

# Creating a User Pool in AWS Cognito

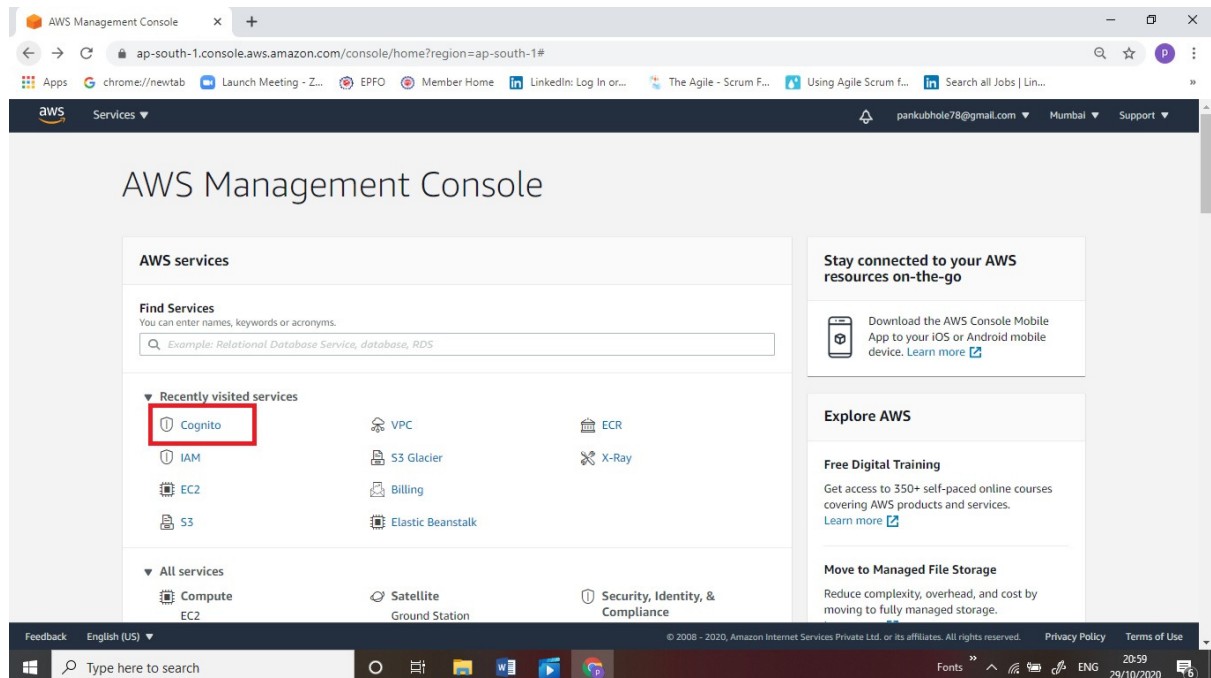
## Lab Tasks

1. Log into AWS Management Console.
2. **Create a User Pool** in AWS Cognito.
3. We will navigate to **Steps through each setting to make your choices** to understand the settings in a detailed manner.
4. We will go through the **Attributes**.
5. We will walk through the **Policies, MFA and Verification**.
6. We will go through the **Message Customizations**, finally Review and create a User Pool

