Introduction to Amazon Cognito

Vassanon Chotsittirit / Nattawat Kitticharoenjit
AWS User Group Thailand

JAWS-UG
AWS User Group - Japan

aws USER GROUP • THAILAND

Who are we ?

Vassanon Chotsittirit

Community Leader and
Software Engineer at Dailitech, Bangkok

Nattawat Kitticharoenjit

Community Leader and
Software Engineer at Dailitech, Bangkok

JAWS-UG
AWS User Group - Japan

aws USER GROUP • THAILAND

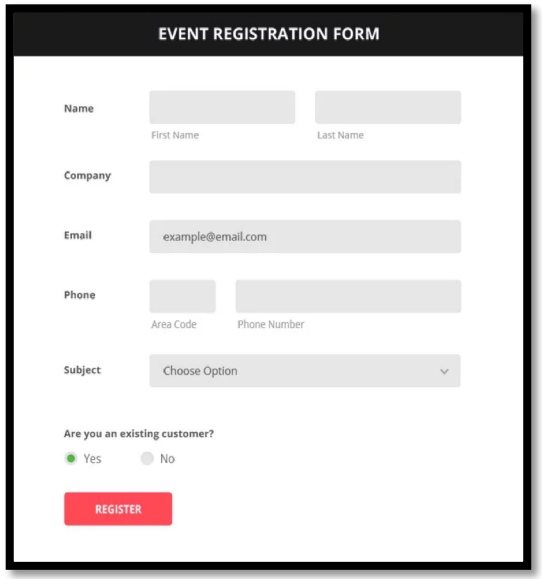
Agenda

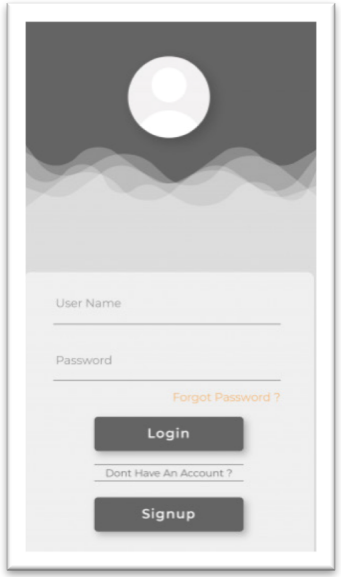
- Problem : Difficulty of User Management Development.
- Amazon Cognito
  - Introduction
  - Features
  - Scenarios
- Using Amazon Cognito in AWS Amplify
- Demo

Problem :
Difficulty of User Management Development

Implementation many authentication flows

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





Have to support social login or enterprise login

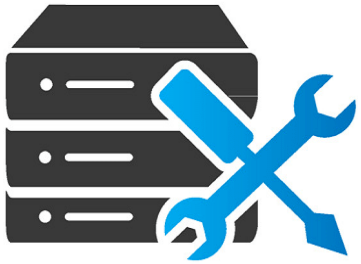
- Facebook Log In
- Google Sign-In
- Sign in with Apple
- Connect with OpenID
- Enterprise Identity Provider

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

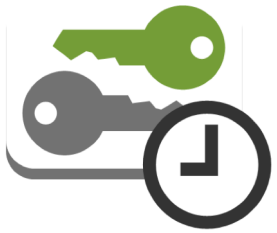
Integrate with social and enterprise IdP

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.

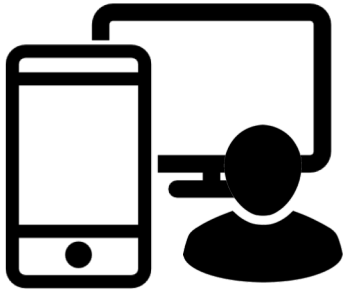
Unique Identities from multi IdP



Provide temporary AWS credentials

Map users to difference role

Amazon Cognito Overview



Web and Mobile apps

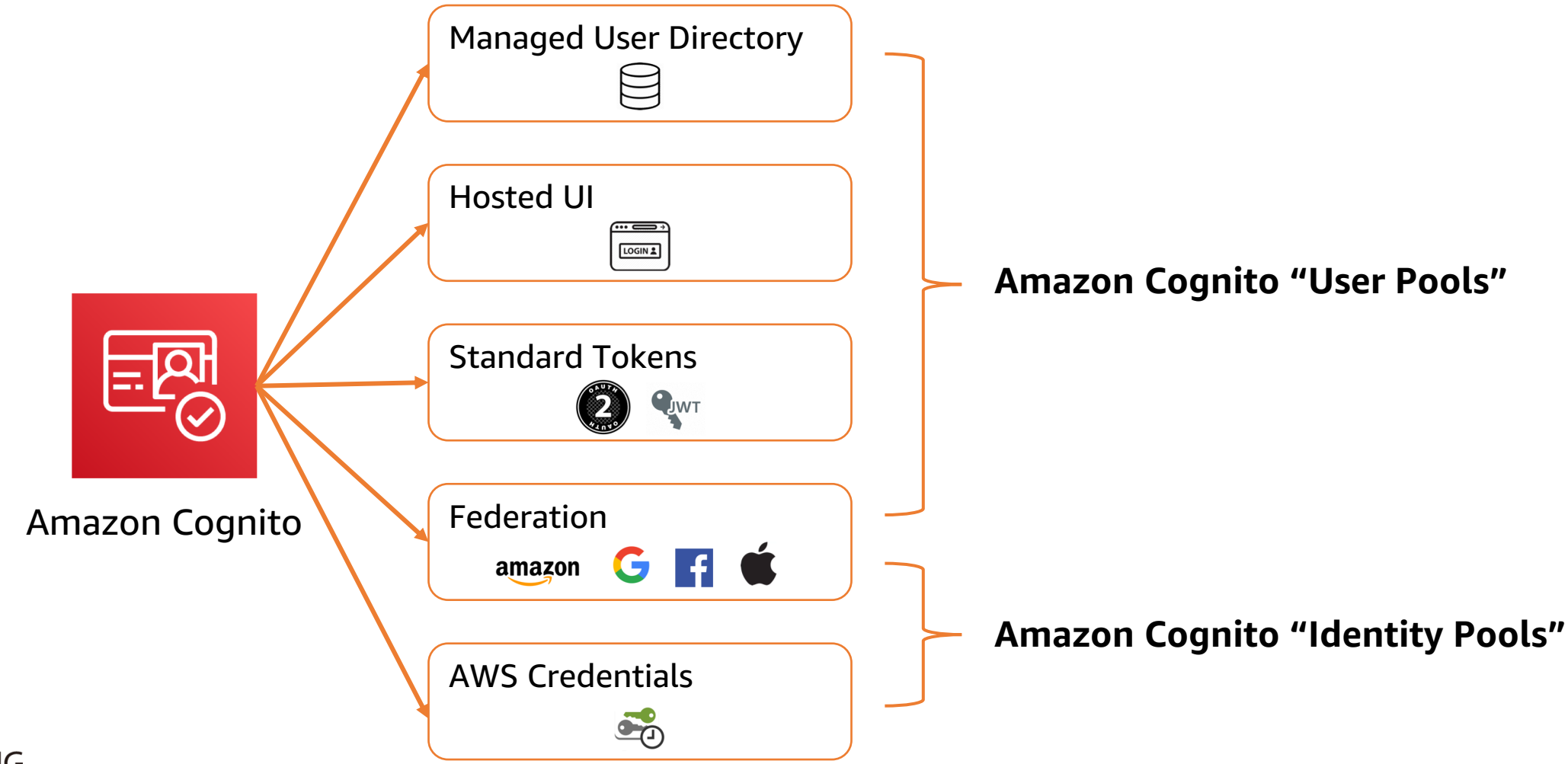
Developer focus on what is special about their app

Amazon Cognito

Cognito handles auth and identity

- Managed User Directory
- Hosted UI
- Standard Tokens
- Federation
- AWS Credentials

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	

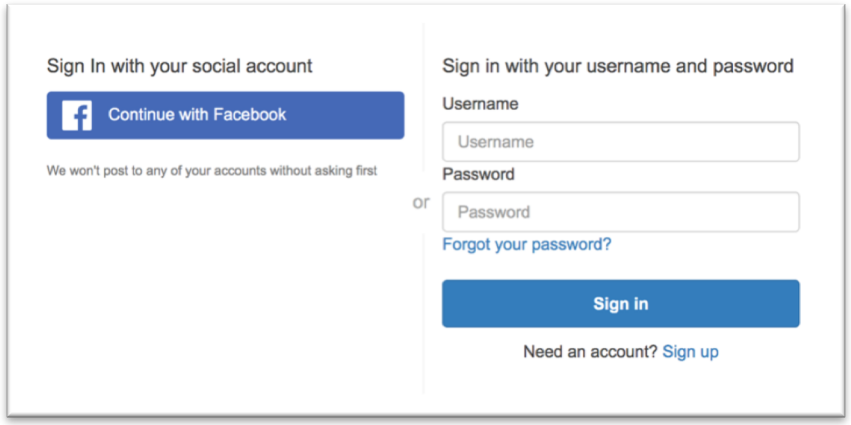
Features of Amazon Cognito **User Pools**

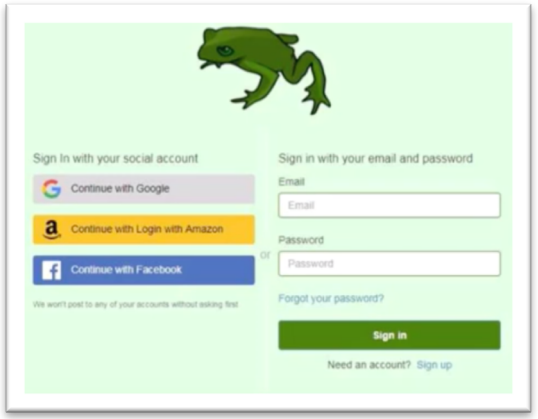
Serverless Authentication and User Management

- 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





Integrate with social or enterprise Identity Providers

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

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

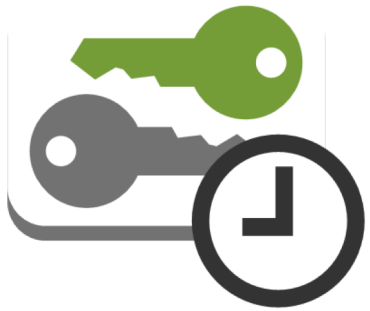
Features of Amazon Cognito **Identity Pools**

