Creating a User Pool in AWS Cognito

Level: **Fundamental**

Amazon Web Services Amazon Cognito User Pools

0h 20m 2s left

15 MIN

End Lab

Open Console

Validation

Lab Credentials

User Name

Whiz_User_80425.70355567

Password

b337a3d2-84ed-429a-9bf3-0130be95be24

Access Key

AKIA2VQ5WFSQ5B76KMUE

Secret Key

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

Lab Resources

No Lab Resources Found

Support Documents

Need help?

- How to use Hands on Lab
- Troubleshooting Lab
- FAQs

Submit Feedback | Share

Lab Overview | Lab Steps | Lab Validation | Lab FAQs

Cloud Architect, Cloud Developer, Cloud Security Engineer

Security

Lab Steps

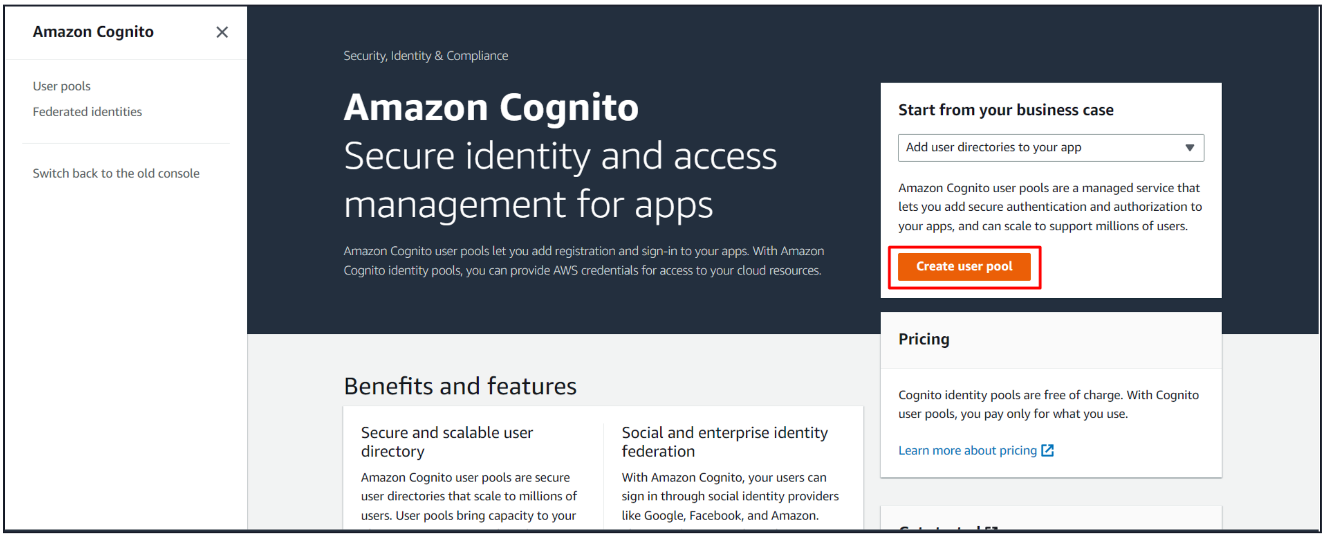
Task 1: Sign in to AWS Management Console

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**.


Amazon Cognito
User pools
Federated identities
Switch back to the old console
Security, Identity & Compliance
Add user directories to your app
Create user pool

Amazon Cognito
Secure identity and access management for apps

Amazon Cognito user pools let you add registration and sign-in to your apps. With Amazon Cognito identity pools, you can provide AWS credentials for access to your cloud resources.

Start from your business case

Amazon Cognito user pools are a managed service that lets you add secure authentication and authorization to your apps, and can scale to support millions of users.

Pricing

Cognito identity pools are free of charge. With Cognito user pools, you pay only for what you use.

Learn more about pricing

Benefits and features

Secure and scalable user directory

Amazon Cognito user pools are secure user directories that scale to millions of users. User pools bring capacity to your

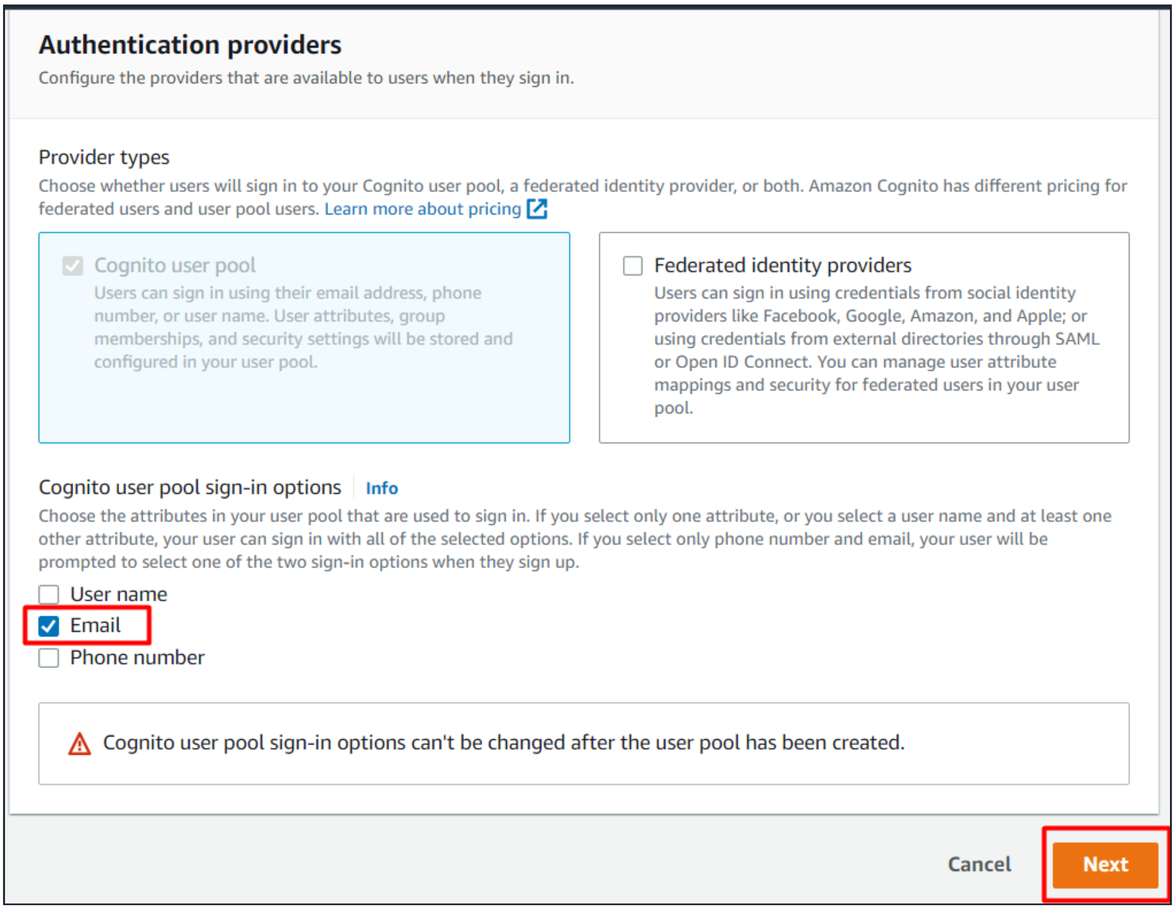
Social and enterprise identity federation

