Sign in with Apple

Fast, easy sign-in with privacy built in

November 2019

Overview

Sign in with Apple is a new service from Apple that allows users to sign in to apps and websites quickly and easily using the Apple IDs they already have. It's a privacy-friendly alternative to other single sign-on solutions and provides users with the convenience of one-tap sign-in combined with superior security and improved privacy and control over their personal information.

Social login services from major internet brands are convenient to use, but this convenience can come at the cost of the user's privacy. It's common for users to be asked to share their name, email address, friends list, and other profile information when setting up an account with a new app. And the data sharing may not stop there. The persistent identity provided by a social login can be combined with data from tracking pixels and other analytics inside of apps that track the user's browsing habits, clicks, searches, and more, without their knowledge. This collected data amounts to a comprehensive profile of the user's behavior and preferences that may be shared not only with the app the user is engaging with, but also with the company the user has trusted with their identity. And of course, personal data collected in this way can leak, be stolen, and be vulnerable to misuse by any third parties that gain access to it.

Apple believes that great user experiences and great privacy can go hand-in-hand, and that users should be able to enjoy the convenience and security of one-tap sign-in without compromising their privacy. With that principle in mind, Sign in with Apple has been built from the ground up to limit the amount of information that users are required to share, and to provide them with the peace of mind that Apple will not track them as they interact with their apps.

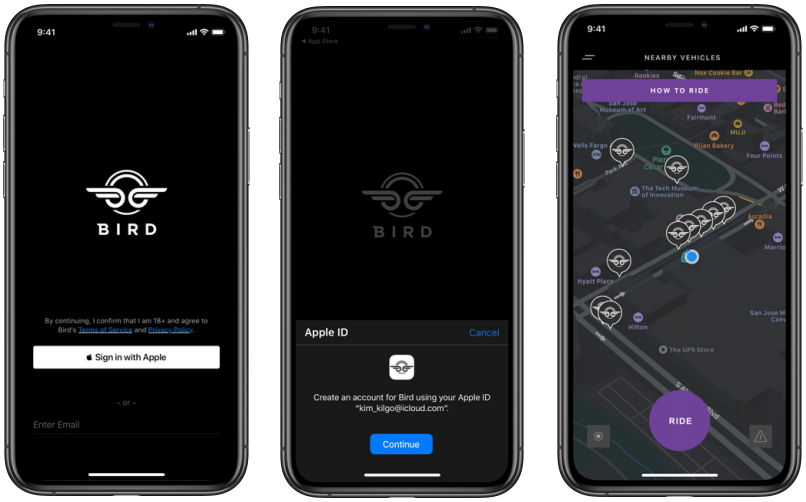
For developers, Sign in with Apple is an opportunity to engage new users quickly and easily. Sign in with Apple provides a superior, one-tap experience for starting an account, superior security with two-factor authentication, and includes a new tool to help fight fraud and scripted account creation.

A simple set of APIs allows any developer to add Sign in with Apple to their app or website. It works on iOS, iPadOS, macOS, watchOS, and tvOS, as well as on the web and other platforms, so developers can implement it anywhere they deploy their apps, including on Android or Windows.

Fast, easy account setup

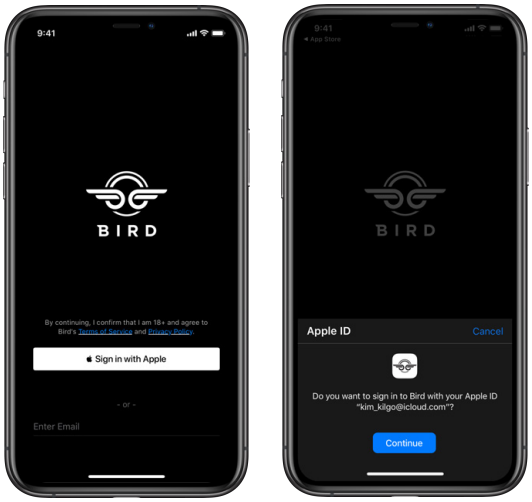
When it's time to set up an account and sign in to a participating app or website, the user can simply look for the "Sign in with Apple" button and give it a tap.

A native sheet appears that allows the user to review relevant information and then tap Continue and complete a simple Apple-approved authentication like Face ID or Touch ID to sign in automatically. Users can sign in to a new app without filling out any forms or sharing any personal information at all. Just a unique, stable identifier that allows the user to sign in again anytime using the Apple ID they already have.