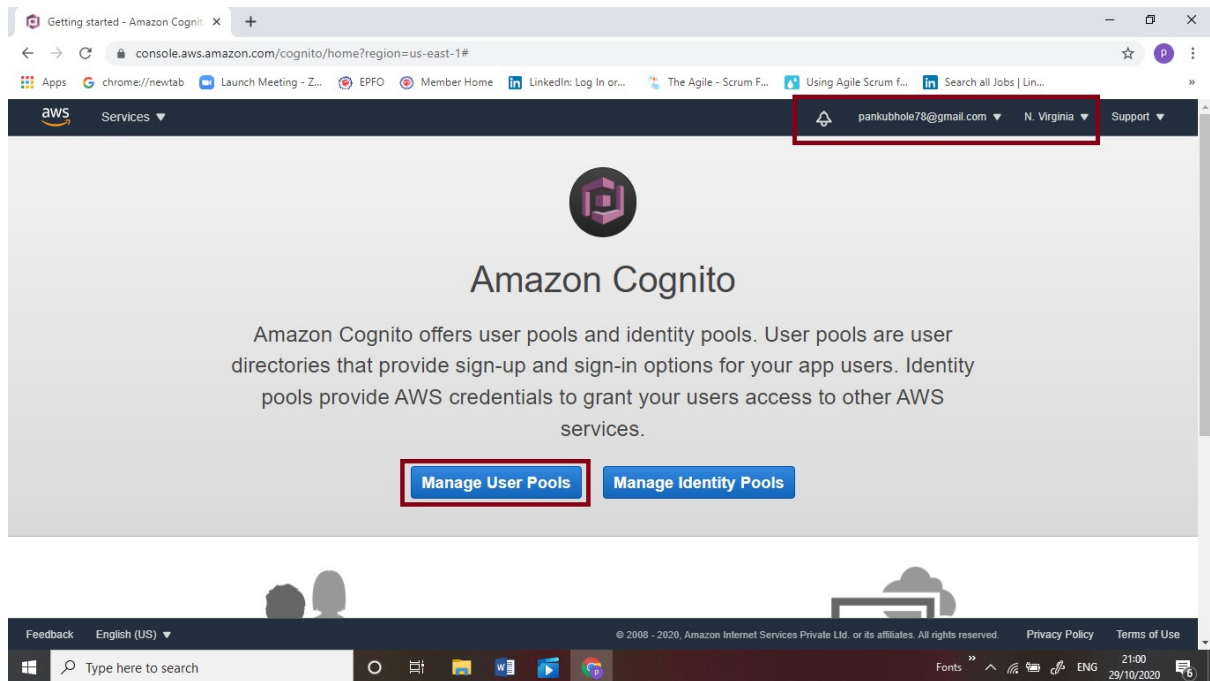
## Steps

### Creating a User Pool:

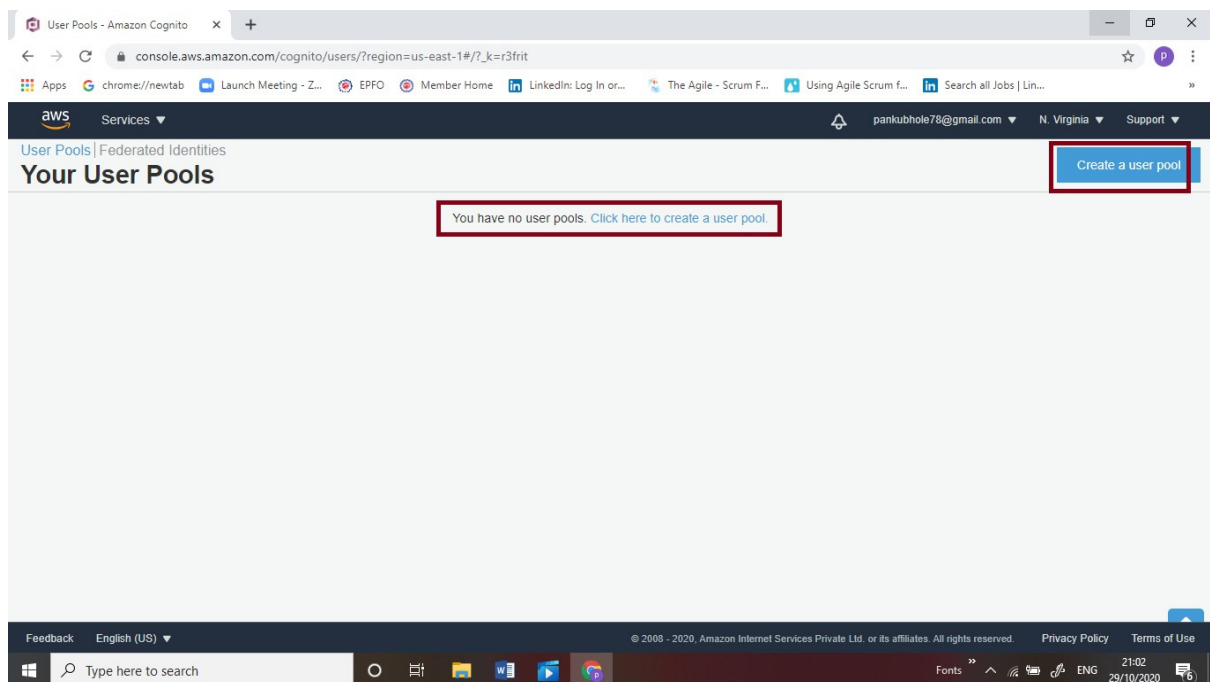
1. Log into AWS Management Console.



