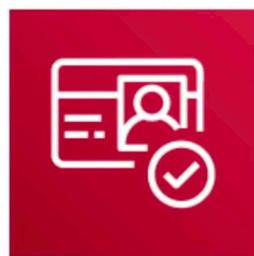


Amazon Cognito



Decentralized Managed **Authentication**.
Sign-up, sign-in integration for your apps.
Social identity provider eg. Facebook, Google.



Introduction to Amazon Cognito

Cognito User Pools

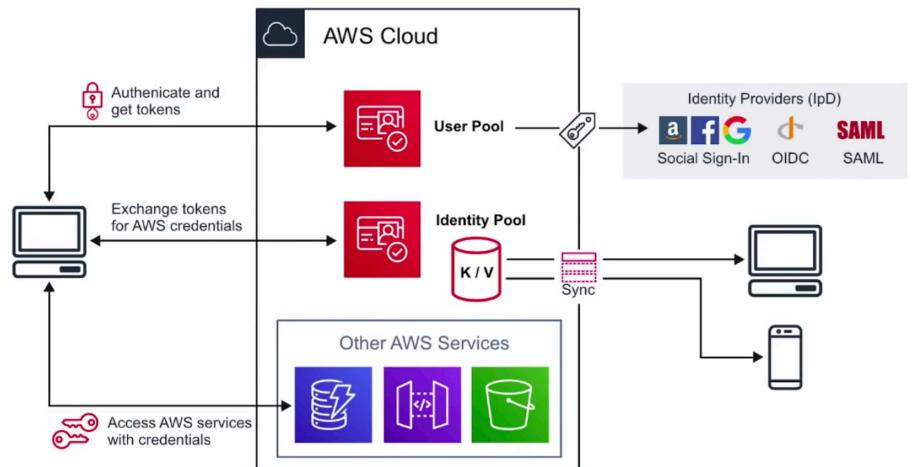
User directory with authentication to IdP to grant access to your app

Cognito Identity Pools

Provide temporary credentials for users to access AWS Services

Cognito Sync

Syncs user data and preferences across all devices





Web Identity Federation and IdP

Web Identity Federation

To exchange identity and security information between an identity provider (IdP) and an application

Identity Provider (IdP)

a trusted provider of your user identity that lets you use authenticate to access other services.

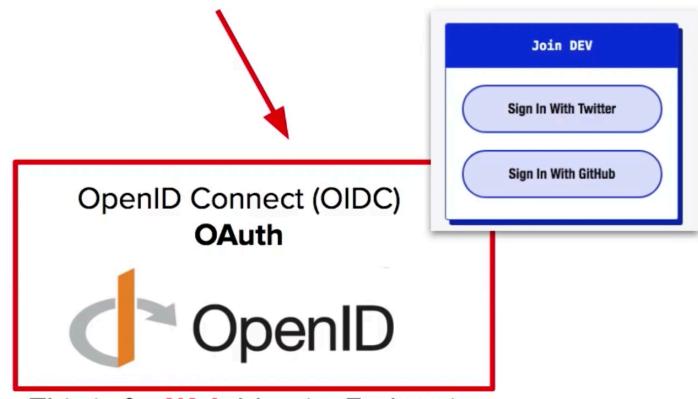
Identity Providers could be: **Facebook, Amazon, Google, Twitter, Github, LinkedIn**

Types of Identity Providers

The technology that behind the Identity Providers

Security Assertion Markup Language (SAML)
Single Sign On (SSO)

SAML





Cognito User Pools

User Pools are user directories used to manage the actions for web and mobile apps such as:

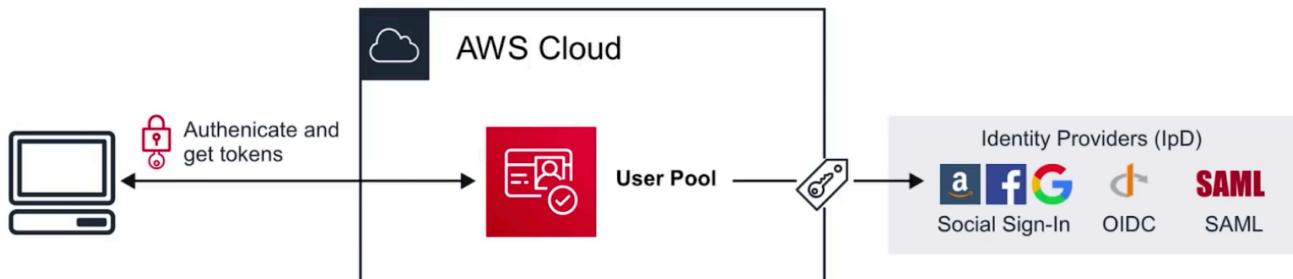
- **Sign-up**
- **Sign-in**
- **Account recovery**
- **Account confirmation**

Allows users to sign-in directly to the User Pool, or using Web Identity Federation.

Uses AWS Cognito as the identity broker between AWS and the identity provider.

Successful user authentication generates a JSON Web Token (JWTs).

User Pools can be thought of as the account used to access the system (ie email address and password)





Cognito User Pools

| |
|------------------------|
| General settings |
| Users and groups |
| Attributes |
| Policies |
| MFA and verifications |
| Advanced security |
| Message customizations |
| Tags |
| Devices |
| App clients |
| Triggers |
| Analytics |

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

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".

