iCloud encryption explained: How secure is your data?

Apple services use one of two different encryption methods, and one is more secure and private than the other.

By Jason Cross Senior Editor, Macworld FEB 14, 2025 3:15 am PST

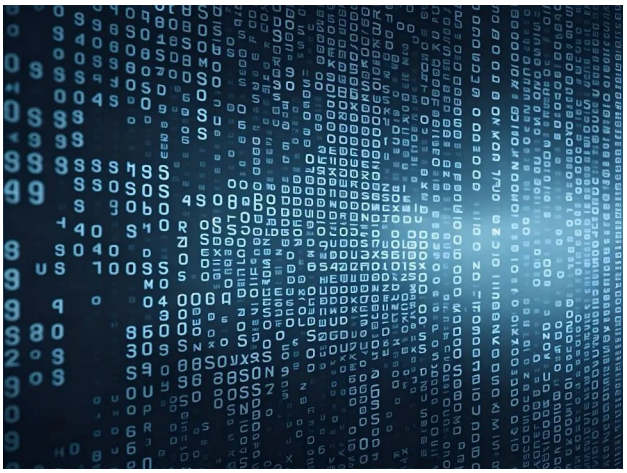

Image: Pixabay

With all the marketing Apple does around privacy, and all the talk lately of government surveillance around the globe, you would hope that the data for all your Apple cloud services is locked down tight.

You may be surprised that a lot of it, depending on the settings you choose, is not nearly as secure as you may think. Here, we'll spell out the difference between Apple's two different encryption methods, discuss the Advanced Data Protection mode, and let you know which services are encrypted in which ways.

All encryption is not the same

Apple employs two different forms of encryption for iCloud services. The most basic type is what the company calls "In Transit & On Server" encryption. The other, more secure method is end-to-end encryption.

In Transit & On Server: Your Apple device has a decryption key, and so does Apple's servers. When you save data to the cloud, it is encrypted on your device so that prying eyes spying on your network can't understand it. It is stored encrypted on Apple's servers, so if a hacker gets access it will all be scrambled and useless.

But, and this is crucial, Apple *does* hold the decryption key and *can* decrypt the data on its servers. It could do this for regular use (to analyze data to provide services) or at the request of governments (the laws for how these requests are made vary from one country to the next).

If you ever lose access to your account, Apple can help you recover your data if you prove you're the legit owner of the account.

End-to-End: E2E encryption means your Apple device has the decryption key, which is tied to your passcode and Face ID/Touch ID biometric, and stored in the secure element hardware. It is encrypted on your device and stays encrypted as it is transmitted to Apple's servers, where it is stored encrypted.

Apple does *not* have the decryption key and has no way to make your data readable at all. It doesn't matter if it gets a legitimate law enforcement request or it wants to analyze your data to provide services–Apple can't see your data and has no way of accessing it.

If you ever lose access to your Apple account and need to recover it, Apple has no way to help you recover E2E encrypted data.

Advanced Data Protection

In 2022, Apple made available a new feature called Advanced Data Protection. To use it, your Apple account must have two-factor authentication enabled, and you must have a recovery key set or recovery contact.

Explore frequently asked questions

Advanced Data Protection takes nearly all the iCloud services and upgrades them to E2E encryption. This makes them *much* more secure, as Apple cannot decrypt your data even if it wants to, but it has the tradeoff of making it possible to permanently lose your data if you lose access to your Apple account and can't recover it with a recovery key or contact.

To enable ADP on your iPhone or iPad, go to Settings, tap on your name, and then tap *iCloud*. Select *Advanced Data Protection* and turn it on. You can read more about Advanced Data Protection here.

How your iCloud data is encrypted

The following table lists the various types of iCloud data for each of Apple's services and the ways they're encrypted.

Note that three types of data are never end-to-end encrypted, even with Advanced Data Protection enabled: iCloud Mail, Contacts, and Calendar. This a necessary compromise to make sure the data is usable in third-party apps. Other mail/contact/calendar clients, especially those you access on something other than your own Apple device, would not be able to use this data if it was E2E encrypted.

Data Type	Standard Encryption	Advanced Data Protection
iCloud Mail	In transit & on server	In transit & on server
Contacts	In transit & on server	In transit & on server
Calendars	In transit & on server	In transit & on server
iCloud Backup (device and Messages)	In transit & on server	End-to-end
iCloud Drive	In transit & on server	End-to-end
Photos	In transit & on server	End-to-end
Notes	In transit & on server	End-to-end
Reminders	In transit & on server	End-to-end
Safari Bookmarks	In transit & on server	End-to-end
Siri Shortcuts	In transit & on server	End-to-end
Voice Memos	In transit & on server	End-to-end
Wallet passes	In transit & on server	End-to-end
Freeform	In transit & on server	End-to-end
Apple Invites	In transit & on server	*special
Passwords and Keychain	End-to-end	End-to-end
Health data	End-to-end	End-to-end
Journal data	End-to-end	End-to-end
Home data	End-to-end	End-to-end
Messages in iCloud	End-to-end	End-to-end
Payment information	End-to-end	End-to-end
Apple Card transactions	End-to-end	End-to-end
Maps	End-to-end	End-to-end
QuickType Keyboard learned vocab	End-to-end	End-to-end
Safari	End-to-end	End-to-end
Screen Time	End-to-end	End-to-end
Siri information	End-to-end	End-to-end
Wi-Fi passwords	End-to-end	End-to-end
W1 and H1 Bluetooth keys	End-to-end	End-to-end
Memoji	End-to-end	End-to-end

* Apple's new Invites app has some special-case rules if you have ADP turned on. If so, unpublished invites are E2E encrypted, but once published, they apply standard "In-transit & on server" encryption unless *all* invitees are also Apple users who have ADP enabled.

Several services, such as Messages and Mail, have specific exceptions and caveats you might want to be aware of. You can read more about them in this Apple support document.

Also note that certain *metadata* is always stored with standard encryption. Your device backup may be E2E encrypted, but Apple stores data like the name, model, color, and serial number using standard encryption, as well as the list of apps and file formats for each backup and the date and time of the backups.

Author: Jason Cross, Senior Editor, Macworld

Jason has written about technology for more than 25 years - first in the gaming press, then focusing on enthusiast PCs and general technology. He enjoys learning how complicated technology works and explaining it in a way anyone can understand.