2. Navigate to Cognito by clicking on the menu at the top, click on Cognito under the section.
3. Make sure you are in the **US East (N. Virginia) us-east-1** Region. Click on **Manage User Pools**.



4. Click on **Create a User Pool**



# Name and Attributes

1. Give your User Pool a descriptive name, (which is required for the identity).
2. We choose **Step through settings** to make each setting our own choice as shown below.

The screenshot shows the 'Create a user pool' page in the AWS IAM console. The 'Name' tab is selected, and the 'Pool name' field contains 'Demo User Pool'. The 'Step through settings' button is highlighted with a red box. The page title is 'Create a user pool' and the subtitle is 'What do you want to name your user pool?'. The 'Step through settings' button is blue and contains the text 'Step through settings' and 'Step through each setting to make your choices'.

3. In the Attributes page, we can mention how a user could perform a sign in.
4. You can choose to have users sign in with an email address, phone number, username or preferred username plus their password.

The screenshot shows the 'Attributes' tab of the 'Create a user pool' page. The 'Attributes' tab is selected, and the 'How do you want your end users to sign in?' section is visible. The 'Email address or phone number' option is selected for sign-in. The 'Which standard attributes do you want to require?' section is also visible. The 'Attributes' tab is highlighted with a red box. The 'How do you want your end users to sign in?' section is highlighted with a yellow box. The 'Email address or phone number' option is selected for sign-in. The 'Which standard attributes do you want to require?' section is also visible.

Required	Attribute	Required	Attribute
<input checked="" type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input checked="" type="checkbox"/>	phone number
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username
<input checked="" type="checkbox"/>	gender	<input checked="" type="checkbox"/>	profile
<input type="checkbox"/>	given name	<input type="checkbox"/>	zoneinfo
<input type="checkbox"/>	locale	<input type="checkbox"/>	updated at
<input type="checkbox"/>	middle name	<input type="checkbox"/>	website
<input checked="" type="checkbox"/>	name		

- Here we choose **Email address or Phone number**, where Users can use an email address or phone number as their **username** to sign up and sign in. Here, choose **Allow email addresses**.
- We can choose the **Standard Attributes**, which will be required while performing a sign up. Here, we choose Email, Name, Preferred Username, and Phone Number which are required to perform a signup.
- We can also customize our attributes that are required while signup by clicking **Add another attribute**.

**Create a user pool**

**Attributes**

**How do you want your end users to sign in?**

You can choose to have users sign in with an email address, phone number, username or preferred username plus their password. [Learn more.](#)

☐ Username - Users can use a username and optionally multiple alternatives to sign up and sign in.

☐ Also allow sign in with verified email address

☐ Also allow sign in with verified phone number

☐ Also allow sign in with preferred username (a username that your users can change)

☒ Email address or phone number - Users can use an email address or phone number as their "username" to sign up and sign in.

☒ Allow email addresses

☐ Allow phone numbers

☐ Allow both email addresses and phone numbers (users can choose one)

You can choose to enable case insensitivity on the username input for the selected sign-in option. For example, when this option is selected, the users can sign in using either "username" or "Username".

☒ (Recommended) Enable case insensitivity for username input

**Which standard attributes do you want to require?**

All of the standard attributes can be used for user profiles, but the attributes you select will be required for sign up. You will not be able to change these requirements after the pool is created. If you select an attribute to be an alias, users will be able to sign-in using that value or their username. [Learn more about attributes.](#)

Required	Attribute	Required	Attribute
<input checked="" type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input checked="" type="checkbox"/>	phone number
<input checked="" type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username
<input checked="" type="checkbox"/>	gender	<input checked="" type="checkbox"/>	profile
<input type="checkbox"/>	given name	<input type="checkbox"/>	zoneinfo
<input type="checkbox"/>	locale	<input type="checkbox"/>	updated at
<input type="checkbox"/>	middle name	<input type="checkbox"/>	website
<input checked="" type="checkbox"/>	name		

- Click on Next Step.