With Amazon Cognito, your users can sign in through social identity providers like Google, Facebook, and Amazon.

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**



Authentication providers

Configure the providers that are available to users when they sign in.

Provider types

Choose whether users will sign in to your Cognito user pool, a federated identity provider, or both. Amazon Cognito has different pricing for federated users and user pool users. Learn more about pricing

☑ Cognito user pool
Users can sign in using their email address, phone number, or user name. User attributes, group memberships, and security settings will be stored and configured in your user pool.

□ Federated identity providers
Users can sign in using credentials from social identity providers like Facebook, Google, Amazon, and Apple; or using credentials from external directories through SAML or Open ID Connect. You can manage user attribute mappings and security for federated users in your user pool.

Cognito user pool sign-in options Info

Choose the attributes in your user pool that are used to sign in. If you select only one attribute, or you select a user name and at least one other attribute, your user can sign in with all of the selected options. If you select only phone number and email, your user will be prompted to select one of the two sign-in options when they sign up.

□ User name
☑ Email
□ Phone number

⚠ Cognito user pool sign-in options can't be changed after the user pool has been created.

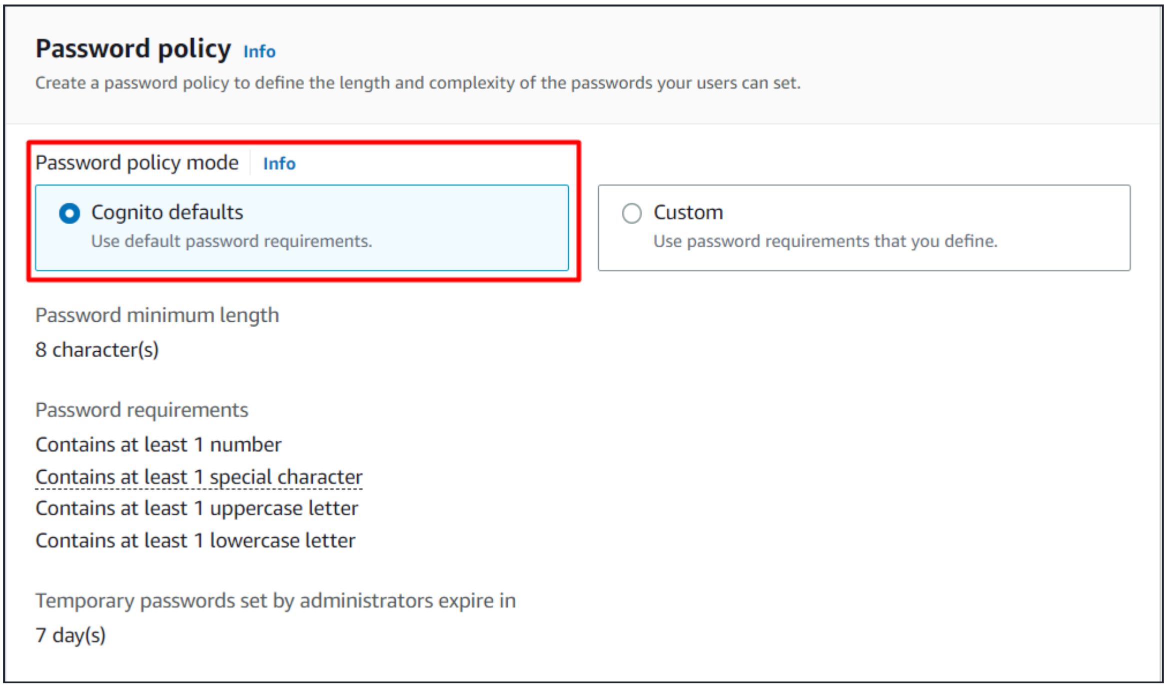
2. Click on **Next** Button.

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**



Password policy Info

Create a password policy to define the length and complexity of the passwords your users can set.

Password policy mode Info

● Cognito defaults
Use default password requirements.