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

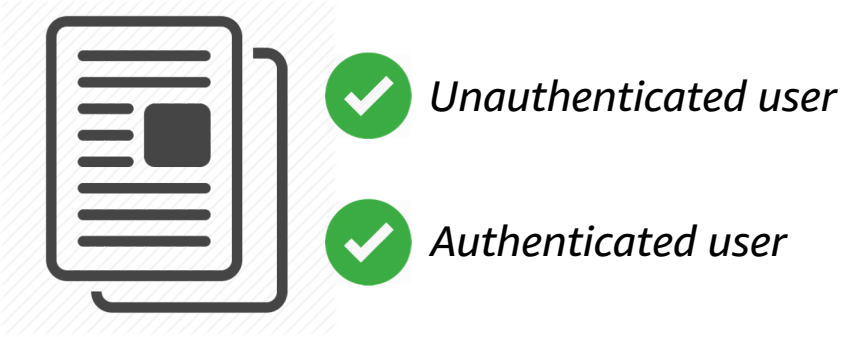
API Gateway

DynamoDB

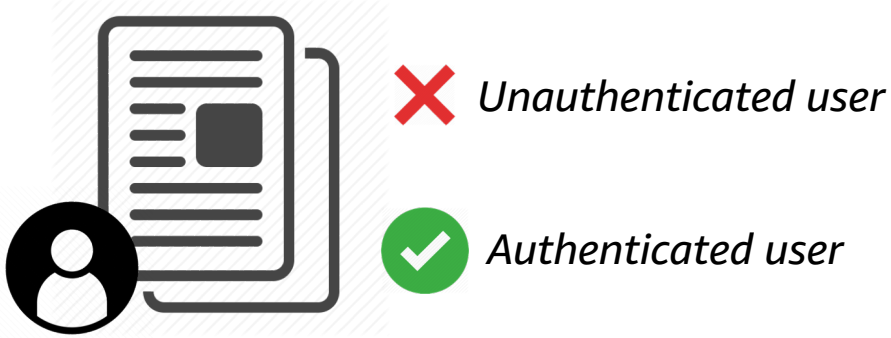
AppSync

Map users to difference role

- Unauthenticated Users
- Authenticated Users



Public content



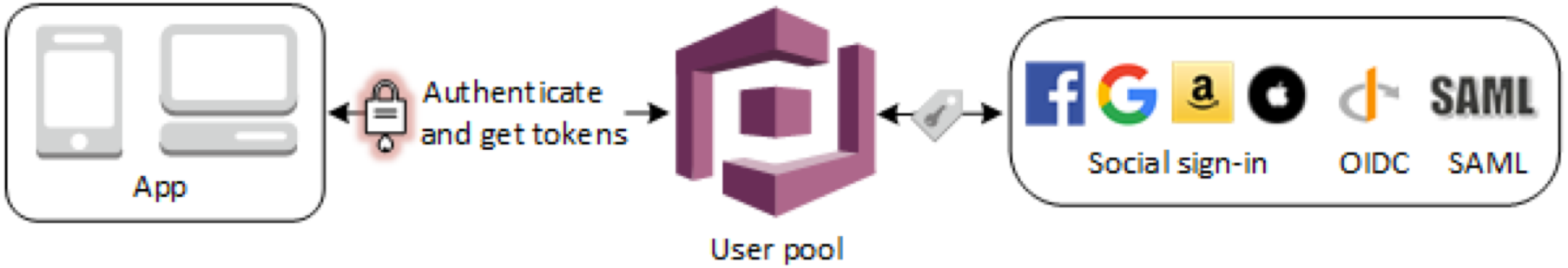
Private user profile

Supports Multiple Compliance Programs

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

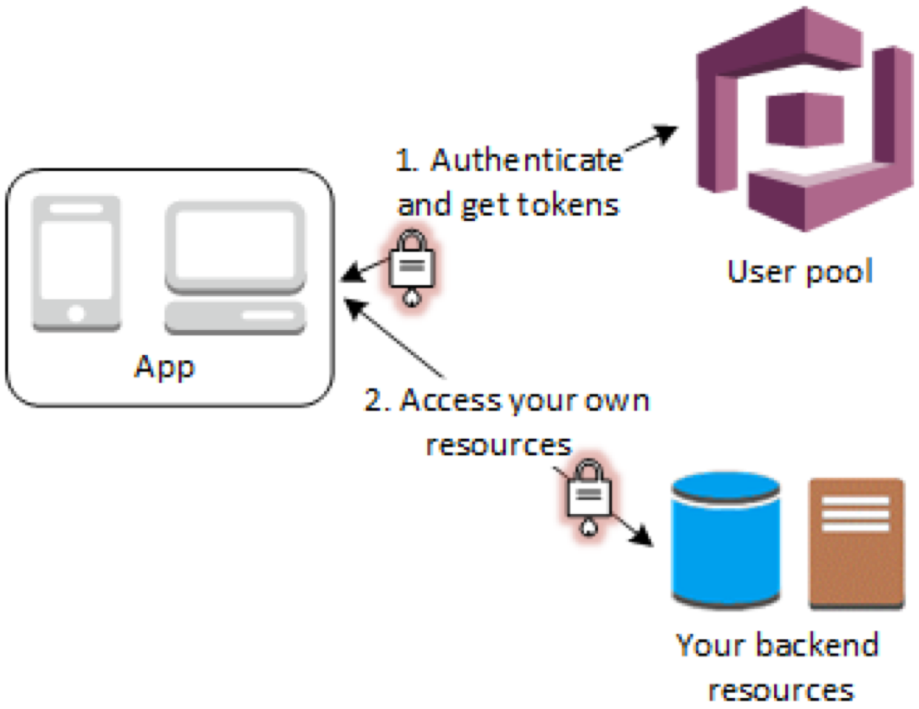
Scenarios

Authenticate with a User Pool



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

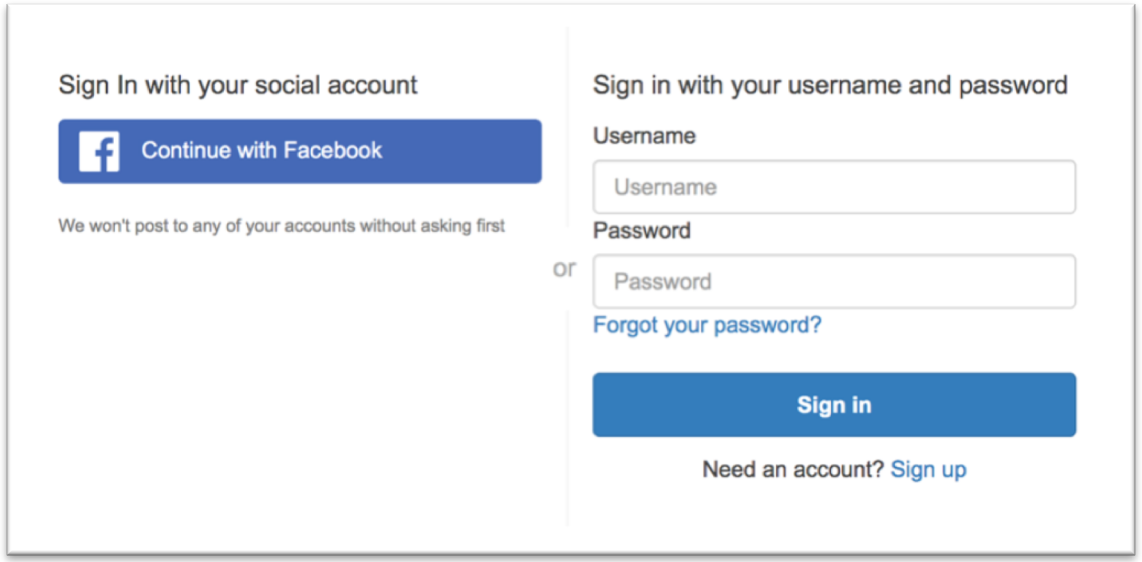
Access Backend Resources with a User Pool



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

For more information on using groups to control access your resources see
https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-user-groups.html

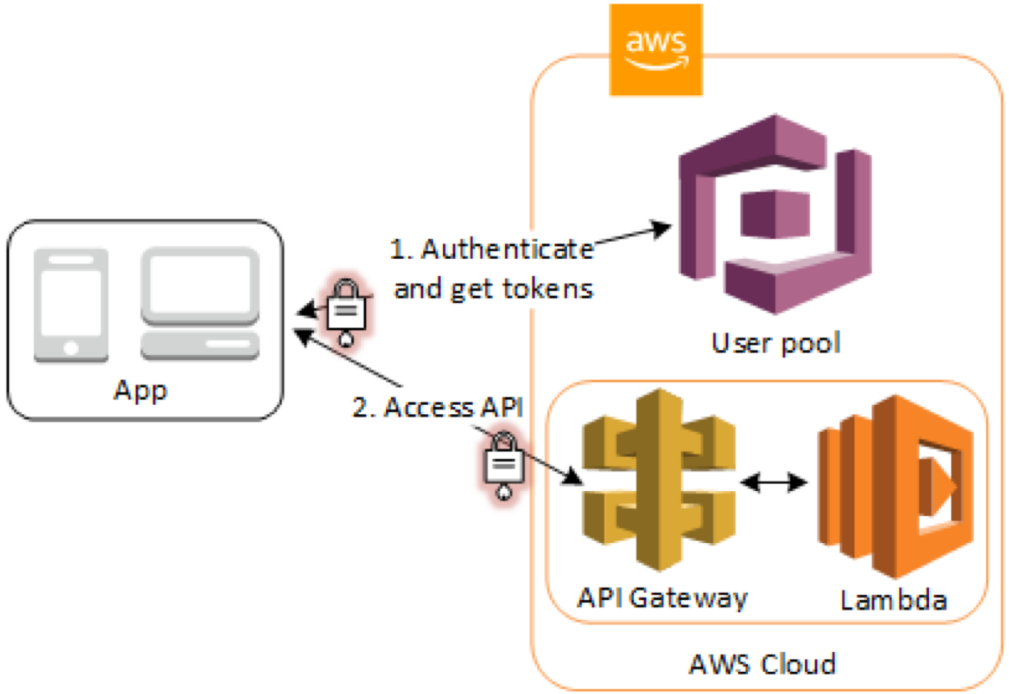
Portal web UI for sign-up, sign-in



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

For more information : https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-pools-app-integration.html

