EBOOK EXTRAS: v9.1
Downloads, Updates, Feedback

TAKE CONTROL OF

iCLOUD

by JOE KISSELL

$14.99

9TH EDITION

Table of Contents

Read Me First

Welcome to *Take Control of iCloud, Ninth Edition,* version 9.1, published in January 2024 by alt concepts. This book was written by Joe Kissell and edited by Glenn Fleishman.

iCloud is Apple's suite of internet services. This book helps you make sense of iCloud, configure it for your needs, and choose the best ways of using each feature.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: "lend" it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted classroom and Mac user group copies are available.

Updates and More

You can access extras related to this book on the web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Access the book in both PDF and EPUB formats. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control website, it has been added to your account, where you can download it in other formats and access any future updates.

Settings vs. Preferences

In macOS 13 Ventura, Apple replaced System Preferences with System Settings, and in most apps, the Preferences window became a Settings window. In this book, I sometimes use a shorthand like "go to Mail > Settings/Preferences" or "open System Settings/System Preferences" to reflect both possibilities; when the details are significantly different, I spell them out separately for Ventura and later, and Monterey and earlier.

What's New in Version 9.1

This update covers changes in iCloud since the previous version of the book was released in February 2023. It also adds coverage of iOS 17/iPadOS 17 while dropping coverage of iOS 15/iPadOS 15 and older releases. The most significant changes are:

- Updated iCloud Feature Changes to include major revisions
- Indicated increased prices for Apple One; see Apple One
- Added a sidebar, Mysterious Confirmation Requests, to reassure you that you haven't done anything wrong if your device prompts you out of nowhere to confirm your identity
- Noted two additional iCloud+ storage tiers (6 TB and 12 TB); see Increase Your Storage
- Explained how to add payment methods for Family Sharing and provided details as to what happens if you disable purchase sharing; see Use iCloud Family Sharing
- Removed a sidebar about My Photo Stream, now that Apple has definitively killed it
- Updated references to the Photos app's People album to People & Pets, as Photos now recognizes recurring animal faces

- Added a new topic, Prevent Items from Syncing, that tells you how to keep any file or folder in iCloud Drive on a Mac from being synced to the cloud
- In Troubleshoot iCloud Drive, provided more detail about dealing with "stuck" uploads and downloads
- Added a sidebar, Other Syncing Issues, about syncing problems for data other than iCloud Drive
- Added a detailed description of how you can access passwords and passkeys from iCloud Keychain in browsers other than Safari; see Use iCloud Keychain in Other Mac Browsers
- Revised much of Use the iCloud Website to reflect mostly small user interface changes
- Made some small changes in Use iCloud on an Apple TV to reflect new ways of doing things in tvOS 17

What Was New in Version 9.0.1

Version 9.0.1 was a minor update to address the following:

- Added two sidebars, About Card Verification Numbers or CVVs and Apple Pay, Safari-Stored Cards, and Safari Settings, which clarify Safari's use of CVV codes for credit cards
- Made another clarification about credit cards in Use iCloud Keychain with Another Password Manager
- Corrected a misleadingly worded statement and a typo in the sidebar iCloud Drive and Backups
- Removed a few lingering references to two-step verification

What Was New in the Ninth Edition

This edition added coverage of Ventura, iOS 16, and iPadOS 16, plus recent changes to the iCloud website. Besides detailing the many adjustments to settings and apps in the latest operating systems, I made the following changes:

- Apple's prices for Apple Music and Apple One increased in October 2022. Current prices now appear in Apple One, Use iCloud Family Sharing, and Understand Apple's Music Services.
- I covered new and significantly changed features for Windows users; see Set Up iCloud for Windows, Use iCloud Music Features, and Manage Your Photos.
- You can disable Private Relay for a single webpage; see Enable and Configure Private Relay. Apple also removed the "beta" label from Private Relay toward the end of 2022.
- I added an overview of how to Share a Photo Library in Ventura, iOS 16, iPadOS 16, or later, as Apple created a newer system than the one in place for years.
- The topics Share Files and Folders on a Mac or PC and Use the Files App for iOS or iPadOS were fully revised to cover interface changes in Ventura, iOS 16, and iPadOS 16.
- Starting in iOS 16 and iPadOS 16, you can create and edit groups of contacts (which can then be used as distribution lists in Mail). See Work with Contact Groups.
- Apple redesigned the iCloud website, so I made the appropriate adjustments in the chapter Use the iCloud Website.
- macOS, iOS, and iPadOS support hardware security keys for two-factor authentication; I mentioned these in Use a Security Key.
- The Protect Your Privacy topic is now divided into a revised discussion of how to Take Basic Privacy Steps and a new topic, Use Advanced Data Protection.

Introduction

iCloud, Apple's collection of online services, offers a simple way to keep all your important data in sync across your devices. iCloud's mission is to propagate your documents, music, TV shows, movies, photos, contacts, calendars, passwords, and other data to all your devices so immediately and automatically that you never think about where your data resides anymore.

But iCloud goes far beyond the concept of syncing. Many features you use on a Mac, iOS/iPadOS device, Apple TV, or Apple Watch want to involve iCloud in some way. You *can* use your Apple device without an iCloud account, but many common tasks will be more awkward or even impossible. And, from Apple's point of view, why would you want to use a device without iCloud? A basic account for syncing, email, and locating devices and people is free, and the iCloud infrastructure makes everything work together much more smoothly.

That's not to say iCloud always works as advertised! When it does, it's wonderful, but the set of services is so complex that problems are bound to occur—and frequently do. Since Apple has made so much of your experience dependent on iCloud, a network outage, software bug, or server malfunction can make the simplest tasks frustrating.

And what about privacy? You can sync your photos and videos instantly across all your devices—great! And the data from your iOS devices is automatically backed up to the cloud—great! And you can share anything with a couple of taps or clicks—great! But storing your private data in the cloud could mean that if someone cracks your account, your private visual moments, your home address, and tons of other personal details could be accessible to identity thieves, financial criminals, and people with prurient interests. You must learn about and take additional steps to address these threats.

And while iCloud is pretty good at keeping your own data in sync, it's poor at sharing data between users. Features like Shared Photo Library, Shared Albums, and Family Sharing point in the right direction, and

they're useful as far as they go. But you still can't easily share a whole address book with your spouse, or a keychain containing usernames and passwords with your family.

There's also the question of hardware support. Apple provides ever-greater support for many of iCloud's features in Windows, but only a smaller subset can be used (after a fashion) on Linux and Android devices. Since Apple is in the business of selling hardware, it stands to reason that iCloud works most fluidly and fully on Apple devices. Macs, iOS and iPadOS devices (iPhone, iPad, and iPod touch), Apple TVs, and Apple Watches offer the best support for iCloud.

In this fully revised ninth edition of *Take Control of iCloud,* I focus on what I consider the interesting parts of iCloud. I show you what iCloud is capable of, how to think about it, and how to put its key features to good use. In the process, I hope to expose you to useful capabilities you never knew existed. But I also tell you how to keep private information secure (even if it reduces iCloud's utility), point out cases in which iCloud may not be the best tool, and occasionally mention other options you can consider.

This version you're reading, 9.0, incorporates the very latest updates to iCloud, including a revamped website, significant improvements to Windows support, a new way to share photos, and major new cloud-storage privacy features. (Apple made some of the largest changes to iCloud in the last several months than they have in years!)

In the pages ahead, you'll find out all you need to know to master iCloud to your best advantage and troubleshoot services when things go awry.

Note: While book covers iCloud features that may work across a range of operating systems, the significant changes in recent years, including the addition of the paid iCloud+ service, require that I focus on macOS 10.15 Catalina and later (especially macOS 13 Ventura and macOS 14 Sonoma), iOS 16/iPadOS 16 and later, Windows 11, and tvOS version 15 and later.

iCloud Quick Start

Although you can skip around freely in this book to learn about the topics that interest you most, I encourage you to read (or at least skim) two early chapters before moving on to the rest: Get to Know iCloud and Set Up iCloud. Those chapters provide important foundational information, which help make sense of material later in the book. If you already read an earlier edition, start with Catch Up with iCloud Changes and then skip those foundational chapters.

Get started:

- Discover what's new in the last year or so—and do a quick Storage Checkup of your iCloud online data storage needs and costs—in Catch Up with iCloud Changes.
- Learn about iCloud and iCloud+ features in Get to Know iCloud.
- Set up all your devices to use iCloud. See Set Up iCloud.
- Get your family set up to share purchases, calendars, location data, and more. See Use iCloud Family Sharing.
- Become familiar with iCloud+, Apple's new name for a collection of storage and services offered with paid tiers. See Use iCloud+.

Keep your data in sync across devices:

- Apple has two cloud-based music services: Apple Music and iTunes Match. Learn how these services work and interact, and find details about iTunes Match in Use iCloud Music Features.
- Use iCloud Photos to sync all your photos among Macs, iOS and iPadOS devices, and the cloud, and use Shared Albums to share photos with other people. See Manage Your Photos.
- Keep your documents and app data current everywhere using iCloud Drive and other forms of in-app syncing. See Keep Documents and App Data in Sync.

- Make sure your major forms of personal data (email, contacts, and calendars) are automatically mirrored across all your devices. See Keep Mail, Contacts, and Calendars in Sync.
- Learn about syncing data from other apps, including Messages, News, Safari, Siri, and more. See Sync Other iCloud Data.
- Keep usernames, passwords, and credit card numbers in sync across devices, generate new random passwords, and edit your saved credentials as you Work with iCloud Keychain.

Use the other iCloud features:

- Cut, copy, and paste from one device to another when you Use Universal Clipboard.
- Access web-based versions of the core iCloud apps on nearly any platform. See Use the iCloud Website.
- Locate a wayward Apple device, find a friend or family member, and track AirTags and Find My items. See Find My Nouns.
- Learn how iCloud can back up and restore crucial data from your iOS devices in Back Up and Restore iOS/iPadOS Data.
- Own an Apple TV? Find out which iCloud features your streaming box can use and how. Read Use iCloud on an Apple TV.
- Update your iCloud account details. See Manage Your Account.
- Keep your account safe and protect your private data, including deciding whether to enable Advanced Data Privacy (ADP) for extra protection. See Manage iCloud Security and Privacy.
- Understand and configure account recovery options for yourself and with the help of trusted people while you're alive, as well as appointing helpers after you're gone. See Manage Account Recovery.

Catch Up with iCloud Changes

If you've been using iCloud for a while, the bits that have changed recently will be of most interest to you. This chapter highlights major changes to take advantage of, points you to chapters where I discuss those features in detail, and offers a suggestion about managing your iCloud data storage.

iCloud Feature Changes

Apple sometimes makes changes to iCloud when it suits them, but significant changes commonly appear alongside with updated versions of Apple's operating systems—particularly macOS and iOS/iPadOS. Since the eighth edition of this book (version 8.0) was released, the following changes were made and incorporated into the ninth edition you virtually hold in your hands:

- **Higher prices:** Apple raised the cost of Apple Music and Apple One; see Apple One, Use iCloud Family Sharing, and Understand Apple's Music Services.
- **Higher storage tiers:** You can now increase your iCloud+ storage to 6 TB or 12 TB. See Increase Your Storage.
- **More flexible Family Sharing payments:** You can now have more than one payment method available for Family Sharing members, and it's possible for each family member to use an individual payment method, too. See Use iCloud Family Sharing.
- **Private Relay improvement:** You can disable Private Relay for a single webpage; see Enable and Configure Private Relay.
- **New Windows features:** Windows users gain access to several features. A Windows user can access iCloud Photos in the Microsoft

Photos app (see Manage Your Photos); sync iCloud bookmarks with Edge, Chrome, or Firefox; and sync iCloud passwords with Edge or Chrome (see Set Up iCloud for Windows). Plus, Apple has previewed new apps to take over some of the duties of the increasingly out-of-date iTunes for Windows; see Use iCloud Music Features.

- **Shared Photo Library:** In addition to sharing individual albums and photos, you can now share an entire Photo Library with up to five other people. See Share a Photo Library.
- **Sharing iCloud Drive data:** In Ventura, iOS 16, and iPadOS 16, Apple completely revamped the user interface for sharing files and folders. See Share Files and Folders on a Mac or PC and Use the Files App for iOS or iPadOS.
- **Contact groups:** Although not a change to iCloud as such, iOS 16 and iPadOS 16 and later support creation and editing of groups in Contacts, which can be used as distribution lists in Mail (and sync across devices using iCloud). See Work with Contact Groups.
- **Revamped iCloud website:** The iCloud.com website was redesigned, so I've updated Use the iCloud Website accordingly.
- **More privacy:** Apple added an Advanced Data Protection feature that can encrypt more of your data end-to-end…if you can meet the stringent requirements. See Use Advanced Data Protection.
- **Expanded iCloud Keychain support:** It's now possible to access passwords and passkeys in your iCloud Keychain from browsers other than Safari. See Use iCloud Keychain in Other Mac Browsers.

Storage Checkup

Some iCloud features (especially Desktop and Documents folder syncing) eat into your iCloud storage quota quickly, but the cost of extra storage is low enough that it shouldn't be a hardship for most users to store as much data as they want. If you're still trying to make do with the 5 GB Apple offers for free, my professional advice is to *give*

up! It's no longer worth the effort to avoid what could be as little as a 99-cent monthly charge for a 50 GB iCloud+ upgrade.

A backup of a single iOS or iPadOS device almost always surpasses 5 GB, after all, and by the time you add saved email, files in iCloud Drive, and other smaller bits of information, you're in for some frustration if you try to whittle the figure down to avoid paying a dollar a month. With upgraded storage, you can freely back up your iOS and iPadOS devices, add files to iCloud Drive, and so on, without worrying that you'll bump into your limit.

A few years ago, Apple brought their storage prices down to comparable offerings from other giants, like Microsoft and Google, and iCloud+ adds more services to help justify the price. The mid-tier offering, 2 TB, is now an affordable $9.99 per month. If you have that much space available, you may find interesting uses for it that hadn't occurred to you before. (Apple added 6 TB and 12 TB tiers in 2023.)

Note: I talk about what data Apple includes in your iCloud storage ahead, in About iCloud Storage. I cover how to buy more storage in Check and Modify Your Storage Usage. iCloud+ has its own chapter: Use iCloud+.

Apple provides an additional incentive for upgrading for family groups by allowing pooled storage as part of Family Sharing. If members of your family currently pay for various tiers of storage, it's almost always cheaper to consolidate into a pool—see Share iCloud+ Features for details. Apple One subscriptions can save a family even more, as I discuss next.

Apple One

The Apple One bundles offer different combinations of Apple's paid subscription services at a discount off purchasing three or more separately. There are three tiers:

- **Individual:** Apple Music, Apple tv+, Apple Arcade, and iCloud+, including 50 GB of storage for $19.95 per month

- **Family:** Apple Music, Apple tv+, Apple Arcade, and iCloud+, including 200 GB of storage for $25.95 per month
- **Premier:** Apple Music, Apple tv+, Apple Arcade, Apple News+, Apple Fitness+, and iCloud+, including 2 TB of storage for $37.95 per month

Family Sharing groups can obviously subscribe to the Family tier or can opt for Premier, allowing the subscriptions to be shared among as many as six family members. (See Use iCloud Family Sharing.)

If you sign up for an Apple One plan, you can still buy *even more* storage—for example, you could purchase the Premier plan and also buy 2 TB of storage for an additional $9.99 per month, 6 TB for $29.99 per month, or 12 TB for $59.99 per month, to get a total of 4 TB, 8 TB, or 14 TB of storage, all of which can be shared with family members.

Get to Know iCloud

Before you dive in and start setting up and using this mysterious thing called iCloud, you should take a few moments to get your bearings and understand what you're dealing with.

In addition to explaining what you can and cannot do with iCloud, this chapter discusses what you need to know About iCloud System Requirements, About Your Apple ID, and About iCloud Storage.

What Is iCloud?

The cloud is a general computing concept: a set of software, services, and storage located (gestures broadly) *out there somewhere*. Companies that offer cloud services maintain all the hardware, and you don't need to know where any of it lives. Your access to the cloud is mediated by the service provider.

iCloud follows this notion precisely: it's a cloud-based set of services and storage defined and controlled by Apple that exists as a collection of servers in data centers around the world. As presented to you, it's a bunch of services you can just use with no server knowledge.

