

# Introduction to Amazon Cognito

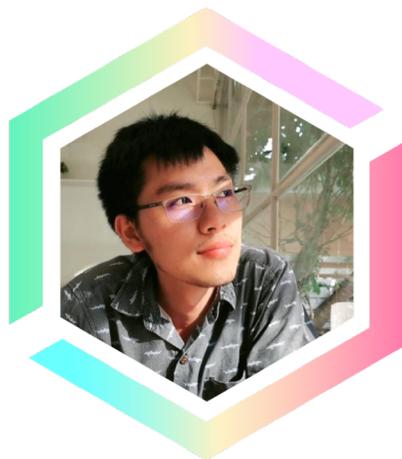
Vassanon Chotsittirit / Nattawat Kitticharoenjit  
AWS User Group Thailand



**JAWS-UG**  
AWS User Group - Japan



# Who are we ?



**Vassanon Chotsittirit**

Community Leader and  
Software Engineer at Dailitech, Bangkok



**Nattawat Kitticharoenjit**

Community Leader and  
Software Engineer at Dailitech, Bangkok

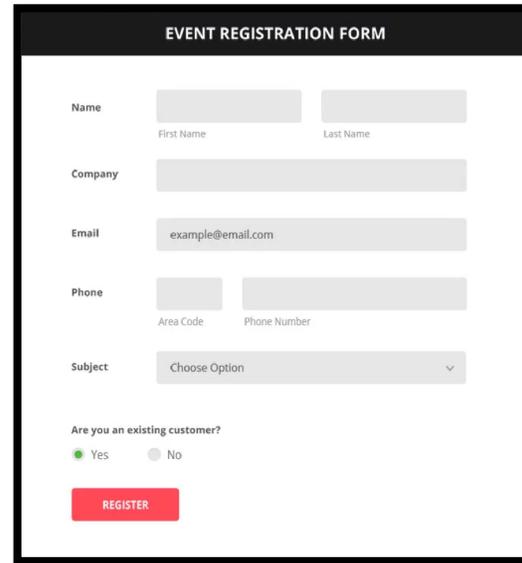
# Agenda

- Problem : Difficulty of User Management Development.
- Amazon Cognito
  - Introduction
  - Features
  - Scenarios
- Using Amazon Cognito in AWS Amplify
- Demo

# Problem : Difficulty of User Management Development

# Implementation many authentication flows

- Sign-Up
- Sign-In
- Forgot-Password
- Change-Password
- Verify Email
- Verify Phone Number
- MFA



EVENT REGISTRATION FORM

Name    
First Name Last Name

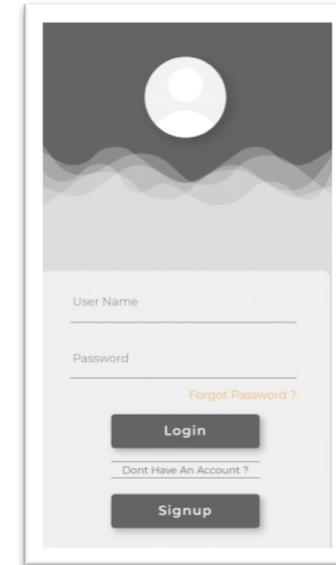
Company

Email

Phone    
Area Code Phone Number

Subject

Are you an existing customer?  
 Yes  No

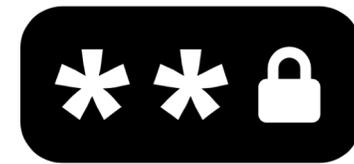


User Name

Password

[Forgot Password ?](#)

[Dont Have An Account ?](#)



# Have to support social login or enterprise login

- Facebook Log In
- Google Sign-In
- Sign in with Apple
- Connect with OpenID
- Enterprise Identity Provider



# Must do security for user data and APIs

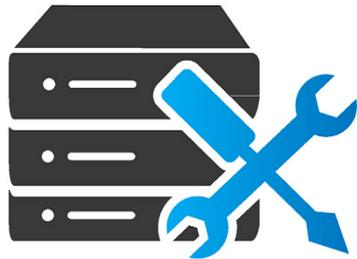
- Generate token-based (JWT)
- Manage token expiration
- Protect user data and passwords
- OAuth 2.0



# Infra needs to support Compliance Programs

- Infrastructure

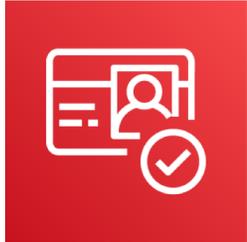
- Servers
- Databases
- Network



- Compliances

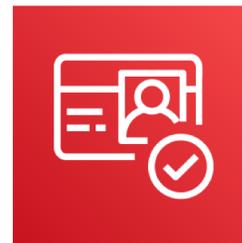
- HIPAA
- PCI DSS
- SOC
- ISO/IEC 27001





# Amazon Cognito

# Introduction to Amazon Cognito



**Amazon Cognito** is serverless authentication and user management for your application.



User Sign-Up, Sign-In

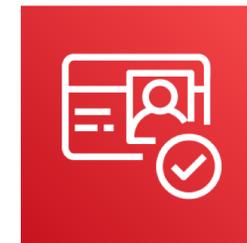


Secure and scalable user directory



Support Social Sign-In

# Introduction to Amazon Cognito



**Amazon Cognito** consist of 2 components.



**Cognito User Pools**



**Cognito Identity Pools**

# Amazon Cognito User Pools



**Amazon Cognito User Pools** : You can quickly create your own user directory to sign up and sign in users, and to store user profiles using Amazon Cognito User Pools.



Manage user directory

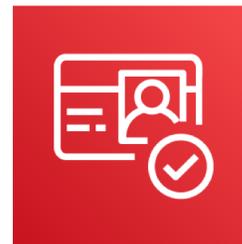


Integrate with social and enterprise IdP



Manage Token-based Auth

# Amazon Cognito Identity Pools



**Amazon Cognito Identity Pools** : You can control access to your backend AWS resources and APIs through Amazon Cognito Identity Pools so users of your app get only the appropriate access.