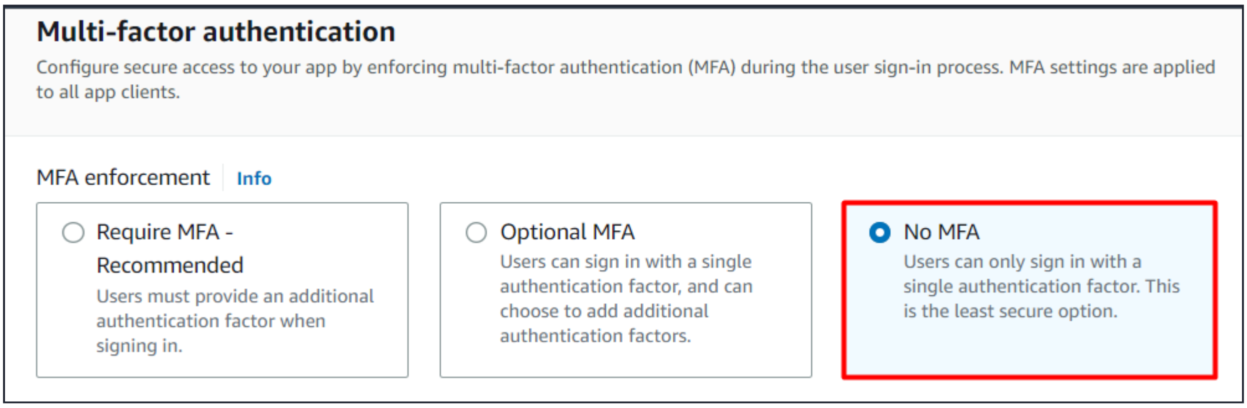
○ Custom
Use password requirements that you define.

Password minimum length
8 character(s)

Password requirements
Contains at least 1 number
Contains at least 1 special character
Contains at least 1 uppercase letter
Contains at least 1 lowercase letter

Temporary passwords set by administrators expire in
7 day(s)

2. 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.
3. **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.



Multi-factor authentication

Configure secure access to your app by enforcing multi-factor authentication (MFA) during the user sign-in process. MFA settings are applied to all app clients.

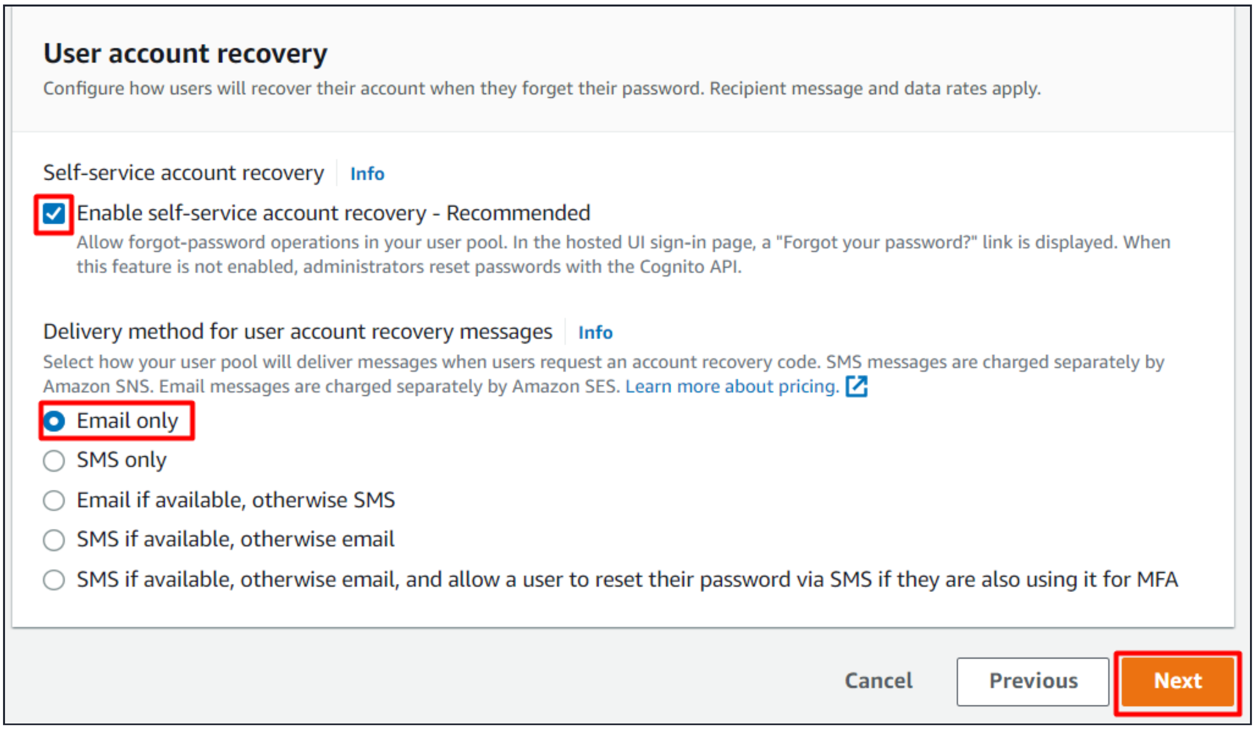
MFA enforcement Info

○ Require MFA - Recommended
Users must provide an additional authentication factor when signing in.

○ Optional MFA
Users can sign in with a single authentication factor, and can choose to add additional authentication factors.

● No MFA
Users can only sign in with a single authentication factor. This is the least secure option.

4. **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.**
5. **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.



User account recovery

Configure how users will recover their account when they forget their password. Recipient message and data rates apply.

Self-service account recovery | Info

☑ Enable self-service account recovery - Recommended

Allow forgot-password operations in your user pool. In the hosted UI sign-in page, a "Forgot your password?" link is displayed. When this feature is not enabled, administrators reset passwords with the Cognito API.

Delivery method for user account recovery messages | Info

Select how your user pool will deliver messages when users request an account recovery code. SMS messages are charged separately by Amazon SNS. Email messages are charged separately by Amazon SES. Learn more about pricing.

