**Lab Steps**

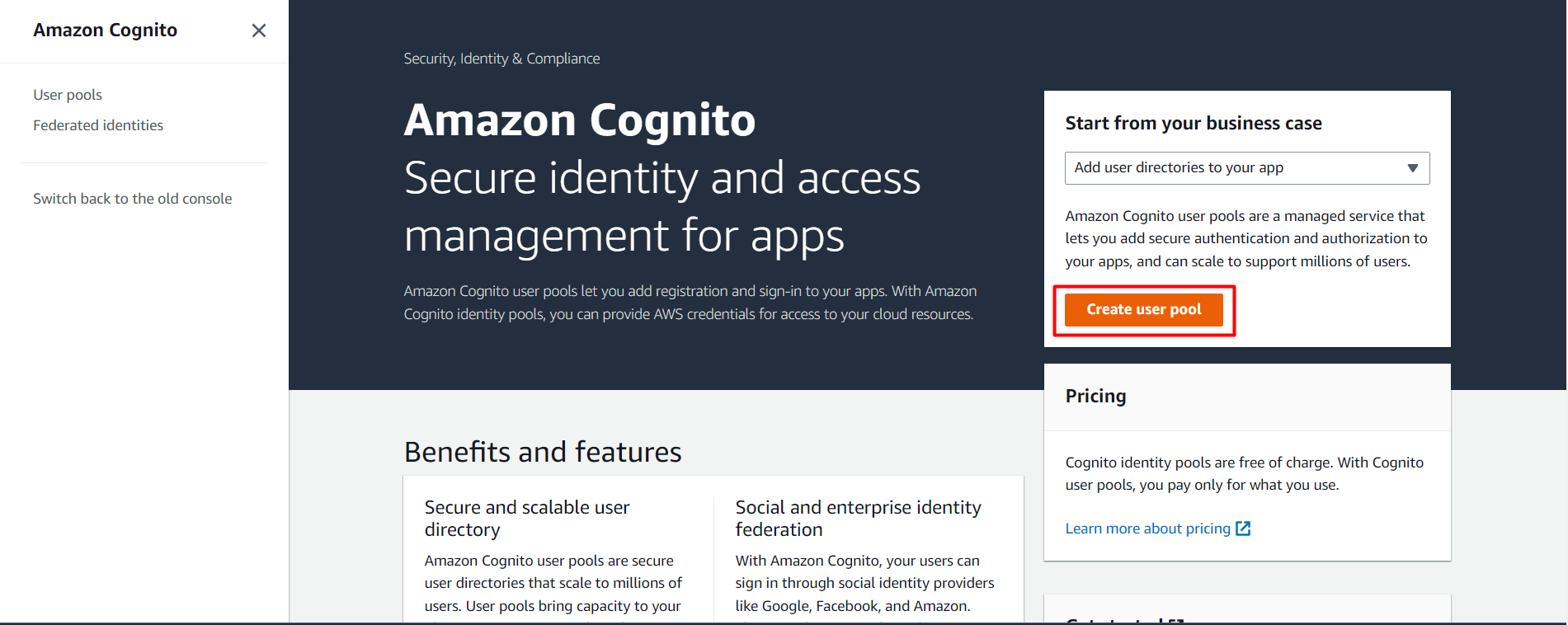
**Task 1: Sign in to AWS Management Console**

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
   * Leave the Account ID as default. Never edit/remove the 12-digit Account ID present in the AWS Console. Otherwise, you cannot proceed with the lab.
   * Now copy your **Username** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign-in** button.
3. Once Signed In to the AWS Management Console, make the default AWS Region as **US East (N. Virginia) us-east-1.**
4. Select Maybe later in New AWS Console Home page pop-up

**Task 2: Creating a User Pool**

In this task, we are going to guide users through the process of creating a user pool in AWS Cognito. Creating a user pool is the first step in setting up user authentication and authorization for an application. It establishes the foundation for managing user accounts, sign-up, and sign-in processes.

1. Navigate to Cognito by clicking on the **Services** menu at the top, click on Cognito under the **Security, Identity, and Compliance** section.
2. Make sure you are in the **US East (N. Virginia) us-east-1** Region. Click on **Create user pool**.