Unique Identities from multi IdP

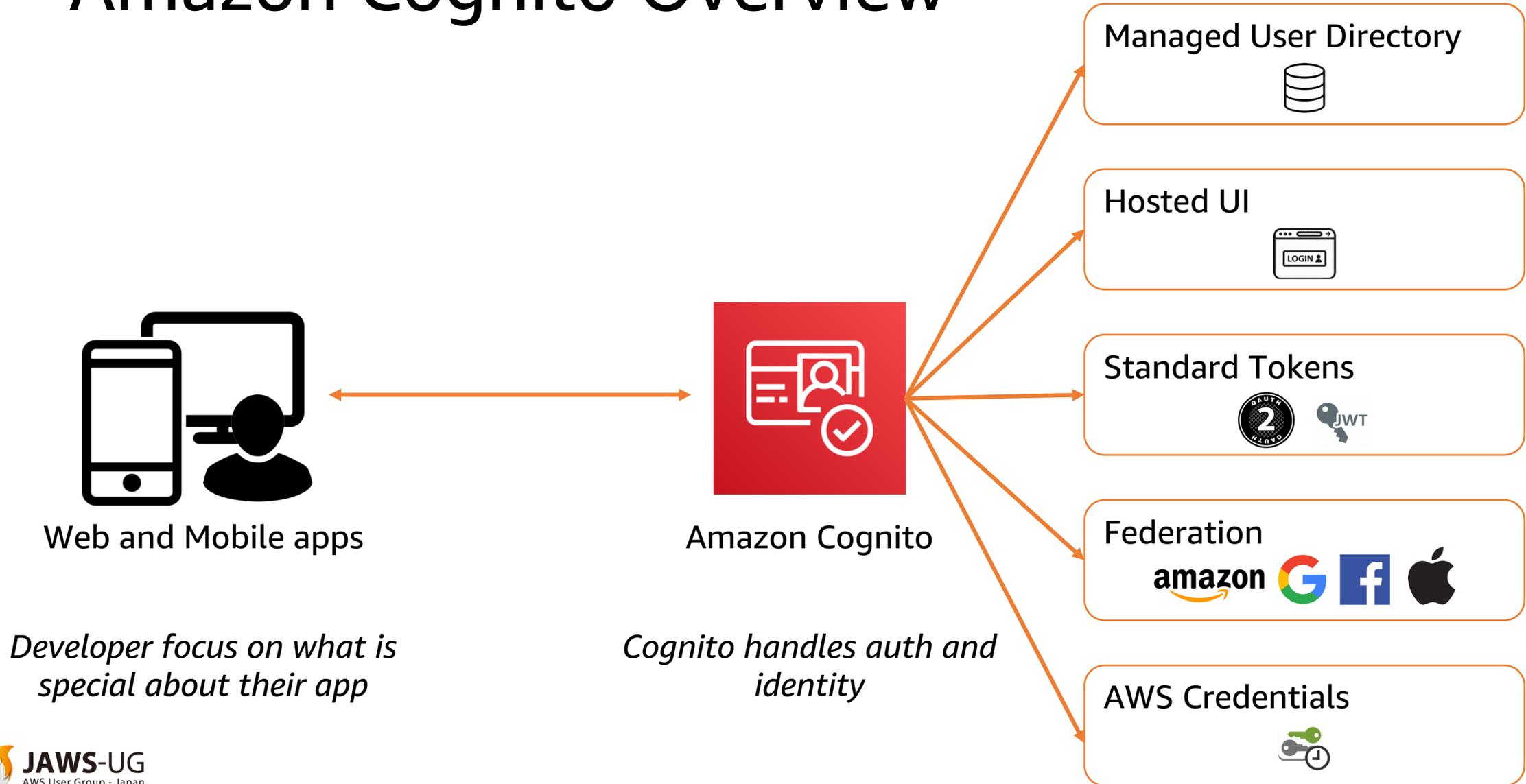


Provide temporary AWS credentials

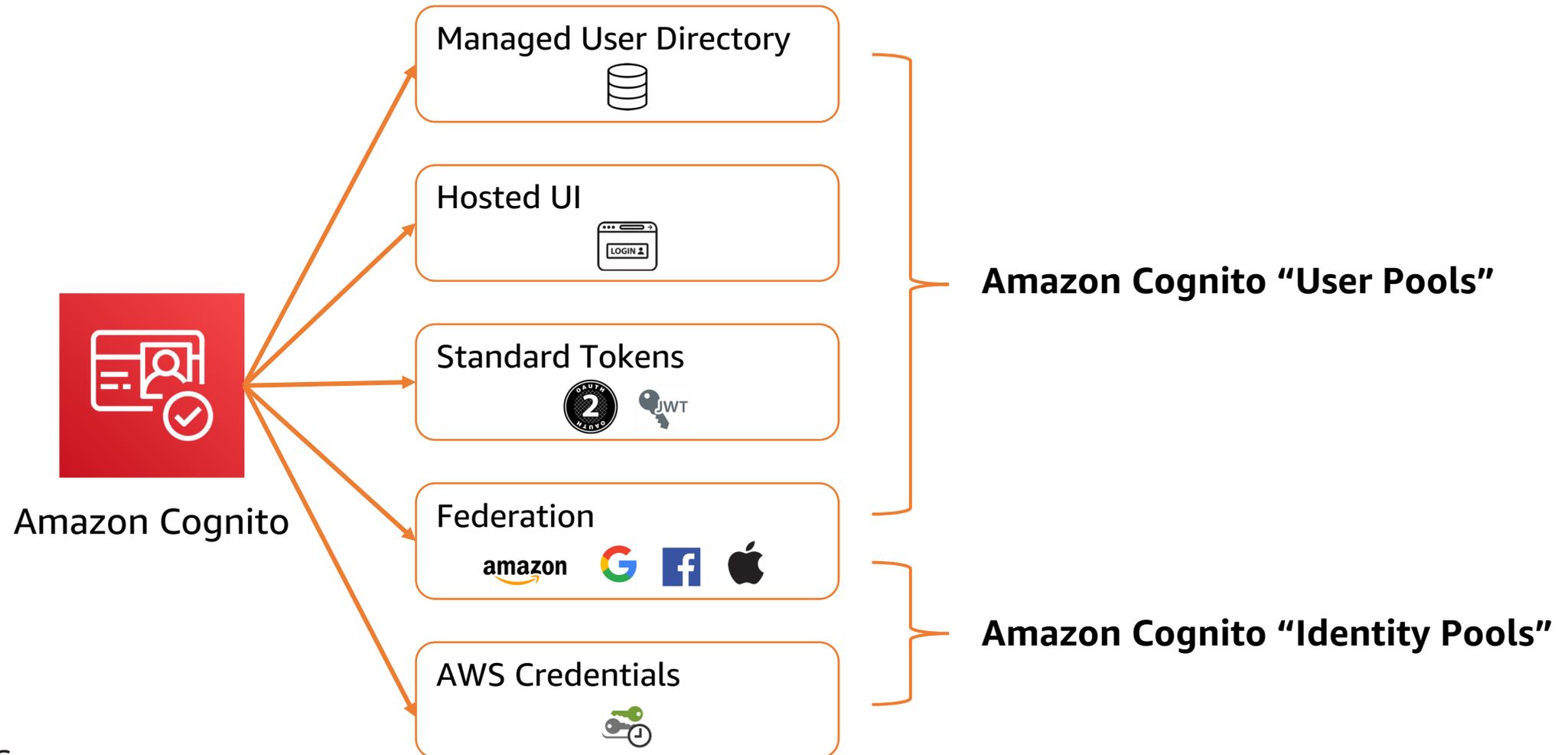


Map users to different role

# Amazon Cognito Overview



# Amazon Cognito Overview



# User Pools vs Identity Pools



Cognito User Pools	Cognito Identity Pools
Authentication	Authorization
Handles the IdP interactions for you	Provide AWS credentials for accessing resource on behalf of users
Provide profiles to manage users	Support rule to map user to different IAM roles
Provide OpenID Connect to OAuth2.0 standard tokens	Free
Priced per monthly active users	

# Features of Amazon Cognito User Pools

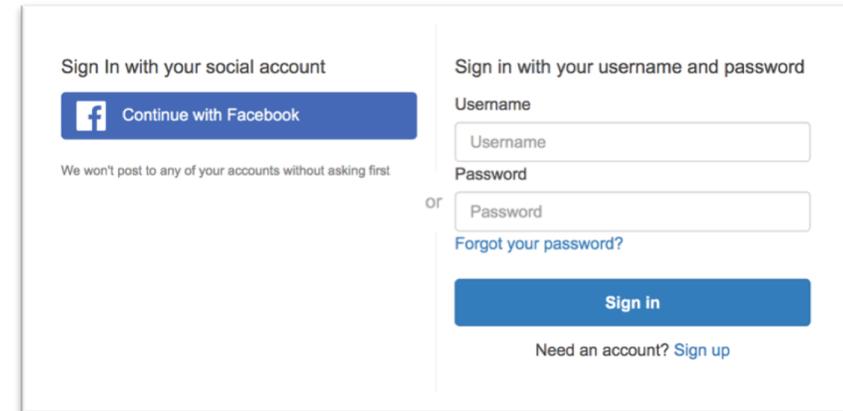
# Serverless Authentication and User Management

- User sign-in, sign-up
- Forget Password, Change Password
- Protected User Profile Data
- Email/Phone Number Verification
- Multi-Factor Authentication (MFA)

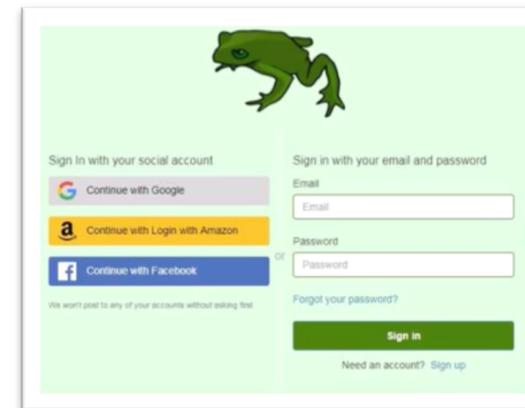


# Built-in Hosted UI for Sign-Up and Sign-In

- Define your domain
- Upload your own logo
- Customize CSS and style



This screenshot shows a default AWS-hosted sign-in interface. It is divided into two main sections. The left section, titled "Sign In with your social account", features a blue button labeled "Continue with Facebook" and a small disclaimer: "We won't post to any of your accounts without asking first". The right section, titled "Sign in with your username and password", contains input fields for "Username" and "Password", a "Forgot your password?" link, and a blue "Sign in" button. At the bottom, there is a link that says "Need an account? Sign up".