● Email only

○ SMS only

○ Email if available, otherwise SMS

○ SMS if available, otherwise email

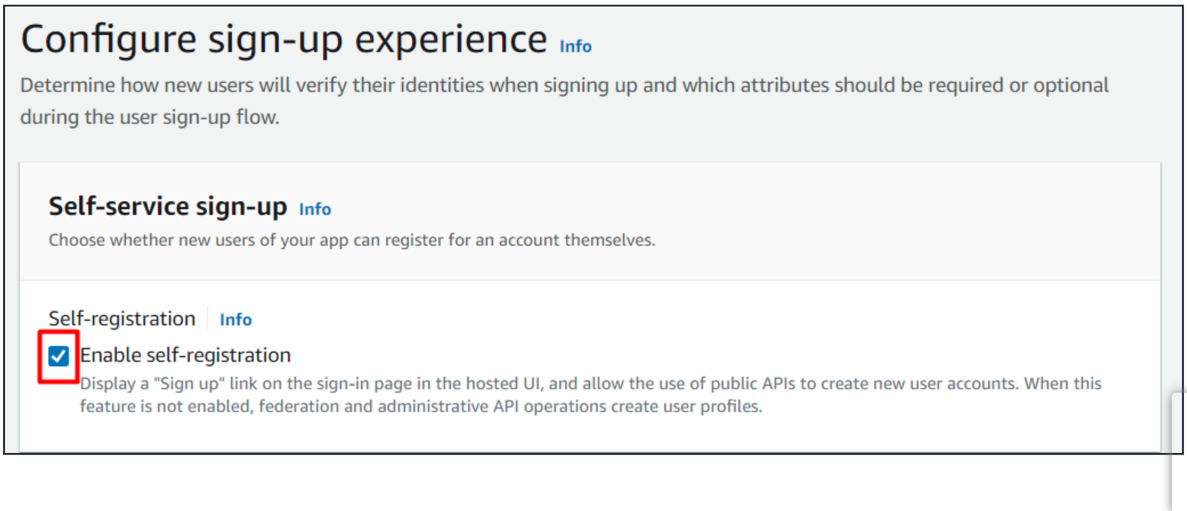
○ SMS if available, otherwise email, and allow a user to reset their password via SMS if they are also using it for MFA

4. 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



Configure sign-up experience Info

Determine how new users will verify their identities when signing up and which attributes should be required or optional during the user sign-up flow.

Self-service sign-up Info

Choose whether new users of your app can register for an account themselves.

Self-registration | Info

☑ Enable self-registration

Display a "Sign up" link on the sign-in page in the hosted UI, and allow the use of public APIs to create new user accounts. When this feature is not enabled, federation and administrative API operations create user profiles.

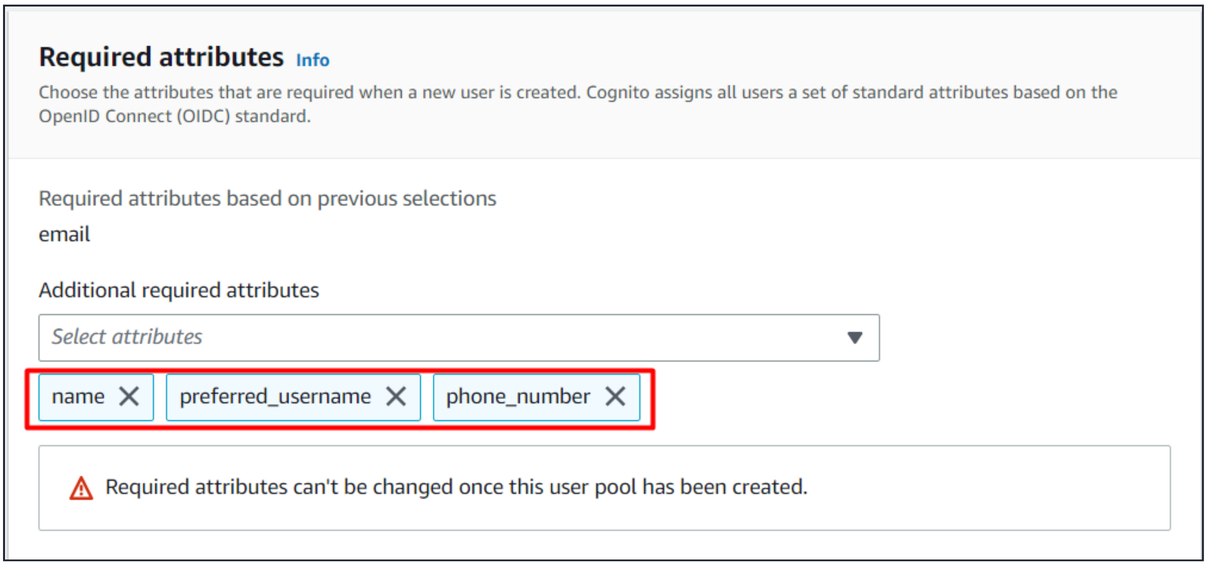
3. We choose to **allow users to sign themselves up,** where the users can sign up themselves without administrator interference.

4. Attribute verification and user account confirmation:

   - Keep the changes as default.

5. 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**.



Required attributes Info

Choose the attributes that are required when a new user is created. Cognito assigns all users a set of standard attributes based on the OpenID Connect (OIDC) standard.

Required attributes based on previous selections

email

Additional required attributes

Select attributes

name ✕ preferred_username ✕ phone_number ✕

⚠ Required attributes can't be changed once this user pool has been created.