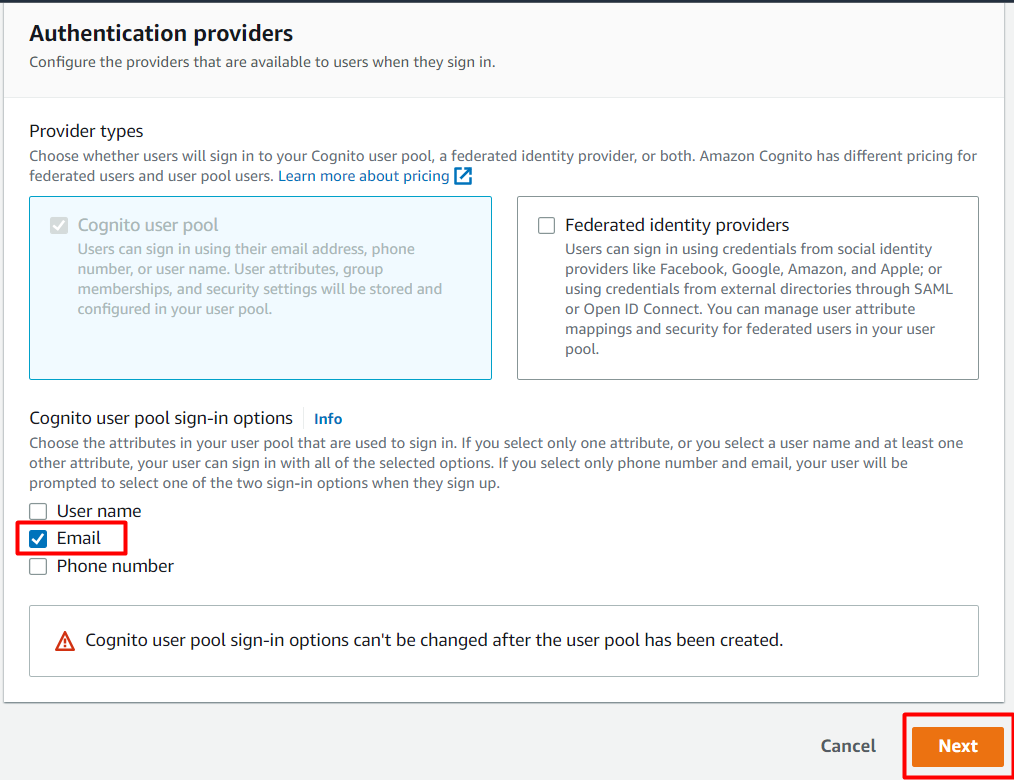
****

**Task 3: Configure sign-in experience**

In this task, we are going to allow users to configure the sign-in options for their user pool. By selecting the appropriate provider types and sign-in options, users can define how users can authenticate and sign in to their application, such as using email, social logins, or other identity providers.

1. Add details in the configure sign-in experience :

* Provider Types : Select **Cognito user pool**
* Cognito user pool sign-in options : Select **Email**

****

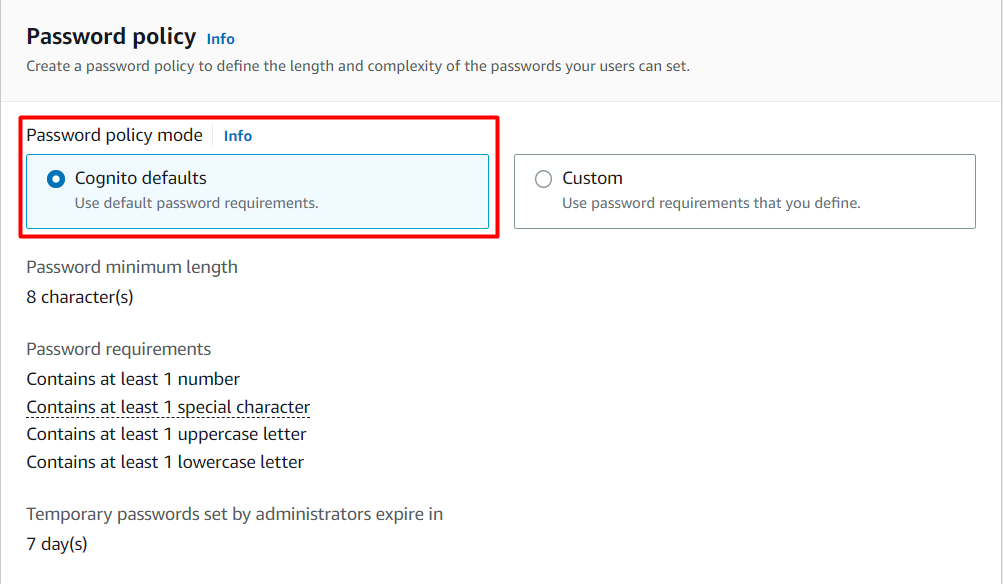
1. Click on **Next** Button.