## Policies

- We give the **Minimum Password Strength** and can add the required parameters like numbers, lowercase, uppercase and special characters. Here, we select all the parameters.
- You can choose to **only allow administrators to create users or allow users to sign themselves up**.
- We choose the **allow users to sign themselves up** where the users can sign up themselves without administrator interference.
- As admin, you can configure when temporary passwords should expire. This includes accounts created by administrators i.e. if you choose **only allow administrators to create users**. Here, we can leave the option as we don't select it.

aws Services

User Pools | Federated Identities

## Create a user pool

Cancel

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

### What password strength do you want to require?

Minimum length  
8

☒ Require numbers  
☒ Require special character  
☒ Require uppercase letters  
☒ Require lowercase letters

### Do you want to allow users to sign themselves up?

You can choose to only allow administrators to create users or allow users to sign themselves up. [Learn more.](#)

☒ Only allow administrators to create users  
☐ Allow users to sign themselves up

### How quickly should temporary passwords set by administrators expire if not used?

You can choose for how long until a temporary password set by an administrator expires if the password is not used. This includes accounts created by administrators.

Days to expire  
7

Back Next step

Feedback English (US) © 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

5. Click on Next Step.

## MFA and Verifications

1. **Multi-Factor Authentication (MFA)** increases security for your end users. Phone numbers must be verified if MFA is enabled. We choose **off** for this lab.
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.
3. **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 **Email**.
4. **Define Role:** Amazon Cognito needs your permission to send SMS messages to your users on your behalf. We do not create any Role as we are marking MFA **off**. We will leave it as is.

**Create a user pool**

**Do you want to enable Multi-Factor Authentication (MFA)?**

Multi-Factor Authentication (MFA) increases security for your end users. If you choose 'optional' individual users can have MFA enabled. You can only choose 'required' when initially creating a user pool and if you do, all users must use MFA. Phone numbers must be verified if MFA is enabled. You can configure adaptive authentication on the Advanced security tab to require MFA based on risk scoring of user sign in attempts. [Learn more about multi-factor authentication.](#)

*Note: separate charges apply for sending text messages.*

☒ Off ☐ Optional ☐ Required

**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.](#)

☐ 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

**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

DemoUserPool-SMS-Role

**Create role**

5. Click on Next Step.

## Message Customizations

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 **No - Use Cognito (Default)**.
3. **Verification Type:** You can choose to send a code or a clickable link and customize the message to verify email addresses. We keep it default as code.
4. **User Invitation messages:** We can customize the SMS message, Email subject and Email message as how you want the text to be delivered to the user.



**Create a user pool**

**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: e.g. John Smith <john@smith.com>

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)

**Do you want to customize your email verification messages?**

You can choose to send a code or a clickable link and customize the message to verify email addresses. [Learn more about email verification.](#)

