



Amazon Cognito FAQs

- [General](#)
- [Add User Signup & Sign-in to your mobile and web apps](#)
- [Federate identities and provide secure access to AWS resources](#)
- [Store and Sync Data Across Devices](#)
- [Pricing](#)

Get Started with
Amazon Cognito

General

Q: What is Amazon Cognito?

Amazon Cognito lets you easily add user sign-up and authentication to your mobile and web apps. Amazon Cognito also enables you to authenticate users through an external identity provider and provides temporary security credentials to access your app's backend resources in AWS or any service behind Amazon API Gateway. Amazon Cognito works with external identity providers that support SAML or OpenID Connect, social identity providers (such as Facebook, Twitter, Amazon) and you can also integrate your own identity provider.

In addition, Amazon Cognito enables you to synchronize data across a user's devices so that their app experience remains consistent when they switch between devices or upgrade to a new device. Your app can save data locally on users' devices allowing your applications to work even when the devices are offline and then automatically synchronize the data when the device is back online.

With Amazon Cognito, you can focus on creating great app experiences instead of worrying about building, securing, and scaling a solution to handle user management, authentication, and sync across platforms and devices.

Q: Who should use Amazon Cognito?

Amazon Cognito is designed for developers who want to add user management and sync functionality to their mobile and web apps. Developers can use Cognito



data across devices, platforms, and applications.

Q: How do I start using Amazon Cognito?

You can easily get started by visiting the [AWS Console](#). If you do not have an Amazon Web Services account, you can create an account when you sign in to the console. Once you have created a user pool for user management or an identity pool for federated identities or sync operations, you can download and integrate the [AWS Mobile SDK](#) with your app. Alternatively you can call the Cognito server-side APIs directly, instead of using the SDK. See our [developer guide](#) for more information.

Q: Does Amazon Cognito expose server-side APIs?

Yes. Cognito exposes server-side APIs. You can create your own custom interface to Cognito by calling these APIs directly. The server-side APIs are described in the Developer Guide.

Q: Which platforms does Amazon Cognito support?

Support for Cognito is included in the optional AWS Mobile SDK, which is available for iOS, Android, Unity, and Kindle Fire. Cognito is also available in the AWS SDK for JavaScript. Cognito Your User Pools is currently supported in the AWS Mobile SDKs for iOS and Android and in the JavaScript AWS SDK for Cognito. Visit our [resource page](#) to download the SDKs.

Q: Do I have to use the AWS Mobile SDK?

No. Cognito exposes its control and data APIs as web services. You can implement your own client library calling the server-side APIs directly.

Add User Sign-up & Sign-in to your mobile and web apps

Q: Can I have my own identity provider to support user sign-up and sign-in?

Yes, you can easily and securely add sign-up and sign-in functionality to your apps with Cognito Identity. Your users can sign-up and sign-in using email, phone number, or user name. You can also implement enhanced security features, such as email verification, phone number verification, and multi-factor authentication. Cognito Identity also enables you to customize workflows by, for example, adding app-specific logic to user registration for fraud detection and user validation through AWS Lambda. To learn more, visit our docs.

Q: What is a User Pool?

A User Pool is your user directory that you can configure for your web and mobile apps. A User Pool securely stores your users' profile attributes. You can create and manage a User Pool using the AWS console, AWS CLI, or AWS SDK.



attributes (such as user name, phone number, address, time zone, etc.) or customize to add app-specific user attributes.

Q: Can I enable my application's users to sign up or sign in with an email address or phone number?

Yes, you can use the aliasing feature to enable your users to sign up or sign in with an email address and a password or a phone number and a password. To learn more, visit our [docs](#).

Q: Can I set up password policies?

Yes, you can set up password policies, such as strength of password and character type requirements, when setting up or configuring your user pool.

Q: Can I verify the email addresses and phone numbers of my application's users?

Yes, with Cognito Identity you can require your users' email addresses and phone numbers to be verified prior to providing them access to your application. During sign-up, a verification code will be sent to the user's phone number or email address, and the user must input the verification code to complete sign-up and become confirmed.

Q: Does Cognito Identity support SMS-based multi-factor authentication (MFA)?

Yes, you can enable the end users of your application to sign in with SMS-based MFA. With SMS-based MFA enabled, your users will be prompted for their password (the first factor—what they know), and for a security code that can only be received on their mobile phone via SMS (the second factor—what they have).