**Task 4: Configure Security Requirements**

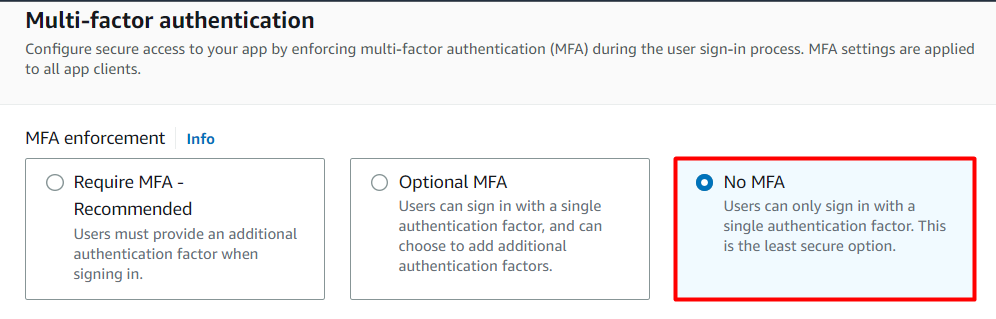
In this task, we are going to define the security requirements for user passwords in the user pool. By setting up a password policy, users can enforce specific rules for password strength and complexity to enhance the security of user accounts.

1. Password Policy:

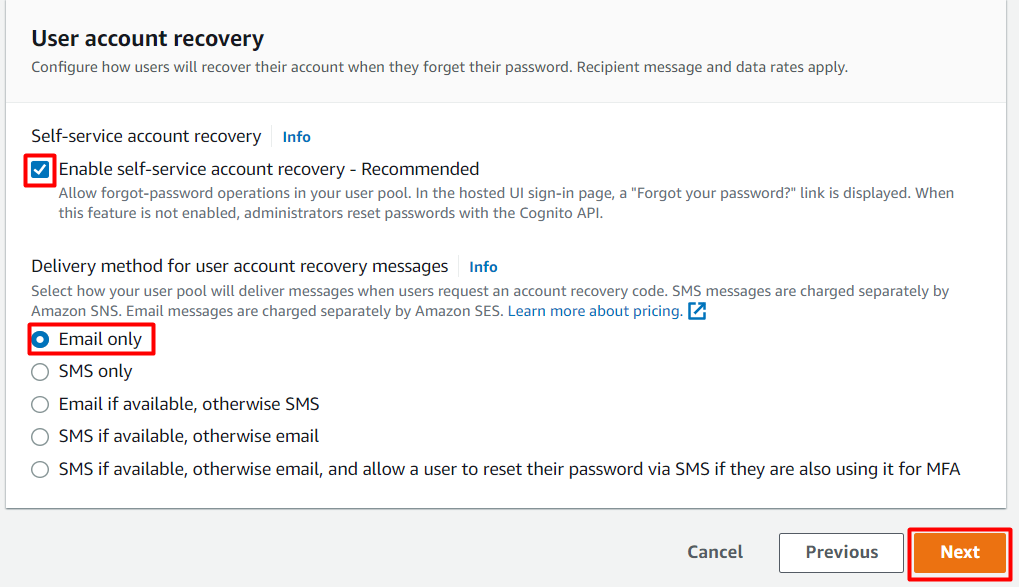
* Password Policy Mode : Select **Cognito defaults**

****

1. We give the **Minimum Password Strength** and can add the required parameters like numbers, lowercase, uppercase and special characters. Here, we are selecting Cognito defaults. We can customize this password as well.
2. **Multi-Factor Authentication (MFA)** increases security for your end users. Phone numbers must be verified if MFA is enabled. We choose **No MFA** for this lab.