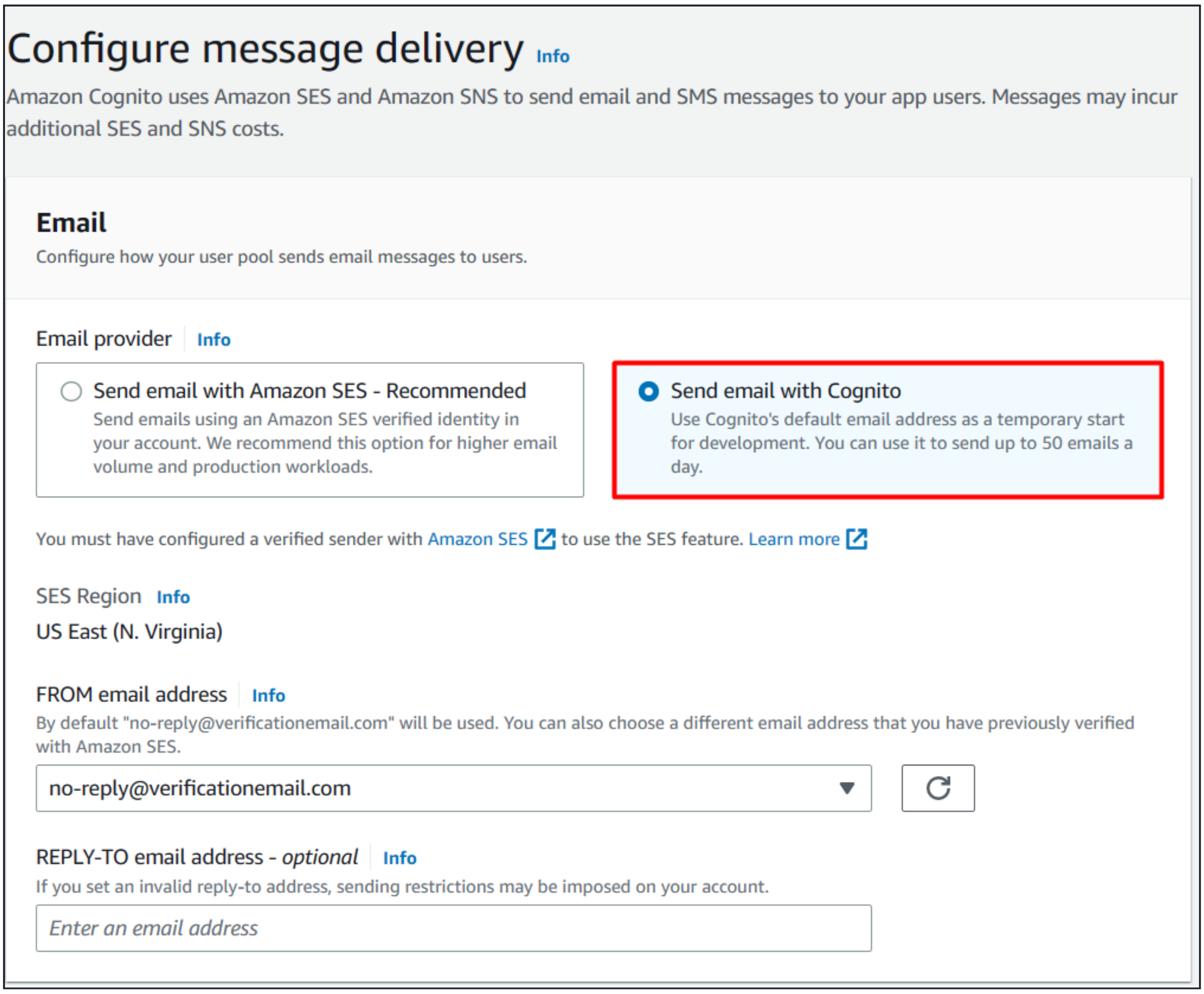
3. Click on **Next** button.

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**.



Configure message delivery Info

Amazon Cognito uses Amazon SES and Amazon SNS to send email and SMS messages to your app users. Messages may incur additional SES and SNS costs.

Email

Configure how your user pool sends email messages to users.

Email provider Info

○ Send email with Amazon SES - Recommended
Send emails using an Amazon SES verified identity in your account. We recommend this option for higher email volume and production workloads.

● Send email with Cognito
Use Cognito's default email address as a temporary start for development. You can use it to send up to 50 emails a day.

You must have configured a verified sender with Amazon SES to use the SES feature. Learn more

SES Region Info

US East (N. Virginia)

FROM email address Info

By default "no-reply@verificationemail.com" will be used. You can also choose a different email address that you have previously verified with Amazon SES.

no-reply@verificationemail.com

REPLY-TO email address - *optional* Info

If you set an invalid reply-to address, sending restrictions may be imposed on your account.

Enter an email address

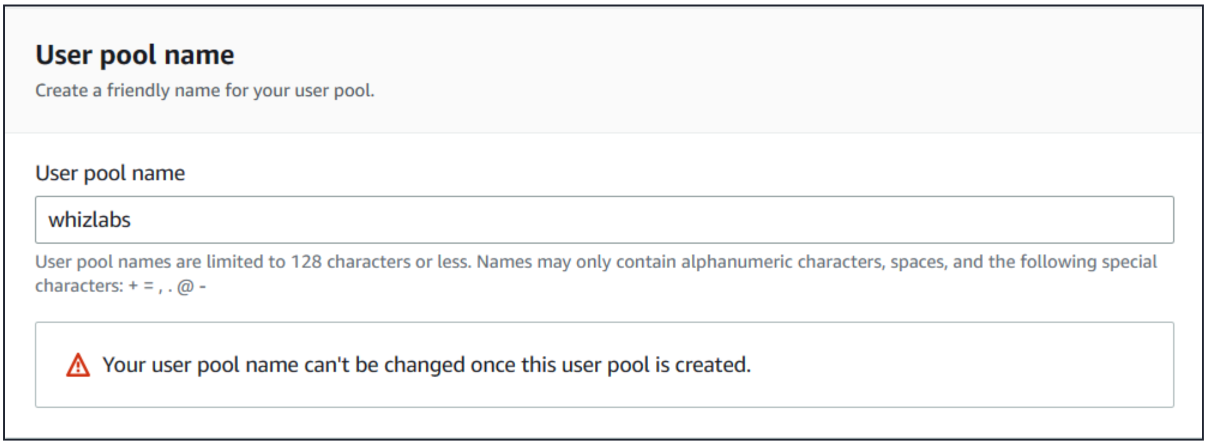
3. Click on **Next** button.

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 **whizlabs**



User pool name

Create a friendly name for your user pool.