Verification type: ☒ Code ☐ Link

Email subject: Your verification code

**NEXT STEP**

## 5. Click on Next Step

## Tags:

### 1. You can create new tags by entering tag keys and tag values.

- Tag Key : Enter **Name**
- Tag Value: Enter **MyUserPool**

**Create a user pool**

**Do you want to add tags for this user pool?**

You can create new tags by entering tag keys and tag values below

Tag Key	Tag Value
Name	My User Pool

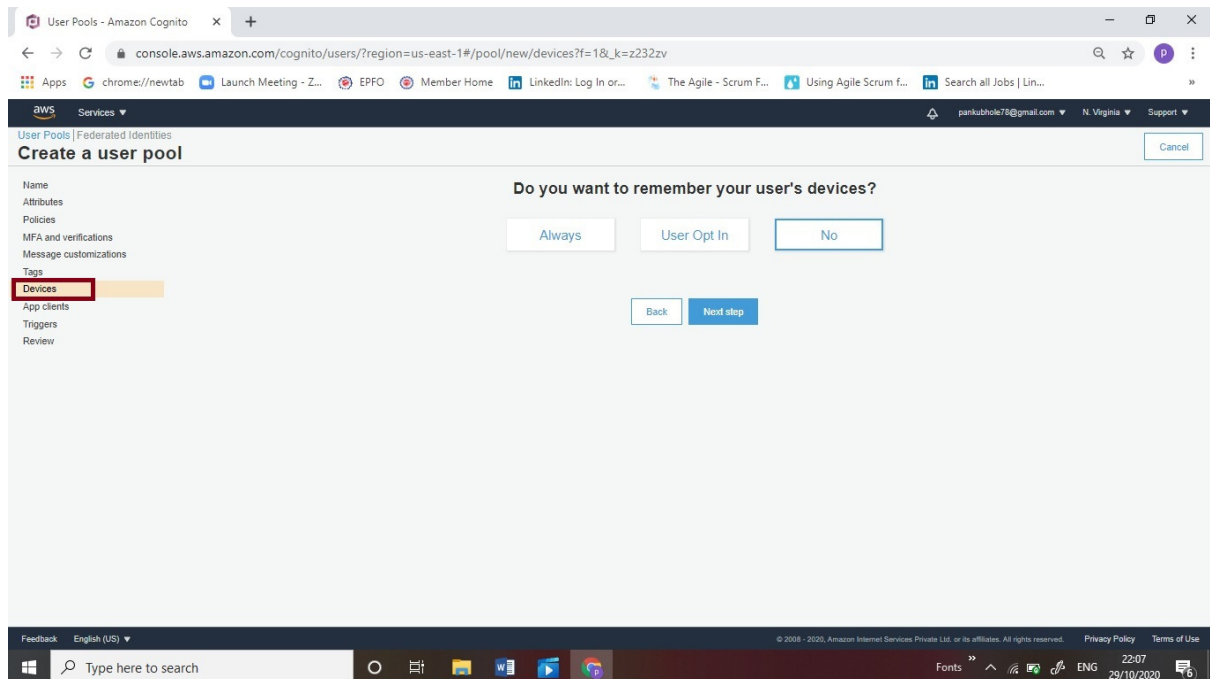
[Add another tag](#)

[Back](#) [Next step](#)