1. **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. In this case, we choose **Enable self-service account recovery.**
2. **Account Recovery:** 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. Here, we choose **Email** only.

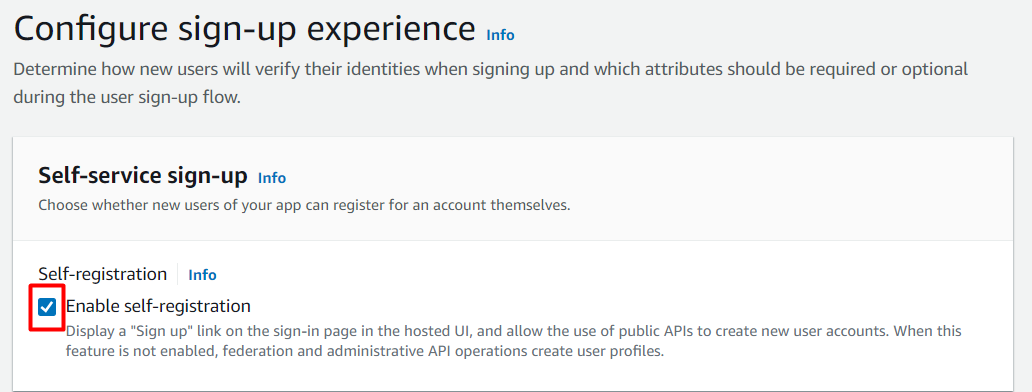


1. Click on **Next** button.

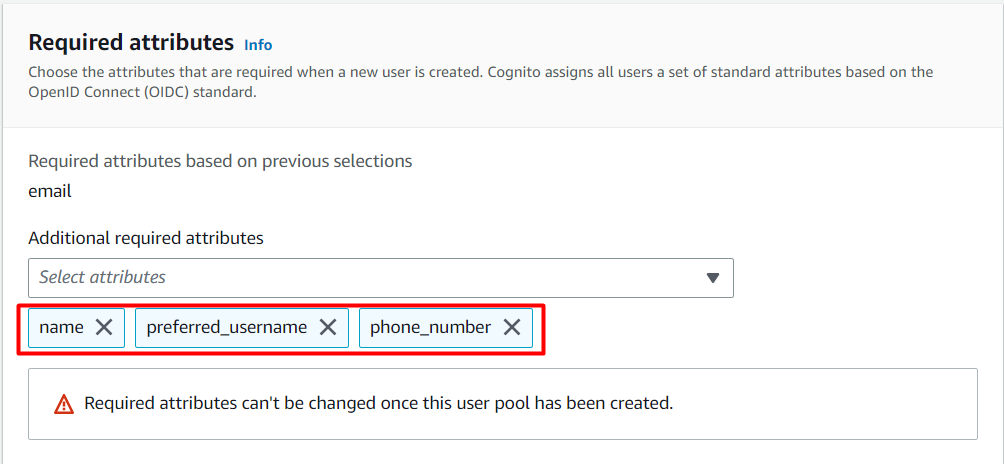
**Task 5: Configure sign-up experience**

In this task, we are going to allow users to define the sign-up experience for their app users. Users can choose whether to enable self-registration, which allows users to sign up themselves without administrator interference. They can also specify the required attributes during the sign-up process, such as email, name, preferred username, and phone number.

1. You can choose to **only allow administrators to create users or allow users to sign themselves up**.
2. Self-service sign-up:
   * Self-registration : **Check** the Enable self-registration checkbox



1. We choose to **allow users to sign themselves up,** where the users can sign up themselves without administrator interference.
2. Attribute verification and user account confirmation:
   * Keep the changes as default.
3. Required Attributes:
   * We can choose the **Standard Attributes**, which will be required while performing a sign-up. Here, we choose **Name, Preferred Username, Phone Number** which are required to perform a signup.
   * We can also customize our attributes that are required while signup by clicking **on Add custom attribute**.