In some respects, iCloud has much in common with services like Dropbox, Google Docs, and Microsoft 365. Yet because of iCloud's tight integration with Apple's hardware, iCloud is designed to achieve specific goals that Apple has in mind as opposed to the general availability of stuff. Google Photos doesn't work only on Android phones, while Apple's iCloud Photos is deeply tied in to iPhones, iPads, and Macs.

Note: Amazon (via Ring) and Google (via its own brand and Nest) integrate home-security hardware and services with their cloud, a little more Apple-like.

Apple uses the label iCloud to cover an ever-growing broad collection of features, services, and settings. The common thread is that they rely on communication among Apple devices (Macs, iOS and iPadOS devices, Apple TVs, HomePods, and Apple Watches), Apple's servers in the cloud, and the broader internet (for anonymized browsing).

Here's what iCloud does for you:

- **iCloud lets iOS and iPadOS devices stand alone.** Originally, the only way to move certain kinds of data on and off your iPhone, iPad, or iPod touch was to connect it to a Mac or PC—at first, with a USB cable, and later, via Wi-Fi. A computer was required to activate the device; to back up or restore its data; to sync photos, music, movies, books, and apps; to transfer documents to and from certain apps; and to install operating system updates.

  With iCloud, your iOS or iPadOS device can operate as a completely standalone product. iCloud lets you transfer data to and from Apple's servers using either a Wi-Fi or cellular connection.

- **iCloud integrates your devices with each other.** If you have more than one device—say, two Macs; or a PC and an iPhone; or an iPhone, an iPad, and an Apple Watch; or an iPad and an Apple TV—it's only natural to want all your devices to share data.

  iCloud syncing encompasses many kinds of data. In fact, the word "sync" almost becomes an anachronism; for the most part, iCloud pushes new or changed data almost instantly to all your devices. You can switch between devices with impunity, knowing your data is always wherever you need it.

- **iCloud replaces (some) local storage with streaming.** iCloud reduces the need to keep all your important media on all your devices. As long as you have a good internet connection, your Mac and iOS/iPadOS devices can now do what the Apple TV has done for many years: fetch the content you want from the cloud in near real time. This makes it practical to get by with less storage space. You also no longer have to decide which content to put on which device; in a sense, everything can be everywhere, automati-

cally, with Apple caching local copies of frequently used stuff. You can also still store local copies of crucial data for times when an internet connection is unavailable.

- **iCloud facilitates (limited) sharing.** Although sharing data between people is one of iCloud's biggest weaknesses, iCloud does help in certain categories. For example, Family Sharing enables family members to easily share purchases, photos, a calendar and reminder list, location information, and more. Shared Albums can pool images and access among a group of people. iCloud Drive lets you send read-only or read-write links to selected files and folders, or even permit others to collaborate with you in real time using iWork apps. And Mail Drop lets Apple Mail (on all platforms) send ginormous email attachments without overloading either the sender's or recipient's mail server.
- **iCloud increases security and convenience.** With Find My, iCloud lets you locate a wayward device (and lock or erase it if it's stolen), see where someone is (if they've granted permission), and track misplaced or stolen belongs that have Find My trackers attached. Even if you find yourself without any Apple device at your disposal (unthinkable!), you can get to your email, contacts, calendars, and more (or find your wayward Mac or iOS/iPadOS device) from nearly any device with a web browser and internet connection.

Tip: If you're curious to know the extent to which Apple encrypts your iCloud data and what other privacy and security measures are in place, read Apple's article iCloud data security overview.

- **iCloud is infrastructure.** Apple designed iCloud to be mostly invisible; you shouldn't have to think much about iCloud day to day. With everything working correctly, iCloud functions in the background, hopefully like your home's electrical wiring or plumbing, transporting the right bits to the right places without any manual intervention. You'll notice iCloud's effects—increased ease of use, less aggravation, more flexibility—even if you're not conscious of interacting with it deliberately.

Major iCloud Features

iCloud constantly gains and loses features over time due to Apple's changing priorities and as its hardware and software evolve. As of January 2024, iCloud (and iCloud+ as noted) include the following major features, all of which I discuss later:

- **Media syncing:** Even without iCloud, you can buy music, apps, or books from Apple on any Mac, PC, or iOS/iPadOS device and have them automatically pushed to all your other devices. You can also re-download previously purchased media (including TV shows and movies) from any of your devices.

  An optional paid feature, iTunes Match, extends media syncing to work with music from sources other than the iTunes Store. iTunes Match is separate from Apple Music, but both use the same mechanism to sync tracks across your devices. (If you subscribe to Apple Music, there's no utility in also paying for iTunes Match.) See Use iCloud Music Features.

- **Family Sharing:** iCloud Family Sharing lets families of up to six people link their individual accounts into a family group. This gives each person access to most apps, in-app purchases, subscriptions, and media purchased by the others; a shared calendar, reminder list, and photo album; home security video footage stored with iCloud+; and location information. Family members can share a payment method (such as a credit/debit card or PayPal) for all Apple media purchases, and children can use the Ask to Buy feature to get parental approval for downloads. You can opt for the iCloud+ 200 GB or 2 TB tiers as a family group, and then that space is shared with other family members. See Use iCloud Family Sharing.

- **iCloud Photos:** Continuing with the theme of automatically propagating data, iCloud Photos lets you sync all your photos and videos (including your People & Pets album) across all your Apple devices. Shared Albums lets you share albums containing photos and videos with others, as well as stream photos from iCloud to an Apple TV. A Shared Library feature lets you go even further by

adding a parallel library that lets you share everything in it with a group of up to five other people; see Share a Photo Library. You can also share individual photos or videos; see Manage Your Photos.

Note: If you choose to identify faces or pets in the People & Pets album on any of your devices, Apple syncs only an abstraction of that information, using end-to-end encryption, which prevents Apple or anyone else from gaining access to the names, faces, and pets you've associated. (Pets were added in fall 2023.)

- **Syncing files via the iCloud Drive folder:** iCloud Drive provides centralized cloud storage for your documents, synced automatically across your Macs using the iCloud Drive folder. Files are also accessible via the Files app in iOS and iPadOS and the iCloud Drive web app on the iCloud website. See Keep Documents and App Data in Sync.
  - **Desktop and Documents folder sync:** You can sync the entire contents of a Mac's Desktop and Documents folders with iCloud and from there to other Macs. As with other files, they're also accessible in the Files app for iOS/iPad and on the iCloud website. This folder sync optionally removes the least-used files from your Mac if you start running low on space while leaving them available in cloud storage. macOS puts placeholders in the Finder for files it removes like this, and automatically downloads offloaded files when you attempt to open them. See Sync Your Desktop and Documents Folders (or Don't).
  - **Sharing documents and folders:** Not only can you store stuff for yourself on iCloud Drive via macOS, the Files app in iOS/iPadOS, or the iCloud Drive web app; you can also share files and folders with others—either read-only or read-write. See Share Files and Folders on a Mac or PC and Use the Files App for iOS or iPadOS.
- **App data syncing:** macOS, iOS, iPadOS, watchOS, and tvOS apps that don't use documents per se can take advantage of iCloud's infrastructure for storing and syncing other data, such as prefer-

ences and database entries. Apps available across multiple Apple operating systems can access that synced data.

- **Calendar, Contacts, Home, Mail (settings, Mail Drop), News, Notes, Reminders, Safari (bookmarks, reading list, browser tabs), Stocks, and Voice Memos:** With this set of apps and services, iCloud keeps your personal data in sync among your devices, and lets you access much of this data from any web browser. In addition, Mail Drop, a feature in Apple Mail for macOS, iOS, iPadOS, and the Mail web app, uses iCloud to simplify sending large attachments. See Keep Mail, Contacts, and Calendars in Sync and Sync Other iCloud Data.

Note: Mail uses the standard IMAP protocol to sync messages to iCloud's mail server. iCloud syncs Mail settings and lets you use Mail Drop within the Mail app in macOS, but doesn't sync mail archives stored in On My Mac mailboxes in Mail for macOS.

- **iCloud Private Relay (iCloud+):** Use Safari for anonymized web browsing to keep your travels private in iOS, iPadOS, and macOS. See Browse the Web Privately.
- **Hide My Email (iCloud+):** Use Hide My Email to create unique email addresses to send messages from, and Apple relays any replies back to you. See Hide Your Email Address.
- **Messages in iCloud:** iCloud can sync all your iMessage and SMS conversations from Messages across your devices. See Sync Messages.
- **Other app data:** You can sync Siri across your devices, so that what Siri learns about you on one device can inform its responses to you on other devices. And, you can sync data from the Health app (iPhone only) to other iPhones. See Sync Data from Other Apps.
- **Universal Clipboard:** Merely by having two or more Macs, iOS, or iPadOS devices signed in to the same iCloud account, you can copy or cut something on one device and paste it on another. See Use Universal Clipboard.

Continuity and iCloud

Apple considers Universal Clipboard to be part of Continuity, which also includes Handoff, support for cellular calls and SMS/MMS on Macs and iPads without cellular radios, Instant Hotspot, Auto Unlock (which lets an Apple Watch unlock a Mac), AirPlay to Mac (starting in Monterey), and Apple Pay from a Mac without Touch ID via an iPhone or Apple Watch.

Apple also uses Continuity for a set of hardware sharing features, which now includes:

- **Continuity Camera for capture:** Take a photo or video with your iOS or iPadOS device and insert it instantly into a Mac app.
- **Continuity Camera for streaming:** A Mac running macOS 13 Ventura or later can use your iPhone (iOS 16 or later) as a webcam.
- **Universal Control:** Use one keyboard and pointing device for multiple Macs and iPads.

Apple doesn't mention Continuity features on their iCloud User Guide page or otherwise lump them in with iCloud, so it's unclear to me whether Apple regards them as part of iCloud as such. However, all the features require users to be signed in to the same iCloud account on the various devices involved.

- **iCloud Keychain:** iCloud Keychain securely syncs passwords, credit card numbers, and account information among devices. It includes other features, too, such as a random password generator built into Safari. And third-party apps can also access items in your iCloud Keychain. See Work with iCloud Keychain. (iCloud Keychain uses device-based end-to-end security, so it can't be accessed from the iCloud website.)
- **icloud.com:** Apple's iCloud website contains web apps, accessible from nearly any browser, that let you work with many types of data—email, contacts, calendars, reminders, notes, photos, and iCloud Drive documents—as well as web-based versions of Pages, Numbers, and Keynote. See Use the iCloud Website.
- **Find My:** The Find My app shows you the exact location of any of your Apple devices; you can even remotely lock or wipe any of these

devices. You can also locate friends—via their iOS/iPadOS devices or Series 3 or later Apple Watches—who have given you permission to follow them. And a clever crowdsourcing feature lets Find My securely discover the location of your lost or stolen hardware even if the device lacks an active internet connection, as well as Find My items, which includes Apple's AirTag trackers. See Find My Nouns.

- **iCloud Backup:** iCloud securely and automatically backs up all the personal data from your iOS and iPadOS devices to Apple's servers and lets you restore it over the air. See Back Up and Restore iOS/iPadOS Data.
- **Apple TV:** Your Apple TV can access not only any media you purchased on your other Apple devices but also your Music library and iCloud Photos. You can also access an Apple TV+ subscription associated with your account. See Use iCloud on an Apple TV.

Tip: Apple TV+ has almost nothing to do with an Apple TV. You can watch Apple TV+ programming via more devices and browsers than any other Apple service.

- **Home:** Devices you set up using the Home app in iOS, iPadOS, or macOS become available through iCloud across all your devices.
- **HomeKit Secure Video (iCloud+):** A number of home security cameras can store their video recordings using HomeKit Secure Video, part of iCloud+. This video storage doesn't count against your iCloud+ storage totals. See Add Security Camera Features.

Peer-to-Peer Networking

iCloud automatically recognizes other devices on a local network and syncs content between them where appropriate instead of using the cloud. You won't waste internet bandwidth downloading data that's already on another local device—plus copying that data is quicker over your local network. (iCloud-connected services will upload content as necessary to the cloud after syncing it locally.)

About iCloud System Requirements

Since iCloud is a heterogeneous collection of services and capabilities, it doesn't have a fixed set of system requirements. Some aspects of iCloud require at least iOS 16.1, iPadOS 16.1, macOS 13 Ventura, Windows 11, or an Apple TV HD or Apple TV 4K with tvOS 16 or later, although many services are supported as far back as iOS 5, 10.7.5 Lion, the second-generation Apple TV, or Windows 7. Other parts of iCloud are accessible from nearly any web browser or from any of numerous third-party apps.

Apple would love it if you had the latest of everything, of course, and this book focuses on the last few releases of everything, as described in the Introduction.

Apple's System requirements for iCloud page lists the oldest support offered among Apple's operating systems for iCloud's various features. However, that list omits third-party client software requirements for email, calendars, and contacts. Here are the details:

- **Email:** Any IMAP client with SSL support, on any platform, should be able to connect with your iCloud email account. The server addresses may be different from what you expect, however; see the sidebar Access iCloud Mail with Other Email Clients.
- **Calendars and Contacts:** iCloud uses standard protocols: CalDAV for calendars and CardDAV for contacts. However, for reasons that aren't entirely clear to me, not all CalDAV and CardDAV clients can connect to iCloud accounts.

  BusyCal and BusyContacts are the only third-party Mac apps I'm aware of that can connect to iCloud for calendar and contact syncing, respectively. Under Windows, eM Client also supports iCloud calendars and contacts.

About Your Apple ID

To use iCloud, you need a username called an *Apple ID,* which identifies you across numerous Apple products and services. You probably already have an Apple ID. If not, it's easy (and free) to get one.

Tip: For far more detail on understand and managing Apple IDs than I can provide here—including extensive troubleshooting help and guidance on using two-factor authentication—see Glenn Fleishman's book *Take Control of Your Apple ID*.

Although Apple once allowed any unique name to be an Apple ID, now they require all Apple IDs to be email addresses. If you already have an email address ending in `@icloud.com`, `@me.com`, or `@mac.com`, that's an Apple ID for sure. If you used a different email address when buying something from Apple, registering for an Apple developer program, or using any of several other Apple services, that address is also an Apple ID.

That's all fairly straightforward, but iCloud's reliance on Apple IDs has several consequences that may not be apparent—for example, you might have more than one Apple ID and not know which one to use for iCloud, or you might share an Apple ID with someone else. Read on to find out what to do about cases like these.

What If I Have Multiple Apple IDs?

In a perfect world, each person would have exactly one Apple ID, all the person's data and purchases would be associated with it, and the question of which Apple ID to use where wouldn't come up. However, for a variety of reasons, a great many people have accumulated more than one *personal* Apple ID over the years.

Note: People who were members of MobileMe or .Mac may have me.com, mac.com, and/or icloud.com addresses with the same characters before the `@` sign. Apple regards those variants as identical; use any of them to sign in to iCloud. But read the sidebar Apple IDs with Multiple Email Addresses, ahead, for qualifications.

Apart from the clutter of multiple accounts and having one's data in several places, there's one big practical problem with having multiple Apple IDs. Whereas you can copy personal data, such as contacts and email messages, from one account to another, you can't do the same thing with *purchases*. Once you've made a purchase from Apple with a given Apple ID, the purchase is tied to that ID permanently. You can't transfer a purchase to a different Apple ID, and you can't merge two Apple IDs in order to consolidate your purchases into one account.

iCloud Family Sharing (see Use iCloud Family Sharing) mostly erases the irritation of purchases under multiple Apple IDs within a family. Each person signs in with an individual Apple ID, but because they're all linked (up to six of them), each family member can access most purchases the others have made.

But if Family Sharing isn't appropriate for your situation—namely, you need to share purchases with someone who's not in your family—you can often work around the problem. Although Music, the Mac App Store, the iOS or iPadOS App Store, and the Book Store can each log in with only one Apple ID at a time, you can switch between IDs without losing any content. In the relevant app, find the Sign Out button or menu command, and then sign back in with the other account. Note that doing so requires you to know (or have someone else enter) the password for the other account.

Some people have multiple personal Apple IDs because they have more than one iCloud account that they need to keep separate—perhaps a home account and a work account, or a personal account and a club account. Others register different Apple IDs for different countries in which they live or travel to for extended periods. It is possible to sign in to multiple iCloud accounts on a Mac at the same time, although as I explain ahead shortly, doing so carries a few restrictions.

What If I Share an Apple ID with Someone?