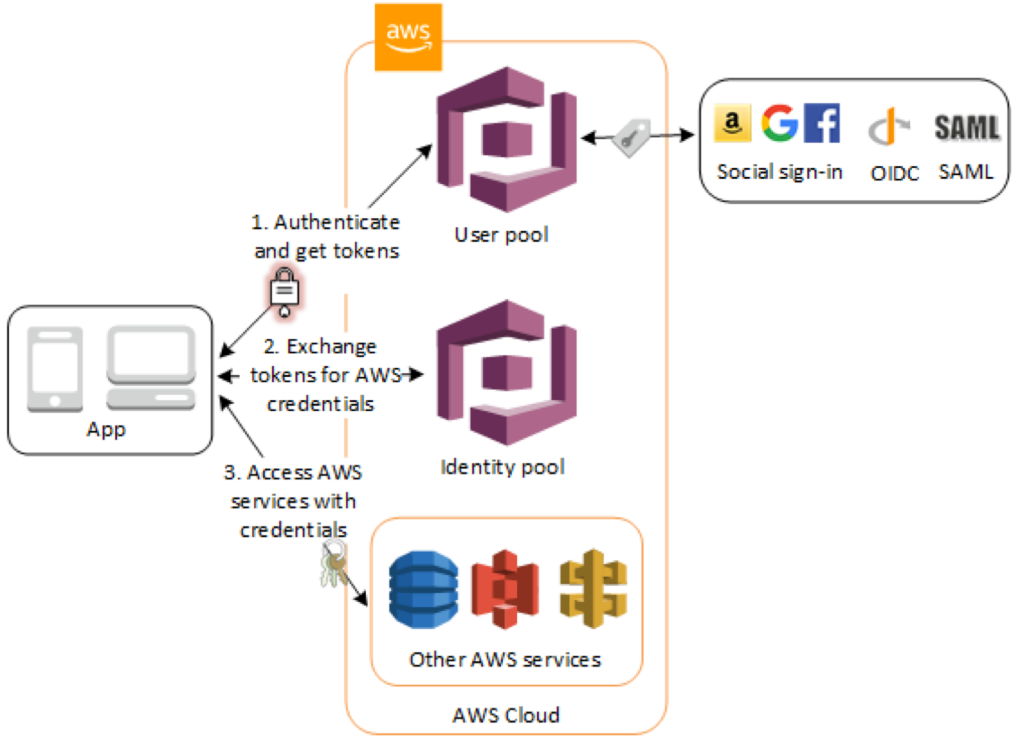
Using a User Pool as an Authorizer API Gateway



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

For more information : https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-integrate-with-cognito.html

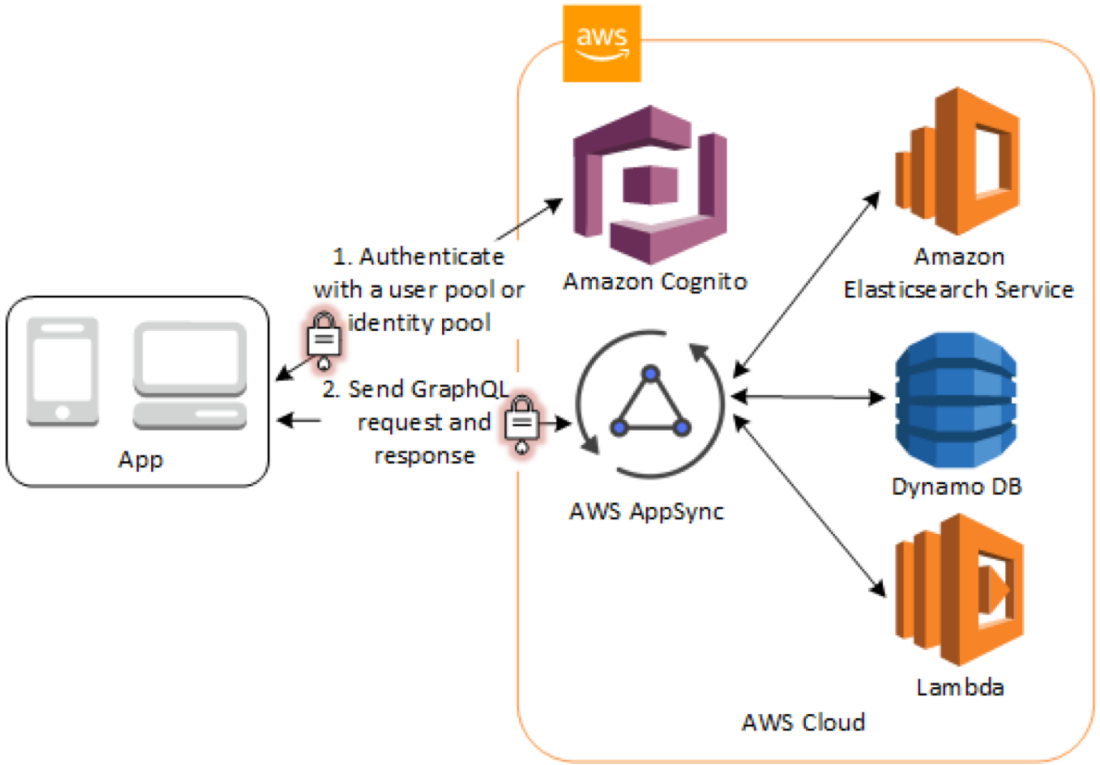
Access AWS Services with a User Pool and an Identity Pool



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.

For more information : https://docs.aws.amazon.com/cognito/latest/developerguide/amazon-cognito-integrating-user-pools-with-identity-pools.html

Access AWS AppSync Resources with Amazon Cognito



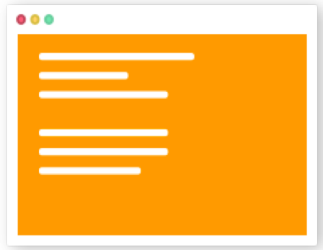
You can grant your users access to AWS AppSync resources with tokens from a successful Amazon Cognito authentication.

For more information : https://docs.aws.amazon.com/appsync/latest/devguide/security.html