This screenshot shows a customized version of the AWS-hosted sign-in interface. The background is a light green color. At the top center, there is a green frog logo. The left section, titled "Sign In with your social account", includes three buttons: "Continue with Google" (grey), "Continue with Login with Amazon" (yellow), and "Continue with Facebook" (blue). Below these is the same disclaimer as in the default version. The right section, titled "Sign in with your email and password", has input fields for "Email" and "Password", a "Forgot your password?" link, and a green "Sign in" button. At the bottom, the link says "Need an account? Sign up".

# Integrate with social or enterprise Identity Providers

- Social sign-in (Facebook, Google, Apple, Amazon)
- OpenID Connect
- Enterprise identity provider (SAML 2.0)



**SAML**

# Managed Token-based Authentication

- JWT Token for your APIs
- Token Expiration



# Support for OAuth 2.0

- OAuth 2.0 flows
  - Authorization code
  - Implicit
  - Client credential
- Custom scope defined for resource server



# Features of Amazon Cognito Identity Pools

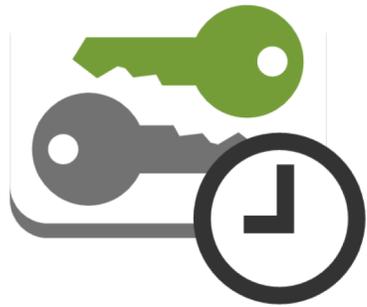
# Unique Identities from multi Identity Providers

