Amazon Cognito

lets you add user sign-up, sign-in, and access control to your web and mobile apps quickly and easily.

Amazon Cognito provides authentication, authorisation, and user management for your web and mobile apps.

Your users can sign in directly with a username and password, or through a third party such as Facebook, Amazon, or Google.

## **Web Identity Federation**

AWS Cognito works with external identity providers that support SAML or OpenID Connect, social identity providers (such as Facebook, Twitter, Amazon)

Federation allows users to authenticate with a Web Identity Provider (e.g. Google, Facebook, Amazon).

The user authenticates first with the Web ID provider and receives an authentication token, which is then exchanges for temporary AWS credentials allowing them to assume an IAM role allowing access to the required resources.

Cognito is an Identity Broker which handles interaction between your applications and the Web ID provider (you don’t need to write your own code to do this).

You can use Amazon, Facebook, Twitter, Digits, Google and any other OpenID Connect compatible identity provider.

You can also integrate your own identity provider.

## 

## **User Pools and Identity Pools**

The two main components of AWS Cognito are user pools and identity pools:

* User pools are user directories that provide sign-up and sign-in options for your app users.
* Identity pools enable you to grant your users access to other AWS services.

You can use identity pools and user pools separately or together.

No need for the application to embed or store AWS credentials locally on the device and it gives users a seamless experience across all mobile devices.

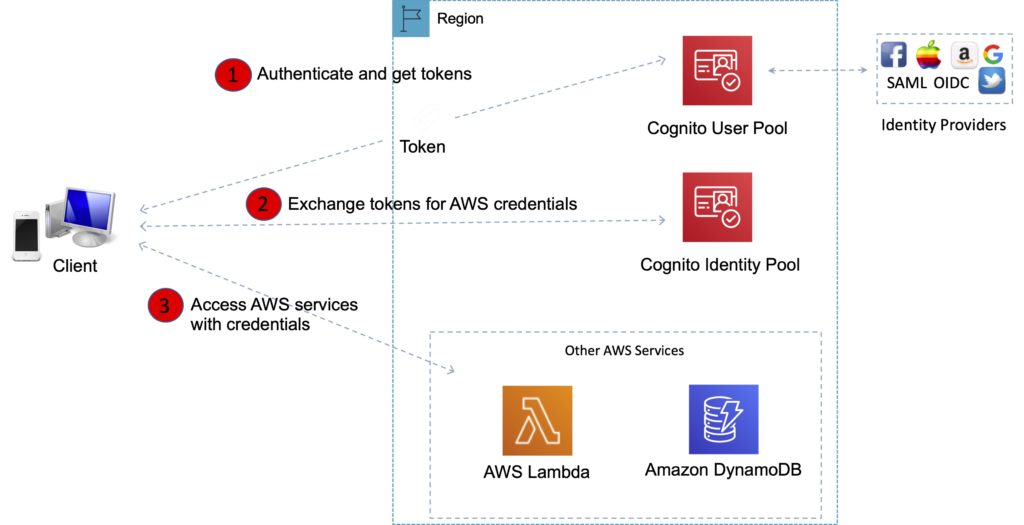
Cognito Identity provides temporary security credentials to access your app’s backend resources in AWS or any service behind Amazon API Gateway.

Cognito exposes server-side APIs.

Users can sign-up and sign-in using email, phone number, or user name.

End users of an application can also sign in with SMS-based MFA.

There is an import tool for migrating users into an Amazon Cognito User Pool.



## 

## **User Pools**

Cognito User Pools are user directories used to manage sign-up and sign-in functionality for mobile and web applications.

With a user pool, users can sign in to your web or mobile app through Amazon Cognito.

Users can also sign in through social identity providers like Facebook or Amazon, and through SAML identity providers.

