Amazon Cognito

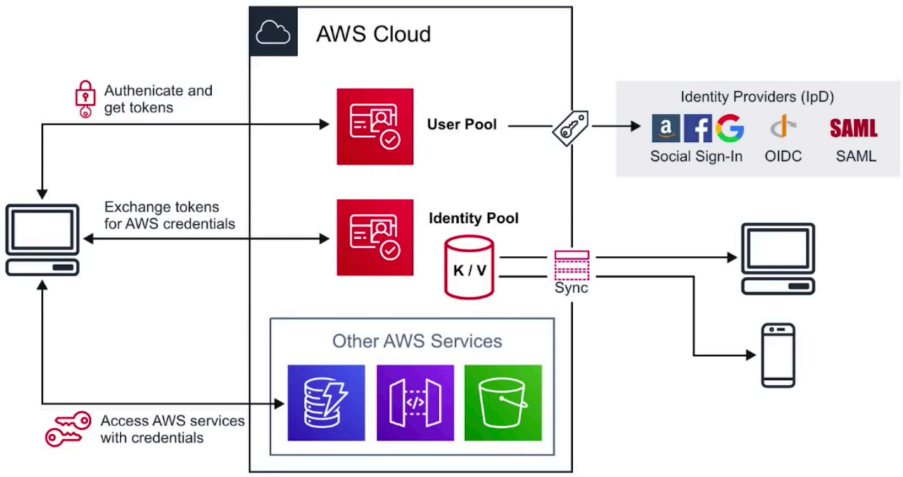
Decentralized Managed **Authentication**.
Sign-up, sign-in integration for your apps.
Social identity provider eg. Facebook, Google.

Introduction to Amazon Cognito

Cognito User Pools
User directory with authentication to IpD 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 IpD

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

OpenID Connect (OIDC)
OAuth

OpenID

This is for **Web** Identity Federation

Cognito User Pools

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

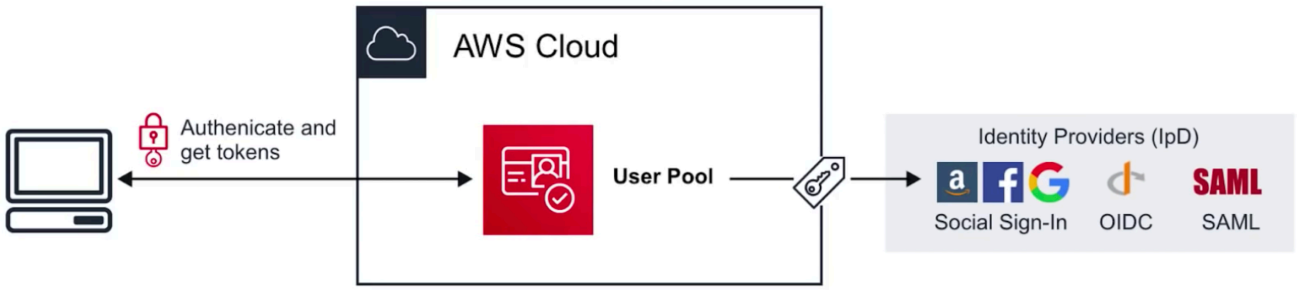
- **Sign-up**
- **Sign-in**
- **Account recovery**
- **Account confirmation**

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

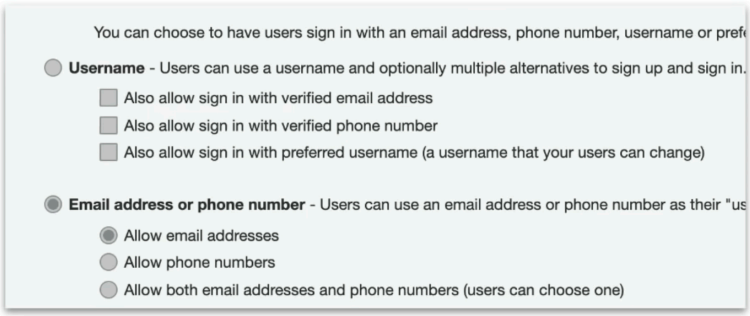
Uses AWS Cognito as the identity broker between AWS and the identity provider.

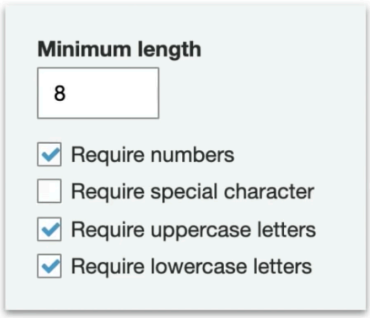
Successful user authentication generates a JSON Web Token (JWTs).