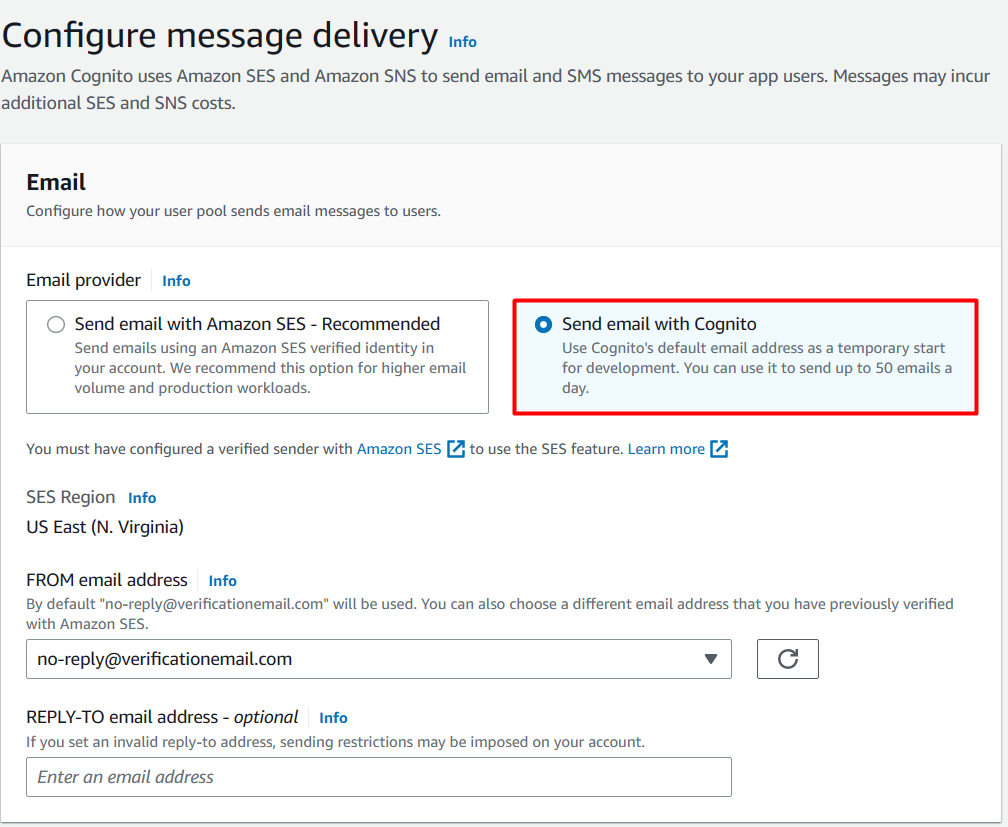


1. Click on **Next** button.

**Task 6: Configure Message delivery**

In this task, we are going to provide users with the option to configure message delivery, specifically email delivery, from the user pool. Users can choose to send emails using Amazon SES (Simple Email Service) and specify whether higher daily email limits are required. This task allows users to set up email communication for various purposes, such as user verification or password recovery.

1. You can send emails from an SES verified identity. Before you can send an email using Amazon SES, you must verify each identity that you're going to use as a From, Source, Sender, or Return-Path address to prove that you own it. For now, we leave it blank.
2. **Amazon SES Configuration:** Cognito will send emails through your Amazon SES configuration. Select Yes if you require higher daily email limits, otherwise select No. Here, we select **Send email with Cognito** in the **Email provider**.



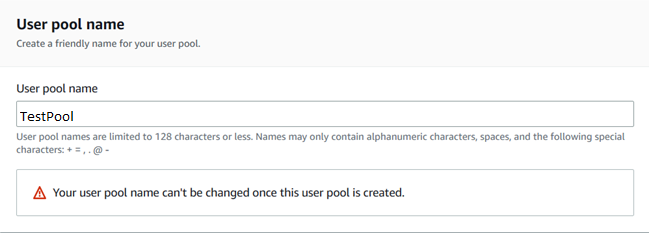
1. Click on **Next** button.

**Task 7: Integrate your app**

 In this task, we are going to guide users in integrating their app with the user pool. Users can specify the user pool name and create an initial app client with a unique ID and an optional secret key. This integration step enables the app to authenticate and interact with the user pool for user management and authentication purposes.