Q: Is it possible to customize user sign-up and sign-in workflows?

Yes, you can customize sign-up and sign-in by adding app-specific logic to the user sign-up and sign-in flows using AWS Lambda. For example, you can create AWS Lambda functions to identify fraud or perform additional validations on user data. You are able to trigger developer-provided Lambda functions at pre-registration, at post-confirmation, at pre-authentication, during authentication to customize the challenges, and at post-authentication. You can also use Lambda functions to customize messages sent as part of email or phone number verification and multi-factor authentication.

Q: Can I remember the devices associated with my application's users in a Cognito user pool?



user pool. You can also opt to use remembered devices to suppress second factor challenges for your users when you have set up multi-factor authentication.

Q: How can I migrate my existing users into an Amazon Cognito user pool?

You can use our import tool to migrate your existing users into an Amazon Cognito user pool. User attribute values are imported from a .csv file, which can be uploaded through the console, our APIs, or CLI. When imported users first sign in, they confirm their account and create a new password with a code sent to their email address or phone. There is no additional cost for using the import tool. To learn more, see the [import tool documentation](#).

The import tool does not migrate passwords. If you want to retain your users' current passwords, you might consider an alternative approach to migrate users one at a time as they sign-in to your app during a transition period. With this approach, your app first tries to sign-in the user with your Cognito user pool. If that user doesn't exist in the user pool, your app will sign the user in with your existing identity system and temporarily retain the username and password used to do so. After a user successfully signs in with your existing identity system, your app would then use the same username and password to create the user in your Cognito user pool. This approach requires maintaining your existing identity system during the transition period, but after the transition period ends, you can use our import tool to import the remaining users (without their passwords).

Federate identities and provide secure access to AWS resources

Q: Can I use Cognito Identity to federate identities and secure access to AWS resources?

Yes, Cognito Identity enables you to authenticate users through an external identity provider and provides temporary security credentials to access your app's backend resources in AWS or any service behind Amazon API Gateway. Amazon Cognito works with external identity providers that support SAML or OpenID Connect, social identity providers (such as Facebook, Twitter, Amazon) and you can also integrate your own identity provider.

Q: Which public identity providers can I use with Amazon Cognito Identity?

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

Q: What is an Identity Pool?

Identity pools are the containers that Cognito Identity uses to keep your apps' federated identities organized. Identity Pool associates federated identities from social identity providers with a unique user specific identifier. Identity Pools do



will have a different unique identifier in each Identity Pool.

Q: How does the login flow work with public identity providers?

Your mobile app authenticates with an Identity Provider (IdP) using the provider's SDK. Once the end user is authenticated with the IdP, the OAuth or OpenID Connect token or the SAML assertion returned from the IdP is passed by your app to Cognito Identity, which returns a new Cognito ID for the user and a set of temporary, limited-privilege AWS credentials.

Q: Can I register and authenticate my own users?

Cognito Identity can integrate with your existing authentication system. With a simple API call you can retrieve a Cognito ID for your end users based on your own unique identifier for your users. Once you have retrieved the Cognito ID and OpenID Token Cognito Identity provides, you can use the Cognito Identity client SDK to access AWS resources and synchronize user data. Cognito Identity is a fully managed identity provider to make it easier for you to implement user sign-up and sign-in for your mobile and web apps.

Q: How does Cognito Identity help me control permissions and access AWS services securely?

Cognito Identity assigns your users a set of temporary, limited privilege credentials to access your AWS resources so you do not have to use your AWS account credentials. The permissions for each user are controlled through AWS IAM roles that you create. You can define rules to choose the IAM role for each user, or if you are using groups in a Cognito user pool, you can assign IAM roles based on groups. Cognito Identity also allows you to define a separate IAM role with limited permissions for guest users who are not authenticated. In addition, you can use the unique identifier that Cognito generates for your users to control access to specific resources. For example you can create a policy for an S3 bucket that only allows each user access to their own folder within the bucket.

Q: When using public identity providers, does Amazon Cognito Identity store users' credentials?

No, your app communicates directly with the supported public identity provider (Amazon, Facebook, Twitter, Digits, Google, or an Open ID Connect-compliant provider) to authenticate users. Cognito Identity does not receive or store user credentials. Cognito Identity uses the token from the identity provider to obtain a unique identifier for the user and then hashes it using a one-way hash so that the same user can be recognized again in the future without storing the actual user identifier.