Apple expects a single individual to use each Apple ID (and each iCloud account). Indeed, the very design of most iCloud features assumes this is the case. As a result, if you try to share an iCloud

account with someone else, all sorts of undesirable results occur. Nevertheless, many people do share a single account with a spouse, an entire family, or another group.

Although I've met couples who truly do want to share *everything* in common, including email, the most common reason for sharing Apple IDs apart from consolidating purchases (for which purpose you should now Use iCloud Family Sharing if possible) is sharing contacts. Because iCloud doesn't offer any form of contact sharing, some people have an extra iCloud account for the express purpose of adding it to multiple users' devices in order to achieve the effect of shared contacts without having to share *all* data.

I explain just ahead how to handle a shared Apple ID. But even if you have a shared account, you should *also* have an individual account—partly to keep your personal settings separate from those of other family members and partly to avoid syncing errors and other random problems that can occur when a shared accounts is also each person's *primary* account. If you have *only* a shared account, you should create an individual account for yourself when setting up iCloud.

Which Apple ID Should I Use for iCloud?

All that said, which Apple ID should you use when you set up iCloud? Here are my suggestions. If you have…

- **A single, *personal* Apple ID:** That's the one to use—Done!
- **A single, *shared* Apple ID:** Create a new Apple ID for yourself. Afterward, you can go to System Settings/System Preferences > Internet Accounts and add the shared Apple ID as a secondary account (see Work with Multiple iCloud Accounts).
- **Multiple individual Apple IDs:** Use the Apple ID associated with whichever you consider your primary or personal account—the one that contains most of your data. Later, you can go to System Settings/System Preferences > Internet Accounts (or, in iOS/iPadOS, Settings > Accounts & Passwords > Add Account) and add

one or more secondary iCloud accounts—for example, to sync shared contacts or to provide access to another email account.

Note, however, that any iCloud account you sign in to after the first one can be used on that particular device only for email, contacts, calendars, reminders, and notes; it can't access Safari data, photos (iCloud Photos or Shared Albums), iCloud Drive, iCloud Keychain, or Find My *Device*. (I say more about this later, in Use Multiple iCloud Accounts on a Mac and Work with Multiple iCloud Accounts.)

So, for example, if you wanted to share iCloud contacts with your spouse, the ideal way would be for each of you to configure an individual iCloud account on your respective devices, which then becomes the primary account for each device. Next, set up another iCloud account, just for contacts, which each of you adds as a secondary account on each device (see Share Your Contacts with Someone Else). You could, in theory, make another account for notes, but for any other data type, this sort of sharing either won't work at all or is highly likely to cause problems.

Note: If you're the organizer for an iCloud Family Sharing group (see Use iCloud Family Sharing), you should enter the Apple ID associated with Family Sharing as your primary iCloud login.

- **A personal Apple ID *plus* a separate Apple ID you've used for shared purchases:** The best way to handle this is to use only your personal Apple ID, set it up to use your preferred credit card, and add other family members to iCloud Family Sharing. If that won't work in your situation—for example, if you use a business credit card for purchases—enter your personal Apple ID during iCloud setup. Later, you can open the Music app (and the Mac App Store and Books or iBooks) and sign in with the other Apple ID you use for purchases.

Note: Game Center, FaceTime, and iMessage also use Apple IDs, but these services are not part of iCloud, so if you prefer, you can use a different Apple ID for them than you do for iCloud.

- **One or more Apple IDs, but *not* an iCloud account:** The process of setting up iCloud will turn your Apple ID into an iCloud account. Enter your Apple ID; if you have more than one, pick the ID that you've made the most purchases with. You will be prompted to provide additional information for the conversion, including selecting an email address in the icloud.com domain.
- ***No* Apple ID:** If you have never had an Apple ID at all—unlikely, I realize, for users of Apple products—you can create one now at the Create Your Apple ID page on the Apple ID site.

Apple IDs with Multiple Email Addresses

It has always been possible to associate additional email addresses with any Apple ID. These can serve a number of purposes, but the most important one is that extra addresses give Apple another way to verify your identity and give you access to your account if your main address changes. (For example, that's extremely helpful if you used your work address to set it up and you leave your job.)

That's all well and good, but it leads to a subtle yet common problem. If you try to sign up for a new Apple ID using an email address that has already been added as an alternative address to another Apple ID, you'll get an error message—Apple doesn't allow this. You must first remove an email address as an alternative from all other Apple IDs before using it for a new one.

The tricky part is that Apple offers no surefire way to match any given email address to a specific Apple ID. Apple previously offered a webpage that let you look through any existing Apple IDs you may have for the email address in question. However, that page no longer exists, and even when it did, the process was hit-or-miss.

About iCloud Storage

A basic iCloud account includes 5 GB of free storage space. You can upgrade to iCloud+ for more storage if that's not enough while gaining access to additional services. Prices vary by location; in the United States, you pay the following monthly prices: 50 GB of iCloud+, $0.99;

200 GB, $2.99; 2 TB, $9.99; 6 TB, $29.99; 12 TB, $59.99. There is no annual payment plan or discount.

Many types of data *don't* count against that 5 GB limit. A partial list:

- **Purchases from the iTunes Store:** Music, TV shows, movies, apps, and books don't take up any of your personal space, because Apple already has copies of that data on their servers.
- **Photos outside iCloud Photos:** Photos you've shared with Shared Albums don't count, no matter how many you have or what their resolution is. (I explain this in Manage Your Photos.)
- **Mail Drop attachments:** Email attachments sent with Mail Drop (see Use Mail Drop) also don't count against your quota.
- **Shared iCloud Drive data:** If you accepted a shared folder in iCloud Drive from someone else, the storage consumed by that folder doesn't count towards your total.
- **HomeKit Secure Video:** Any iCloud+ account includes support for home security cameras that use HomeKit Secure Video: the 50 GB plan allows one camera; the 200 GB plan, up to five cameras; and the 2 TB and higher tiers, any number of cameras. The storage doesn't count against your iCloud total. You can access stored video only via the native Home app in iOS, iPadOS, or macOS because it relies on device-based end-to-end encryption for your privacy and security. (See Add Security Camera Features.)

What *does* count against your storage quota is documents, including everything kept in iCloud Drive; your iCloud Photos (including a Shared Photo Library, if you're the one doing the sharing); iCloud email, including attachments sent *without* Mail Drop; iCloud for Messages (messages and attachments); Pages, Numbers, and Keynote for iCloud files; and—if you've enabled iCloud Backup—each of your iOS/iPadOS devices' personal settings, app data, locally stored photos, and a few other items that would appear at first glance to occupy little space altogether.

Those backups can require more iCloud storage than you might think. For example, at this moment my iPhone uses 13.3 GB of space for iCloud backups, and my iPad Pro uses 13.9 GB—and remember, that's for data that isn't already on Apple's servers somewhere. A backup of just one of those devices puts me well over the 5 GB limit, and I have other data I need to store in iCloud. (iCloud doesn't require you to back up iOS or iPadOS devices to the cloud; you can back them up to your Mac or PC via the Finder—or iTunes for Windows—if you prefer).

Note: In the likely event that you want to understand the specifics of what's taking up space in your iCloud storage or you want to buy more storage, see Check and Modify Your Storage Usage, later.

Set Up iCloud

iCloud setup, in and of itself, is easy and largely self-explanatory: you enter your Apple ID and password, and click a few buttons on each of your devices. There's no software to install on a Mac or iOS/iPadOS device and it includes only a few options you can turn on or off. You have to go through a few more steps under Windows.

However, you may encounter questions about certain settings, wonder how to handle multiple iCloud accounts, or need help disabling iCloud. So in this chapter I walk you through those topics for Macs and iOS/iPadOS devices.

> **Note:** The Apple TV is covered later, in Use iCloud on an Apple TV. And, for help with the iCloud website, see Use the iCloud Website.

If you've already set up iCloud, you can skim most of this chapter, starting with Set Up iCloud on a Mac—just to make sure you've enabled all the features you may want to use.

Update Your Software

If you want to access all the latest iCloud features, make sure the Apple software that uses iCloud is up to date on each platform you use. Here's what you need to do:

- **iOS/iPadOS:** For any iOS or iPadOS device you haven't already upgraded, tap Settings > General > Software Update and follow the prompts to install the latest update.
- **Mac:** Choose Apple > App Store and click Updates. If newer versions of macOS, Photos, or the iWork apps (Pages, Numbers, and Keynote) are found, follow the prompts to install them. In particular, be sure to install macOS 13 Ventura—a free upgrade—if you have not already done so and your Mac supports it.

- **Windows:** Download and install iCloud for Windows from the Microsoft Store.

> **Note:** If you had a much older version of iCloud for Windows installed, and if you downloaded that version directly from Apple, Apple Software Update may *not* update it to this new version. Be sure to install the latest version from the Microsoft Store.

- **Apple TV:** For information on updating the Apple TV software, see Apple's article Update the software on your Apple TV.

Set Up iCloud on a Mac

Your Mac may already have prompted you to set up iCloud—in which case, just skim this section to make sure everything is configured to your liking. If not, you can set it up manually. The exact sequence of steps depends on your circumstances.

> **Note:** Each user account on a Mac can have its own iCloud account, although only one account per Mac can use Find My Mac at a time. In addition, you can set up multiple iCloud accounts within a single user account with some limitations; for more on such configurations, see Work with Multiple iCloud Accounts, later in this chapter.

To begin, I'll show you what to do if you ignored any prompts to set up iCloud earlier (or if you subsequently signed out completely). Follow these steps:

1. Go to System Settings > *Account Name* (Ventura or later) or System Preferences > Apple ID (Monterey or earlier); if you haven't yet signed in, that pane may be marked "Sign in" (**Figure 1**).

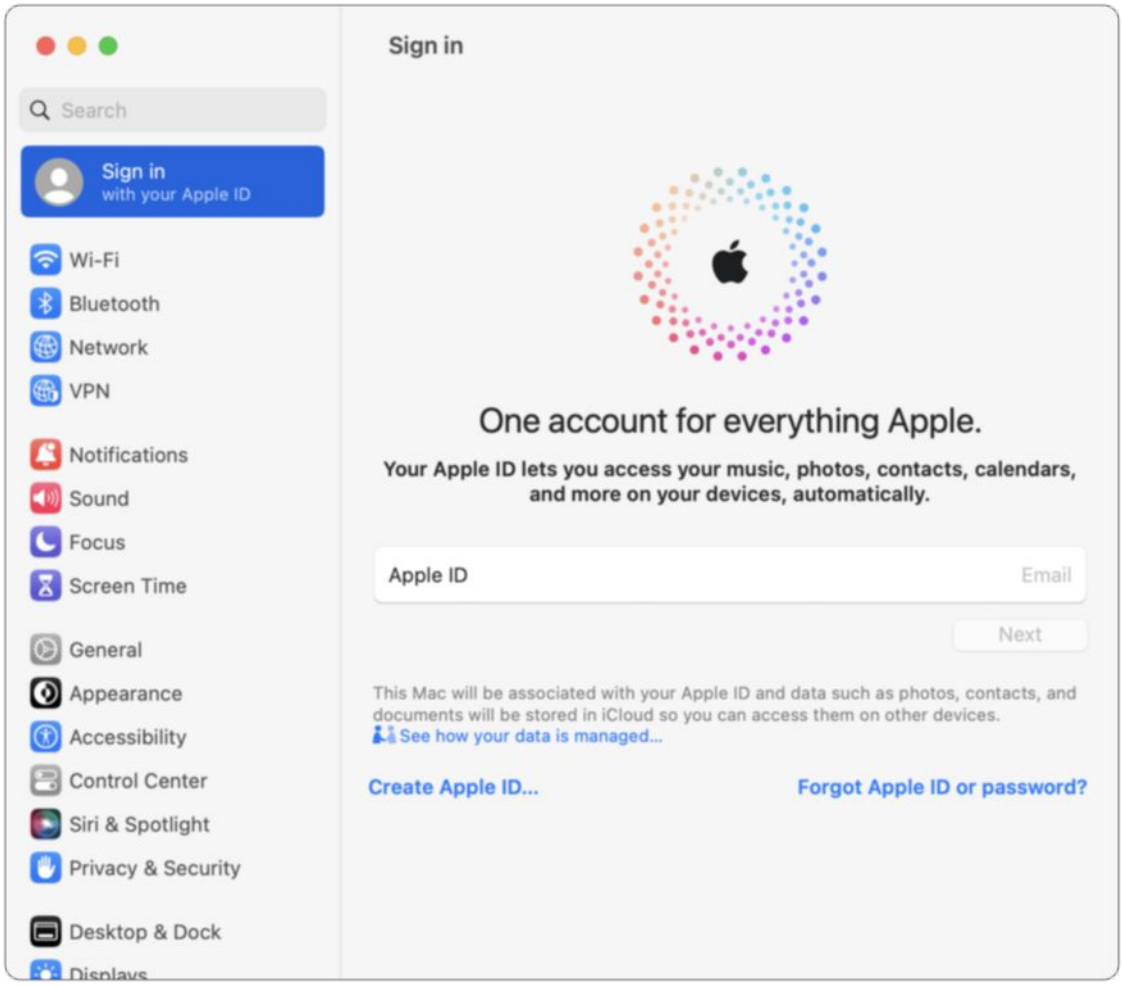


Figure 1: Start by signing in on the Apple ID pane.

2. Enter the Apple ID you want to use (see About Your Apple ID for more details), click Next.

3. Enter your password, and click Next again.

Tip: In the unlikely event that you don't yet have an Apple ID, refer back to About Your Apple ID for advice, then click Create Apple ID (or Create New Apple ID) and follow the prompts to create one now.

4. You may be prompted with one or more of the following depending on the setup state of your iCloud account and version of macOS:

   - The iCloud Terms of Service may appear; if so, agree to them.
   - macOS may prompt you to reenter your iCloud password, or to enter the password for your Mac's user account, or both (possibly

more than once). Be sure to read the text carefully to see which password it's asking for.

- You may be prompted to click Allow to confirm that iCloud can use your Mac's location for Find My Mac.
- If you're signing back in after having signed out, you may also be asked whether you want to merge data from apps such as Calendar, Safari, and News with iCloud—you almost certainly do!
- Even after signing in, you may see text in the window reading "Update Apple ID Settings." If so, click Continue and follow the prompts, which may ask you to reenter your iCloud password and/or your Mac's user account password.

5. Once you've responded to the alerts, you'll see the full Apple ID pane. If it's not already selected, click iCloud to see your iCloud settings (**Figure 2**). Many services will already be enabled.

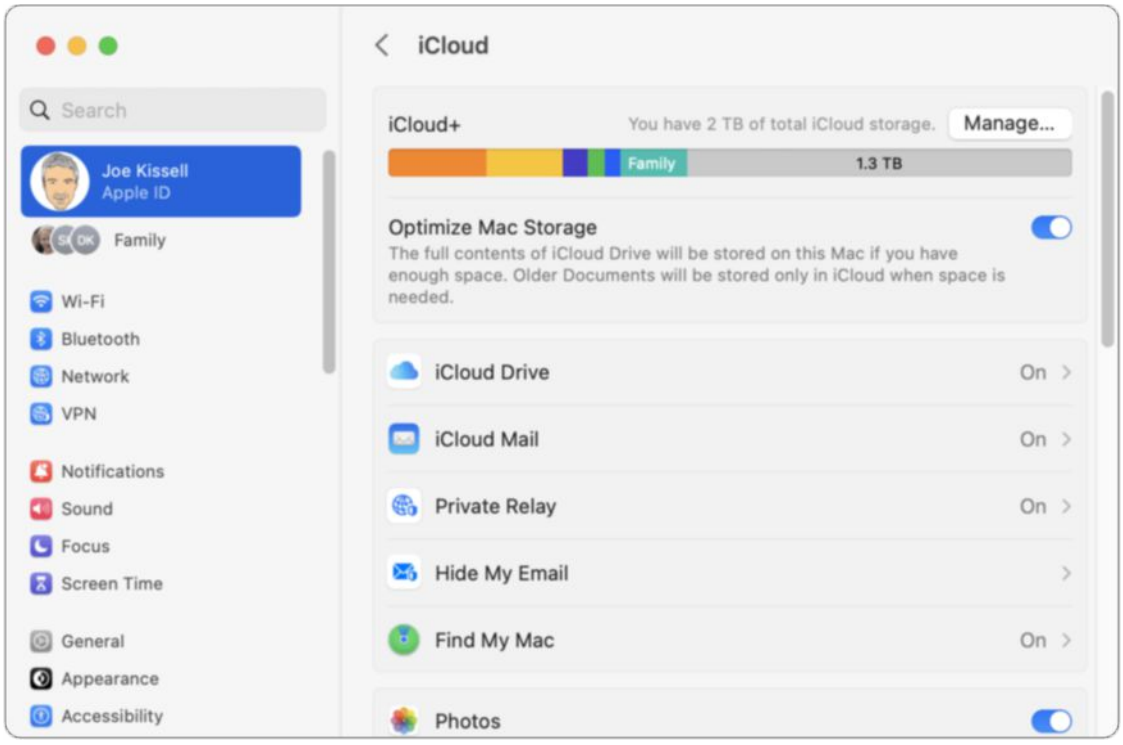


Figure 2: iCloud is finally (almost) ready to go in Ventura. (The layout is quite a bit different in Monterey and earlier.)