- Facebook
- Google
- Twitter
- Apple
- SAML 2.0

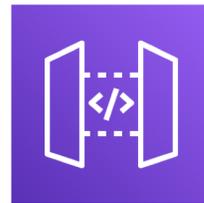


# Unique Identities from multi Identity Providers

- Access AWS Service
- Access Backend resources via APIs



S3



API Gateway



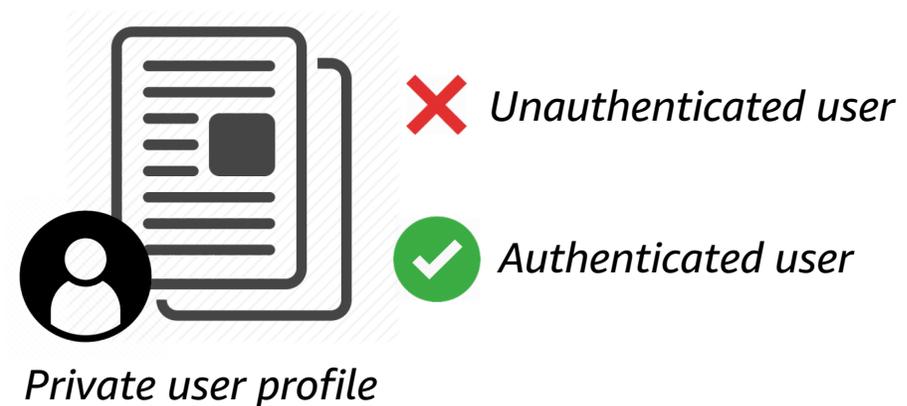
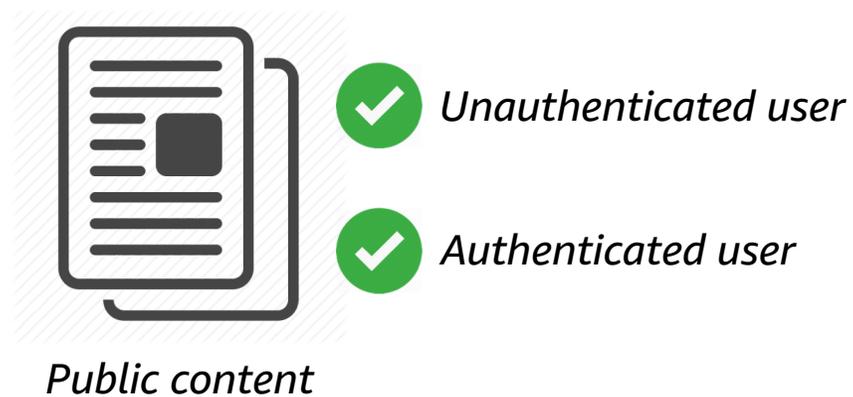
DynamoDB



AppSync

# Map users to difference role

- Unauthenticated Users
- Authenticated Users



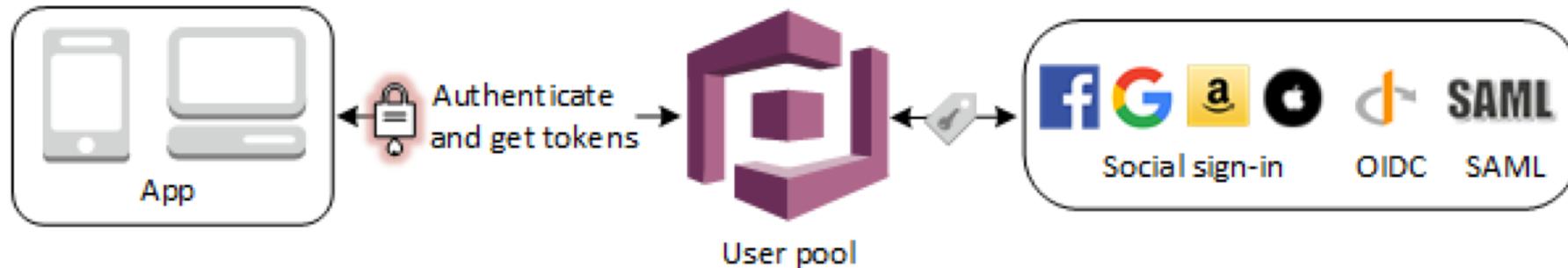
# Supports Multiple Compliance Programs

- HIPAA
- PCI DSS
- SOC
- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27018
- ISO 9001