Q: Does Cognito Identity receive or store confidential information about my users from the identity providers?

**Q: Do I still need my own backend authentication systems with Cognito Identity?**

No. Cognito Identity supports login through Amazon, Facebook, Twitter, Digits, and Google, as well as providing support for unauthenticated users. With Cognito Identity you can support federated authentication, profile data sync store and AWS access token distribution without writing any backend code.

Q: What if I don't want to force my users to log in?

Cognito Identity supports the creation and token vending process for unauthenticated users as well as authenticated users. This removes the friction of an additional login screen in your app, but still enables you to use temporary, limited privilege credentials to access AWS resources.

Q: What are unauthenticated users?

Unauthenticated users are users who do not authenticate with any identity provider, but instead access your app as a guest. You can define a separate IAM role for these users to provide limited permissions to access your backend resources.

Q: Does Cognito Identity support separate identities for different users on the same device?

Yes. Cognito Identity supports separate identities on a single device, such as a family iPad. Each identity is treated separately and you have complete control over how your app logs users in and out and how local and remote app data is stored.

Q: How do I store data associated with Cognito Identity?

You can programmatically create a data set associated with Cognito Identity and start saving data in the form of key/value pairs. The data is stored both locally on the device and in the Cognito sync store. Cognito can also sync this data across all of the end user's devices.

Q: Does the number of identities in the Cognito Identity console tell me how many users are using my app?

The number of identities in the Cognito Identity console shows you how many identities were created via the Cognito Identity APIs. For Authenticated Identities (those logging in with a login provider such as Facebook or an OpenID Connect provider), each call to Cognito Identity's GetId API will only ever create a single identity for each user. However, for Unauthenticated identities, each time the client in an app calls the GetId API will generate a new identity. Therefore, if your app calls GetId for unauthenticated identities multiple times for a single user it will appear that a single user has multiple identities. So it is important that you cache the response from GetId when using unauthenticated identities and not call it multiple times per user.



solution for your app, including the ability to track unique users, please look at [Amazon Mobile Analytics](#).

Store and sync data across devices

Q: What is the Amazon Cognito sync store?

The Amazon Cognito Sync store is a key/value pair store linked to an Amazon Cognito identity. There is no limit to the number of identities you can create in your identity pools and sync store. Each Amazon Cognito identity within the sync store has its own user information store.

Q: Is data saved directly to the Amazon Cognito sync store?

No. The optional AWS Mobile SDK saves your data to an SQLite database on the local device, this way the data is always accessible to your app. The data is pushed to the Amazon Cognito sync store by calling the `synchronize()` method and, if push synchronization is enabled, all other devices linked to an identity are notified of the data change in the sync store via Amazon SNS.

Q: How is data stored in the Amazon Cognito sync store?

Data associated with an Amazon Cognito identity are organized as key/value pairs. A key is a label e.g. "MusicVolume", and a value e.g. "11". Key/value pairs are grouped and categorized using data sets. Data sets are a logical partition of key/value pairs and the most granular entity used by Amazon Cognito to perform sync operations.

Q: What is the maximum size of a user information store within the Amazon Cognito sync store?

Each user information store can have a maximum size of 20MB. Each data set within the user information store can contain up to 1MB of data. Within a data set you can have up to 1024 keys.

Q: What kind of data can I store in a data set?

Both keys and values within a data set are alphanumeric strings. There is no limit to the length of the strings other than the total amount of values in a dataset cannot exceed 1MB. Binary data can be stored as a base64 encoded string as a value provided it does not exceed the 1MB limit.

Q: Why are data sets limited to 1MB?

Limiting the data set size to 1MB increases the chances of a synchronization task completing successfully even when bandwidth is limited without lots of retries that consume battery life and data plans.

Q: Are user identities and user information stores shared across developers?

No, a user identity and information store is tied to a specific AWS account. If



publisher.

Q: How can I analyze and query the data stored in the Cognito Sync store?

With Cognito Streams, you can push sync store data to a Kinesis stream in your AWS account. You can then consume this stream and store the data in a way that makes it easy for you to analyze such as a Amazon Redshift database, an RDS instance you own or even an S3 file. We have published sample Kinesis consumer application to show how to store the updates data in Amazon Redshift.