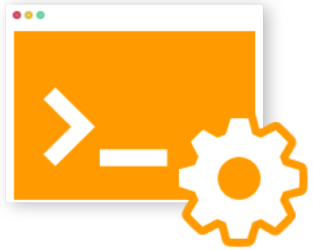
Using Amazon Cognito on AWS Amplify

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

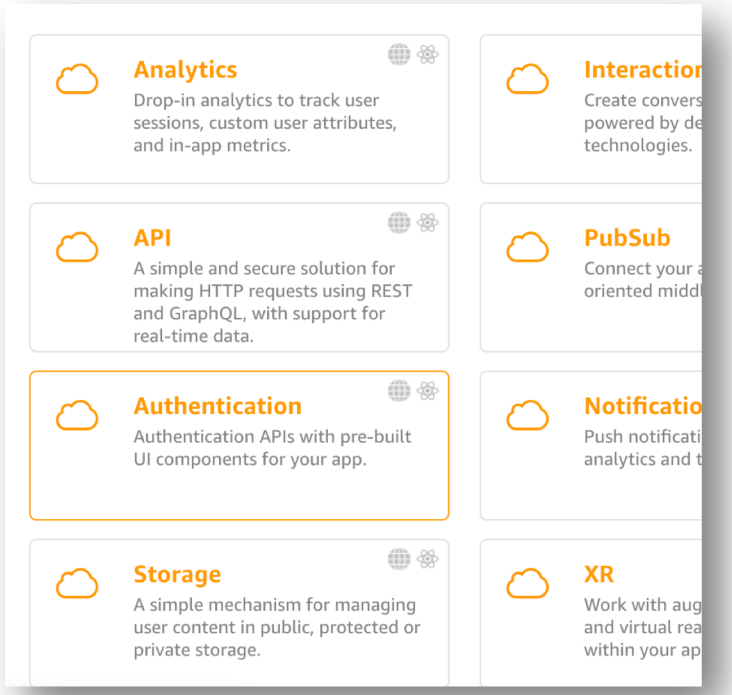


Powerful Toolchain

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

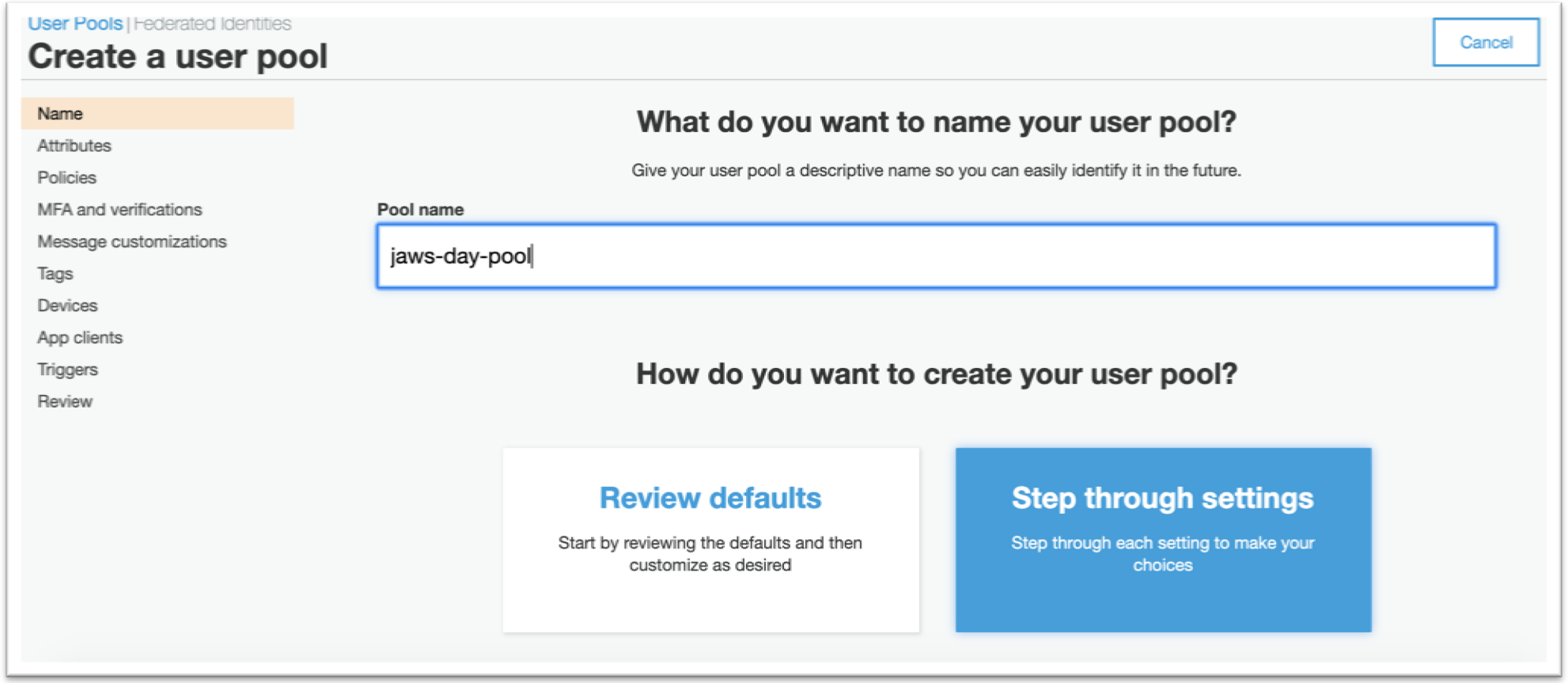
- Sample code

JavaScript

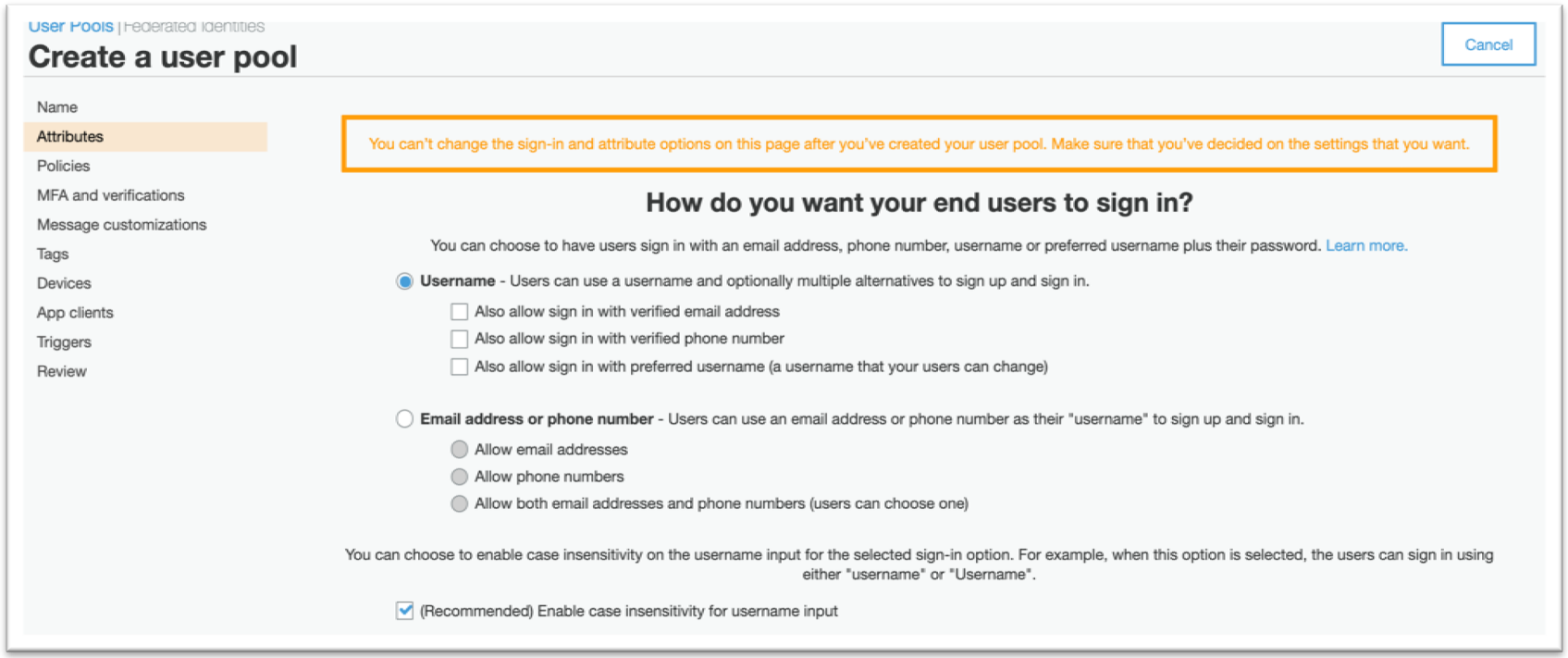
```
// Add 'aws-amplify' library into your application

// Configure Auth category with your Amazon Cognito credentials
Amplify.configure({
    Auth: {
        identityPoolId: 'XX-XXXX-X:XXXXXXXX-XXXX', // Amazon Cogni
        region: 'XX-XXXX-X', // Amazon Cognito Region
    }
});

// Call Auth.signIn with user credentials
Auth.signIn(username, password)
    .then(user => console.log(user))
    .catch(err => console.log(err));
```