6. Use the switches or checkboxes to enable the types of data you want to manage with iCloud; in some cases, you must first click a general

category (such as iCloud Drive) to display controls that enable the feature and configure its settings. Unless you have some special reason to avoid one of these, I suggest enabling them all.

If you never previously set it up, Keychain requires an additional series of steps to set up, beyond merely turning on its switch or selecting its checkbox. If you want to set it up now, flip ahead to Work with iCloud Keychain for instructions. Or leave it disabled for the moment and return to it when you're ready. If you had Keychain enabled, turned it off, and are now turning it back on, you may again be faced with a series of alerts and password prompts.

Note: At the very bottom of this pane in Ventura or later is a switch labeled Access iCloud Data on the Web. If you want to be able to Use the iCloud Website, this switch must be on; it's enabled by default. To restrict access to your iCloud data to Apple's built-in apps on your trusted devices, turn it off. See Use Advanced Data Protection for more on protecting your data on the web.

7. When you're satisfied with your settings, close System Settings/ System Preferences.

iCloud is now activated on your Mac, although you must take further steps to use features specific to the Music app (see Use iCloud Music Features). Repeat this iCloud configuration process for any other user accounts on your Mac, as well as for any other Macs you may have, and then move on to set up your other devices.

The All-Purpose iCloud Troubleshooting Procedure

Lots of things can and do go wrong with iCloud, and some of those problems only Apple can fix, or result from fleeting server issues that affect lots of people. (Check Apple's status page to see whether that might be the case.)

Most random iCloud problems, especially those that involve syncing, can be solved with a simple procedure. On *each* of your devices, go to the iCloud settings or preferences screen, turn *off* the service you're having trouble with, *restart all your devices*, and then turn it back on everywhere. That's it—wait a few minutes for things to sync, and you'll probably be OK.

If that doesn't work, try this option, which is more of a hassle:

1. Go to System Settings > *Account Name* (Ventura or later), System Preferences > Apple ID (Monterey or earlier), or Settings > *Account Name* (iOS/iPadOS).
2. Click or tap Sign Out. You'll have to respond to a long series of prompts asking whether various data should be kept on your device or deleted. Answer however you like; we'll be restoring all that data in just a moment, anyway. (Note, though, that re-uploading photos can in some cases be a time-consuming operation; see Adam Engst's TidBITS article Bad Apple #1: iCloud Photo Library Re-uploading. And, if you enabled syncing of Desktop and Documents folders in iCloud Drive, it's going to be a pain and a half to put everything right later; see Sync Your Desktop and Documents Folders (or Don't).)
3. On a Mac, choose Apple > Restart; on an iOS or iPadOS device, turn off the device and then turn it back on. (Don't skip this step!)
4. Return to System Settings > *Account Name*, System Preferences > Apple ID, or Settings > *Account Name,* and sign back in.
5. Reenable all the iCloud features you want to use.

In rare cases, you may need to do steps 1–3 on *all* your devices, and then sign back in on all of them. It usually takes just a few minutes to get everything back to the way it was, except your photos and items in your Desktop and Documents folders, which may take longer. This second process often solves random iCloud problems that disabling and enabling individual features does not.

Mysterious Confirmation Requests

The Apple ID pane of Settings/System Settings/System Preferences may sometimes tell you to confirm your identity using your Apple ID password, your Mac's login password, or another device's passcode (depending on the situation).

This may seem like a phishing attack because it happens arbitrarily, but as long as you confirm that the request is occurring within Apple's interface and not popping up in a browser or via email, you're safe. After correctly entering the requested password, you generally also must follow additional steps (see Use Two-Factor Authentication).

Although I can explain some of these situations, others crop up for no apparent reason. All I can really say is: Apple is going out of their way to protect your privacy and security *just in case* something suspicious may be going on, and the unfortunate trade-off is the inconvenience of repeatedly authenticating.

Set Up iCloud for Windows

After you install iCloud for Windows (see Update Your Software), you can configure it with just a few steps.

Note: iCloud for Windows also installs two standalone apps: iCloud Shared Albums (see Share Albums from Windows) and iCloud Passwords (see Use iCloud Keychain in Windows).

The iCloud app may open automatically. If not, locate the iCloud app in the Start menu and open it. Then configure it as follows:

1. If prompted, enter your Apple ID and password, and click Sign In. If you use two-factor authentication (see Use Two-Factor Authentication), follow the verification prompts.

2. For each service you want to enable, select the corresponding checkbox. (Unless you have a special reason not to, I suggest enabling them all.) However, note the following:

   - **Photos:** Microsoft Photos for Windows 11 integrates directly with iCloud Photos. Since this is now the easiest and most reliable way to use iCloud Photos in Windows, that's the only method I cover here. To use this capability, make sure you're running the latest version of both Windows 11 and the Microsoft Store app, and install or update the Microsoft Photos app if necessary. Then select Photos, click its Options button, and enable iCloud Photos. You can also optionally select Shared Albums to share photos with others. (See Manage Your Photos for more on working with iCloud Photos in Windows.)

Tip: You can specify a different iCloud Photos folder or Shared Albums folder, if you don't want to use the default path that starts `C:\Users\your username\Pictures\iCloud Photos\`. Click Change to select a new folder and click Done when you're finished.

   - **Contacts and Calendars:** You can sync these items only with Microsoft Outlook 2016 or later. If your version of Outlook is earlier than 2016—or if you don't have Outlook installed at all—this item will be absent from the iCloud app, though you can still access this data from a web browser. With Outlook 2016 or later installed, when you enable Contacts and Calendars, you may be asked for your iCloud password one or more times.

Note: If you're running the ARM build of Windows 11 in a virtual machine (using, say, Parallels Desktop or VMware Fusion) on an M-series Mac, you will be unable to enable Contacts and Calendars.

   - **Bookmarks:** You can sync your iCloud bookmarks with Edge, Google Chrome, or Firefox. After selecting Bookmarks, click the Install Extension button for each browser you want to use and follow the prompts. When you click Apply after selecting Bookmarks, an alert asks whether you want to merge your local bookmarks with any bookmarks already in iCloud. Click Merge.

- **Passwords:** You can opt to install an extension for Edge or Chrome (but not Firefox) that lets you use iCloud Keychain securely. After installing the extension, an iCloud Keychain icon appears in the toolbar. On your first use, Apple sends a code to iCloud for Windows to validate the plugin just like a second factor. It displays a key knocked inverted from a blue cloud on pages that have items that can be filled in. Click and there's a delay while iCloud checks to see whether there's a matching entry; if so, it appears as an option you can select (**Figure 3**).

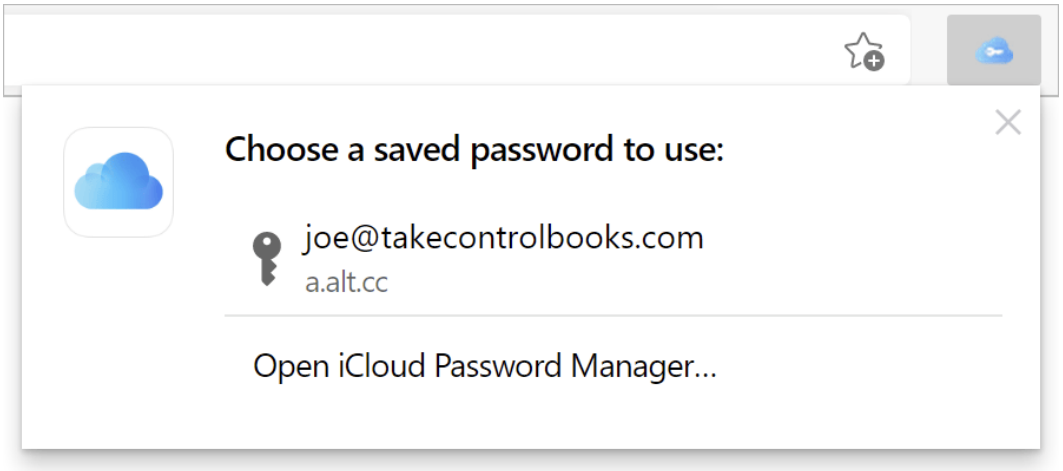


Figure 3: You can access iCloud Keychain in Edge for Windows.

3. Click Apply to activate the selected services. (Don't skip this step! Merely closing the window won't activate the services.) Depending on the options you selected, other windows and processes may open as iCloud completes its setup process and transfers your data. The window should look something like **Figure 4** if you have Outlook installed, selected all the available options, and downloaded both of the extensions for Edge (but no other browser).

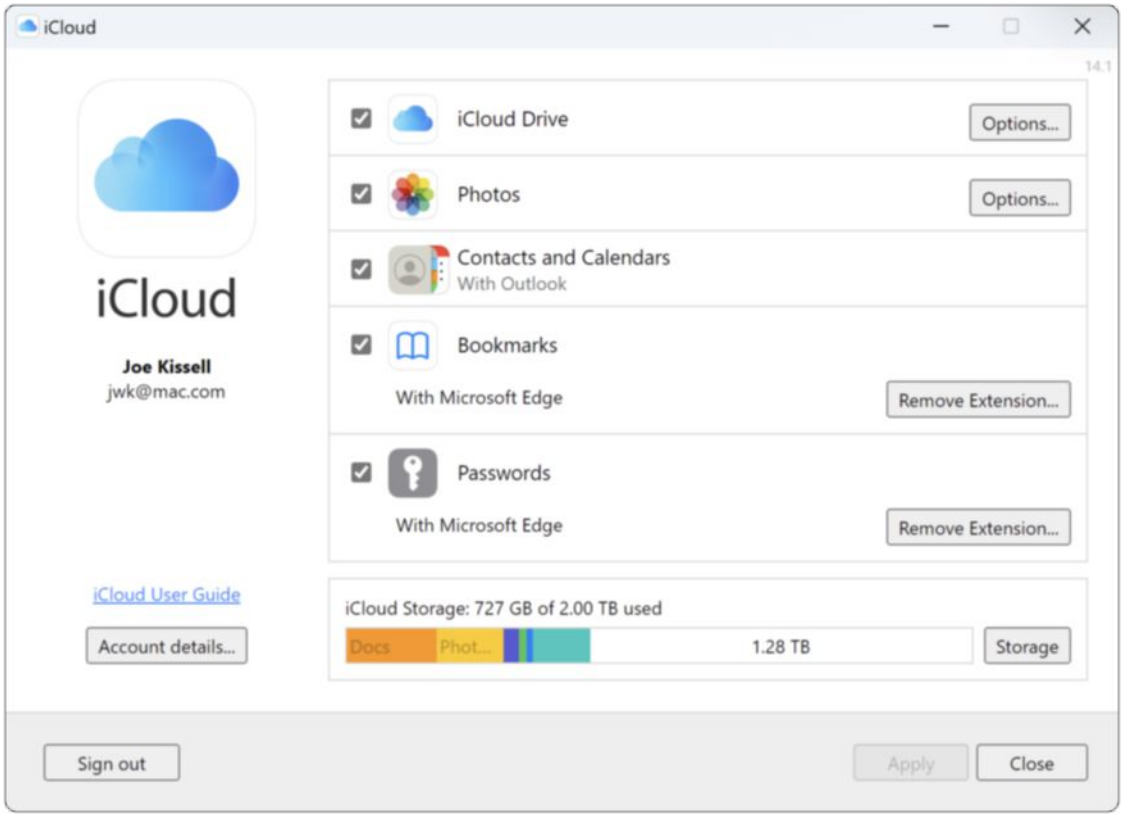


Figure 4: The iCloud app with all options selected.

4. Click Close to close the iCloud app.

iCloud is now running in Windows. You must take more steps to use the iTunes-specific features (read Use iCloud Music Features).

Set Up iCloud in iOS or iPadOS

On an iOS or iPadOS device, proceed with the following tasks:

1. Tap Settings > Sign in to your *Device*. (After you sign in, you'll instead see your name in this spot.)
2. Enter your Apple ID and password, and tap Sign In. If you have two-factor authentication enabled, follow the prompts to enter your verification code. You may also be prompted to enter your device's passcode and, in certain situations, respond to other alerts.
3. Tap iCloud to reveal more detailed settings (**Figure 5**).

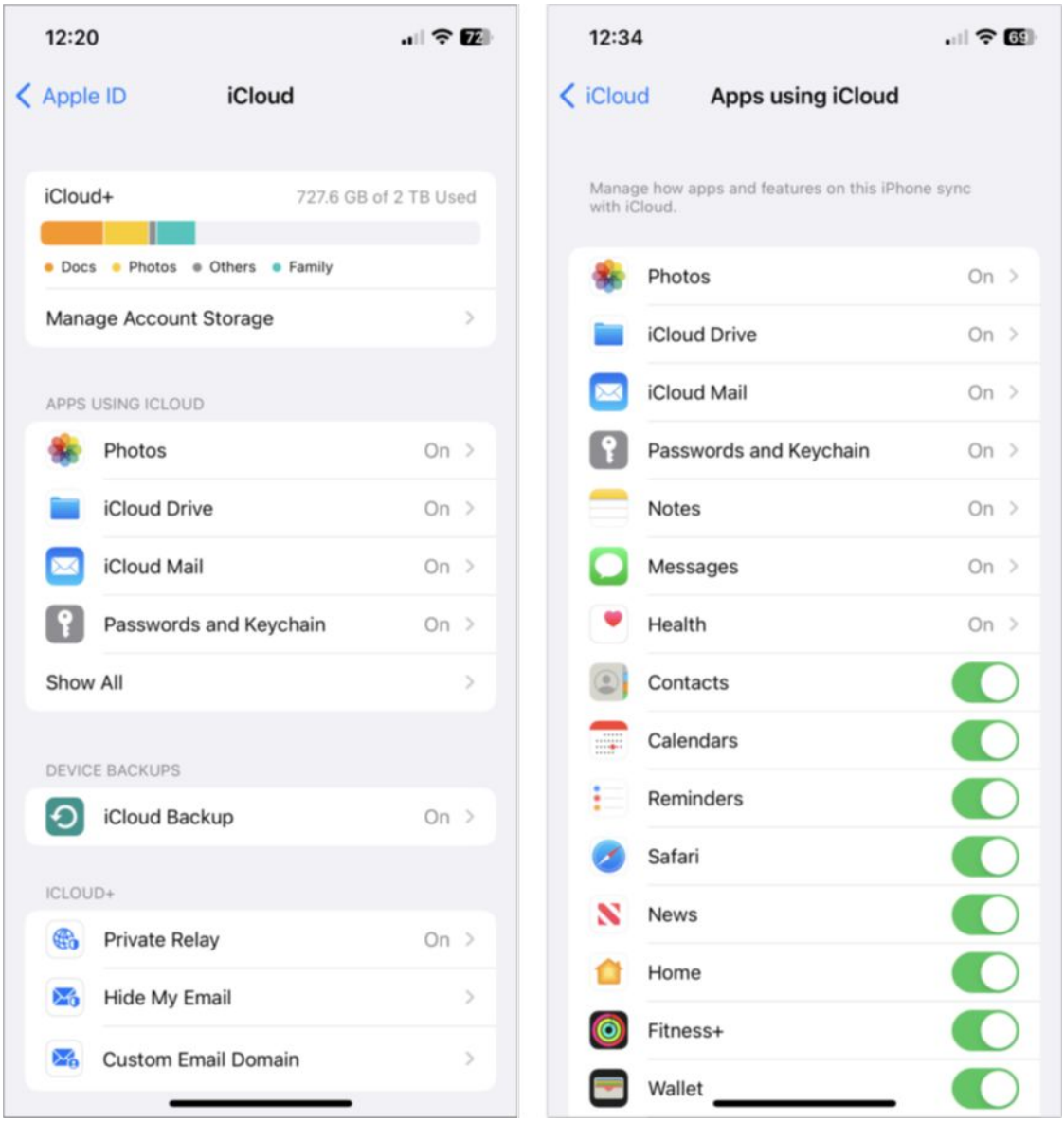


Figure 5: Turn iCloud services on or off here. Tap Show All (as shown at left) to reveal a long scrolling list of apps and services (top portion shown at right). Options vary by device and version.