User pool name

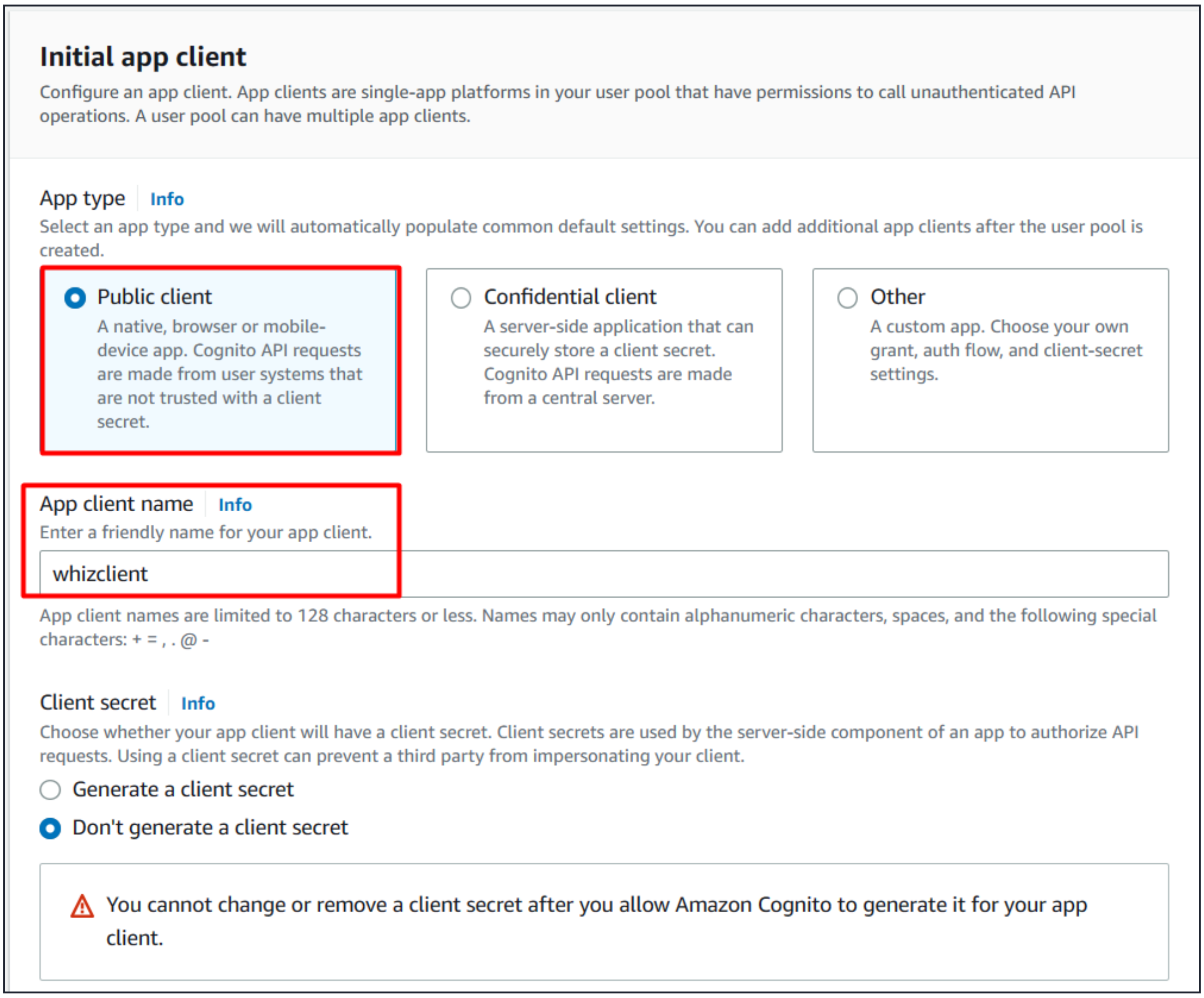
whizlabs

User pool names are limited to 128 characters or less. Names may only contain alphanumeric characters, spaces, and the following special characters: + = , . @ -

⚠ Your user pool name can't be changed once this user pool is created.

2. 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 **whizclient**



Initial app client

Configure an app client. App clients are single-app platforms in your user pool that have permissions to call unauthenticated API operations. A user pool can have multiple app clients.

App type | Info

Select an app type and we will automatically populate common default settings. You can add additional app clients after the user pool is created.

● Public client
A native, browser or mobile-device app. Cognito API requests are made from user systems that are not trusted with a client secret.

○ Confidential client
A server-side application that can securely store a client secret. Cognito API requests are made from a central server.

○ Other
A custom app. Choose your own grant, auth flow, and client-secret settings.

App client name | Info

Enter a friendly name for your app client.

whizclient

App client names are limited to 128 characters or less. Names may only contain alphanumeric characters, spaces, and the following special characters: + = , . @ -

Client secret | Info

Choose whether your app client will have a client secret. Client secrets are used by the server-side component of an app to authorize API requests. Using a client secret can prevent a third party from impersonating your client.