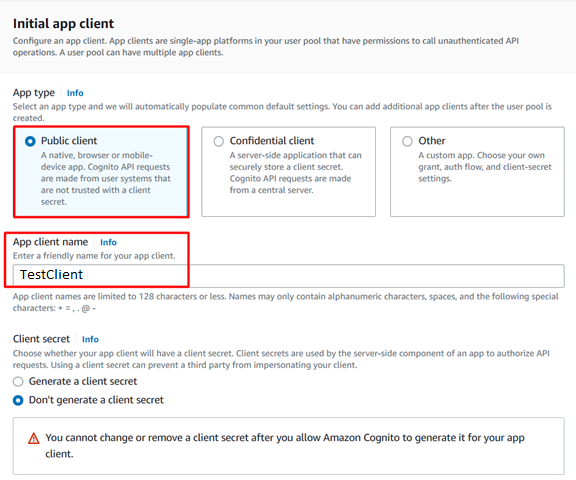
1. You can create a user pool.

* User pool name: Enter **TestPool**



1. The app clients that we add will be given a unique ID and an optional secret key to access this user pool. Initial app client:

* App client name: Enter **TestClient**

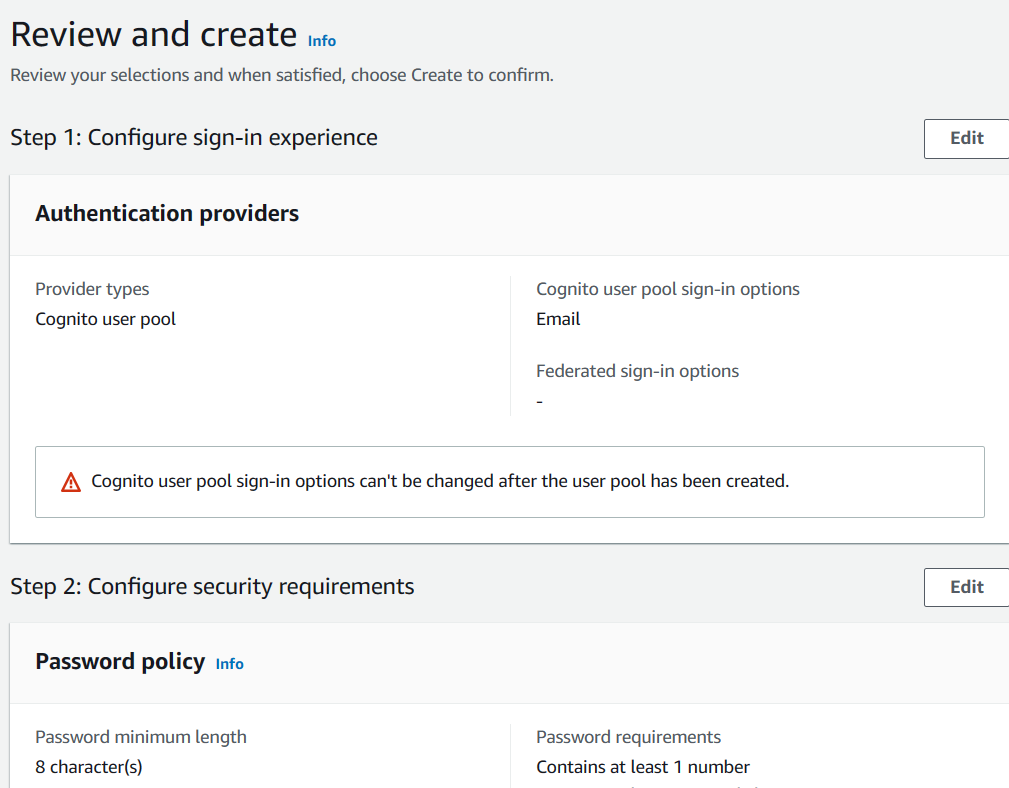


1. Click on **Next** button.

**Task 8: Review**

In this task, we are going to provide users with an opportunity to review all the settings and configurations they have made so far. It allows users to ensure that everything is correctly set up before creating the user pool. By reviewing the settings, users can identify any potential errors or adjustments that need to be made.

* Review all the settings and click on **Create Pool** as shown below.