Sign in with a tap

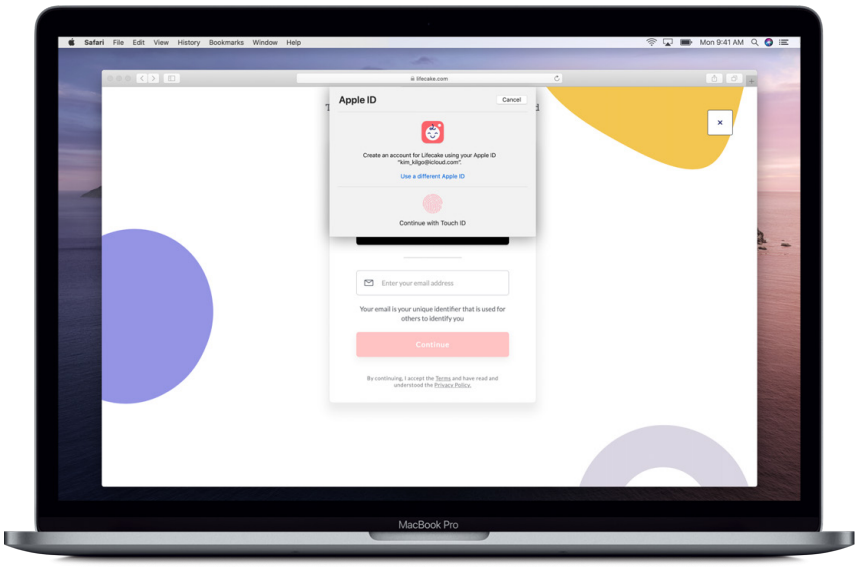
Once an Apple ID–backed account is established with the developer, users can sign in to the app again anytime they like by tapping the Sign in with Apple button again and providing a quick Apple-approved authentication such as Face ID or Touch ID. This seamless sign-in to apps is available on any device where the user is signed in to iCloud with their Apple ID.



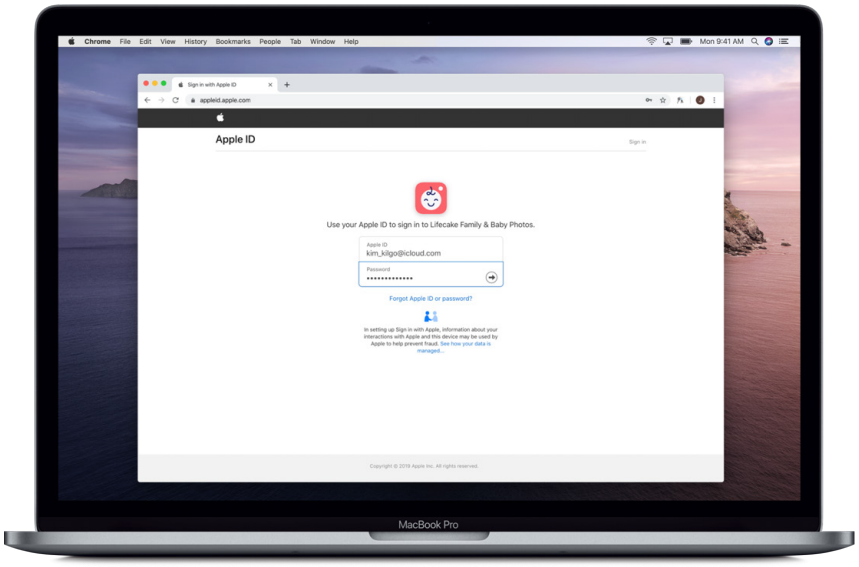
Signing in on the web and other platforms

Users can also use Sign in with Apple to sign in to websites using Safari, Chrome, Firefox, Edge, and other browsers, and to sign in to apps on other platforms such as Android or Windows.

When a user is using Safari on a Mac or any WebKit browser on iOS or iPadOS, a sheet drops down from the navigation bar that allows the user to sign in quickly and easily just as if they were in a native app.



When using other browsers or signing in on a non-Apple platform, the user will need to enter their Apple ID and password into a secure, Apple-hosted web page to identify themselves and complete the sign-in. Otherwise, the experience is the same.