○ Generate a client secret

● Don't generate a client secret

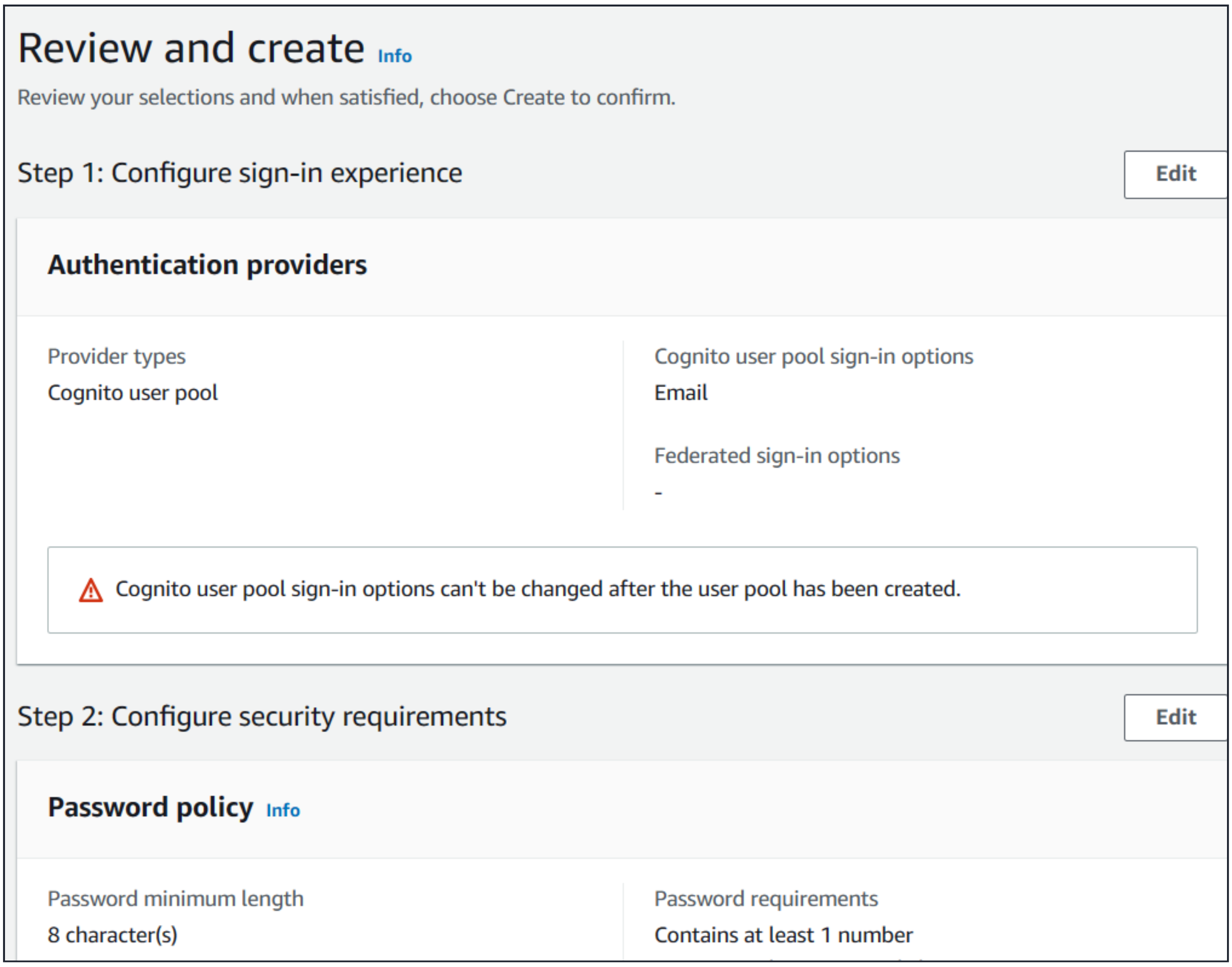
⚠ You cannot change or remove a client secret after you allow Amazon Cognito to generate it for your app client.

3. 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.



Review and create

Review your selections and when satisfied, choose Create to confirm.

Step 1: Configure sign-in experience

Authentication providers

Provider types
Cognito user pool

Cognito user pool sign-in options
Email

Federated sign-in options
-

⚠ Cognito user pool sign-in options can't be changed after the user pool has been created.

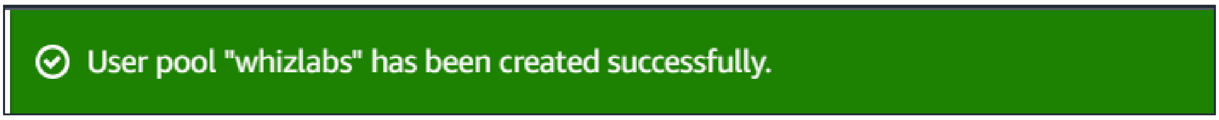
Step 2: Configure security requirements

Password policy

Password minimum length
8 character(s)

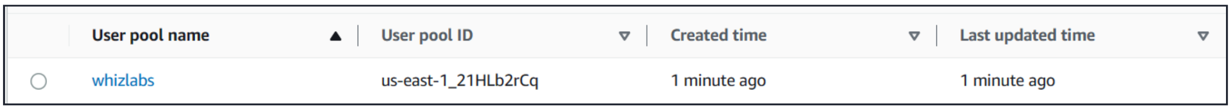
Password requirements
Contains at least 1 number

- You'll get a message as the **User pool "whizlabs" has been created successfully**. Ignore the error if any,



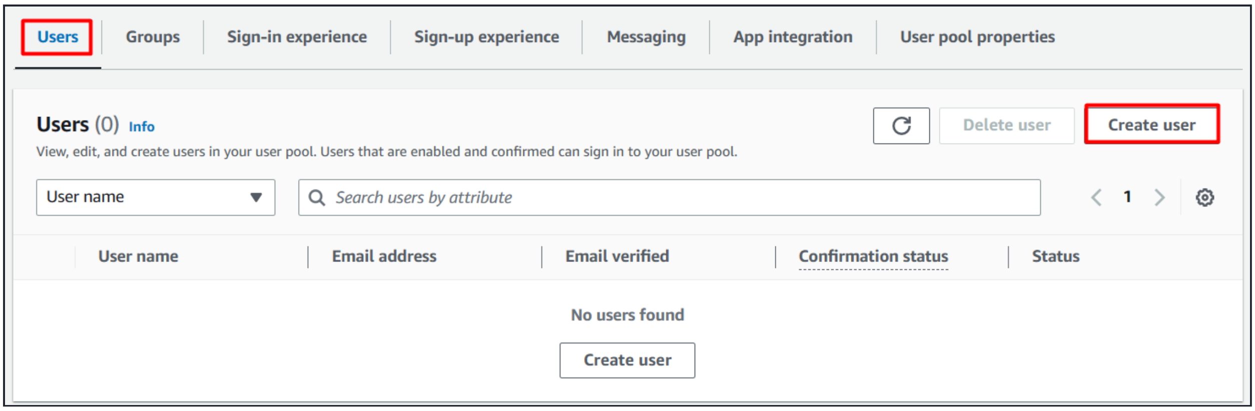
User pool "whizlabs" has been created successfully.