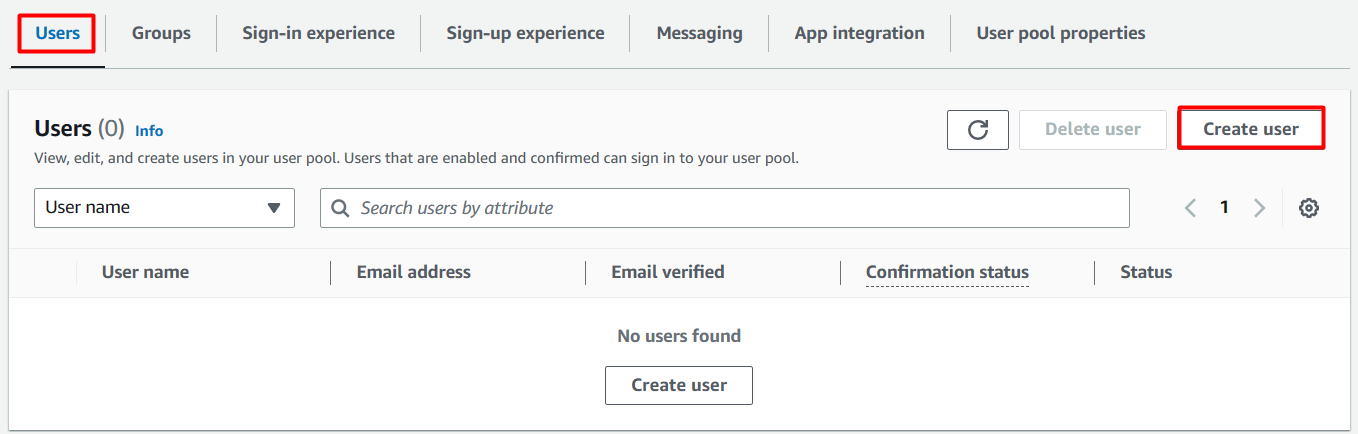
* You’ll get a message as the **User pool “TestPool” has been created successfully**. Ignore the error if any,



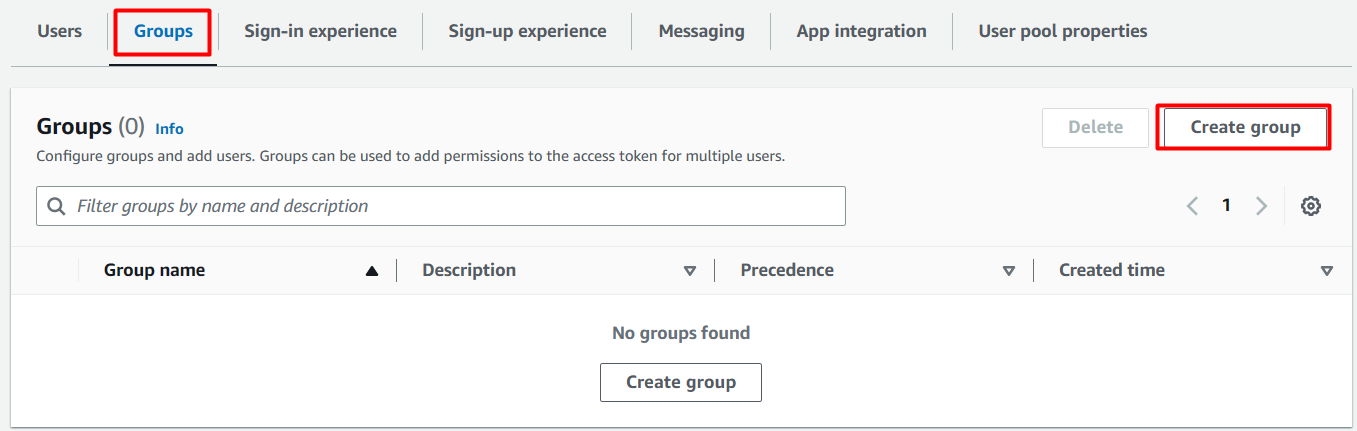
* You can see that the user pool is created successfully.



* Click on the user pool. You can see that you can create user.



* Navigate to **Groups** tab and Click on **Create Group** if you want to create a group.



* From an Administrative perspective, if we have an application, the application would then invoke the Amazon Cognito to create User itself.

**Do you Know?**

By leveraging social sign-in with AWS Cognito, developers can streamline the registration and sign-in process for their users. It eliminates the need for users to create new usernames and passwords specifically for the app, as they can simply use their existing social media accounts to authenticate. This not only enhances user convenience but also reduces friction during the onboarding process.

**Completion and Conclusion**

1. You have successfully used AWS management console to create a User Pool.
2. You learned how to use each setting in a detailed manner.
3. You learned how to do settings for Policies, MFA and Verifications.