

iOS Development: Security

iCloud Keychain is a feature of your Apple account that you can use to keep your website login credentials, personal details, credit card details, and wireless network information up to date and available across all your Apple devices.

Keychain offers a secure alternative to saving sensitive data, such as user names and passwords, with `NSUserDefaults`, plist or similar methods.


With so many usernames and passwords to remember these days, iCloud Keychain provides a convenient way of always having this information at hand. And with its AutoFill feature, iCloud Keychain can even enter your credentials for you when required.

It's also very secure, thanks to Apple's use of end-to-end encryption. This means that only you can access your information, and only on devices where you're signed in to iCloud.

Turn on iCloud Keychain on your iPhone, iPad or iPod touch

- 1 Tap Settings, tap [your name] and then choose iCloud.
- 2 Tap Keychain.*
- 3 Turn on iCloud Keychain. You may be asked for your passcode or Apple ID password.

Turn on iCloud Keychain on your Mac

- 1 Choose Apple menu  > System Preferences.
- 2 Click Apple ID, then click iCloud in the sidebar.
- 3 Select Keychain.*

iCloud protects your information with end-to-end encryption, which provides the highest level of data security. Your data is protected with a key that's made from information unique to your device and combined with your device passcode, which only you know. No one else can access or read this data, either in transit or storage.

When you turn off iCloud Keychain, the password and credit card information is stored locally on the device. If you sign out of iCloud on that device while Keychain is turned on, you'll be asked to keep or delete that information. If you choose to keep the information, it won't be deleted or updated when you make changes on other devices. If you choose not to keep the information on at least one device, your Keychain data will be deleted from your device and the iCloud servers.

Sandboxing

Sandboxing significantly increases the security and integrity of the operating system by limiting what an application is allowed to do. On iOS, for example, an application cannot access the sandbox of another application.

For historical reasons, sandboxing rules for macOS are less strict than those for iOS, tvOS, and watchOS. The macOS operating system and its file

system operate differently and are structured differently.