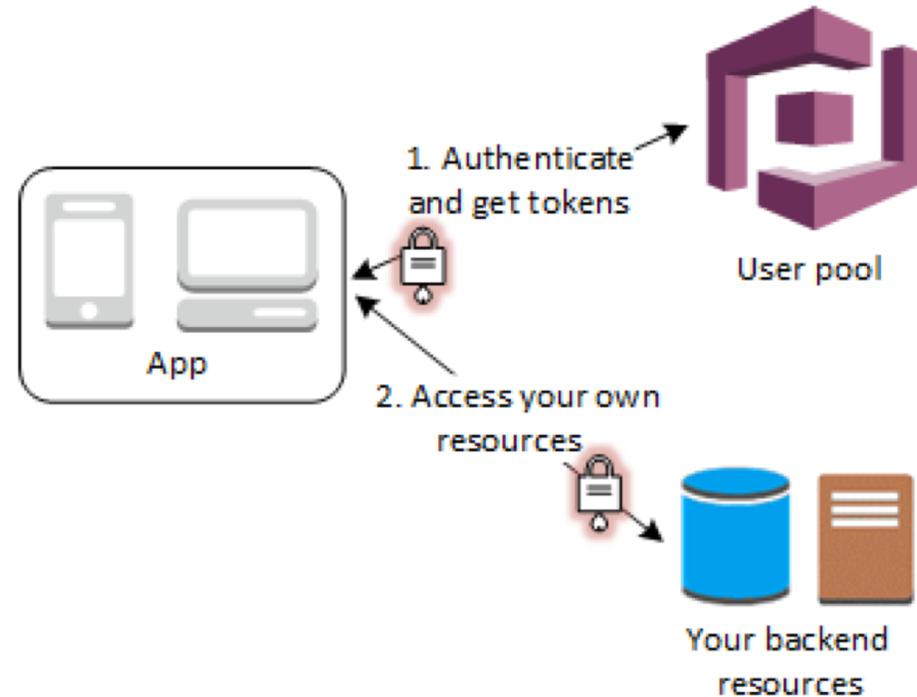
# Scenarios

# Authenticate with a User Pool



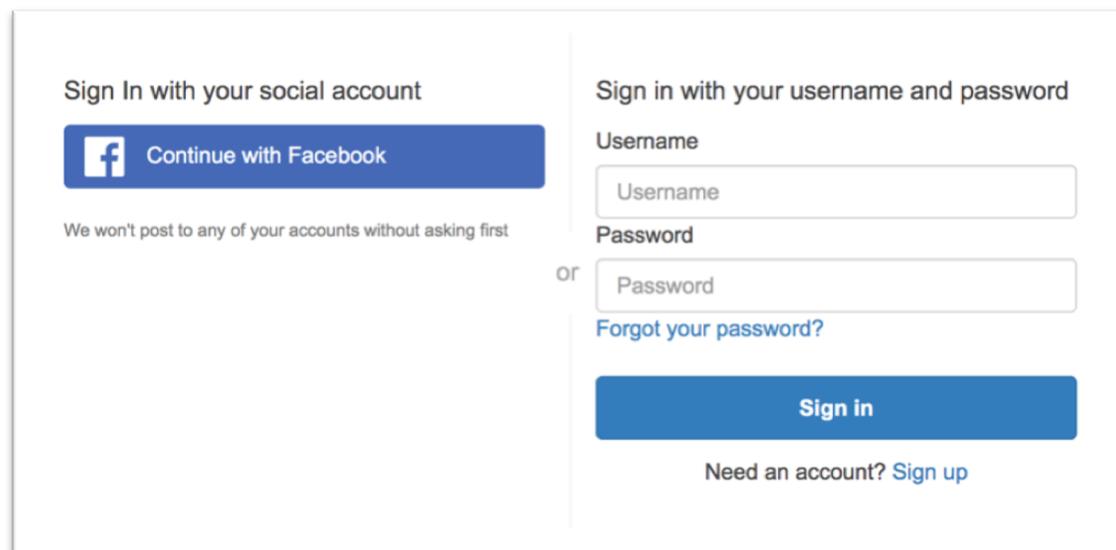
*Users can sign in either directly through a user pool, or federate through a third-party identity provider. (IdP)*

# Access Backend Resources with a User Pool



*You can use those tokens to control access to your backend resources.*

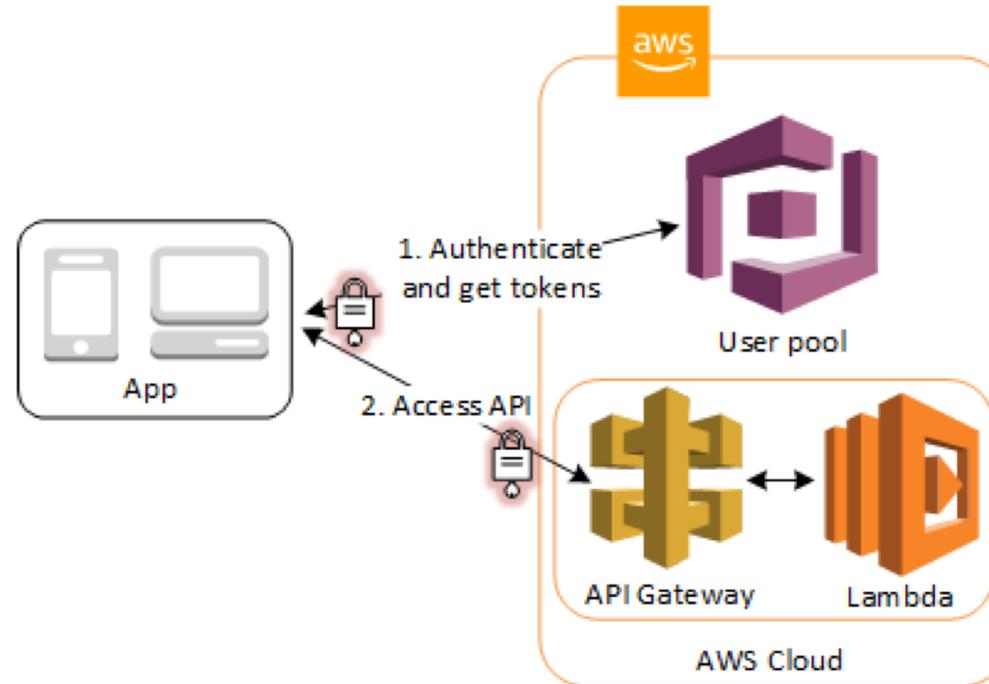
# Portal web UI for sign-up, sign-in



The image shows a web UI for sign-in, divided into two main sections. The left section is titled "Sign In with your social account" and features a blue button with the Facebook logo and the text "Continue with Facebook". Below this button, a smaller line of text reads "We won't post to any of your accounts without asking first". The right section is titled "Sign in with your username and password" and contains two input fields: "Username" and "Password". Below these fields is a blue "Sign in" button. A link "Forgot your password?" is positioned above the "Sign in" button. At the bottom of the right section, there is a link "Need an account? Sign up". The word "OR" is placed between the two main sections.

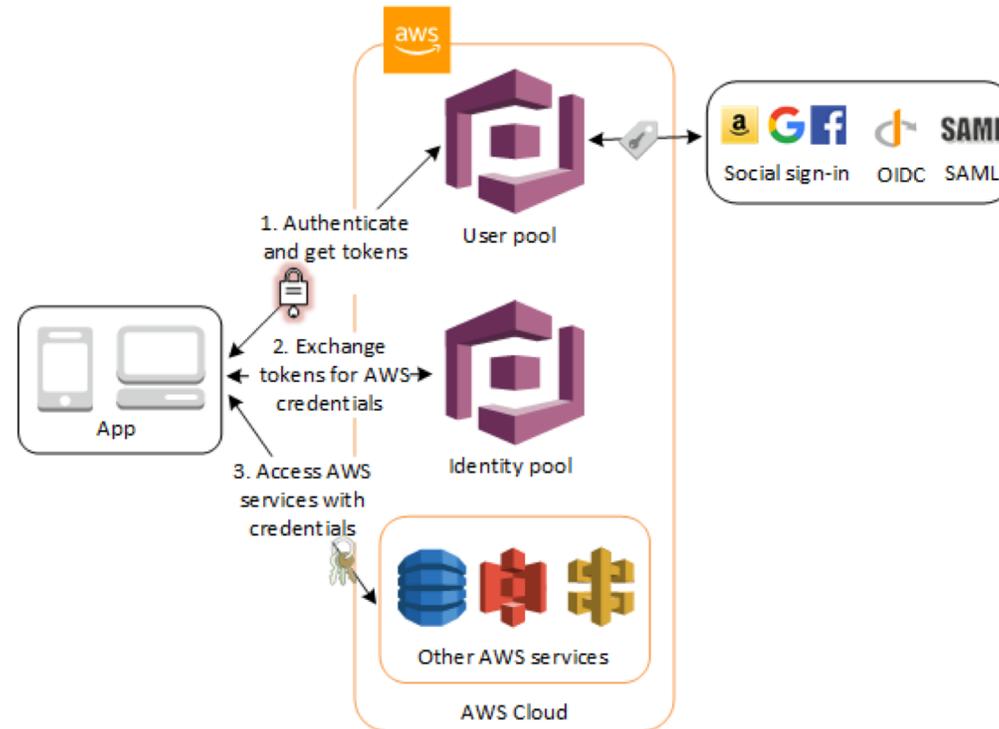
*Amazon Cognito provisions a hosted web UI that allows you to add sign-up and sign-in pages to your app.*