## 2. Click on Next Step

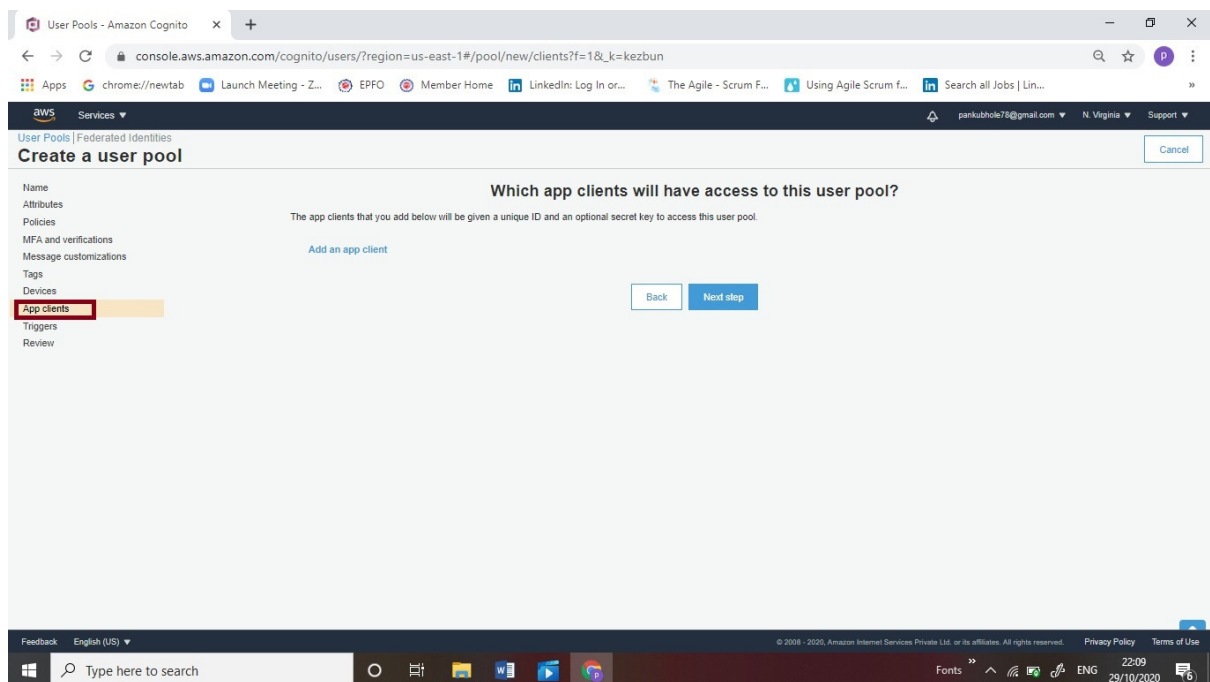
## Devices

- We can choose to remember our User's devices. Here, we choose **No** and click on Next step.



## App Client

The app clients that we add will be given a unique ID and an optional secret key to access this user pool. We are not using any App Client here, so we proceed to the click on Next Step.





# Customize Workflows

1. You can make advanced customizations with AWS Lambda functions. Pick AWS Lambda functions to trigger with different events if you want to customize workflows and user experience.
2. You can go through all the Events. We skip this and proceed to Customize Workflows
3. You can make advanced customizations with AWS Lambda functions. Pick AWS Lambda functions to trigger with different events if you want to customize workflows and user experience.
4. You can go through all the Events. We skip this and proceed to Next step

The screenshot shows the AWS IAM console interface for creating a user pool. The left sidebar contains a navigation menu with the following items: Name, Attributes, Policies, MFA and verifications, Message customizations, Tags, Devices, App clients, **Triggers** (highlighted with a red box), and Review. The main content area is titled 'Create a user pool' and features a sub-header 'Do you want to customize workflows with triggers?'. Below this, a paragraph explains that users can make advanced customizations with AWS Lambda functions. The page displays seven trigger configuration cards, each with a title, description, and a 'Lambda function' dropdown menu. The triggers are: Pre sign-up, Pre authentication, Custom message, Post authentication, Post confirmation, Define Auth Challenge, and Verify Auth Challenge Response. All dropdown menus are currently set to 'none'. At the bottom of the page, there is a footer with 'Feedback', 'English (US)', and copyright information.

aws Services

User Pools | Federated Identities

Create a user pool

Do you want to customize workflows with triggers?

You can make advanced customizations with AWS Lambda functions. Pick AWS Lambda functions to trigger with different events if you want to customize workflows and the user experience. Visit the [AWS Lambda console](#) to create your functions before selecting them below. [Learn more about triggers.](#)

**Pre sign-up**

This trigger is invoked when a user submits their information to sign up, allowing you to perform custom validation to accept or deny the sign up request.

Lambda function

none

**Pre authentication**

This trigger is invoked when a user submits their information to be authenticated, allowing you to perform custom validations to accept or deny the sign in request.

Lambda function

none

**Custom message**

This trigger is invoked before a verification or MFA message is sent, allowing you to customize the message dynamically. Note that static custom messages can be edited on the Verifications panel.

Lambda function

none

**Post authentication**

This trigger is invoked after a user is authenticated, allowing you to add custom logic, for example for analytics.

Lambda function

none

**Post confirmation**

This trigger is invoked after a user is confirmed, allowing you to send custom messages or to add custom logic, for example for analytics.

Lambda function

none

**Define Auth Challenge**

This trigger is invoked to initiate the custom authentication flow.

Lambda function

none

**Verify Auth Challenge Response**

This trigger is invoked to verify if the response from the end user for a custom

Feedback English (US)

© 2008 - 2020, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

## Review:

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

**Create a user pool**

Pool name: Demo User Pool

Required attributes: address, email, gender, name, phone\_number, profile

Alias attributes: Choose alias attributes...