4. Tap a category name (such as Photos) to enable the service and set its options; to see a complete list of apps and services, tap Show All. Then turn on the switches for services and apps whose data you want to sync with iCloud. Most should already be on (shown by a green switch).

Most people will want to have all the apps and services turned on; as the book progresses, I discuss these in more detail, but a few items that you may want to pay attention to now include:

- To turn on or off iCloud Photos or Shared Albums, tap Photos (see Manage Your Photos for further details).
- To switch your iOS or iPadOS backup to iCloud from the Finder (or iTunes for Windows), set iCloud Backup to On. (For more about iCloud Backup, see Understand How iCloud Backup Works.)
- The Passwords and Keychain (or just Keychain) item, which controls iCloud Keychain, may require more than just a tap or two to configure. For full instructions, flip ahead to Work with iCloud Keychain.
- The Private Relay and Hide My Email services, part of iCloud+, rely on iCloud but don't store data there. For details on configuring them, see Browse the Web Privately and Hide Your Email Address.
- The Home switch lets iCloud sync settings from the Home app (for smart home products) across your iOS and iPadOS devices.

Note: Home is not otherwise part of iCloud, so I don't cover it in this book. (You can, however, learn all about the Home app and working with HomeKit devices in *Take Control of Apple Home Automation* by Josh Centers.)

- The Health switch lets you sync data from the Health app on an iPhone with the cloud and with other iPhones you own. (Health data doesn't sync with any other kinds of Apple hardware.)
- The Wallet switch appears only on the iPhone and iPod touch, and lets you sync wallet items among multiple devices. These include Apple Pay credit cards, loyalty cards, concert tickets, and coupons. (Because Wallet as such isn't an iCloud feature, I don't discuss it here.)

- The Siri switch enables information Siri learns about you on one of your devices to be shared with the others, to improve the quality of its responses.

Note: You can choose whether your iCloud data can be accessed via the iCloud website with Access iCloud Data on the Web at the bottom of iCloud settings. To Use the iCloud Website, this switch must be on; it's enabled by default. Otherwise, turn it off. See Use Advanced Data Protection for more on protecting your data on the web.

5. Your current storage statistics for iCloud Drive appear at the top of the screen. To get more detail about what's backed up using iCloud Backup, or to delete the backed-up data for any app, tap Manage Account Storage (or Manage Storage). (See Activate and Configure iCloud Backup for details.)

iCloud is now set up on your iOS or iPadOS device. If you want to use iTunes Match or any of the other Music-related features, you must take steps that I describe in the next chapter. If you have any other iOS or iPadOS devices, repeat the above steps with each one now.

Local Sync for Contacts and Calendars

You can also sync contacts and calendars between an iOS or iPadOS device and a Mac via a USB or Wi-Fi connection without going through the cloud, whether iCloud or another service.

First, on your iOS or iPadOS device, go to Settings > *Account Name* > iCloud and turn off Contacts and/or Calendars. Next, in the Finder, select your iOS or iPadOS device, click Info, select Sync Contacts and/or Sync Calendars, and select any other desired options. Then click Sync.

Just remember, this is a manual process, not an automatic push synchronization as with iCloud. Whenever you want your device to be fully up to date, you have to click Sync in the Finder.

Work with Multiple iCloud Accounts

In this book, I generally assume that each person has a single iCloud account. Some people use a separate Apple ID for purchases from the iTunes Store (see About Your Apple ID). A separate account was often used to share purchases within a family, although Family Sharing largely eliminates that need (see Use iCloud Family Sharing).

However, in some situations a person may have more than one active iCloud account, each with its own set of data (such as email, contacts, and calendars). For example, you may have a personal account and a work account, or an individual work account and a departmental account that you're in charge of monitoring. In cases such as these, you can set up your Mac or iOS/iPadOS device to access multiple iCloud accounts at once—with some restrictions. (You can also use this technique to share a set of contacts with a family member or friend; see Share Your Contacts with Someone Else, later.)

Use Multiple iCloud Accounts on a Mac

On a Mac, each user account can be signed in to a different iCloud account and receive nearly the full benefit of that iCloud account. There's one important exception: Find My Mac can only be active for one iCloud account at a time, regardless of how many *user* accounts you've set up. If you want to enable Find My Mac under a different user's account, first disable it under the user account where it's active.

Apart from that, each user account on a Mac can have a primary iCloud account—with full access to all available services—as well as secondary iCloud accounts with more limited access. Once a given user has signed in to an iCloud account, that iCloud account becomes the primary account for that user, and the only one that can use iCloud Photos, iCloud Drive, and iCloud Keychain, or sync data from Home, News, Safari, Siri, and Stocks. If you then add another iCloud account while logged in to the same user account, your Mac treats the new iCloud account as secondary, which means it can be used only for email, contacts, calendars, and reminders. (And yes, you can have more than one secondary iCloud account.)

To add a secondary iCloud account, go to System Settings/System Preferences > Internet Accounts, click iCloud, and follow the prompts to sign in and enable any desired features.

Use Multiple iCloud Accounts on an iOS or iPadOS Device

On an iOS or iPadOS device, as on a Mac, you can have more than one iCloud account set up, but only the first one you configure—the primary account—can be used for Backup, Home, Find My *Device*, iCloud Drive, iCloud Photos, Keychain, News, Safari, Siri, and Stocks. In addition, on an iOS or iPadOS device, push email works only with the primary account. Secondary accounts can be used for email, contacts, calendars, and reminders.

To add a secondary iCloud account, go to Settings > Mail > Accounts, tap iCloud, and follow the prompts.

Switch Primary and Secondary Accounts

You might set up an iCloud account as a secondary account on a Mac or iOS/iPadOS device and later decide you want it to be the primary, so it's the one associated with services like iCloud Photos and iCloud Drive. To make that swap, follow these steps:

1. Remove the secondary account (see Remove an iCloud Account); this is a temporary change.
2. Sign out of the primary account.
3. Sign back in with what was formerly the secondary account that you are now making the primary account.
4. Now you can sign back in with the former primary account that you want to act as the secondary one.

Disable iCloud

Once you've set up an iCloud account, it exists forever. You can manually delete any or all of the information from the account, if you like, or even stop using it permanently, but *Apple provides no way to cancel an iCloud account*. However, even if you plan to continue using iCloud indefinitely, you may want to disable individual iCloud features, remove a device from Find My *Device*, or remove an iCloud account completely from a device.

Disable Individual Features

To disable features you don't need, go to System Settings > *Account Name* > iCloud (Ventura or later) or System Preferences > Apple ID > iCloud (Monterey or earlier), the iCloud app (Windows), or Settings > *Account Name* > iCloud (iOS or iPadOS). Uncheck or turn off the features you don't want to use on that device. In some cases, you are prompted to decide whether you want to keep the associated data on your device or delete it; but even if you delete it from a given device, it will remain in the cloud, meaning it will download again if you later decide to reenable that feature.

Disable a Secondary Account's Services

To disable services for a *secondary* iCloud account:

- In macOS, go to System Settings/System Preferences > Internet Accounts and select that account.
- In iOS/iPadOS, go to Settings > Mail > Accounts > *Account Name* > iCloud.

Then uncheck or turn off features you don't want to use.

Remove a Device from Find My *Device*

Find My *Device* on a Mac or iOS/iPadOS device lets the owner of the associated account lock or even wipe the contents of that device remotely if it's lost or stolen. This feature is called *Activation Lock*, and you can read more about it in Check Activation Lock.

That may have severe consequences if you buy or sell a Mac or iOS/iPadOS device with Find My *Device* still active: if you buy a used Mac or iOS/iPadOS device, the previous owner can erase your new device at any time! Before buying a used device, make sure that person has signed out of Find My *Device*; likewise, if you're selling a device, make sure you're signed out before it leaves your hands—definitely read Check Activation Lock.

You can remove a device from Find My *Device* by turning off Find My *Device* in System Settings > *Account Name* > iCloud (Ventura or later) or System Preferences > Apple ID > iCloud (Monterey or earlier), or in Settings > *Account Name* > iCloud (on an iOS or iPadOS device); removing your iCloud account completely (described next); or, on an iOS or iPadOS device, by erasing it (tap Settings > General > Reset > Erase All Content and Settings). For more details, see Apple's support article Remove a device from Find My iPhone on iCloud.com.

Remove an Item from Find My *Item*

Apple's Find My *Item* includes AirTags and other hardware designed to work only with the crowdsourced Find My network. These devices are paired with a single iOS or iPadOS device, and then trackable only using the Find My app in iOS, iPadOS, and macOS.

Apple calls this *Find My Lock*, a parallel to Activation Lock. Find My Lock can be removed from its paired device only when the item is near that device. If the device is lost, stolen, or destroyed, the item becomes permanently unusable—it can't be re-paired with another device. (You *cannot* use your Apple ID account to remove Find My Lock.)

Apple notes this lock also applies to the AirPods Pro, the AirPods Max, and the iPhone Leather Wallet.

Remove an iCloud Account

To remove an iCloud account from a device, do one of the following:

- **Mac:** Go to System Settings > *Account Name* (Ventura or later) or System Preferences > Apple ID > Overview (Monterey or earlier) and click Sign Out.
- **Windows:** Open the iCloud app and click Sign Out.
- **iOS/iPadOS:** Tap Settings > *Account Name* and then, at the bottom of that screen, tap Sign Out.

Then follow the prompts to specify whether you want any of your iCloud data to remain on the device.

Removing an iCloud account from a device, like disabling individual features, doesn't delete data from Apple's servers. If you later set up the same account on the device, it will re-download data for each iCloud feature you enable.

Use iCloud+

In recent years, Apple added an increasing number of services associated with iCloud storage. In 2021, they made a branding decision to split services available for free as *iCloud* (such as 5 GB of storage) and additional features, like Private Relay and HomeKit Secure Video, as *iCloud+*. All paid storage tiers starting at 50 GB are iCloud+.

Each iCloud+ tier includes the same set of services, although in the case of HomeKit Secure Video, the number of cameras you can use varies by tier. All other features are identical.

Let's look at what iCloud+ encompasses.

Increase Your Storage

One of the key reasons to subscribe to iCloud+ is to increase your storage beyond the 5 GB included in the free iCloud tier. In the United States, you can pay $0.99 per month for 50 GB of storage, $2.99 per month for 200 GB, $9.99 per month for 1 TB, $29.99 per month for 6 TB, or $59.99 per month for 12 TB.

Family Sharing users can share that storage with other family members; see Share iCloud+ Features.

You can also opt to get more storage by subscribing to Apple One. Each of the three Apple One subscription levels include a tier of iCloud+: Individual has the 50 MB tier; Family, 200 GB; and Premier, 2 TB. Apple lets Apple One subscribers purchase *additional* iCloud storage on top of what the bundle provides, allowing a maximum of 14 TB.

Note: Both Glenn (this book's editor) and I both meet the criteria to upgrade to 4 TB and beyond, but while I see the option to do so, Glenn does not. Glenn put out a call on Mastodon asking others if they saw this—and received screen captures revealing the same storage split. We are pretty sure it's an account bug.

To buy more storage on a Mac or PC:

1. Go to System Settings > *Account Name* > iCloud (Ventura or later), System Preferences > Apple ID > iCloud (Monterey or earlier), or the iCloud app (Windows).
2. Near the iCloud Storage indicator, click the Manage button (Mac) or Storage (Windows).
3. Click Change Storage Plan (if you're already paying for extra storage and want more) or Add Storage/Buy More Storage (if you're not yet paying for extra).
4. Click the plan you want to purchase, and click Next.
5. Enter your password when prompted and click Buy, and Apple upgrades your storage level.

To buy more storage on an iOS or iPadOS device:

1. Tap Settings > *Account Name* > iCloud > Manage Account Storage (or Manage Storage).
2. Tap Change Storage Plan (if you're already paying for extra storage and want more) or Add Storage/Buy More Storage (if you're not yet paying for extra).
3. Tap the plan you want to purchase, and tap Buy.
4. Confirm your purchase when prompted and Apple upgrades your storage level.

No matter the method you used to upgrade, your subscription to additional storage will be renewed automatically each month unless you cancel it before the renewal date.

Note: Follow the same procedure to decrease or remove your iCloud+ plan; if you've subscribed to Apple One, click or tap Change Apple One Plan.

Browse the Web Privately

Private Relay available through iCloud+ performs a neat trick that lets you browse the internet somewhat anonymously. Apple decouples your location on the internet from the webpages you browse. This prevents websites in most cases from targeting you or obtaining information about you that you don't provide explicitly.

Understand How Private Relay Works

Apple sets up a pair of proxy servers—intermediaries between you and a website. The first server is run by Apple and the second by one of a few trusted third-party partners Apple has contracted with. Apple never learns what webpages your copy of Safari requests; the third-party partner never learns your IP address or its associated location.

When you browse with Private Relay on, Safari encrypts its requests and passes them first to Apple's server. Apple strips off the location information and passes it to a partner.

The partner's server decrypts the request and picks a fresh IP address that's not associated with you. You can choose whether the address is geographically associated vaguely in your area or is more coarsely anywhere in your same country and time zone.

The partner's server then makes the query to the website you wanted to visit, encrypts the response, and relays that back through Apple's server. Finally, Apple transfers it on to your copy of Safari, which decrypts and loads the page or other data!

This two-part proxying ensures that no intermediate party knows enough about you to draw inferences, and the website you visit knows only what you choose to disclose about yourself via form entries.

When enabled, Apple also uses Private Relay to protect domain name service (DNS) lookups and insecure HTTP requests from all apps and services on your iPhone, iPad, or Mac. (DNS lookups convert human-readable addresses like `takecontrolbooks.com` to machine-ready ones, like `173.255.252.203`.)

Tip: For more detail about how this all works, consult Glenn Fleishman's books *Take Control of iOS & iPadOS Privacy and Security* and *Take Control of Securing Your Mac*.

Enable and Configure Private Relay

Turning on and tweaking Private Relay is much easier than understanding how it works:

- In iOS/iPadOS, go to Settings > *Account Name* > iCloud > Private Relay. Tap Private Relay to enable it and reveal more options.
- In macOS, go to System Settings > *Account Name* > iCloud (Ventura or later) or System Preferences > Apple ID > iCloud (Monterey or earlier). In Ventura or later, click Private Relay and click Turn On Private Relay; in Monterey or earlier, check the Private Relay box and click Options. You can then set the coarseness of the location that the partner's server offers to a website:
  - **Maintain general location:** This choice picks an IP address that represents your rough area. This would allow a retail site to offer locations somewhat near you if you shared your location with them, but wouldn't let them accurately pinpoint you within a radius of dozens of miles or more.
  - **Use country and time zone:** Opt for this to have the partner server select an IP address within a very broad geographic zone. The reason to have both country and time zone as the criteria helps make sure you can access geo-locked streaming services and your time zone is set correctly by sites that display local time.

You can disable Private Relay at any time by going through the same procedure but clicking Turn Off, deselecting the Private Relay checkbox, or turning off the Private Relay switch. The operating system warns you about what happens when you disable the service, and makes sure you confirm the step with an additional click or tap.

You can also disable Private Relay for an individual webpage in Safari if you're having trouble accessing it with Private Relay enabled:

- **Safari for macOS (Ventura or later):** Choose View > Reload and Show IP Address.
- **Safari for iOS/iPadOS:** Tap the AA AA icon in the address bar and choose Show IP Address from the pop-up menu.

This option persists for the given domain name in that tab until it's closed or reloaded, or you navigate to a new site in the same tab.

Hide Your Email Address

We've all signed up for something or made a single purchase at a site, only to be bombarded forever with follow-up emails, often with unsubscribe links that fail to work. We might also want to register with a site or receive an email newsletter without providing an address that's easily associated with our name and identity.