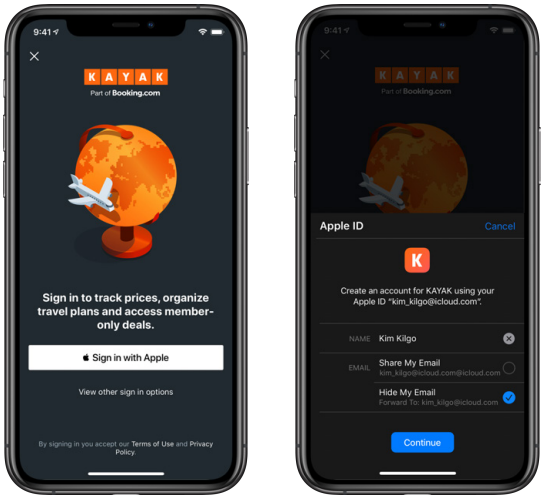
Hide My Email

Some apps and websites require a bit more information to set up a personalized account for their users. To accommodate this, Sign in with Apple allows developers to request a name and email address if required and will pre-populate the requested information from the user's Apple ID account directly to the Sign in with Apple sheet, so the user can review and approve sharing the information with the developer before proceeding. The user can edit their first and last name as needed, and when it comes to their email address, they have a choice: They can choose to share any verified email address on file in their Apple ID account, or choose Hide My Email to share a unique, private relay email address instead. Any email sent by the developer to this address will be forwarded directly to the user's verified inbox. This allows the user to receive useful email messages from the developer, and even respond to messages directly, without revealing their personal email address.

Relay email address
When a user chooses Hide My Email, a private relay email address is created similar to the example below:

56tr9k16b2@privaterelay.appleid.com

Any email messages sent to this address will be forwarded to the user's verified email inbox.



Each relay address is unique to the user and to the developer, so it can't be used for tracking a user across apps or matching with other profile information tied to a personal email address.

To enable sending messages through the private relay service, developers must register the domains and email addresses they use to send messages to their customers. This information allows Apple to forward emails from the developer directly to the participating user's personal inbox and handle direct replies without exposing the user's real email address. It also means that only the developer that controls the registered domains can send emails to the relay email address. The mail system employs standard DKIM, DMARC, and SPF policies to ensure all sending domains are legitimate.

Apple does not read or process any of the content of the email messages that pass through the relay service, except to perform industry-standard spam filtering that is required to maintain Apple's status as a trusted email provider. All email messages are deleted from Apple's servers once they are delivered to the user, usually in a matter of seconds.

The user can turn off their relay address for a given developer at any time. When they do, emails will bounce back to the developer the same way they would if the user's email account had been shut down. The user can decide to provide their real personal email address directly to the developer anytime they like.

No tracking

Perhaps the most significant privacy benefit of using Sign in with Apple is that Apple does not participate in tracking or profiling users and does not seek to profit from users' personal data. Apple will not track users as they engage with their favorite apps and websites, or gather insights about developer's businesses in the process. In fact, Sign in with Apple has been built from the ground up to limit the amount of information Apple can access or store about the user's sign-in behavior.

When a user engages with a new app using Sign in with Apple, Apple generates a unique token for the user/developer pair and stores the email address that the user shares with the developer. This allows Apple to manage secure authentication anytime the user needs to sign in, and allows the user to view and manage their relevant account details. Any subsequent visits to an app can be handled on device without sharing any additional information with Apple. Developers can call a local refresh API (getCredentialsState) to confirm that the user is still securely signed in to iCloud on the device and allow the user to continue using the app seamlessly without ever reaching out to Apple's servers or sharing any additional information.

If an explicit sign-in is required to continue using an app—for example, to sign in to a financial services app with a limited session length—the developer will call an authentication request API (ASAuthorizationAppleIDRequest) that returns a token from Apple's servers to allow the user to quickly sign in again. In this case, Apple receives basic information about the sign-in event, including the IP address and the Apple ID being used, but deletes this information after a maximum of 30 days.

When signing in using a non-Apple web browser or an app running on another platform, Apple is not able to provide an equivalent to the local refresh API. Therefore, developers will need to make a fresh authentication request each time the user needs to sign in. The same token will be returned from Apple's servers and the same 30-day data deletion policy applies.

This is the extent of information that Apple collects regarding users' activity as they use Sign in with Apple. Apple does not provide any tracking tools to developers or receive data from any analytics or advertising tools that might be employed by any particular app. As a result, users can take advantage of the convenience of Sign in with Apple with the peace of mind that Apple is not tracking or profiling them.

Secured with two-factor authentication

Two-factor authentication
Two-factor authentication is an extra layer of security for your Apple ID, designed to ensure that you're the only person who can access your account, even if someone knows your password.

Whenever you sign in to a new device for the first time, you are required to provide your password and a six-digit verification code from one of your other trusted devices, or a trusted phone number.

More detail can be found at:
https://support.apple.com/kb/HT204915

To provide superior security, Sign in with Apple requires the user's Apple ID to be protected with two-factor authentication. This not only protects the user's Apple ID from fraud and other security threats, but also protects the accounts and data that users create in apps they use with their Apple ID. Developers that implement Sign in with Apple get this extra security automatically. Instead of building an elaborate two-factor authentication system themselves, they can employ Sign in with Apple to take care of it for them.