Demo

Create a user pool : Set pool name

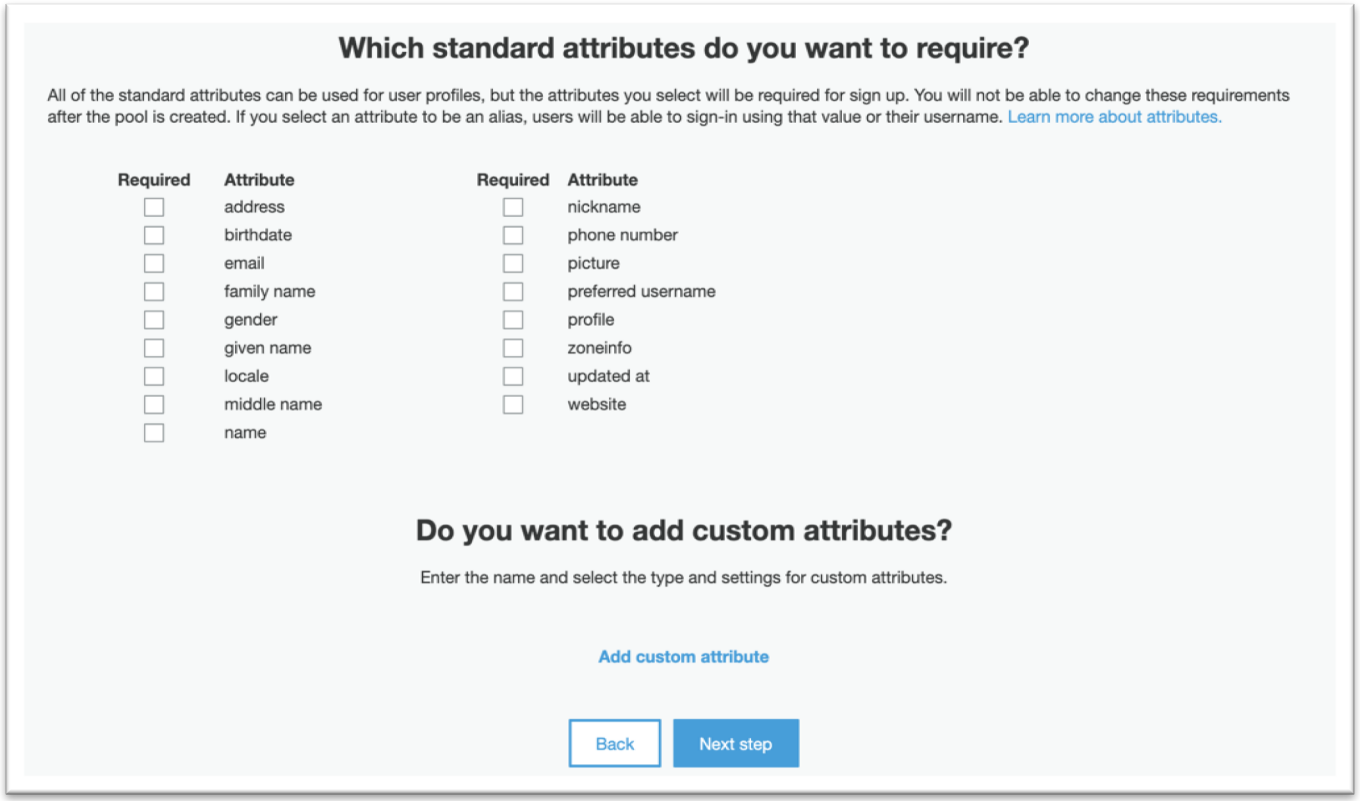


Create a user pool : Set attributes



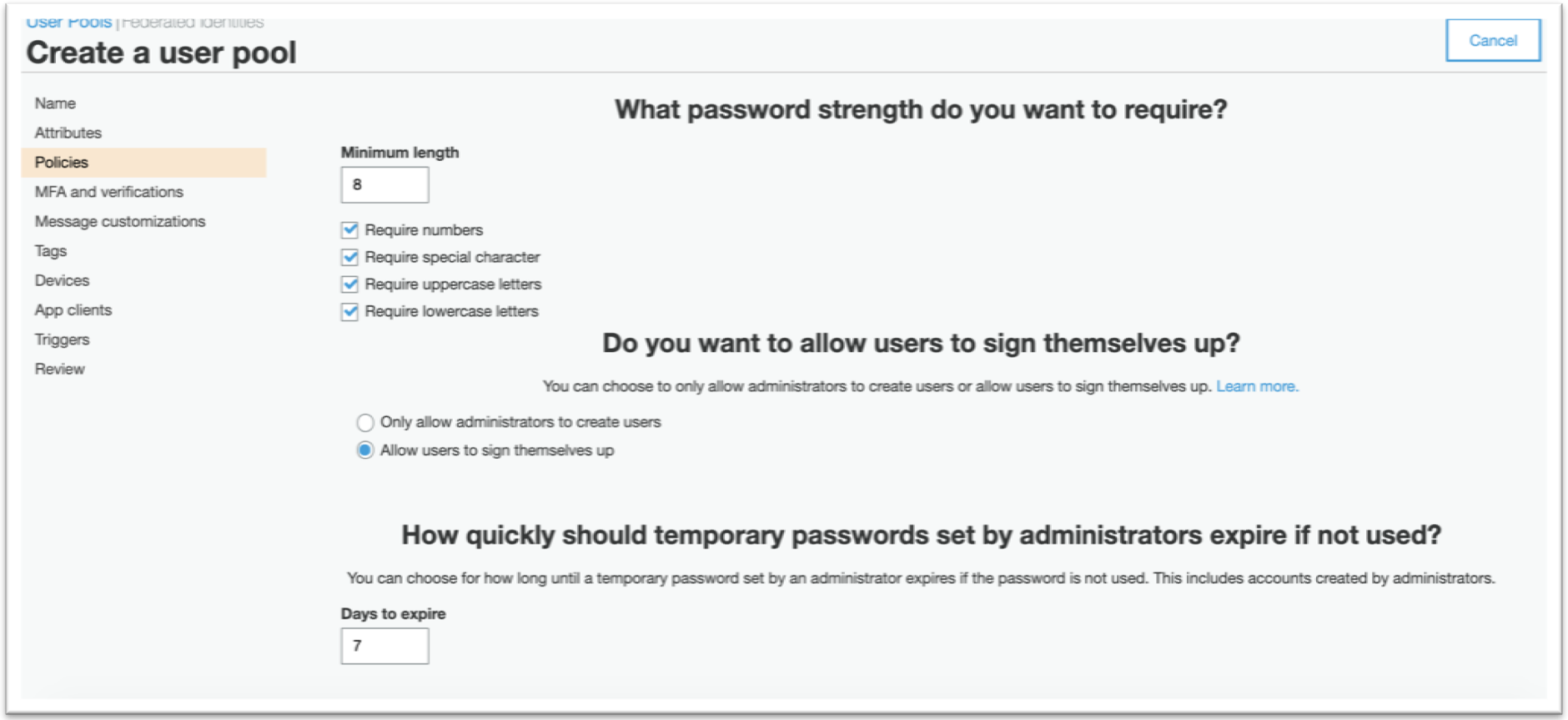
You can choose to have users sign in with an email address, phone number, username or preferred username plus their password.

Create a user pool : Set attributes

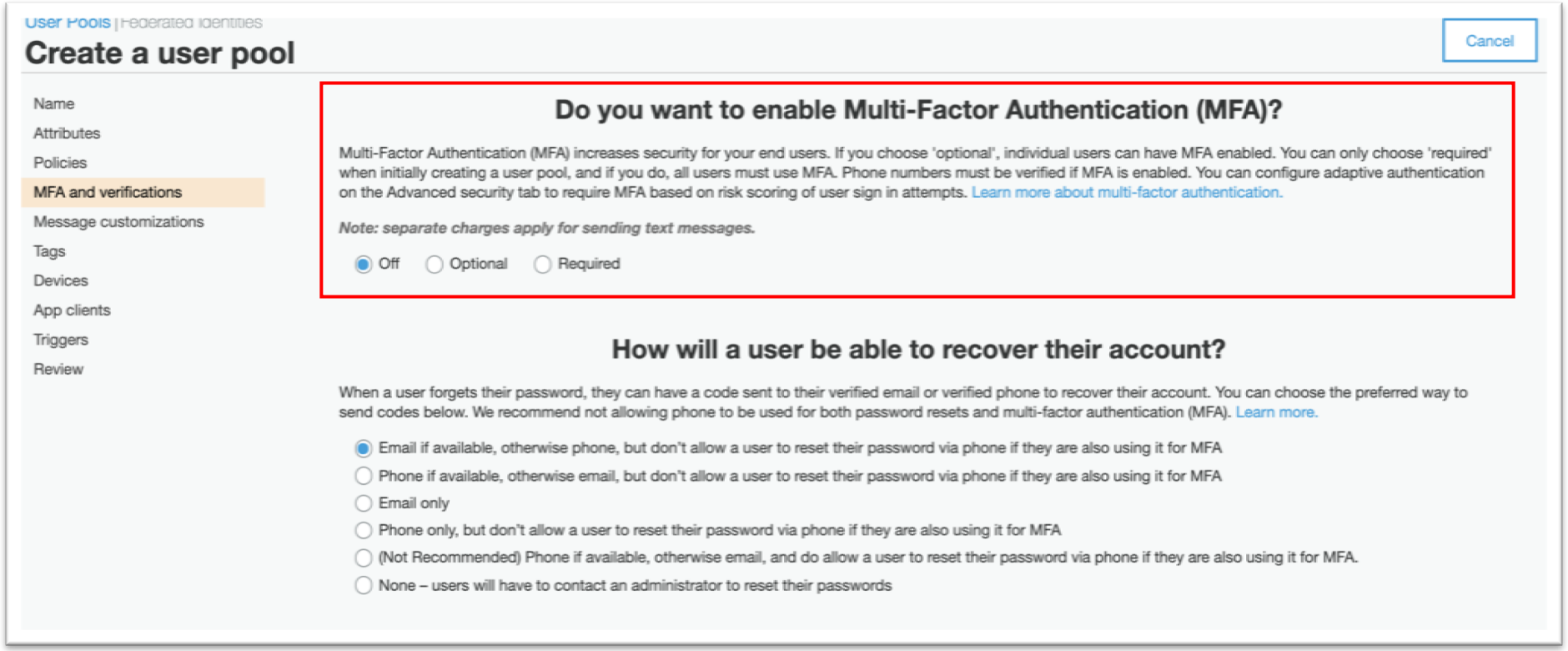


You can choose required attributes for sign-up or add custom attributes

Create a user pool : Set Policies

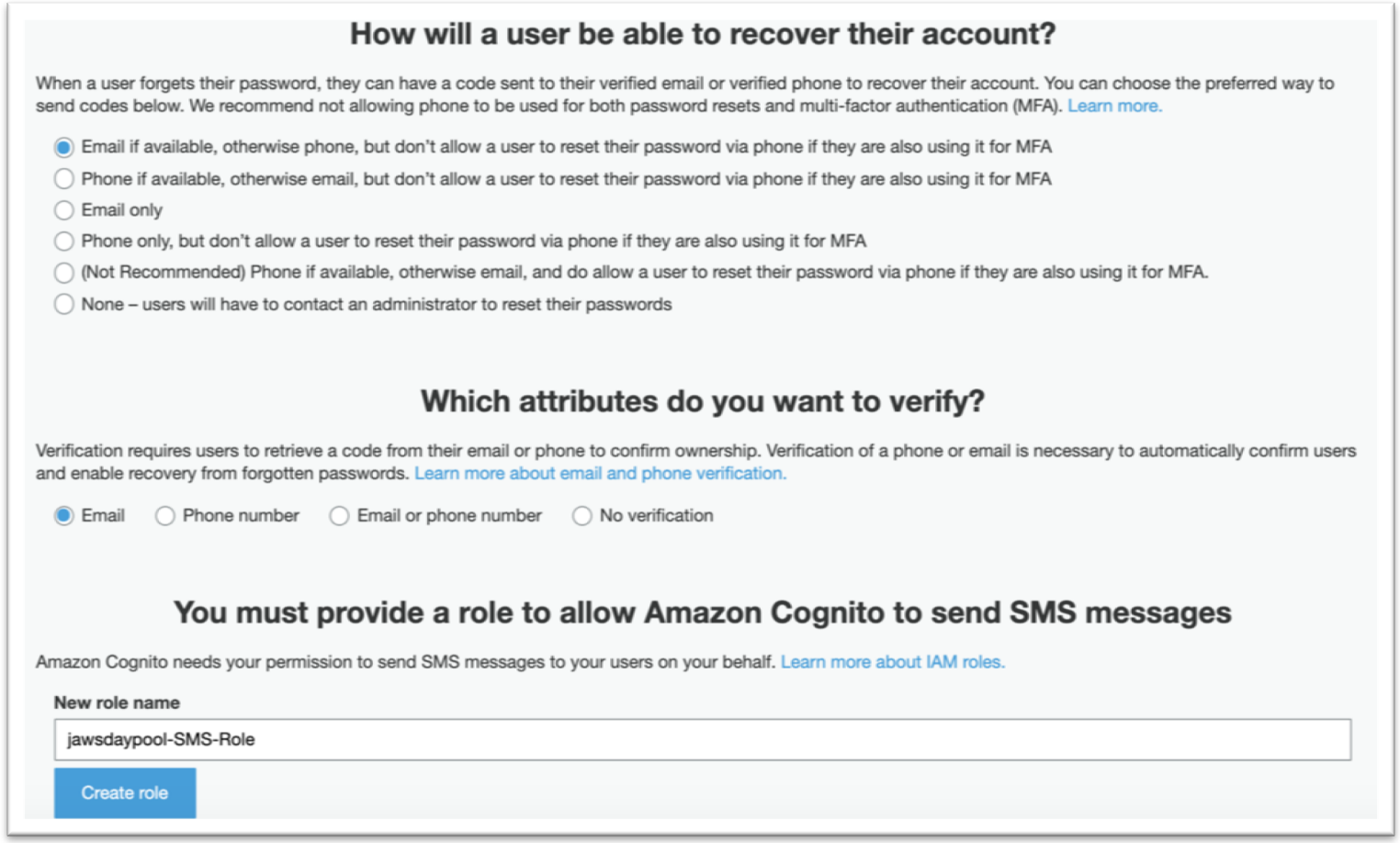


Create a user pool : Enable MFA



Off : Disable
Optional : Individual users can have MFA enabled.
Required: All users must use MFA.