Apple's Hide My Email service for iCloud+ expands on their previous Sign in with Apple offering for websites and developers. With that previous sign-in service, you could opt to use a generated relay address instead of providing your iCloud email address. Hide My Email makes that available on demand as well as integrating it directly within Apple's Mail app in iOS/iPadOS, and Ventura and later. With Hide My Email, you can create a custom, random address for any site, and email to that address is forwarded to your iCloud account without revealing your real address to the sender. You can also deactivate any of these addresses whenever you want.

Apple makes it a breeze to use Hide My Email. You can access it from anywhere you access iCloud:

- **macOS:** In Ventura or later, go to System Settings > *Account Name* > iCloud > Hide My Email; in Monterey or earlier, go to System Preferences > Apple ID > iCloud and click Options next to Hide My Email. Click the plus + icon to create a new address.

- **iOS/iPadOS:** Go to Settings > *Account Name* > iCloud > Hide My Email. Tap “Create new address” to add a new alias.
- **iCloud website:** Click the menu icon at the top followed by Hide My Email. Click the plus + icon to add an address.

In each of those locations, you can select an existing entry and then copy the public address associated with it; change its Label (how its shown in the list) or its Note (a description you can use to remind yourself of what it’s for); or deactivate it, which stops mail to that address from being forwarded.

The entry also shows what address it’s being forwarded to, which is typically your main iCloud address. You can change that as follows:

- **iOS/iPadOS:** Scroll to the bottom of the screen, tap “Forward to,” select an address, and tap Done.
- **macOS Ventura or later:** Click the settings icon at the bottom of the sidebar and choose Change Forwarding Address. Select an address and click Done.
- **macOS Monterey or earlier:** Click Options next to Forward To and select an address.
- **iCloud website:** Select a different radio button under “Forward to.”

In the Mail app, you can simply click the “From:” field when composing a message and choose Hide My Email as the option (**Figure 6**). The Mail app does the rest of the job and fills it in for the email message (**Figure 7**). The entry appears immediately in the Hide My Email list in all your iCloud-associated locations.

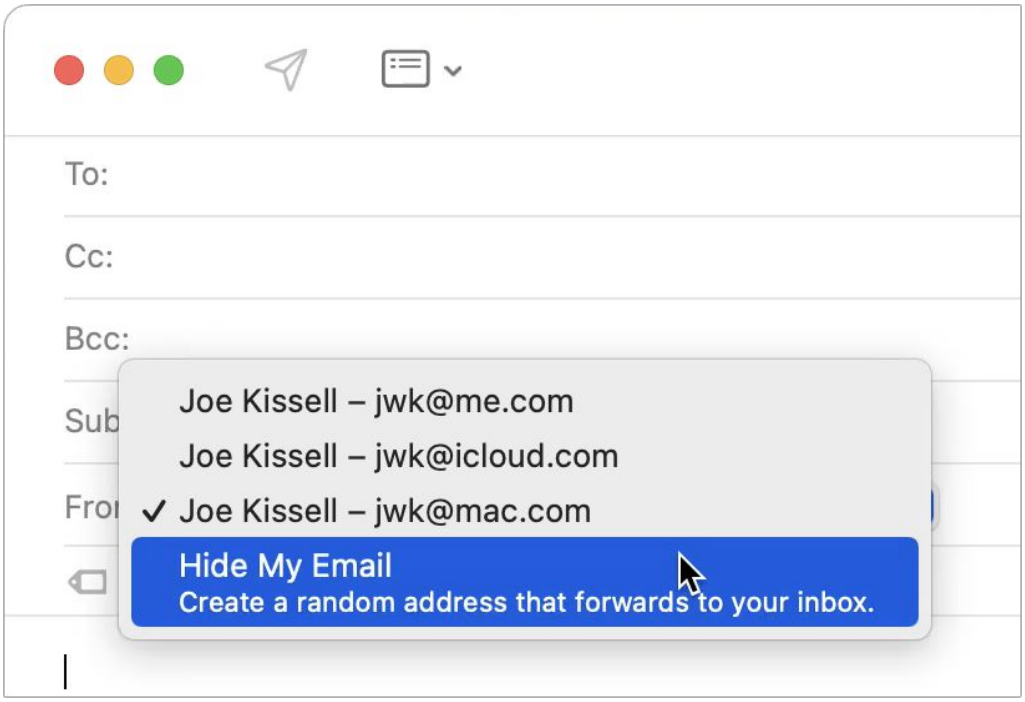


Figure 6: Select Hide My Email from the "From:" menu in Mail to generate an address automatically.

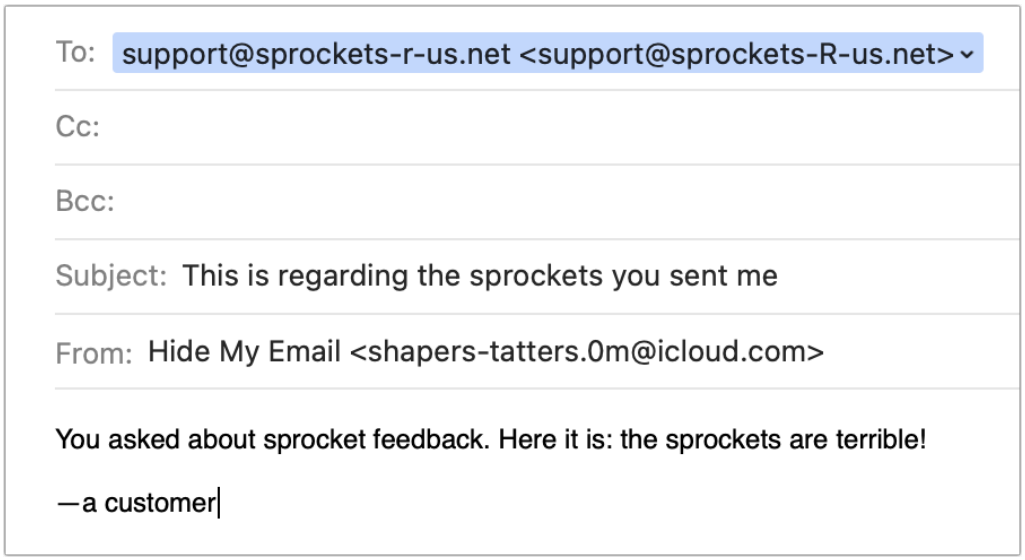


Figure 7: The composed message has the email alias filled in and identified to you (not the recipient) as using Hide My Email.

Configure a Custom Domain

iCloud+ also lets you use a domain name you own with your iCloud Mail and other iCloud services. Once set up, you can use email addresses for domain to receive and send messages. Anyone in a Family

Sharing group can register their own custom domain and choose to share access to it with other members.

Deploying a custom domain requires two-factor authentication enabled for your Apple ID account. Two-factor authentication also has to be set up for any Family Sharing group member who wants to use the custom domain if you share it. You must also have set a primary email address set for iCloud Mail.

Note: Using a custom domain name requires access to the DNS (domain name system) settings for the domain and a little technical knowledge to complete the process.

Apple recommends before you get started that you assemble a list of all incoming email addresses at the custom domain you're setting up with iCloud Mail. These addresses will stop passing through whatever mail server you're currently using when you complete the process, and email to them will bounce if you haven't configured them with iCloud.

Note: If you're using a mail host that lets you forward or act on email to different addresses, iCloud Mail can duplicate this with rules set at iCloud.com and forward or otherwise act on messages.

Apple provides a carefully guided process to set up a custom domain, though details vary depending on your DNS provider and Apple can't provide complete steps for every provider. The general outline is:

1. Start by going to the Custom Email Domain setup page, or log in to your account at iCloud.com, click the menu icon, and choose Custom Email Domain.
2. If you're in a Family Sharing group, choose Only You to retain sole access to the domain or You and Your Family to make it available as a shared option with other members (**Figure 8**).

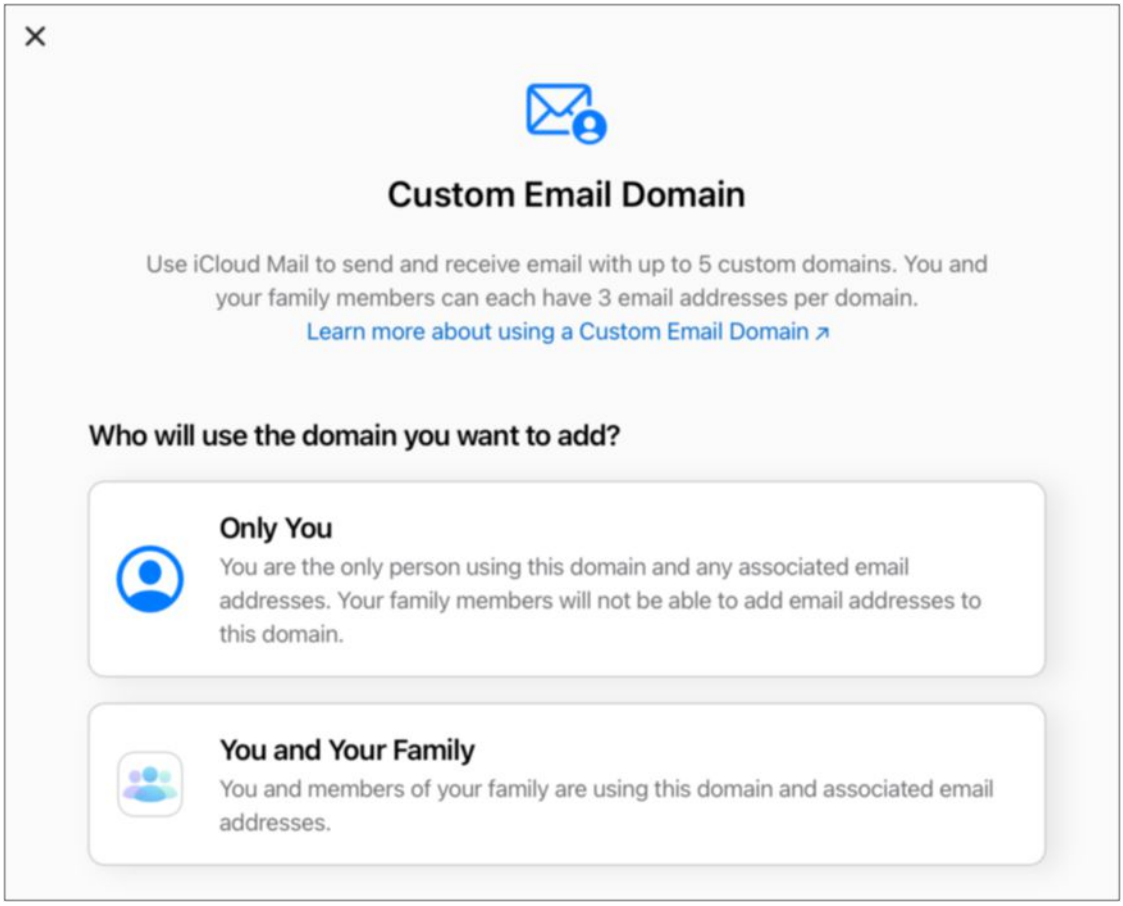


Figure 8: Pick whether the custom domain will be exclusive to you or shared with members of a Family Sharing group.

3. Enter the domain name and click Continue.
4. Apple now shows the domain in what they label Step 1. In "Step 2: Add existing email addresses":
   - Click Skip if you have no email addresses to migrate.
   - Enter email addresses for the domain to migrate (up to three for yourself and three for each Family Sharing member). Click the plus icon to add additional addresses. Click "Add email addresses" to finish.
5. Apple sends an email to each address that you entered. Follow the instructions in the email to verify each address. Even if some of these addresses are aliases that get delivered to the same mailbox, you still must verify each address.

6. Once the emails have been verified, click View under Step 3 to retrieve the domain name system (DNS) settings that must be manually entered in your domain host's systems (**Figure 9**).

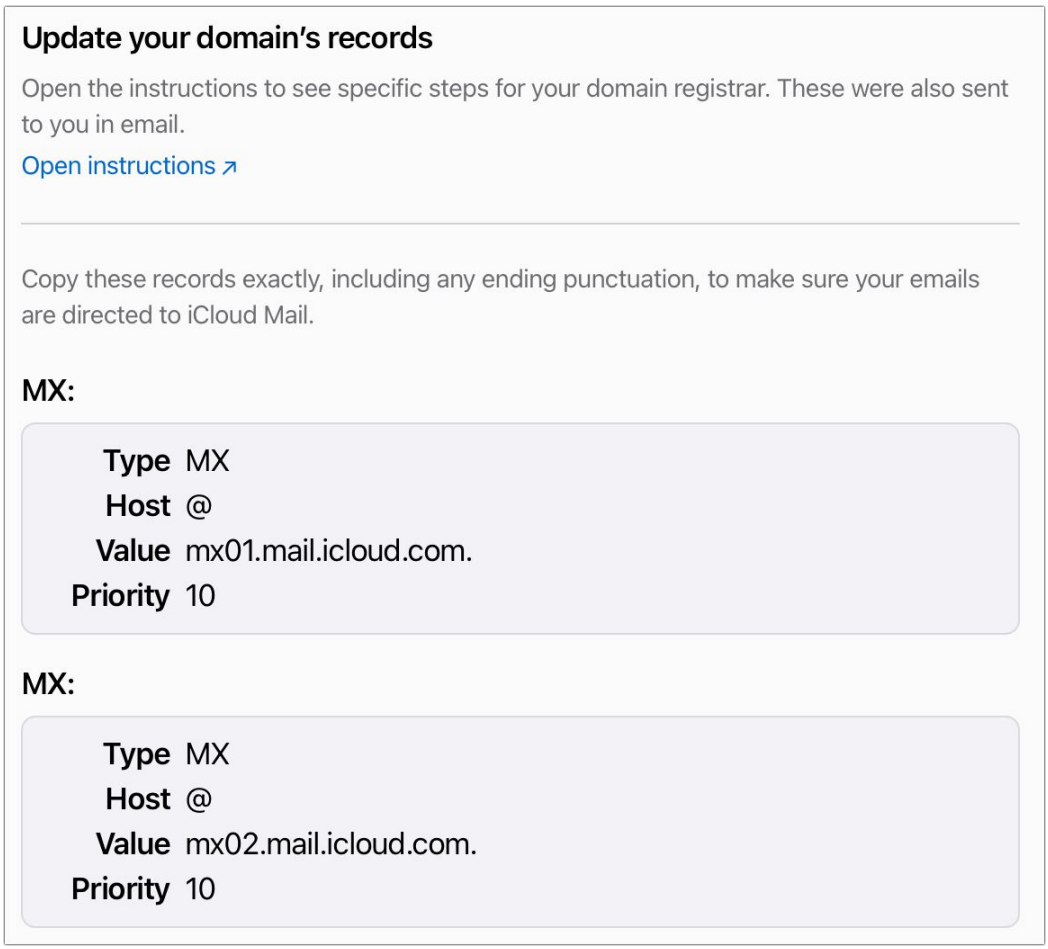


Figure 9: DNS settings require tweaky careful host updates.

7. After you've made those changes and waited the interval your domain host recommends for changes to be available, click "Finish set up" to have Apple validate that the process is complete. You can return to this step later from any browser or log back in and return to the step if the iCloud session has timed out.

When the domain has been added, addresses associated with you and Family Sharing members become available to use just like your primary iCloud address and any iCloud aliases you've set up. You can use these addresses with iCloud Mail, Messages (for iMessage), FaceTime, Calendar, and for device sign-ins—pretty much anywhere an Apple ID account name can be used for iCloud purposes.

For more on using email addresses with iCloud Mail, see Work with iCloud Mail.

Add Security Camera Features

Home security cameras were one of the breakout consumer electronics categories of the last decade. Formerly low-resolution, bad in low-light conditions, and expensive, older cameras produced analog or digital video that was hard to manage and review. The advent of better cameras for mobile phones seemed to have a beneficial effect on home security cameras, too, with prices plunging, quality improving to high-definition or even 4K resolution, and local and online options to store digital video.

Many camera systems come bundled with free online storage systems for motion-detection-based video clips, while others offer tiers of paid service that can include recording all video.

Apple entered this area in what seemed to be a peculiar (but very Apple-like) way. Instead of developing a new kind of hardware that requires a lot of handholding and support, Apple extended their HomeKit licensing program to work with camera manufacturers, while adding features to the paid tiers of iCloud to handle video storage at no extra cost. (Apple currently lists 15 compatible cameras. The list has barely changed in years.)

With the advent of iCloud+, all subscribers can use what's called HomeKit Secure Video (**Figure 10**). The video stored doesn't count against your iCloud+ storage, either. To use the service, you need a HomeKit hub, which can be a HomePod, HomePod mini, or Apple TV.

