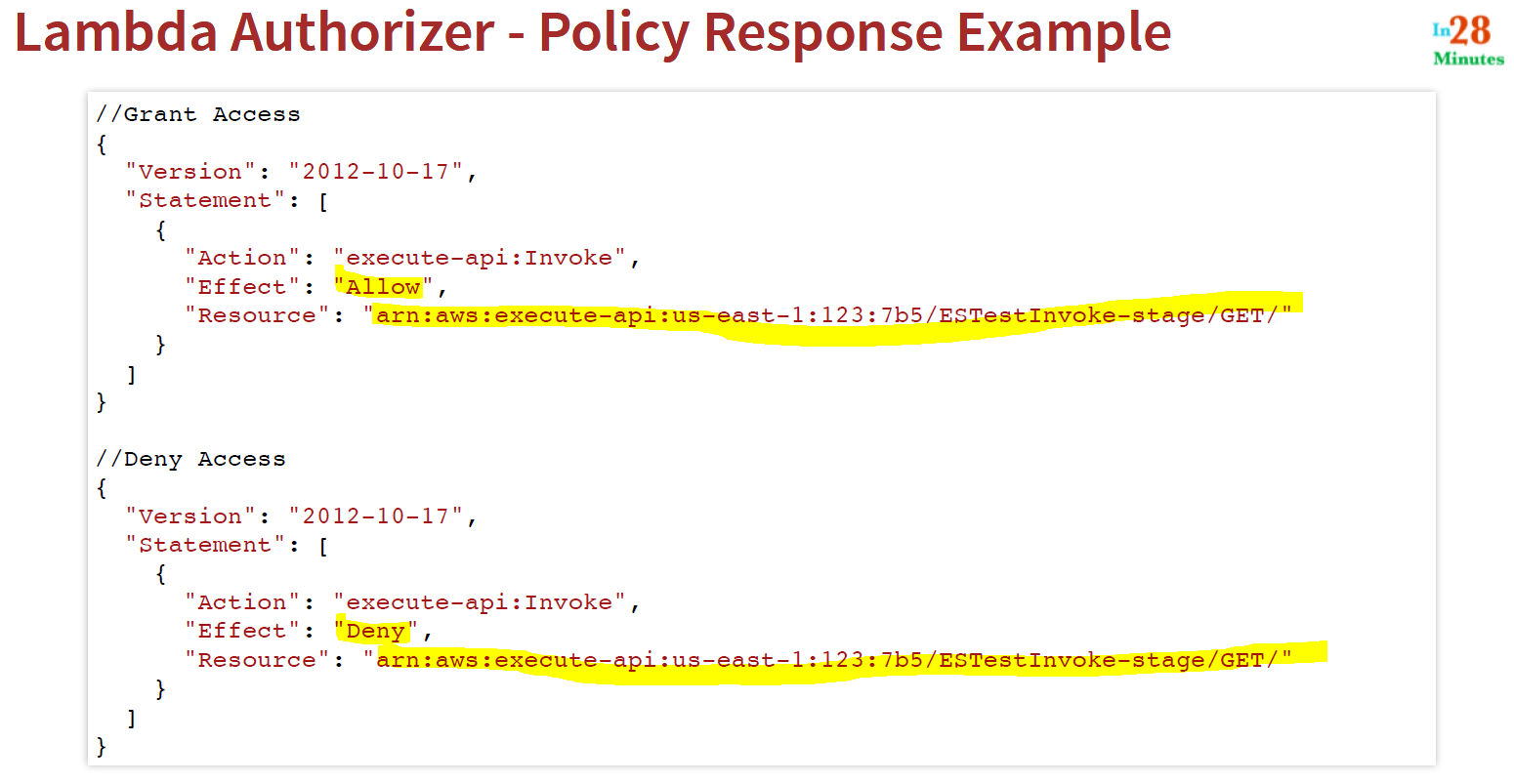




**Finally let’s see Lambda Authorization:**

**Lambda authorizers** - Write custom lambda function to validate the bearer token (OAuth or SAML, FB, Google, for example), or request parameters.





**So we can use the above policy for Allow and Deny Access.**

**116. Step 07 - Exploring API Gateway – Scenarios**