Create a user pool : Set Verifications

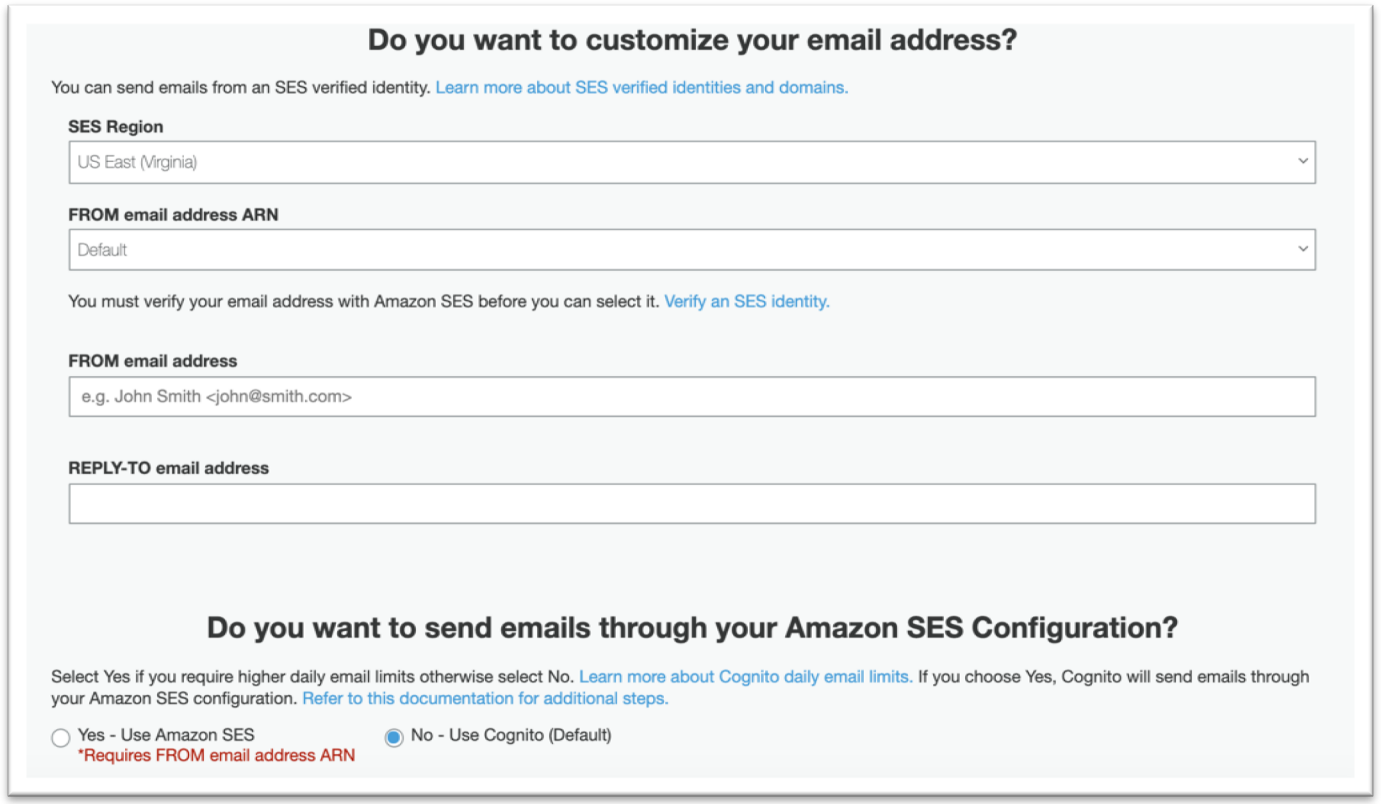


You can choose the preferred way to send verification codes.

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

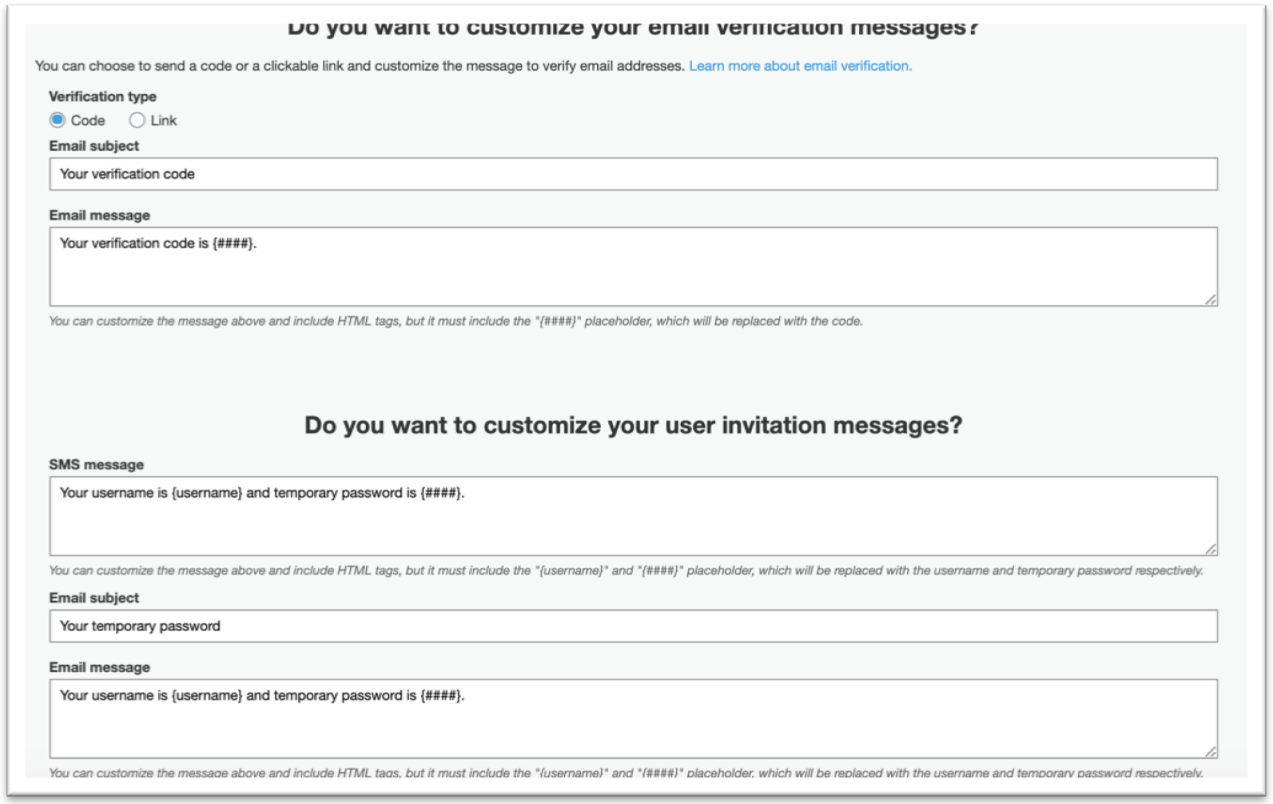


You can customize FROM and REPLY-TO email address for verification email.

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

Learn more : https://docs.aws.amazon.com/cognito/latest/developerguide/limits.html

Create a user pool : Message customizations



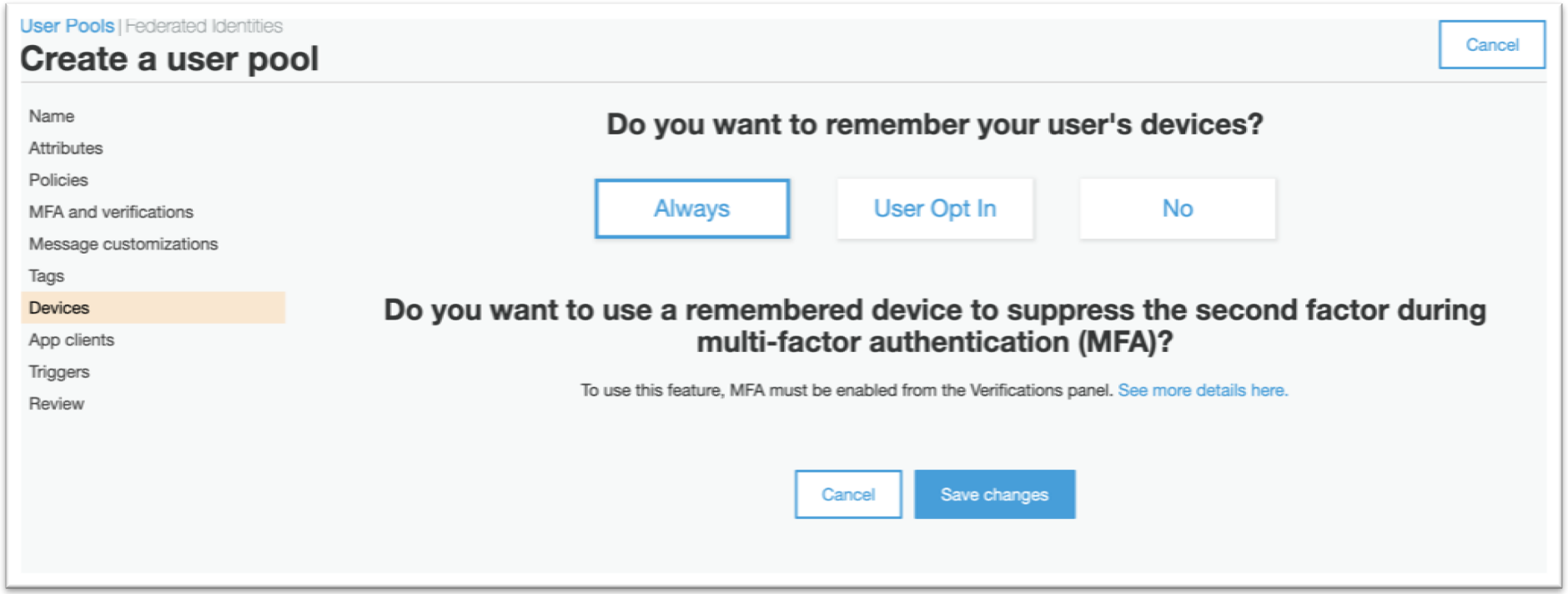
You can customize your email verification messages.

- Code or Link
- Email Subject
- Email Message

You can customize your email invitation messages.