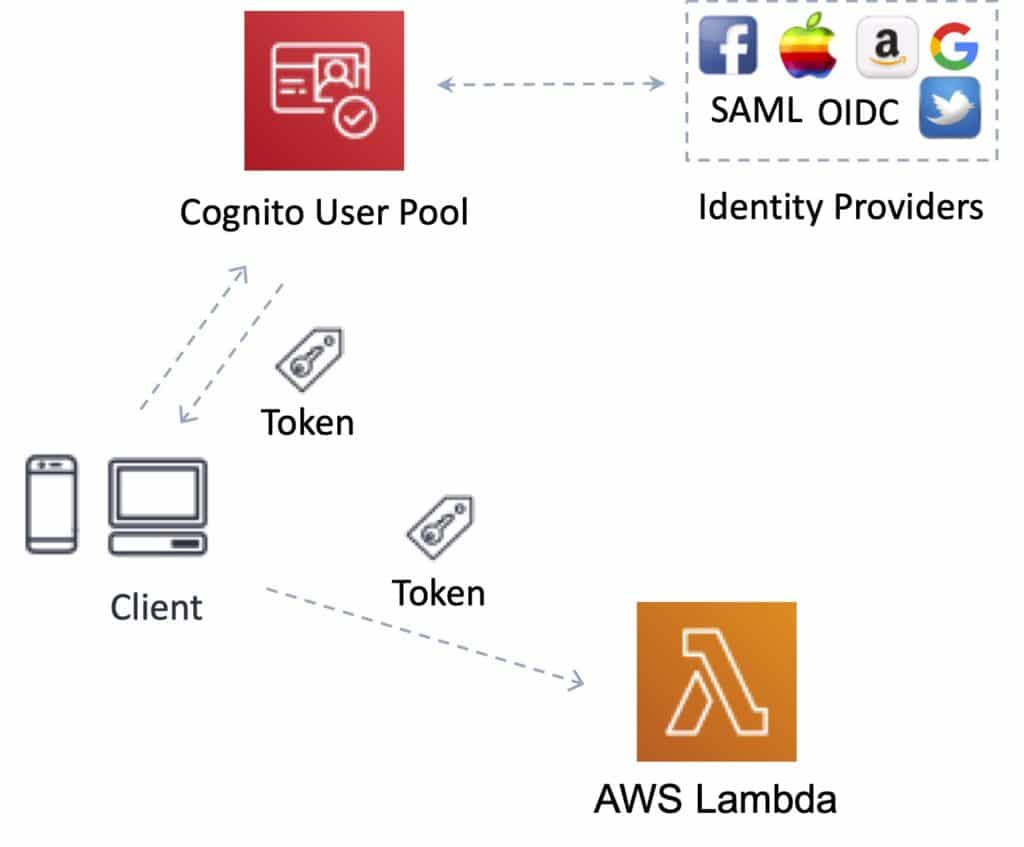
Whether users sign-in directly or through a third party, all members of the user pool have a directory profile that you can access through an SDK.

Cognito acts as an Identity Broker between the ID provider and AWS.

User pools provide:

* Sign-up and sign-in services.
* A built-in, Customisable web UI to sign in users.
* Social sign-in with Facebook, Google, and Login with Amazon, as well as sign-in with SAML identity providers from your user pool.
* User directory management and user profiles.
* Security features such as multi-factor authentication (MFA), checks for compromised credentials, account takeover protection, and phone and email verification.
* Customised workflows and user migration through AWS Lambda triggers.

After successfully authenticating a user, Amazon Cognito issues JSON web tokens (JWT) that you can use to secure and authorise access to your own APIs, or exchange for AWS credentials.



## **Identity Pools**

Identity Pools enable you to create unique identities for your users and authenticate them with identity providers.

With an identity, you can obtain temporary, limited-privilege AWS credentials to access other AWS services.

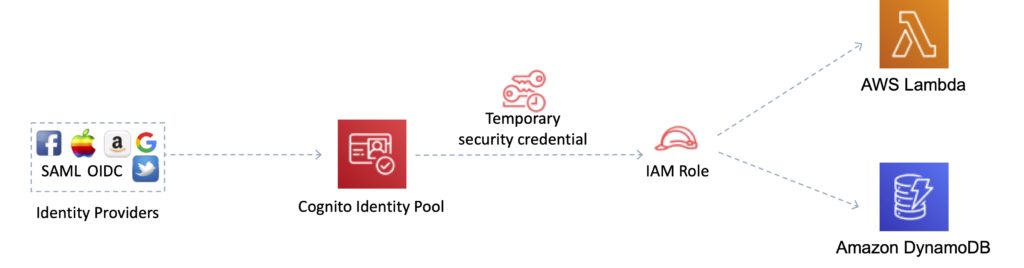
Cognito tracks the association between user identity and the various different devices they sign-in from.

In order to provide a seamless user experience for your application, Cognito uses Push Synchronisation to push updates and synchronise user data across multiple devices.

Amazon SNS is used to send a silent push notification to all the devices whenever data stored in the cloud changes.

Amazon Cognito identity pools support the following identity providers:

* Public providers: Login with Amazon (Identity Pools), Facebook (Identity Pools), Google (Identity Pools).
* Amazon Cognito User Pools.
* Open ID Connect Providers (Identity Pools).
* SAML Identity Providers (Identity Pools).
* Developer Authenticated Identities (Identity Pools).



***Exam tip:*** *To make it easier to remember the different between User Pools and Identity Pools, think of Users Pools as being like IAM Users or Active Directory and an Identity Pools as being like an IAM Role.*

## **Amazon Cognito Sync**

Amazon Cognito Sync is an AWS service and client library that enables cross-device syncing of application-related user data.

You can use it to synchronise user profile data across mobile devices and the web without requiring your own backend.

The client libraries cache data locally so your app can read and write data regardless of device connectivity status.

When the device is online, you can synchronise data, and if you set up push sync, notify other devices immediately that an update is available.

***Exam tip:*** *AWS AppSync is a similar service that has additional capabilities. With AppSync you can synchronise mobile app data across devices and users (Cognito Sync cannot synchronise across users, only devices), it has support for additional devices and data types, and is based on GraphQL.*

### **Related posts:**

* ****