Q: Why should I use Kinesis stream instead of a database export?

By streaming the data to Kinesis you can receive all of the history of changes to your datasets in real-time. This means you receive all the changes an end user makes to a dataset and gives you the flexibility to store this data in a tool of your choice.

Q: What if I already have data stored in Cognito?

When you enable the Kinesis stream feature you will be able to start a bulk publish. This process asynchronously sends all of the data currently stored in your Cognito sync store to the Kinesis stream you selected.

Q: What is the price of this feature?

Cognito pushes the data to a Kinesis stream you own. There is no difference in Cognito's per-synchronization price if this feature is enabled. You will be charged Kinesis' standard rates for your shards.

Q: Can I validate data before it is saved?

Amazon Cognito Events allows developers to run an AWS Lambda function in response to important events in Cognito. The Sync Trigger event is an event that occurs when any dataset is synchronized. Developers can write an AWS Lambda function to intercept the synchronization event. The function can evaluate the changes to the underlying Dataset and manipulate the data before it is stored in the cloud and synchronized back to the user's other devices. Alternatively, the AWS Lambda function could fail the sync operation so that the data is not synchronized to the user's other devices.

Q: How is data synchronized with Amazon Cognito?

You can programmatically trigger the sync of data sets between client devices and the Amazon Cognito sync store by using the `synchronize()` method in the AWS Mobile SDK. The `synchronize()` method reads the latest version of the data available in the Amazon Cognito sync store and compares it to the local, cached copy. After comparison, the `synchronize()` method writes the latest updates as necessary to the local data store and the Amazon Cognito sync store. By default Amazon Cognito maintains the last-written version of the data. You can override this behavior and resolve data conflicts programmatically. In addition, push synchronization allows you to use Amazon Cognito to send a silent push

**Q: What is a silent push notification?**

Amazon Cognito uses the Amazon Simple Notification Service (SNS) to send silent push notifications to devices. A silent push notification is a push message that is received by your application on a user's device that will not be seen by the user.

Q: How do I use push synchronization?

To enable push synchronization you need to declare a platform application using the Amazon SNS page in the AWS Management Console. Then, from the identity pool page in the Amazon Cognito page of the AWS Management Console, you can link the SNS platform application to your Cognito identity pool. Amazon Cognito automatically utilizes the SNS platform application to notify devices of changes.

Q: How are conflicts in the synchronization process handled?

By default Amazon Cognito maintains the last-written version of the data. You can override this behavior by choosing to respond to a callback from the AWS Mobile SDK which will contain both versions of the data. Your app can then decide which version of the data (the local one or the one in the Amazon Cognito sync store) to keep and save to the Amazon Cognito sync store.

Pricing

Q: How much does Cognito Identity cost?

With Amazon Cognito, you pay only for what you use. There are no minimum fees and no upfront commitments.

If you are using the Cognito Identity to create a User Pool, you pay based on your monthly active users (MAUs) only. A user is counted as a MAU if within a calendar month there is an identity operation related to that user, such as sign-up, sign-in, token refresh, and password change. You are not charged for subsequent sessions or for inactive users with in that calendar month. Separate charges apply for optional use of SMS messaging as described below.

The Your User Pool feature has a free tier of 50,000 MAUs each month. The Cognito Identity free tier does not expire at the end of your 12 month AWS Free Tier term, and it is available to both existing and new AWS customers indefinitely.

Federated Identities and secure access control for AWS resources are always free with Cognito Identity.

Q: How much does Cognito Sync cost?

Sync charges are based on the total amount of data saved in the Amazon Cognito sync store and the number of sync operations performed. A sync



As part of the AWS Free Tier, eligible AWS customers receive 10 GB of cloud sync store and 1,000,000 sync operations per month for the first 12 months. Outside the Free Tier, Amazon Cognito costs \$0.15 for each 10,000 sync operations and \$0.15 per GB of sync store per month.

Q: What is a sync operation?

When you call the `synchronize()` method using the AWS Mobile SDK, this counts as a sync operation. If you are calling the server APIs directly, a sync operation is initiated when a new sync session token is emitted and is completed with a successful write or a timeout of the session token. Whether you use the SDK `synchronize()` method or call the server API's directly, sync operations are charged at the same rate.