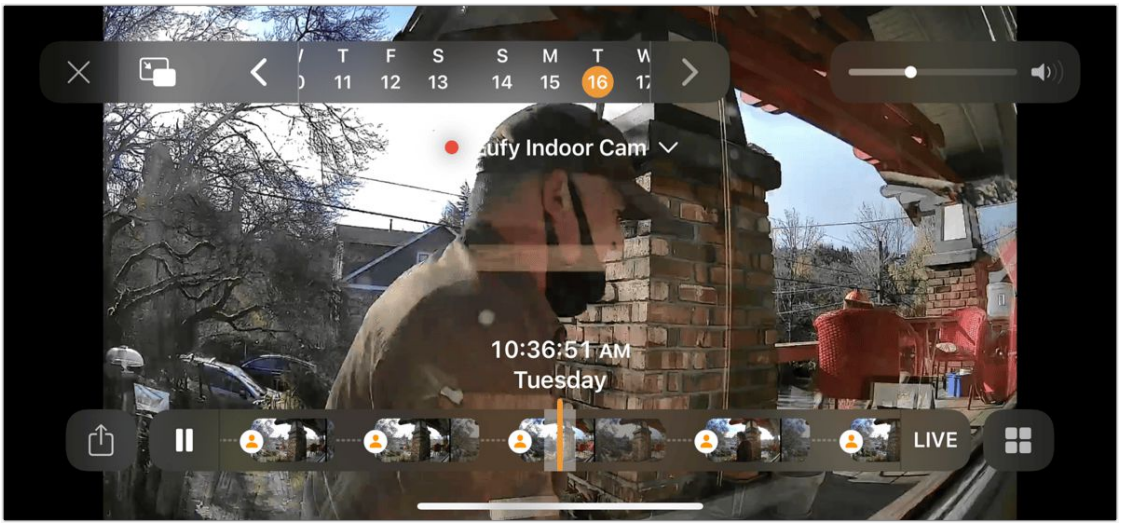


Figure 10: A delivery person arrives with a box at the front porch.

Apple followed their usual practice with private—even intimate—user data by building the system around end-to-end encryption, even though the video is stored on iCloud servers. That level of encryption is identical to what's used by iMessage, iCloud Keychain, and the identification of People in the Photos apps.

You add a camera that supports HomeKit Secure Video to your set of Home devices only using the Home app in iOS or iPadOS. You can use one camera with the 50 GB tier of iCloud+, five with the 200 GB tier, and an unlimited number with the 2 TB tier.

Apple lets you configure the camera's settings, view and hear stored clips, and view and listen live and talk through a camera's speaker (if it has one) via the Home app in iOS, iPadOS, or macOS. You can also view clips and live video through the Apple TV Home app.

HomeKit Secure Video stores motion-triggered clips, which can be restricted to areas you instruct the camera to watch within the frame of the camera. Each clip is retained for 10 days.

You can set each camera to record when there's any motion—or particular kinds of motion. For instance, you can have it detect people (including noting "a group of people"), vehicles, animals, or packages, and receive specific notification based on each category. Every camera can have separate settings, including how you're notified.

You can optionally enable facial recognition, which relies on your locally stored identification in your People & Pets album in Photos (**Figure 11**). Because of the potential for privacy invasion and misuse, Apple offers a lot of ways to limit and shape facial ID.

Figure 11: Editor Glenn Fleishman is tagged via his camera's Photos-based identification on his iPhone.

How Apple Protects Your Video's Privacy

Apple uses end-to-end encryption between the hub on your network and iCloud storage. While Apple doesn't detail this precisely, the system leans on computational power in the hub to perform some analysis—maybe all of it—and for facial recognition. Because unencrypted video isn't uploaded to iCloud and all faces you've identified in the People & Pets album are only available on your devices, the hub is the only entity that could perform matches.

Video is passed between a camera and the hub using secure transport. The hub/camera combination performs analysis of the motion, and sends out notifications as you've configured them via Apple's push system. The hub then encrypts the video using a locally cached encrypted key and uploads it to iCloud storage.

When you browse clips, your Home app retrieves them from iCloud storage and then decrypts them on your device using a locally stored encryption key. When you view footage live, it's either relayed locally via the hub when you're on the same network, or tunneled with end-to-end encryption from the camera through the hub to your device.

Use iCloud Family Sharing

If you live in a household in which multiple family members would like to share the music, movies, TV shows, books, and apps they purchase from Apple—and especially if your family includes children who use Apple devices—you're the target audience for iCloud's Family Sharing feature. (If not, there's nothing to see in this chapter—skip ahead to Use iCloud Music Features.)

Here's what you'll get for up to six family members (including you):

- All family members' purchases of media from Apple can be charged to the payment method(s) of the person designated as the family organizer. (I provide more detail in the "Purchase sharing" bullet point under Configure Apps and Services, ahead.)
- Kids can request media purchases from a parent, who must approve each one individually. (You can register special Apple IDs for kids, even if they're under 13.)
- All family members can access each others' media, although you can hide particular items of your own that you don't want to share.
- Family members can download and use apps, in-app purchases, and subscriptions made by someone else in the group as long as that other person enables purchase sharing.

Note: App developers choose whether to allow Family Sharing for apps; it seems like most do. They can also opt to allow Family Sharing for in-app purchases and subscriptions. That varies a lot more by app.

- iCloud automatically creates a shared family photo album, calendar, and reminder list. (You don't have to use them.)
- Family members can more easily share their locations and locate their devices (with Find My).

- A family can join Apple Music as a group for $16.99 per month instead of paying $10.99 per person per month.
- With an Apple One subscription at the Family or Premier level, all subscriptions are shared. See Apple One.
- If the family organizer is paying for iCloud+, the organizer can turn that into a shared pool of storage. Family members also gain access to iCloud Private Relay and Hide My Email.
- Parents can limit their kids' screen time on iOS/iPadOS devices and Macs.

Note: Every family member's individual settings and data for Apple services remain private, and all files stored in their portion of the shared storage are inaccessible to all other family members unless explicitly shared. The only exception is Find My, where other members' devices are always shown in your Find My app.

I won't pretend Family Sharing is perfect—for example, can't add someone with a billing address in another country, and Family Sharing offers no way to share data like contacts, bookmarks, and passwords within a family—but it's definitely helpful for what it does.

Child Safety Provisions in iCloud

Apple offers a feature they call Communication Safety that lets a parent enable a warning for Family Sharing members under the age of 18. With this feature enabled, the child is warned before they see or send an image or video that Apple's machine-learning system has identified as containing nudity. This applies to Messages, as well as in iOS 17/iPadOS 17 and Sonoma or later when sending or receiving via AirDrop, when selecting media in the Photos library, viewing FaceTime video messages, or seeing Contact Posters for incoming callers.

Parents must choose to opt in to this system; it is not enabled automatically. Apple's system does not notify parents if their children were warned, nor if they bypass the warning. (A similar version is now available for adults for incoming images and video.)

For more about the ins and outs of this feature, see Glenn Fleishman's book, *Take Control of iOS & iPadOS Privacy and Security*.

Enable Family Sharing

You can enable Family Sharing on either a Mac or an iOS/iPadOS device. Once it's enabled on one of your devices, it's enabled on all of them. I'll explain the steps on a Mac here; if you use an iOS or iPadOS device, the process is similar except you go to Settings > *Account Name* > Family Sharing to start. Do this:

1. On a Mac running Ventura or later, go to System Settings > Family and click Set Up Family; or in Monterey or earlier, go to System Preferences > Family Sharing and click Next. Then follow the prompts.
2. Click through several informational screens, confirming that the Apple ID shown is the one you want to use as the family organizer, that you want to share your purchases (or not), that you agree to the terms and conditions, and that you understand purchases will be charged to the credit card associated with your Apple ID.
3. Choose whether you want to share your location with family members, and click Continue.
4. On the Family Members pane of the dialog that appears, click Add Family Member to add one or more family members:
   - **For adults (and children with existing Apple IDs):** Select "Enter a family member's name, email address or Game Center nickname," enter the name or address, click Continue, and follow the prompts. Each invited family member must either enter their password on your computer or follow the steps in an email invitation they receive to join the family account.
   - **For children without Apple IDs:** Select "Create an Apple ID for a child who doesn't have an account," click Continue, and then follow the prompts. (See the sidebar Your Child's Password, ahead, for password advice.) You must select an Apple ID for your child—that is, a string followed by @icloud.com; this will also become the child's email address. If the Apple ID you pick is

unavailable, an alert appears; keep trying new addresses until you pick one that works.

To add another member, click plus + and repeat this process.

5. When you're done, click Done.

To add or remove people later, or adjust their details, go to System Settings > Family (Ventura or later; **Figure 12**) or System Preferences > Family Sharing (Monterey or earlier). (For more about removing people, see Change Family Sharing.)

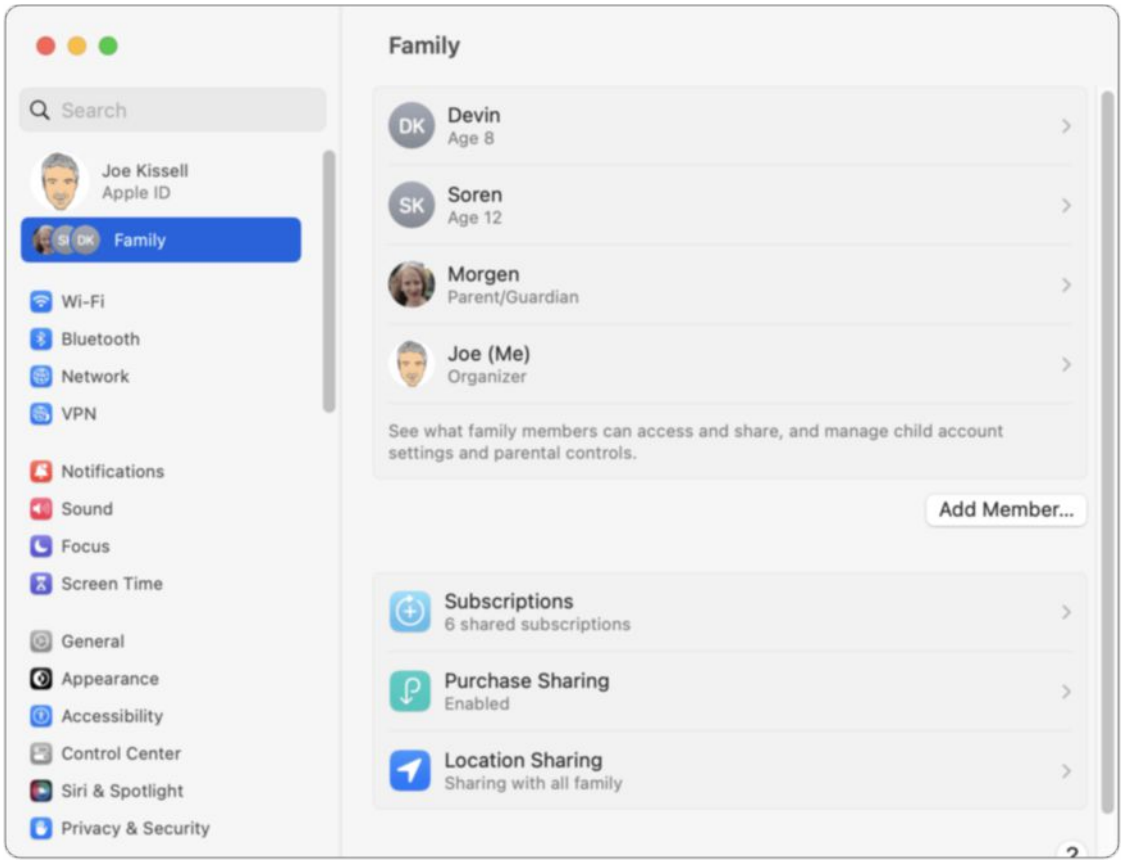


Figure 12: Manage family members and sharing details here.

Your Child's Password

Your child's account password, like any iCloud account password, must meet Apple's minimum requirements: "at least 8 characters, a number, an uppercase letter, and a lowercase letter." I recommend something longer, though not necessarily more complex. (You can read an entire book on my view: *Take Control of Your Passwords*.)

However, for a very young child—I speak from experience here—complexity is a bad move: the *child* will need to enter the password in order to Use Ask to Buy. If your child has to pester you to look up and enter a long, complex password every time they want to download a game, that sort of defeats the child completing the first part of the process independently of the parent.

If you have Ask to Buy enabled, you've reduced the security risk of a weaker password since you have to approve any purchase.

Configure Apps and Services

The setup process I just described is all you need to do in most cases. But you may want to add or adjust certain settings later. The options available and how you access them vary depending on which operating system and version are on your devices:

- **macOS Ventura or later, or iOS 16/iPadOS 16 or later:** Go to System Settings/Settings > Family. Then you can adjust any of the following:
  - *Family member settings:* To view and, in some cases, modify which services a particular family member can use and set their options, click or tap that family member's name, followed by a category.
  - *Add a member:* To add a family member, click or tap Add Member or the People icon.
  - *Subscriptions:* To see any current subscriptions, including additional storage space, Apple One features, and shared app subscriptions, click or tap Subscriptions.

- *Purchase Sharing:* Click or tap Purchase Sharing to see which family members are sharing your purchases, or to stop purchase sharing.

  If you turn off purchase sharing, each family member pays for their own purchases. The payment comes either from a balance in their Apple ID account or a payment method they added separately. Individual items (such as books and apps) purchased by one family member are not available to other family members, but subscriptions (including a subscription to iCloud+ or Apple One) continue to be shared.

Note: Although this view shows your current payment method(s), it doesn't let you change them. To do so on a Mac, open the App Store app, choose Store > Account, click Account Settings, sign in if prompted, and click Manage Payments. Or, in iOS/iPadOS, go to Settings > *Account Name* > Payment & Shipping and tap Add Payment Method to add a new method, or Edit to change an existing one.

- *Location Sharing:* Click or tap Location Sharing to enable or disable location sharing for each family member.

- **macOS Monterey or earlier:** Go to System Preferences > Family Sharing and select a category on the left:

  - *Purchase Sharing:* Enable or disable purchase sharing within the family or for your own purchases, change which iCloud account is used for sharing, or change your payment method.

  - *iCloud Storage:* Change your storage plan, or enable or disable sharing that plan with your family (see Share iCloud+ Features).

  - *Location Sharing:* Select which family members, if any, can see your location.

  - *Screen Time:* If you want to exercise some control over your children's screen access, set or modify that here.

  - *Apple Music:* View or modify an Apple Music family membership. Depending on the specifics of your situation, you may only

be able to see the name of the person sharing an Apple Music family membership with you, or you may be able to click Change Plan to switch to an individual or college student plan.

- *Apple Arcade, Apple News+, Apple TV+:* See the status of these subscriptions, whether individual, family, or part of an Apple One subscription.
- *App subscriptions:* Some app developers offer Family Sharing subscriptions separately from individual ones. Those are listed here.

Share Calendar, Reminders, and Photos

Because Family Sharing is about *sharing*, Apple automatically populates three synced services with Family Sharing items: Calendar, Reminders, and Photos.

iCloud automatically adds a Family calendar to Calendar and a Family reminder list to Reminders. Each Family Sharing member has the calendar and reminder list automatically subscribed and available on all their linked devices and on the iCloud website in the Calendar and Reminders web apps. Any events or reminders you assign to Family will appear for all family members.

In Photos, Family Sharing creates a new shared photo album called Family on all the family's devices. Add photos to this album just like any other album, and they're available to all family members. (For more information on shared photo albums, refer to Share Photos, Videos, and Albums.) But working with the Family album can be quite cumbersome; a much better solution is to share an entire library, though that feature is completely separate from Family Sharing. See Share a Photo Library.

Resolve a Calendar Conflict

If you already had a shared family calendar (whether or not it was called "Family"), Apple's shared addition will exist alongside the new one. But you can switch over to the new Family calendar without losing all the events in your old family calendar. Here's how:

1. In Calendar on a Mac, click the Calendars button on the toolbar to see the sidebar and select your *old* family calendar.
2. Choose File > Export > Export, enter a name and choose a destination, and click Export.
3. Choose File > Import, select the calendar you just exported, and click Import.
4. In the Add Event dialog that appears, choose your new Family calendar. Click OK.
5. After Calendar imports the events into your Family calendar, you'll have two copies of each one—one each on the old and new family calendars. Skim these to make sure all your events are indeed present on the new calendar.
6. Select your *old* family calendar, choose Edit > Delete, and click Delete to confirm.