- SMS Message
- Email Subject
- Email Message

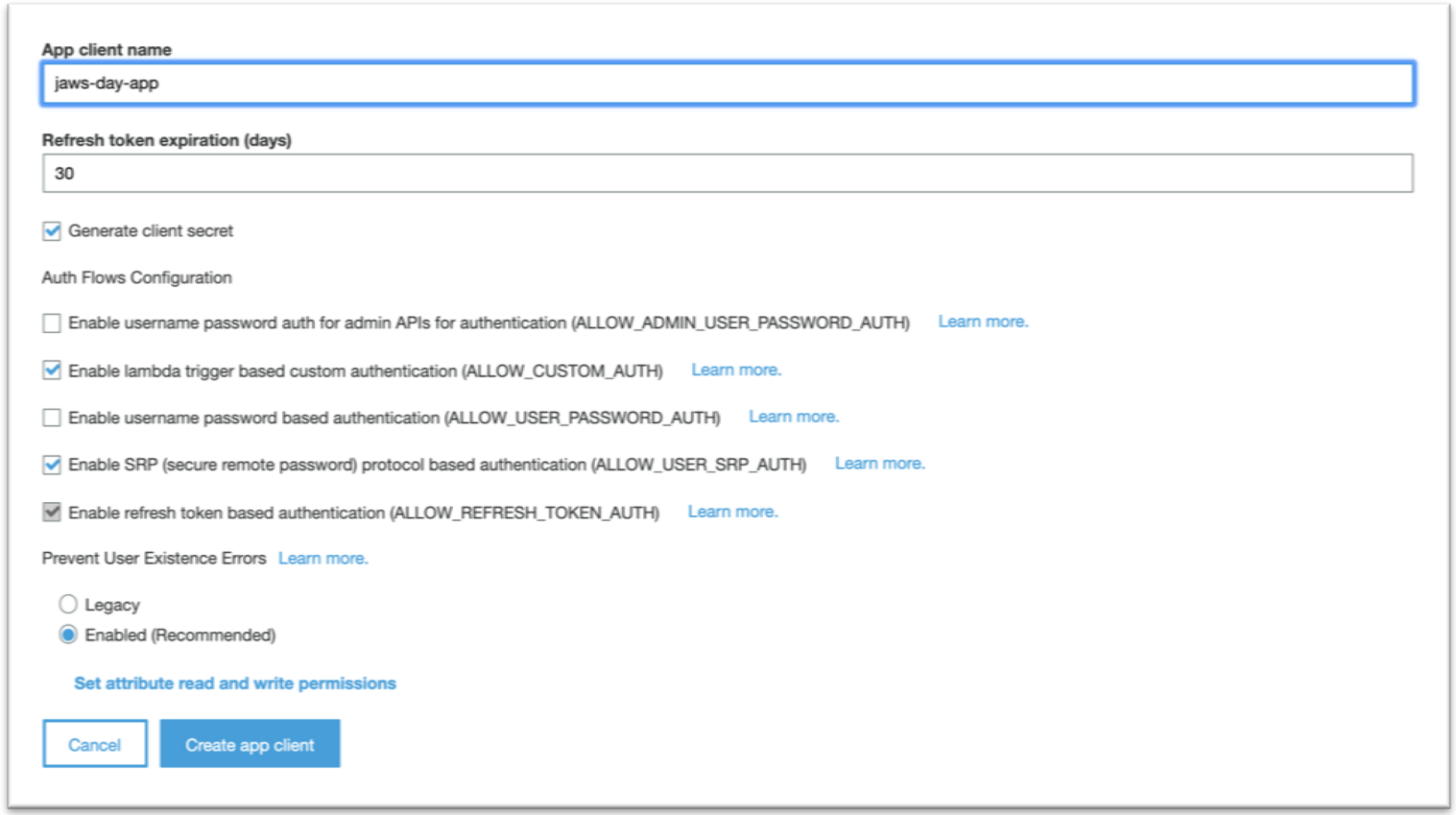
Create a user pool : Remember user's devices



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



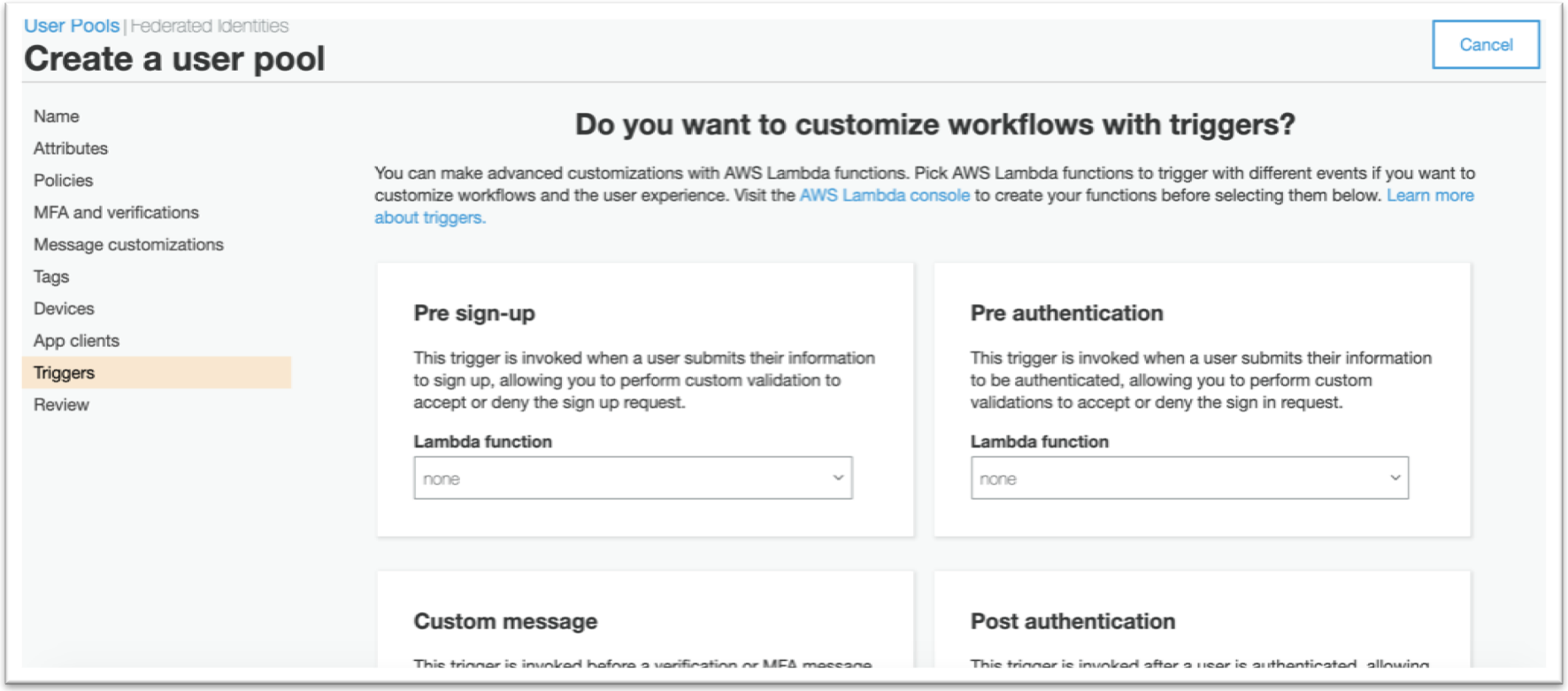
Set app client name

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.