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



Cognito User Pools

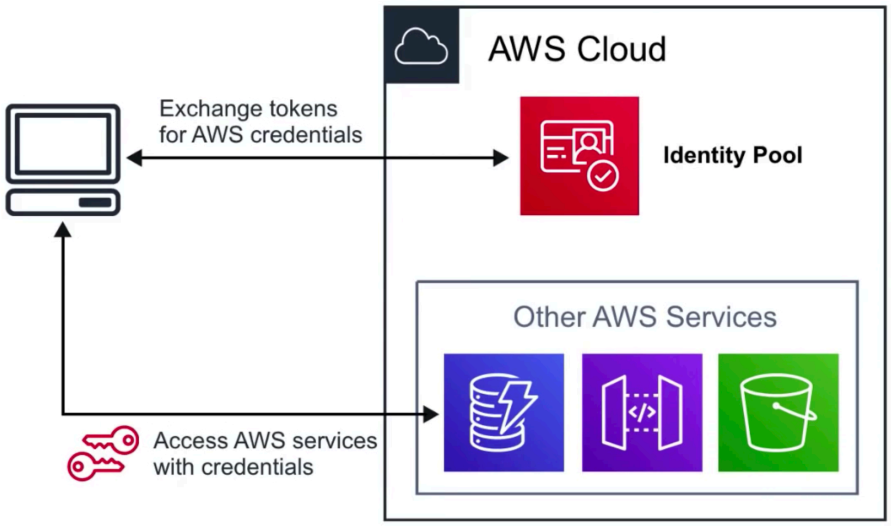




- Choose what attributes
- Choose password requirements
- Apply MFA
- Restrict whether users are allow to sign up on their own or need admin verification
- Analytics with PinPoint for user campaigns
- Trigger custom log via Lambdas after actions such as after signup

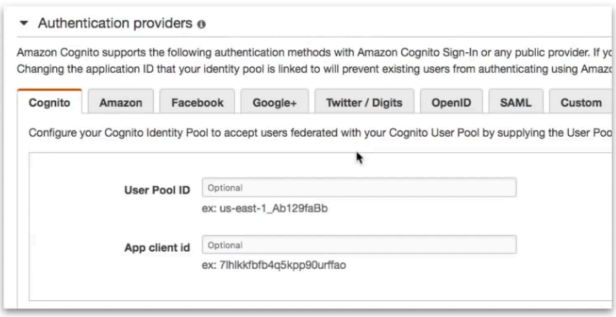
Cognito Identity Pools

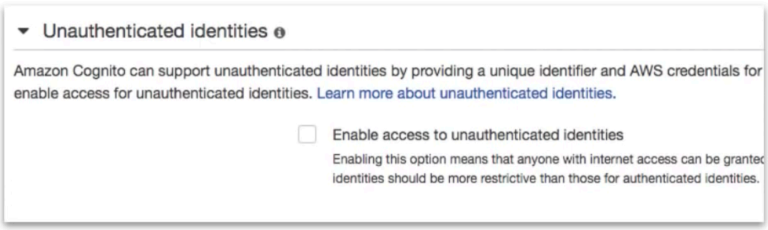
Identity Pools provide **temporary AWS credentials** to access services eg. S3, DynamoDB
Identity Pools can be thought of as the actual mechanism authorizing access to the AWS resources.



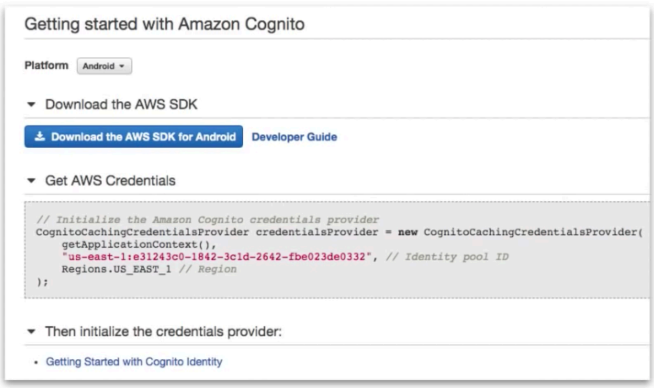
Cognito Identity Pools

Choose who to provide access to:





Use the SDK to get temporary credentials

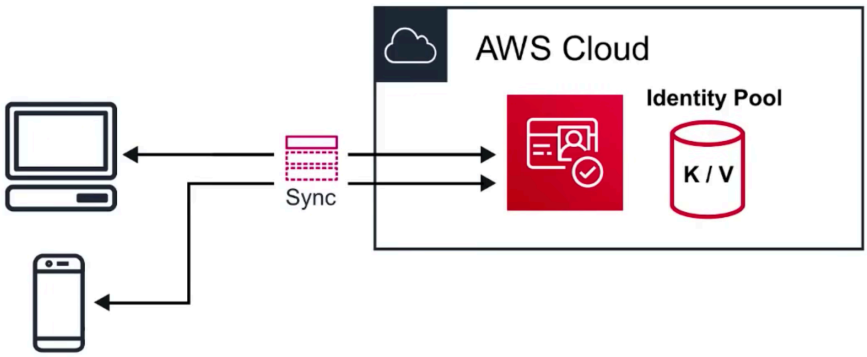


Cognito – Sync

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 IpD such as Facebook, Google, Amazon to connect to web-applications. Cognito User Pool is in itself a IpD
- 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