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



	User pool name ▲	User pool ID ▽	Created time ▽	Last updated time ▽
○	whizlabs	us-east-1_21HLb2rCq	1 minute ago	1 minute ago

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



Users | Groups | Sign-in experience | Sign-up experience | Messaging | App integration | User pool properties

Users (0) Info

View, edit, and create users in your user pool. Users that are enabled and confirmed can sign in to your user pool.

Delete user | Create user

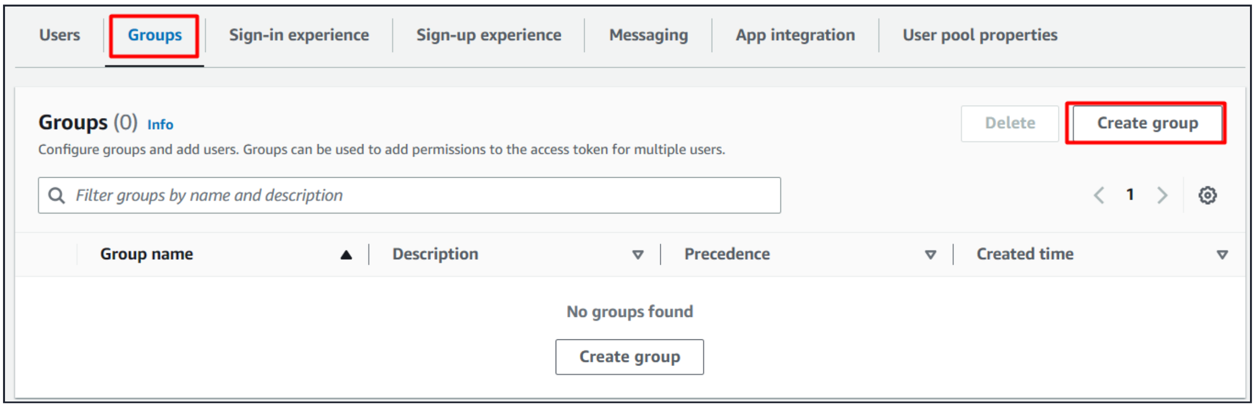
User name ▼ | Search users by attribute

User name	Email address	Email verified	Confirmation status	Status

No users found

Create user

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



Users | Groups | Sign-in experience | Sign-up experience | Messaging | App integration | User pool properties

Groups (0) Info

Configure groups and add users. Groups can be used to add permissions to the access token for multiple users.

Delete | Create group

Filter groups by name and description

Group name ▲	Description ▽	Precedence ▽	Created time ▽

No groups found

Create group

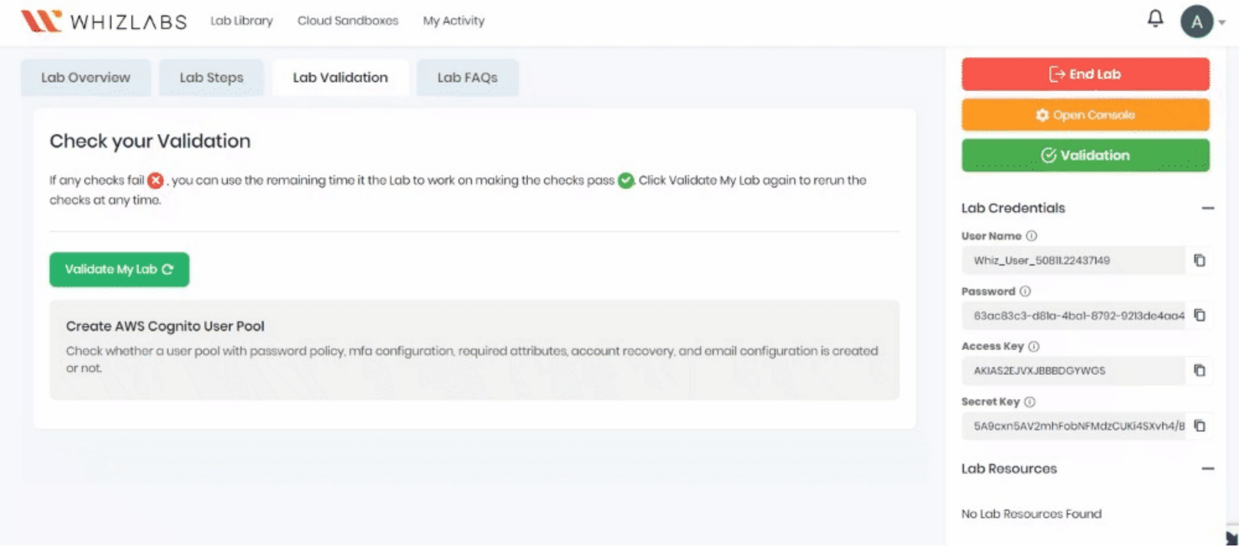
- From an Administrative perspective, if we have an application, the application would then invoke the Amazon Cognito to create User itself.

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.

Task 9: Validation Test

1. Once the lab steps are completed, please click on the **Validation** button on the left side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :



Check your Validation

If any checks fail ☒, you can use the remaining time it the Lab to work on making the checks pass ✓. Click Validate My Lab again to rerun the checks at any time.

Validate My Lab

Create AWS Cognito User Pool

Check whether a user pool with password policy, mfa configuration, required attributes, account recovery, and email configuration is created or not.

Lab Credentials

User Name: Whiz_User_50811.22437149

Password: 63ac83c3-d81a-4ba1-8792-9213de4aa4

Access Key: AKIAS2EJVXJBBBDGYWGS

Secret Key: 5A9cxn5AV2mhFobNFMdzCUKi4SXvh4/B

Lab Resources

No Lab Resources Found

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.

End Lab

1. Sign out of the AWS Account.
2. You have successfully completed the lab.
3. Once you have completed the steps, click on **End Lab** from your whizlabs dashboard.

About Us Subscription Instructions and Guidelines FAQ's Contact Us