As of September 2019, more than 75 percent of all active Apple IDs had already been protected with two-factor authentication and this number continues to grow, so the vast majority of users can take advantage of Sign in with Apple without any additional requirements. Furthermore, since users are persistently and securely signed in on their devices, they will not receive any additional verification prompts when signing in to apps from an Apple device. A simple Face ID or Touch ID verification takes care of it. On non-Apple browsers and other platforms, the user will need to provide their Apple ID, password, and a verification code on their first sign-in from a new device or browser. However, if they wish, they can skip the verification code step for 30 days by choosing to trust the browser they are using.

Real User indicator for anti-fraud

On-device intelligence
Apple uses machine learning to help make the user's experience with their device and apps more intelligent and personalized. It's used for image and scene recognition in Photos, predictive text in keyboards, and more. Sign in with Apple utilizes on-device intelligence to help determine that the user is a real person, without having to store or analyze any sensitive personal information on Apple servers.

In addition to helping developers engage new customers in an easy and privacy-friendly way, Apple is committed to reducing fraud, scripted account creation, and other bad behavior that can have a negative impact on developers and their businesses. Apple actively controls fraud on its own systems and now offers a simple tool called the Real User indicator to assist apps and services that adopt Sign in with Apple.

The Real User indicator is a binary score that indicates whether Apple is confident the user setting up the account is a real person without any signs of fraud on their Apple ID account, or if there is insufficient information to make a determination.

Apple has gone to great lengths to ensure the indicator is calculated in a privacy-preserving manner. First, on-device machine learning (ML) is employed to measure if the device the account is originating from is being used in a way that's consistent with ordinary, everyday behavior such as moving from place to place, sending messages, receiving emails, or taking photos. This analysis yields a tamper-proof numerical score that is sent to Apple indicating a level of confidence that the device is being used by a real person. The score cannot be reverse-engineered by Apple to reveal any personal information, and none of the specific inputs to the ML models ever leaves the user's device.

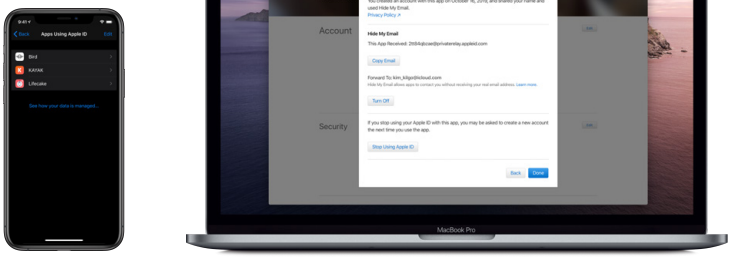
The device score is then combined with select information on recent account activity. The sum of this information is abstracted into the binary Real User indicator that is passed to the developer at account setup time. Developers can

incorporate this information into any existing anti-fraud systems they currently use to help make determinations about how to handle a new customer.

When a developer receives the indication that the account is owned by a real user, they can confidently allow the user to proceed into their app experience without requiring additional verification steps. If the developer receives an "unknown" score, the developer can use the same supplementary verification methods they would normally use for a new account. An unknown score does not necessarily mean that the account is fraudulent or fake, it simply means that there is not enough information available to provide a Real User assertion.

Managing the apps that use your Apple ID

At any time, the user can visit their Apple ID account settings on their device or sign in to https://appleid.apple.com to view all the apps that are using their Apple ID to authenticate. They can review the information they originally shared with each app, view the app's privacy policy, turn off their private relay email address for the app if they wish, or stop using their Apple ID with the app entirely.



Fast, easy sign-in that respects users' privacy

Having a fast, easy, and secure way to sign in to apps and services is essential for both users and app developers. Sign in with Apple was purpose-built to allow for rapid, friction-free on-boarding to new apps, while respecting users' privacy and keeping them in control of their personal information.

Sharing information with apps and services is a natural part of engaging and doing business. Sign in with Apple provides users with more transparency and control when setting up new accounts and using their favorite apps.

Sign in with Apple will be required in any app in the App Store that uses third-party sign-in services to set up and authenticate user accounts. This will help ensure that users always have the choice to use their Apple ID and take advantage of Apple's privacy policies whenever they are also offered the option to use a social login service.

Details on this requirement can be found in Apple's App Store Review Guidelines located at https://developer.apple.com/app-store/review/guidelines. Developers can also visit https://developer.apple.com/sign-in-with-apple for detailed information on how to implement Sign in with Apple in their apps and websites.