# Using a User Pool as an Authorizer API Gateway



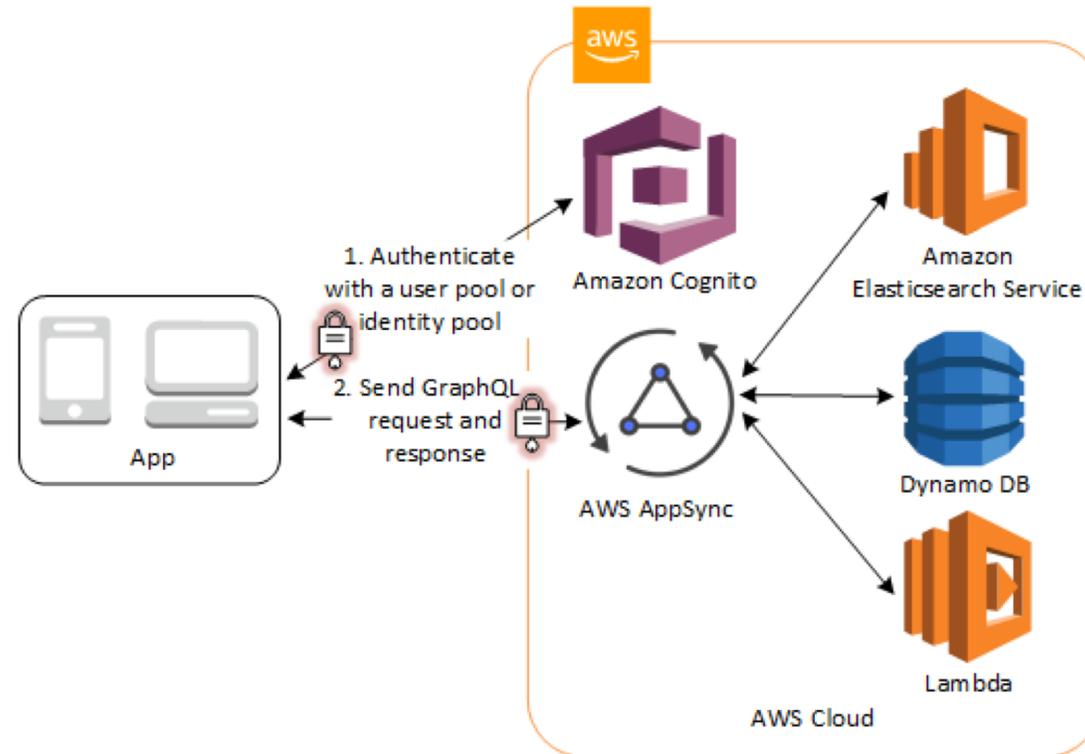
*API Gateway validates the tokens from a successful user pool authentication.*

# Access AWS Services with a User Pool and an Identity Pool



*Your app will receive user pool tokens from Amazon Cognito.  
You can exchange them for temporary access to other AWS services with an identity pool.*

# Access AWS AppSync Resources with Amazon Cognito



*You can grant your users access to AWS AppSync resources with tokens from a successful Amazon Cognito authentication.*

# Using Amazon Cognito on AWS Amplify

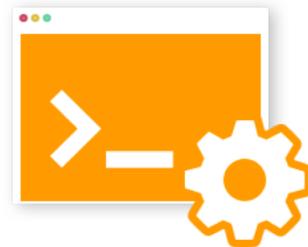
# Using Amazon Cognito on AWS Amplify



**AWS Amplify framework** : Amplify your apps. Build on a flexible, scalable, and reliable serverless backend



Easy-to-Use Library



Powerful Toolchain

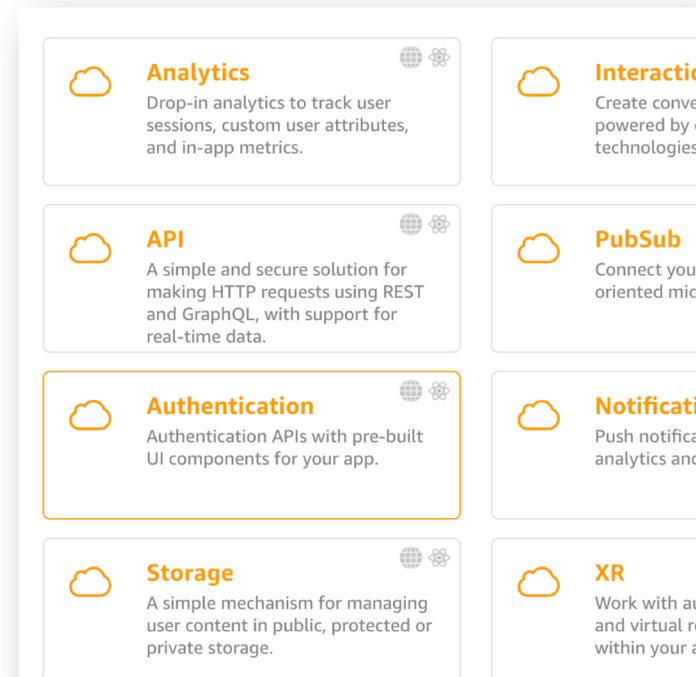


Beautiful UI Components

# Using Amazon Cognito on AWS Amplify



You can use Amazon Cognito via **Authentication module** in AWS Amplify framework.