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

Minimum length

8

- Require numbers
- Require special character
- Require uppercase letters
- Require lowercase letters

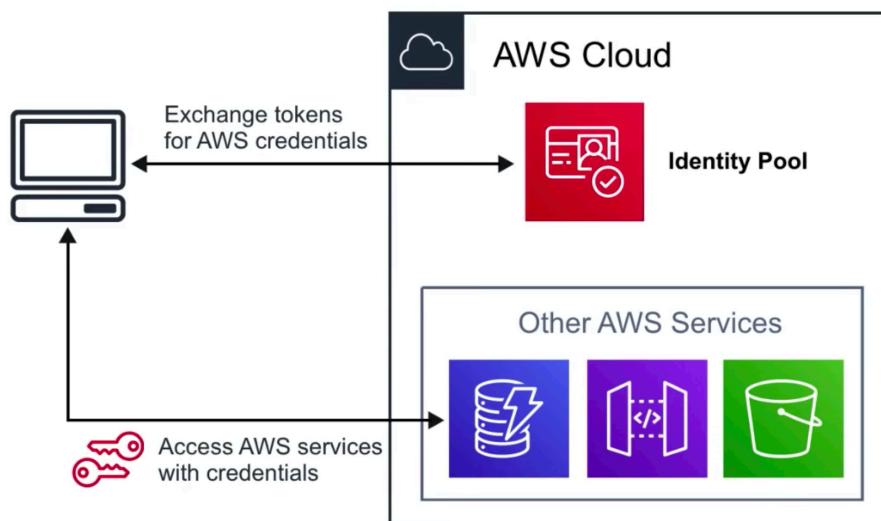
| Required | Attribute | Required | Attribute |
|--------------------------|-------------|--------------------------|--------------------|
| <input type="checkbox"/> | address | <input type="checkbox"/> | nickname |
| <input type="checkbox"/> | birthdate | <input type="checkbox"/> | phone number |
| <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 | | |

- Choose what attributes
- Choose password requirements
- Apply MFA
- Restrict whether users are allowed to sign up on their own or need admin verification
- Analytics with PinPoint for user campaigns
- Trigger custom logs via Lambdas after actions such as after signup



Cognito Identity Pools

Identity Pools provide **temporary AWS credentials** to access services eg. S3, DynamoDB
Identity Pools can be thought of as the actual mechanism authorizing access to the AWS resources.



Cognito Identity Pools

Choose who to provide access to:

▼ Authentication providers ⓘ

Amazon Cognito supports the following authentication methods with Amazon Cognito Sign-In or any public provider. If you change the application ID that your identity pool is linked to, it will prevent existing users from authenticating using Amazon Cognito.

Cognito Amazon Facebook Google+ Twitter / Digits OpenID SAML Custom

Configure your Cognito Identity Pool to accept users federated with your Cognito User Pool by supplying the User Pool ID and App client ID.

User Pool ID ex: us-east-1_Ab129faBb

App client id ex: 7ihlkfbfb4q5kpp90urffao

▼ Unauthenticated identities ⓘ

Amazon Cognito can support unauthenticated identities by providing a unique identifier and AWS credentials for enable access for unauthenticated identities. [Learn more about unauthenticated identities.](#)

Enable access to unauthenticated identities

Enabling this option means that anyone with internet access can be granted identities should be more restrictive than those for authenticated identities.

Getting started with Amazon Cognito

Platform [Android](#) ▾

▼ Download the AWS SDK

[Download the AWS SDK for Android](#) [Developer Guide](#)

▼ Get AWS Credentials

```
// Initialize the Amazon Cognito credentials provider
CognitoCachingCredentialsProvider credentialsProvider = new CognitoCachingCredentialsProvider(
    getApplicationContext(),
    "us-east-1:e31243c0-1842-3cid-2642-fbe023de0332", // Identity pool ID
    Regions.US_EAST_1 // Region
);
```

▼ Then initialize the credentials provider:

- Getting Started with Cognito Identity

Use the SDK to get temporary credentials



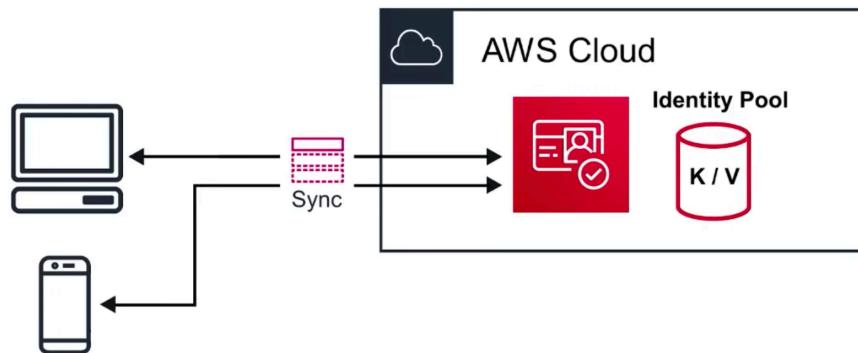


Cognito – Sync

Sync **user data** and **preferences** across devices with one line of code

Cognito uses **push synchronization** to push updates and synchronize data

Uses Simple Notification Service (SNS) to send notifications
to all user devices when data in the cloud changes.





Cognito *CheatSheet*

- Cognito is decentralized managed authentication system. When you need to easily add authentication to your mobile and desktop app *think* Cognito
- **User Pools** user directory, allows users to authenticate using OAuth to IdP such as Facebook, Google, Amazon to connect to web-applications. Cognito User Pool is in itself a IdP
- User Pools use **JWTs** for to persist authentication
- **Identity Pools** provide **temporary AWS credentials** to access services eg. S3, DynamoDB
- **Cognito Sync** can sync **user data** and **preferences** across devices with one line of code (powered by SNS)
- **Web Identity Federation** exchange identity and security information between an identity provider (IdP) and an application
- **Identity Provider (IdP)** a trusted provider of your user identity that lets you use authenticate to access other services. eg. Facebook, Twitter, Google, Amazon
- **OIDC** is a type of Identity Provider which uses Oauth
- **SAML** is a type of Identity Provider which is used for Single Sign-on