Username attributes: email

Enable case insensitivity?: Yes

Custom attributes: Choose custom attributes...

Minimum password length: 8

Password policy: uppercase letters, lowercase letters, special characters, numbers

User sign ups allowed?: Only administrators can create users

FROM email address: Default

Email Delivery through Amazon SES: No

Note: You have chosen to have Cognito send emails on your behalf. Best practices suggest that customers send emails through Amazon SES for production User Pools due to a daily email limit. [Learn more about email best practices.](#)

MFA: Enable MFA...

Verifications: Email

Tags: Name

App clients: Add app client...

Triggers: Add triggers...

**Create pool**

2. You'll get a message as **Your user pool was created successfully**  
On the Top left, click on User Pools to see **Your User Pools**.

**User Pools | Federated Identities**

**Demo User Pool**

General settings

Users and groups

Attributes

Policies

MFA and verifications

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

Your user pool was created successfully.

Pool Id: us-east-1\_1sGEPHmG

Pool ARN: arn:aws:cognito-idp:us-east-1:810639665310:userpool:us-east-1\_1sGEPHmG

Estimated number of users: 0

Required attributes: name, profile, email, gender, phone\_number, address

Alias attributes: none

Username attributes: email

Enable case insensitivity?: Yes

Custom attributes: Choose custom attributes...

Minimum password length: 8

Password policy: uppercase letters, lowercase letters, special characters, numbers