For More information : <https://aws-amplify.github.io/docs/js/authentication>

# Using Amazon Cognito on AWS Amplify



- Sample code

JavaScript

```
1 // Add 'aws-amplify' library into your application
2
3 // Configure Auth category with your Amazon Cognito credentials
4 Amplify.configure({
5   Auth: {
6     identityPoolId: 'XX-XXXX-X:XXXXXXXXX-XXXX', // Amazon Cognito
7     region: 'XX-XXXX-X', // Amazon Cognito Region
8   }
9 });
10
11 // Call Auth.signIn with user credentials
12 Auth.signIn(username, password)
13   .then(user => console.log(user))
14   .catch(err => console.log(err));
```

# Demo

# Create a user pool : Set pool name

User Pools | Federated Identities

**Create a user pool** Cancel

**Name**

Attributes

Policies

MFA and verifications

Message customizations

Tags

Devices

App clients

Triggers

Review

## What do you want to name your user pool?

Give your user pool a descriptive name so you can easily identify it in the future.

Pool name

## How do you want to create your user pool?

**Review defaults**

Start by reviewing the defaults and then customize as desired

**Step through settings**

Step through each setting to make your choices

# Create a user pool : Set attributes

User Pools | Federated Identities

## Create a user pool

Cancel

Name

**Attributes**

Policies

MFA and verifications

Message customizations

Tags

Devices

App clients

Triggers

Review

You can't change the sign-in and attribute options on this page after you've created your user pool. Make sure that you've decided on the settings that you want.

### 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

You can choose to have users sign in with an email address, phone number, username or preferred username plus their password.

# Create a user pool : Set attributes

**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 type="checkbox"/>	address	<input type="checkbox"/>	nickname
<input type="checkbox"/>	birthdate	<input type="checkbox"/>	phone number
<input type="checkbox"/>	email	<input type="checkbox"/>	picture
<input type="checkbox"/>	family name	<input type="checkbox"/>	preferred username
<input type="checkbox"/>	gender	<input 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 type="checkbox"/>	name		

**Do you want to add custom attributes?**

Enter the name and select the type and settings for custom attributes.

[Add custom attribute](#)

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

You can choose required attributes for sign-up or add custom attributes

# Create a user pool : Set Policies

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**

- 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**

# Create a user pool : Enable MFA

The screenshot shows the 'Create a user pool' page in the AWS IAM console. The left sidebar contains navigation links: Name, Attributes, Policies, **MFA and verifications** (highlighted), Message customizations, Tags, Devices, App clients, Triggers, and Review. The main content area is titled 'Create a user pool' and features a 'Cancel' button in the top right corner. A red rectangular box highlights the 'Do you want to enable Multi-Factor Authentication (MFA)?' section. This section includes a descriptive paragraph about MFA, a note about separate charges for text messages, and three radio button options: 'Off' (selected), 'Optional', and 'Required'. Below this, the 'How will a user be able to recover their account?' section is visible, with a descriptive paragraph and five radio button options for account recovery methods.

User Pools | Federated Identities

## Create a user pool

Cancel

### 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

Off : Disable

Optional : Individual users can have MFA enabled.

Required: All users must use MFA.

# Create a user pool : Set Verifications

**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

Create role

You can choose the preferred way to send verification codes.

You can choose the verify attributes.

You must provide a role to allow Amazon Cognito to send SMS messages in verification flow.

# Create a user pool : Message customizations

**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)

You can customize FROM and REPLY-TO email address for verification email.

If you choose Yes, Cognito will send emails through your Amazon SES configuration.

# Create a user pool : Message customizations

**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

**Email message**  
Your verification code is {###}.

You can customize the message above and include HTML tags, but it must include the "{###}" placeholder, which will be replaced with the code.

**Do you want to customize your user invitation messages?**

**SMS message**  
Your username is {username} and temporary password is {###}.

You can customize the message above and include HTML tags, but it must include the "{username}" and "{###}" placeholder, which will be replaced with the username and temporary password respectively.

**Email subject**  
Your temporary password

**Email message**  
Your username is {username} and temporary password is {###}.

You can customize the message above and include HTML tags, but it must include the "{username}" and "{###}" placeholder, which will be replaced with the username and temporary password respectively.

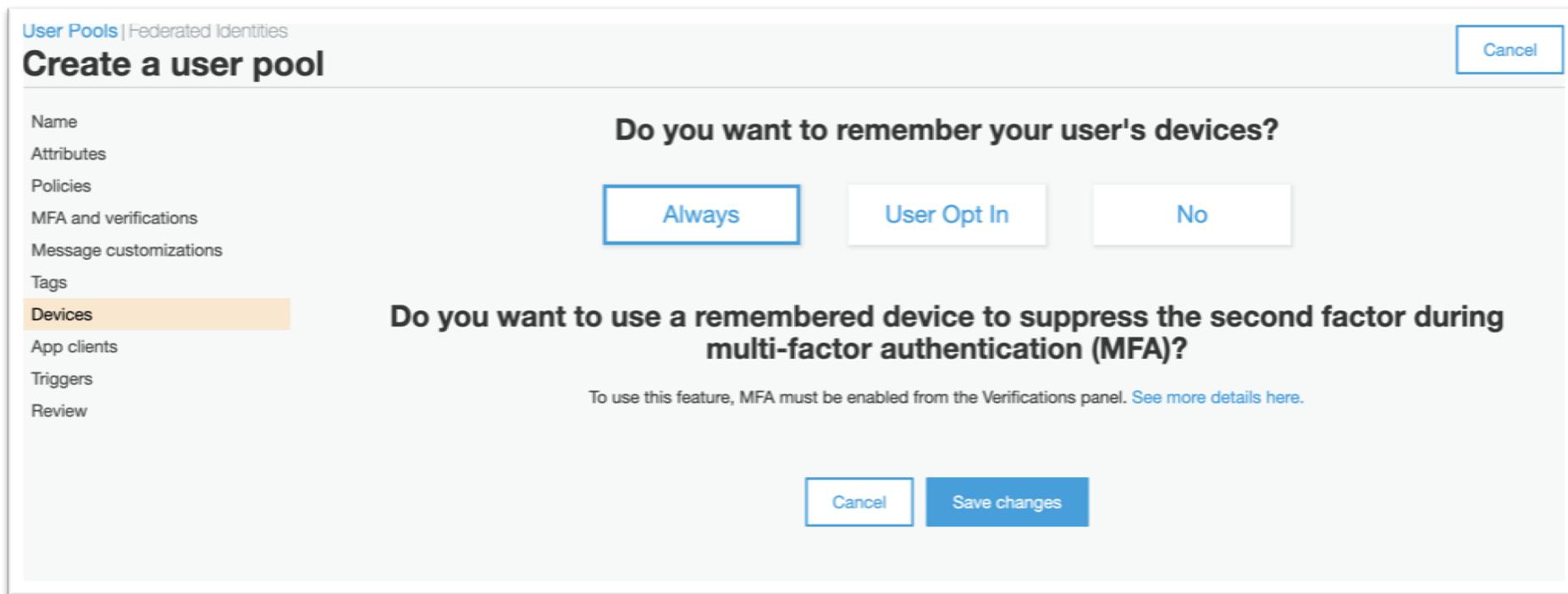
You can customize your email verification messages.