Q. What are Monthly Active Users (MAUs)?

A user is considered active and counted as a MAU when there is an operation (e.g., sign-in, token refresh, sign-up, or password change) associated with the user during the billing month. Therefore, you are not charged for subsequent operations during the billing month or for inactive users. Typically, your total number of users as well as your number of operations will be significantly larger than your total number of MAUs.

Q. What does it cost to use SMS messages with Cognito?

Use of SMS messaging to verify phone numbers, to send codes for forgotten or reset passwords, or for multi-factor authentication is charged separately. See the [Worldwide SMS Pricing](#) page for more information.

Q: Is Amazon Cognito part of the AWS Free Tier?

Yes. As part of the AWS Free Tier, Cognito offers 10GB of sync store and 1,000,000 sync operations in a month for up to the first 12 months of usage. Your user pool for Cognito Identity is free for the first 50,000 MAUs, and we offer volume-based tiers thereafter. The Federated Identities feature for authenticating users and generating unique identifiers is always free with Cognito Identity.

Q: Does every write or read from the app count as a sync operation?

No. You decide when to call the `synchronize()` method. Every write or read from the device is to the local SQLite store. This way you are in complete control of your costs.

Q: What does push synchronization cost

Cognito utilizes Amazon SNS to send silent push notifications. There is no additional charge for using Cognito for push synchronization, but normal [Amazon SNS rates](#) will apply for notifications sent to devices.



functions, but normal rates for your use of AWS Lambda and other AWS services will apply while your Lambda functions are executing. Please see the [AWS Lambda pricing](#) page for details.

[Sign In to the Console](#)

- [Twitter](#)
- [Facebook](#)
- [Podcast](#)
- [Twitch](#)
- [AWS Blog](#)
- [RSS News Feed](#)
- [Email Updates](#)

AWS & Cloud Computing

[What is Cloud Computing?](#)[What is Caching?](#)[What is NoSQL?](#)[What is DevOps?](#)[What is Docker?](#)[Products & Services](#)[Customer Success](#)[Economics Center](#)[Architecture Center](#)[Security Center](#)[What's New](#)[Whitepapers](#)[AWS Blog](#)[Events](#)[Sustainable Energy](#)[Press Releases](#)[AWS in the News](#)[Analyst Reports](#)[Legal](#)

Solutions

[Websites & Website Hosting](#)[Business Applications](#)[Backup & Recovery](#)[Disaster Recovery](#)[Data Archive](#)[DevOps](#)



[High Performance Computing](#)[Mobile Services](#)[Digital Marketing](#)[Game Development](#)[Digital Media](#)[Government & Education](#)[Health](#)[Financial Services](#)[Windows on AWS](#)[Retail](#)[Power & Utilities](#)[Oil & Gas](#)[Automotive](#)[Blockchain](#)[Manufacturing](#)**Resources & Training**[Developers](#)[Java on AWS](#)[JavaScript on AWS](#)[Mobile on AWS](#)[PHP on AWS](#)[Python on AWS](#)[Ruby on AWS](#)[.NET on AWS](#)[SDKs & Tools](#)[AWS Marketplace](#)[User Groups](#)[Support Plans](#)[Service Health Dashboard](#)[Discussion Forums](#)[FAQs](#)[Documentation](#)[Articles & Tutorials](#)[Quick Starts](#)**Manage Your Account**[Management Console](#)[Billing & Cost Management](#)[Subscribe to Updates](#)[Personal Information](#)[Payment Method](#)[AWS Identity & Access Management](#)



[Contact Us](#)

Amazon Web Services is Hiring.

Amazon Web Services (AWS) is a dynamic, growing business unit within Amazon.com. We are currently hiring Software Development Engineers, Product Managers, Account Managers, Solutions Architects, Support Engineers, System Engineers, Designers and more. Visit our [careers](#) page to learn more.

Amazon.com is an Equal Opportunity-Affirmative Action Employer – Minority / Female / Disability / Veteran / Gender Identity / Sexual Orientation.

Language	Bahasa Indonesia	Deutsch	English	Español	Français	Italiano	Português	Tiếng Việt	Türkçe
	Русский	ไทย	日本語	한국어	中文 (简体)	中文 (繁體)			

[Site Terms](#) | [Privacy](#)

© 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.