User sign ups allowed?: Only administrators can create users

FROM email address: Default

Email Delivery through Amazon SES: No

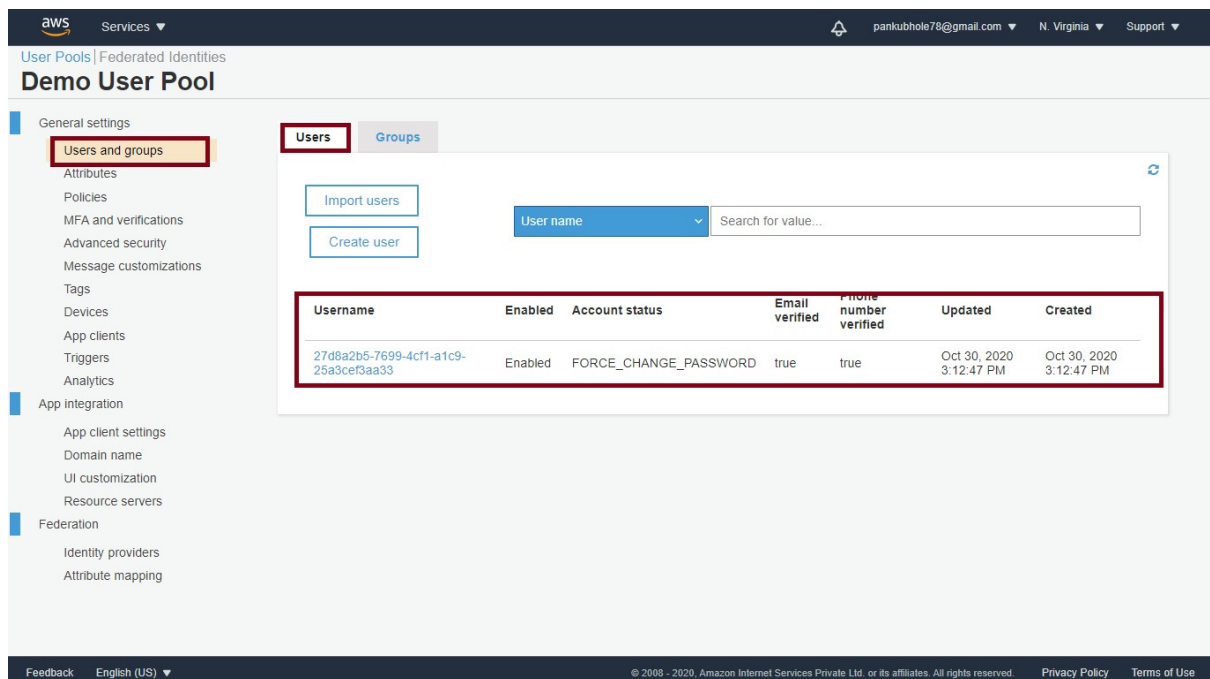
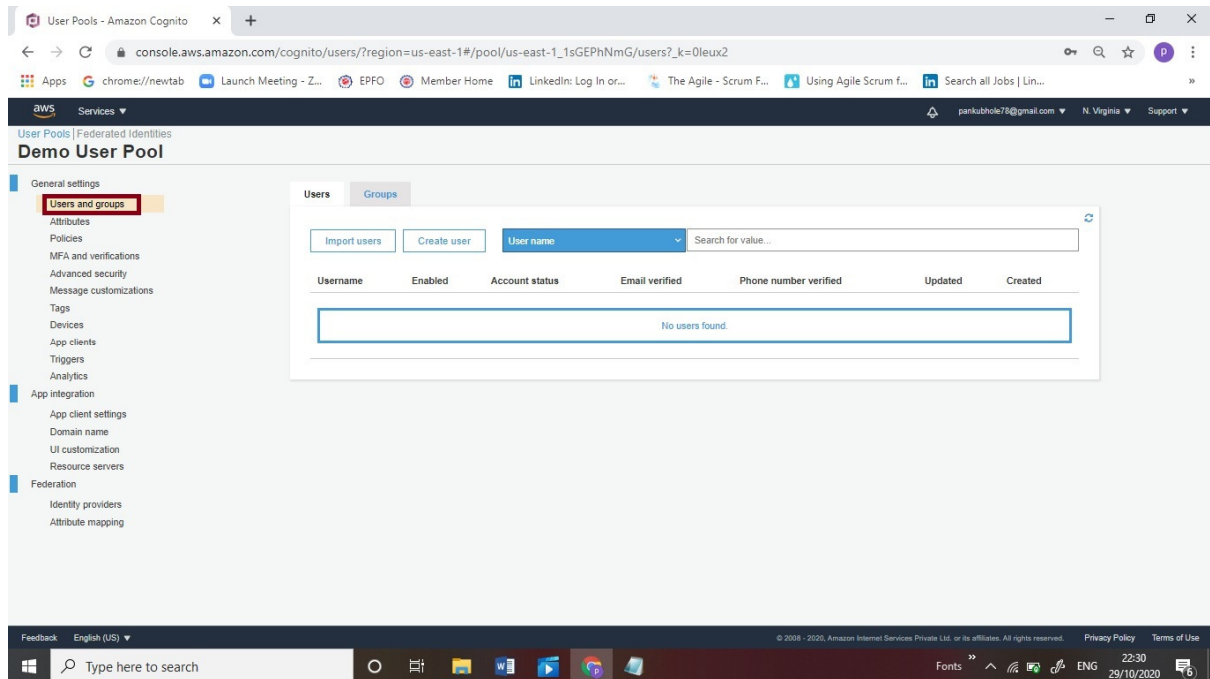
Note: You have chosen to have Cognito send emails on your behalf. Best practices suggest that customers send emails through Amazon SES for production User Pools due to a daily email limit. [Learn more about email best practices.](#)

MFA: Enable MFA...

Verifications: Email

Advanced security: Enable advanced security

3. Navigate to Cognito, click on **Users and groups** to navigate to the Users page as shown below.
4. Here, we can start creating Users and Groups.
5. From an Administrative perspective, if we have an application, the application would then invoke the Amazon Cognito to create User itself.



The screenshot displays the AWS IAM console interface for a 'Demo User Pool'. The left sidebar shows the 'Users and groups' section highlighted. The main content area has two tabs: 'Users' and 'Groups', with 'Groups' being the active tab. A 'Create group' button is visible. Below it, a table lists the groups. The table has five columns: 'Group Name', 'Description', 'Precedence', 'Updated', and 'Created'. One group is listed: 'Development' with description 'Developments', precedence '-', and both 'Updated' and 'Created' timestamps as 'Oct 30, 2020 3:13:18 PM'.

Group Name	Description	Precedence	Updated	Created
Development	Developments	-	Oct 30, 2020 3:13:18 PM	Oct 30, 2020 3:13:18 PM

## 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.