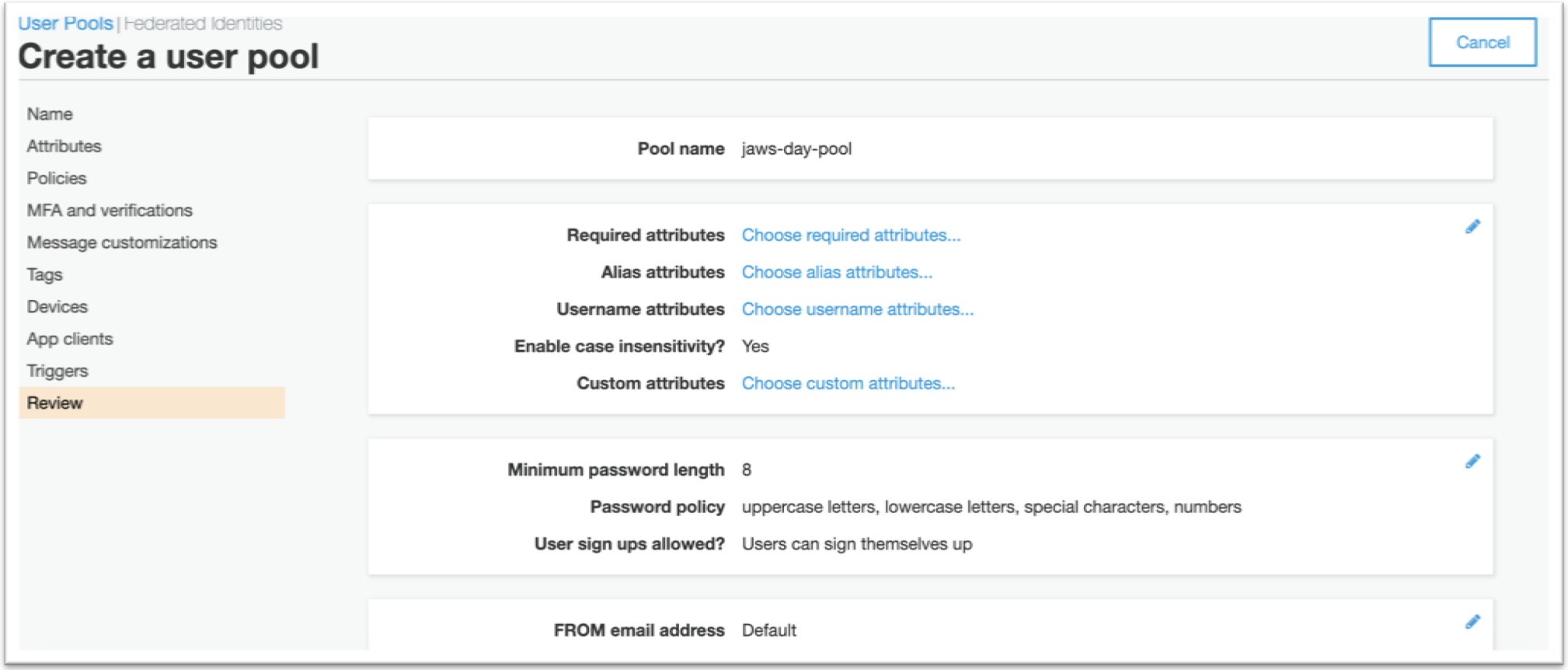
Create a user pool : Trigger events



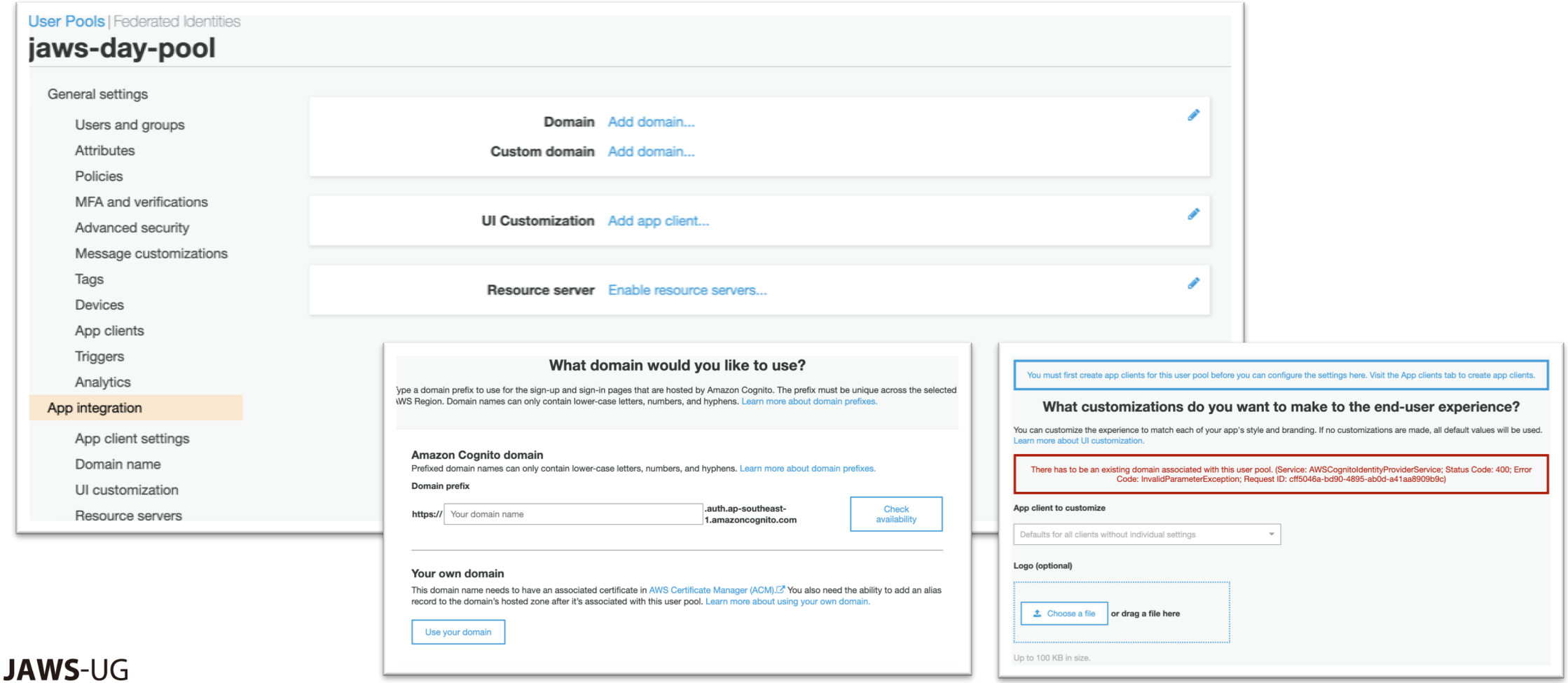
You can make advanced customizations with AWS Lambda functions. Pick AWS Lambda functions to trigger with different events if you want to customize workflows and the user experience

Learn more : https://docs.aws.amazon.com/cognito/latest/developerguide/cognito-user-identity-pools-working-with-aws-lambda-triggers.html

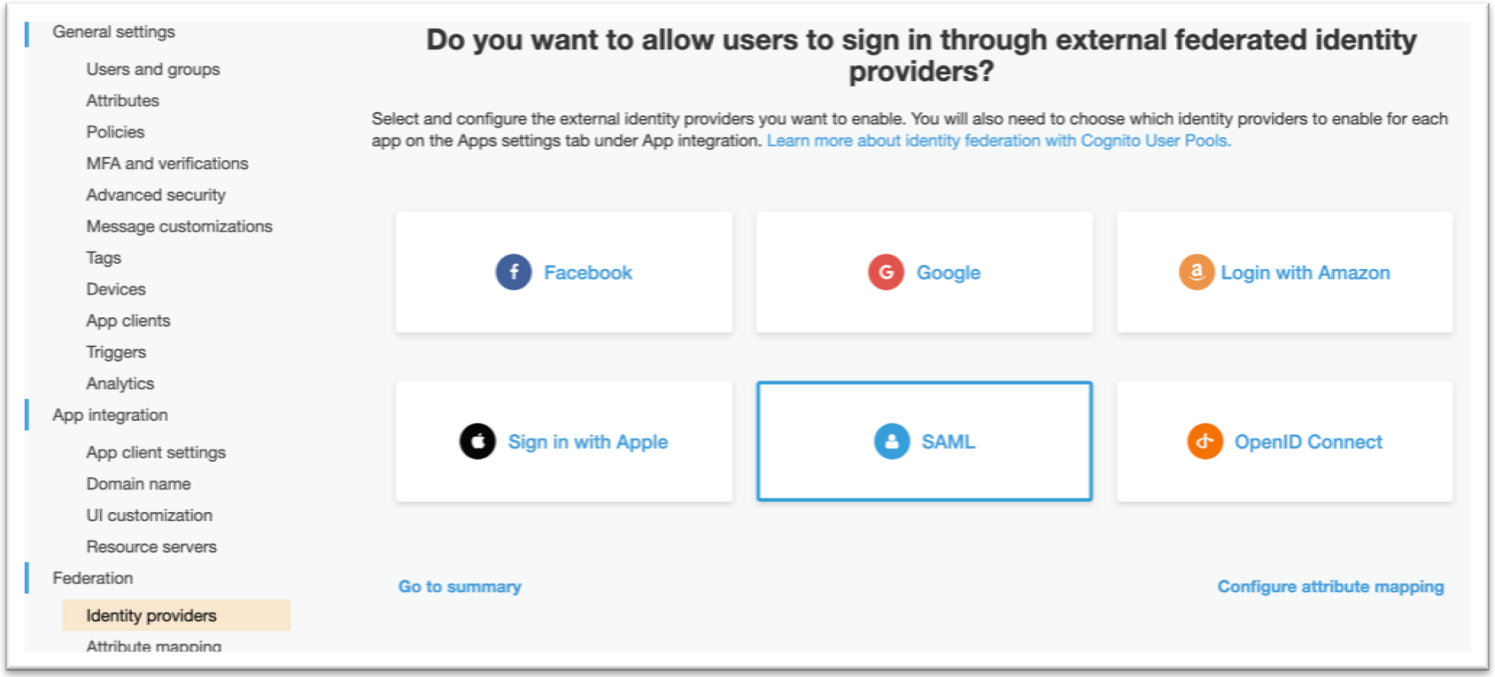
Create a user pool : Review and Confirm

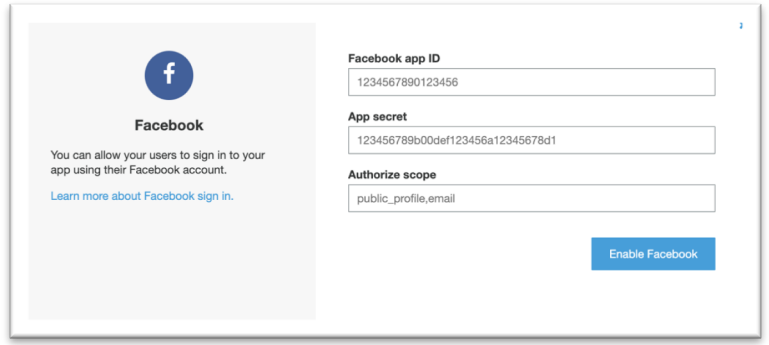


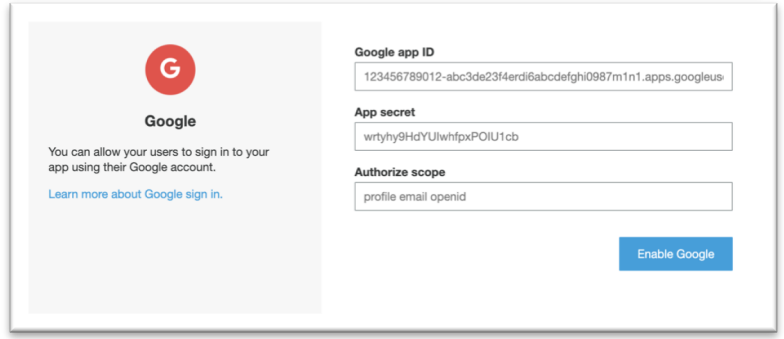
App Integration : Set domain name and add Hosted web UI

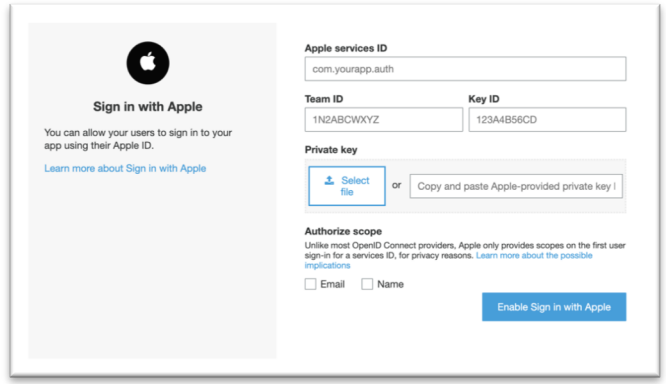


Federation : Identity Providers









JAWS-UG
AWS User Group - Japan

USER GROUP • THAILAND

Thank you