- Code or Link
- Email Subject
- Email Message

You can customize your email invitation messages.

- SMS Message
- Email Subject
- Email Message

# Create a user pool : Remember user's devices



The screenshot shows the 'Create a user pool' wizard in the AWS IAM console. The 'Devices' step is highlighted in the left-hand navigation menu. The main content area contains two questions:

**Do you want to remember your user's devices?**

Buttons: **Always** (selected), **User Opt In**, **No**

**Do you want to use a remembered device to suppress the second factor during multi-factor authentication (MFA)?**

To use this feature, MFA must be enabled from the Verifications panel. [See more details here.](#)

Buttons: **Cancel**, **Save changes**

Amazon Cognito can track and remember devices that users in a user pool use for sign-in

Learn more : <https://aws.amazon.com/blogs/mobile/tracking-and-remembering-devices-using-amazon-cognito-your-user-pools>

# Create a user pool : Add an app clients

App client name  
jaws-day-app

Refresh token expiration (days)  
30

Generate client secret

Auth Flows Configuration

Enable username password auth for admin APIs for authentication (ALLOW\_ADMIN\_USER\_PASSWORD\_AUTH) [Learn more.](#)

Enable lambda trigger based custom authentication (ALLOW\_CUSTOM\_AUTH) [Learn more.](#)

Enable username password based authentication (ALLOW\_USER\_PASSWORD\_AUTH) [Learn more.](#)

Enable SRP (secure remote password) protocol based authentication (ALLOW\_USER\_SRP\_AUTH) [Learn more.](#)

Enable refresh token based authentication (ALLOW\_REFRESH\_TOKEN\_AUTH) [Learn more.](#)

Prevent User Existence Errors [Learn more.](#)

Legacy

Enabled (Recommended)

[Set attribute read and write permissions](#)

Set app client name

Set expiration days for refresh-token

Enable Auth flows configuration.

Learn more

<https://docs.aws.amazon.com/cognito/latest/developerguide/user-pool-settings-client-apps.html>

The app clients that you add below will be given a unique ID and an optional secret key to access this user pool.

# Create a user pool : Trigger events

User Pools | Federated Identities

## Create a user pool

Cancel

Name

Attributes

Policies

MFA and verifications

Message customizations

Tags

Devices

App clients

**Triggers**

Review

### 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

**Post authentication**

This trigger is invoked after a user is authenticated, allowing

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

# Create a user pool : Review and Confirm

User Pools | Federated Identities

**Create a user pool** Cancel

**Name**

**Attributes** **Pool name** jaws-day-pool

**Policies**

**MFA and verifications**

**Message customizations**

**Tags**

**Devices**

**App clients**

**Triggers**

**Review**

**Required attributes** [Choose required attributes...](#)

**Alias attributes** [Choose alias attributes...](#)

**Username attributes** [Choose username attributes...](#)

**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?** Users can sign themselves up

**FROM email address** Default

# App Integration : Set domain name and add Hosted web UI

User Pools | Federated Identities

## jaws-day-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

Domain Add domain...

Custom domain Add domain...

UI Customization Add app client...

Resource server Enable resource servers...

### 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.](#)

**Amazon Cognito domain**

Prefixed domain names can only contain lower-case letters, numbers, and hyphens. [Learn more about domain prefixes.](#)

Domain prefix

https://  .auth.ap-southeast-1.amazonaws.com

**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.](#)

You must first create app clients for this user pool before you can configure the settings here. Visit the App clients tab to create app clients.

### 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.](#)

There has to be an existing domain associated with this user pool. (Service: AWSCognitoIdentityProviderService; Status Code: 400; Error Code: InvalidParameterException; Request ID: cff5046a-bd90-4895-ab0d-a41aa8909b9c)

App client to customize

Defaults for all clients without individual settings

Logo (optional)

or drag a file here

Up to 100 KB in size.

# Federation : Identity Providers

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

## Do you want to allow users to sign in through external federated identity providers?

Select and configure the external identity providers you want to enable. You will also need to choose which identity providers to enable for each app on the Apps settings tab under App integration. [Learn more about identity federation with Cognito User Pools.](#)

 Facebook

 Google

 Login with Amazon

 Sign in with Apple

 SAML

 OpenID Connect

[Go to summary](#) [Configure attribute mapping](#)

### Facebook

You can allow your users to sign in to your app using their Facebook account. [Learn more about Facebook sign in.](#)

**Facebook app ID**  
1234567890123456

**App secret**  
123456789b00def123456a12345678d1

**Authorize scope**  
public\_profile,email

[Enable Facebook](#)

### Google

You can allow your users to sign in to your app using their Google account. [Learn more about Google sign in.](#)

**Google app ID**  
123456789012-abc3de23f4erd6abcdcfghi0987m1n1.apps.googleusercontent.com

**App secret**  
wrtYhy9HdYUlwhtpxPOIU1cb

**Authorize scope**  
profile email openid

[Enable Google](#)

### Sign in with Apple

You can allow your users to sign in to your app using their Apple ID. [Learn more about Sign in with Apple](#)

**Apple services ID**  
com.yourapp.auth

**Team ID**  
1N2ABCWXYZ

**Key ID**  
123A4B56CD

**Private key**  
[Select file](#) or Copy and paste Apple-provided private key

**Authorize scope**  
Unlike most OpenID Connect providers, Apple only provides scopes on the first user sign-in for a services ID, for privacy reasons. [Learn more about the possible implications](#)

Email  Name

[Enable Sign in with Apple](#)

# Thank you