iCloud security overview

iCloud is built with industry-standard security technologies, employs strict policies to protect your information, and is leading the industry by adopting privacy-preserving technologies like end-to-end encryption for your data.

Data security

iCloud secures your information by encrypting it when it's in transit, storing it in iCloud in an encrypted format, and using secure tokens for authentication. For certain sensitive information, Apple uses end-to-end encryption. This means that only you can access your information, and only on devices where you're signed into iCloud. No one else, not even Apple, can access end-to-end encrypted information.

In some cases, your iCloud data may be stored using third-party partners' servers—such as Amazon Web Services or Google Cloud Platform—but these partners don't have the keys to decrypt your data stored on their servers.

End-to-end encryption requires that you have two-factor authentication turned on for your Apple ID. Keeping your software up-to-date and using two-factor authentication are the most important things that you can do to maintain the security of your devices and data.

Here's more detail on how iCloud protects your data.

Data	Encryption		Notes
	In transit	On server	
Backup	Yes	Yes	A minimum of 128-bit AES encryption
Safari History & Bookmarks	Yes	Yes	
Calendars	Yes	Yes	
Contacts	Yes	Yes	
Find My (Devices & People)	Yes	Yes	
iCloud Drive	Yes	Yes	
Messages in iCloud	Yes	Yes	

Notes	Yes	Yes	
Photos	Yes	Yes	
Reminders	Yes	Yes	
Siri Shortcuts	Yes	Yes	
Voice Memos	Yes	Yes	
Wallet passes	Yes	Yes	
iCloud.com	Yes	—	All sessions at iCloud.com are encrypted with TLS 1.2. Any data accessed via iCloud.com is encrypted on server as indicated in this table.
Mail	Yes	No	All traffic between your devices and iCloud Mail is encrypted with TLS 1.2. Consistent with standard industry practice, iCloud does not encrypt data stored on IMAP mail servers. All Apple email clients support optional S/MIME encryption.

End-to-end encrypted data

End-to-end encryption provides the highest level of data security. Your data is protected with a key derived from information unique to your device, combined with your device passcode, which only you know. No one else can access or read this data.

These features and their data are transmitted and stored in iCloud using end-to-end encryption:

- Apple Card transactions (requires iOS 12.4 or later)
- Home data
- Health data (requires iOS 12 or later)
- iCloud Keychain (includes all of your saved accounts and passwords)
- Maps Favorites, Collections and search history (requires iOS 13 or later)
- Memoji (requires iOS 12.1 or later)
- Payment information
- QuickType Keyboard learned vocabulary (requires iOS 11 or later)
- Safari History and iCloud Tabs (requires iOS 13 or later)
- Screen Time
- Siri information
- Wi-Fi passwords
- W1 and H1 Bluetooth keys (requires iOS 13 or later)

To access your data on a new device, you might have to enter the passcode for an existing or former device.

Messages in iCloud also uses end-to-end encryption. If you have iCloud Backup turned on, your backup

includes a copy of the key protecting your Messages. This ensures you can recover your Messages if you lose access to iCloud Keychain and your trusted devices. When you turn off iCloud Backup, a new key is generated on your device to protect future messages and isn't stored by Apple.

Two-factor authentication

With two-factor authentication, your account can only be accessed on devices you trust, like your iPhone, iPad, or Mac. When you want to sign in with your Apple ID on a new device the first time, you need to provide two pieces of information—your password and the six-digit verification code that's auto-displayed on your trusted devices.

Use of secure tokens for authentication

When you access iCloud services with Apple's built-in apps (for example, Mail, Contacts, and Calendar apps on iOS or macOS), authentication is handled using a secure token. Secure tokens eliminate the need to store your iCloud password on devices and computers.

Health data

End-to-end encryption for Health data requires iOS 12 or later and two-factor authentication. Otherwise, your data is still encrypted in storage and transmission but is not encrypted end-to-end. After you turn on two-factor authentication and update iOS, your Health data is migrated to end-to-end encryption.

If you back up your device on your Mac or iTunes, Health data is stored only if the backup is encrypted.

Privacy

Apple has a company-wide commitment to your privacy. Our Privacy Policy covers how we collect, use, disclose, transfer, and store your information. And in addition to adhering to the Apple Privacy Policy, Apple designs all iCloud features with your privacy in mind.

Learn more

Learn more about advanced security features in the iOS Security Guide.

Published Date: April 09, 2020

Ask other users about this article

Submit my question

See all questions on this article ›

Contact Apple Support

Need more help? Save time by starting your support request online and we'll connect you to an expert.

Get started ›