The new family calendar will be used for family events from now on.

If you also had a shared family Reminders list, you can follow the same basic steps in Reminders to move those items to the new Family reminders list.

Use Find My

Family Sharing makes it easier for family members to use Find My. Turning on Family Sharing automatically adds all family members and their devices to each others' Find My native apps:

- The People view tracks family members by their primary device—iPhone, iPad, cellular Watch, or even iPod touch.
- The Devices view shows the location of all of a family member's Apple hardware for which Find My *Device* is active. That includes

any iPhone, iPad, iPod touch, Mac, Watch, set of AirPods or AirPods Pro, AirPods Max headphones, and Beats audio devices!

Note: Find My items like an AirTag can be shared—as of iOS 17/iPadOS 17 and Sonoma—with up to five people, none of whom have to be in a Family Sharing group. These shared items appear in the Items view.

You can control and disable location sharing in People with family members, but you can't disable device location tracking for a family group without disabling it for yourself. For the full rundown on how to manage how you share your location and the location of your devices, see Find My Nouns.

You can see also see family members' devices in the Find Devices web app at iCloud.com.

Share Media and Apps

With Family Sharing set up and purchase sharing enabled, media and most apps purchased from Apple by any family member are available to other family members—this is similar to how you can re-download your own media. All new purchases are first deducted from the purchaser's balance on their Apple ID account; if there is none, then they're charged to the organizer's payment method.

To see and download another family member's purchases:

- **Mac apps:** In the App Store app on your Mac, click your name in the sidebar and then choose a family member's name from the "Purchased by" pop-up menu in the upper-right corner.
- **iOS/iPadOS apps:** In the App Store app, tap your picture at the top of the screen followed by Purchased, and tap a family member's name.

What Limits Shared Apps

Apple lets each developer choose whether any or all of their apps may be used by every member of a Family Sharing group. (I have no idea why a developer would want to prevent sharing within a family.) Apple also lets developers offer in-app purchases and subscriptions for Family Sharing.

You can check an app's description in the App Store to see whether it's shareable: under the "Supports" heading, below "Information," you'll see a Family Sharing label. If an app has no in-app purchases or subscriptions, it reads "Up to six family member can use this app with Family Sharing enabled."

But ones with in-app purchases or subscription have the confusing label "Some in-app purchases and subscriptions may be shareable with your family group when Family Sharing is enabled." Click a "Learn more" link only informs you about Apple's general App Store policy—there's no apparent way to know more before downloading or purchasing an app and trying to make a purchase or subscribe in the app. It's a big missing piece of knowledge.

Some developers have opted to have separate individual and family purchases and subscriptions, with the family version costing less than even two separate individual purchases or subscriptions.

- **Books:** In Books for Mac, go to Store > Book Store Home (or Store Home) and click the Purchased link. Then choose a family member's name from the pop-up menu next to Purchased at the top.

  In Books for iOS/iPadOS, tap Reading Now, and then tap your picture in the upper-right corner. Then tap a family member's name.

- **Music, TV shows, and movies:** In Music for macOS or iTunes for Windows, choose Account > Family Purchases, and choose a family member's name from the pop-up menu next to Purchased at the top.

  On an iOS or iPadOS device, open the iTunes Store app and then go to More > Purchased (iPhone) or Purchased > My Purchases (iPad) and tap a family member's name.

On an Apple TV, go to Movies > Purchased > Family Sharing or TV Shows > Purchased > Family Sharing and select a family member's name (see Use iCloud on an Apple TV for more information).

Note: If you subscribe to iTunes Match, your matched or uploaded tracks won't be available via Family Sharing because they weren't *purchased* from Apple.

Hide Purchased Apps

To hide an app you've purchased from other members of your family, do this:

- **iOS/iPadOS:** Go to App Store > *Your Picture* > Purchased > My Purchases, swipe an app name to the left, and tap Hide.
- **Mac:** In the App Store app, click your name in the sidebar, click the More ··· button that appears when you hover over an app, and choose Hide Purchase from the contextual menu. Click Hide Purchase to confirm.

Unfortunately, there's no comparable feature for Books or TV—you can hide a book, movie, or TV show altogether, but not hide it from family members while keeping it accessible to yourself.

Use Ask to Buy

If your family includes children, you may want to use Family Sharing's Ask to Buy feature. On a Mac running Ventura or later, go to System Settings > Family, click a child's name, and select Ask to Buy in the sidebar. Then click Turn On Ask to Buy and click Done. In Monterey or earlier, go to System Preferences > Family Sharing and click Ask To Buy in the left-hand list, then check any listed child's box. In iOS/iPadOS, go to Settings > *Account Name* > Family Sharing and select Ask to Buy at the bottom of the view, then select a child's entry and enable Ask To Buy.

Note: You may be prompted to enable Ask To Buy before having access to your children's settings. This doesn't enable Ask To Buy for them, but enables the *capability* to use Ask To Buy.

To designate another adult as a parent or guardian who can approve purchases, go to System Settings > Family or System Preferences > Family Sharing (macOS) or Settings > *Account Name* > Family Sharing (iOS/iPadOS) and select the adult. In Ventura or later, select Parent/Guardian and turn on Set as Parent/Guardian; in Monterey or earlier, click Details and click Edit, select Parent/Guardian, and click Done; and in iOS/iPadOS, tap Role, select Parent/Guardian, and tap Back.

After making these changes, whenever the child clicks or taps the Buy or Install button on their device and enters their password (see Your Child's Password), an Ask Permission alert appears. When the child clicks or taps the Ask button in that alert, parents get a notification that they can approve or decline.

Share iCloud+ Features

iCloud+ users can share their extra storage space, along with Private Relay, Hide My Email, Custom Email Domain, and HomeKit Secure Video, with members of their Family Sharing group. (If you have an Apple One Family or Premier subscription, you're an iCloud+ user.)

Note: All files and synced data stored in or managed by iCloud for each member of a Family Sharing group remains absolutely private and unreachable by other members. The "shared" space is really just a financial and accounting option.

To share iCloud+ features as the family organizer:

- **macOS Ventura or later:** Go to System Settings > Family > Subscriptions, click iCloud+ under Available to Share, and click Share with Family.
- **macOS Monterey or earlier:** Go to System Preferences > Family Sharing > iCloud Storage, click Share, and follow the prompts.

- **iOS/iPadOS:** In iOS/iPadOS, go to Settings > Family > Subscriptions > iCloud+. Then follow the prompts. (If you have another family member who's already paying for storage, you can optionally tap Send Invitation to invite them to switch to your plan.)

Other family members on the free 5 GB storage tier can immediately use the shared space, while family members with their own paid plans can choose to use the shared space or to continue paying for their own.

If they choose to use your shared space, they can follow the instructions they receive (if you invited them using iOS or iPadOS). Or, on a Mac running Ventura or later, they can go to System Settings > Family > Subscriptions > iCloud+ and click Use Shared Plan; on a Mac running Monterey or earlier, they can go to System Preferences > Family Sharing > iCloud Storage and click Use Family Storage.

Update a Child's Age

If you mis-entered a child's birthday or set their age as older or younger to enable or disable certain age-based features, you can change this later. Here's how:

1. Log in to the child's Apple ID account at the Apple ID website.
2. Click Personal Information in the left-hand navigation list and then click Birthday.
3. Set the correct birthday and Click Save.
4. Click Continue. A notification appears that the request requires parental consent. (Note this request can be canceled in this view before completion by clicking "Cancel request.")
5. Apple sends an email address to iCloud account of the Family Sharing organizer with a subject line "Update *Person*'s birth date?" (**Figure 13**). Click Approve Request on that email.

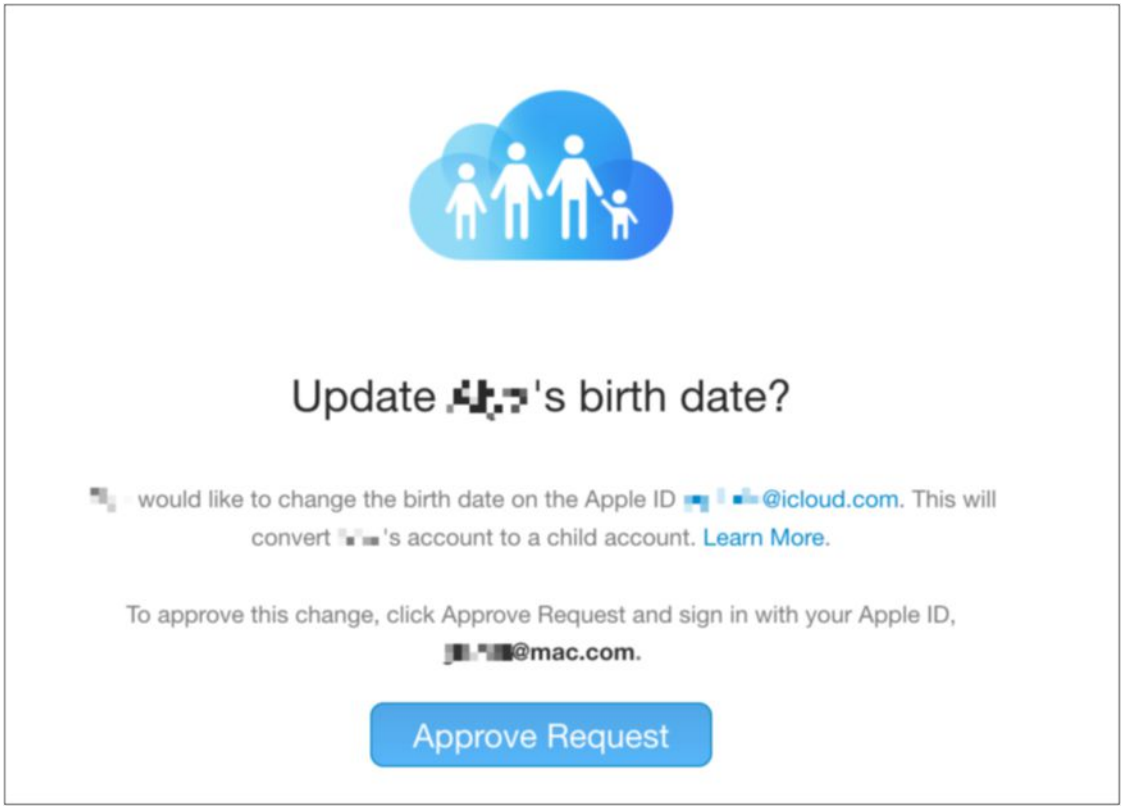


Figure 13: The Family Sharing group's organizer has to approve the account change. (The text here is inaccurate: the account was already set as a child's—just at age 17 instead of 14.)

6. This link takes you to the Apple ID site's page to approve a child's birthdate change. Log in when prompted.

7. Apple displays the new birthdate in a field that can be further changed along with a lengthy disclosure of terms for parents. The system sends you a verification code as a push to all your devices linked to the organizer Apple ID account.

8. Enter the code as received and click Agree to continue. (If you don't receive a code, click "Send a new code.") The birthdate is now changed.

Note: In testing, I was unable to get a verification code delivered.

Change Family Sharing

Families and technical requirements change over time. It may make sense to switch the family organizer, add adults, remove children, or even disband the group as children age or other life events occur. Like many things to do with Apple and iCloud, however, Family Sharing is somewhat brittle.

Among other things, Apple sets a cutoff for a child's age that prevents certain Family Sharing changes for younger children: in most of the world, including the United States, Canada, Australia, and the United Kingdom, it's 13; in some countries, it's 14, 15, or 16. (See Apple's footnote on this support document.)

Here's what you can do:

- Add and remove adults.
- Add children of any age.
- Remove children who have reached the cutoff age.
- Move children below the cutoff age to other Family Sharing groups.
- Disband the family group unless it contains children below the cutoff age.

Here's what you can't do:

- Change the Organizer of the Family Sharing group.
- Disband the family group if it contains children below the cutoff age.

You can work around both of those "can't do" items, as I describe below.

Remove a Member

You can remove a member on a Mac or on an iOS/iPadOS device. Here's how:

1. On a Mac, go to System Settings > Family or System Preferences > Family Sharing; or, in iOS/iPadOS, go to Settings > Family or Settings > *Account Name* > Family Sharing.
2. Select a family member and (in Monterey or earlier only) click Details.
3. Click Remove *Name* from Family and confirm.

The member is immediately removed from the family group.

Move a Child to Another Family

Apple prevents disbanding a Family Sharing group that contains a child below the cutoff age described earlier. However, you can transfer that child's account to another family. Ostensibly, you could remove an adult from your group, that adult could create a new Family Sharing group, and you could transfer the child to that group. It could also obviously happen when parents or families split up or reconfigure.

The process always starts from the new Family Sharing group, with the organizer "inviting the child," something that Apple could word in a less creepy fashion, to be sure. The organizer in the destination group adds the child to the family as they would add another member, but they require the child's Apple ID and password.

The organizer of the existing family group receives a notification and can approve it by proceeding through a series of affirmations. See Apple's support document for the complete process.

Disband the Family Sharing Group

Apple offers no way to shift the organizer of a Family Sharing group to someone else. I'm not sure what happens if that person is incapacitated or dies, or the family breaks up, but a family group can be disbanded and reformed with different members.

If any members fall below the cutoff age, they must first be moved to another family as described just above.

The process is straightforward. From the organizer's account:

- In macOS Ventura or later, go to System Settings > Family > *Organizer Name* and click Stop; in Monterey or earlier, go to System Preferences > Family Sharing, click Details next to your account (or select your account and click the minus – icon), and then click Stop Family Sharing. Confirm at the prompt (**Figure 14**).

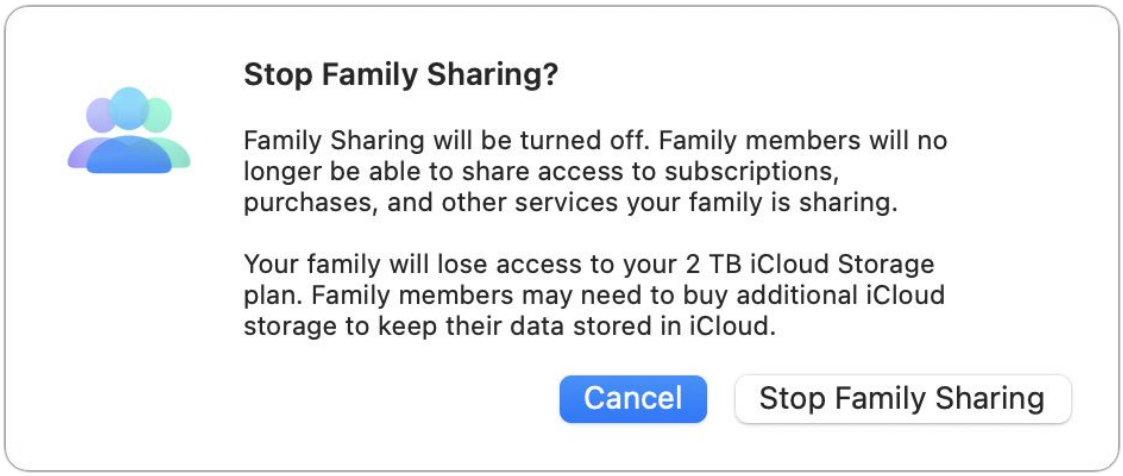


Figure 14: A simple click and confirmation disables the group.

- In iOS/iPadOS, go to Settings > Family > *Organizer Name* or Settings > *Account Name* > Family Sharing > *Organizer Name*, tap Stop Using Family Sharing, and confirm at the prompt.

Use iCloud Music Features

Apple has two different services—iTunes Match and Apple Music—that enable you to sync music to the cloud and share it across your devices, among other capabilities.

The two services have a simple relationship: all the capabilities of iTunes Match are incorporated into Apple Music, which includes many more features. Thus, if you subscribe to Apple Music, iTunes Match becomes irrelevant to you.

In this chapter I help you understand the differences between the two services and decide whether either works for you. I also walk you through setting up and using iTunes Match—but *not* Apple Music, because Apple Music isn't part of iCloud.

About iTunes for Windows

Several years ago Apple replaced iTunes for macOS with separate apps for Music, TV, Podcasts, and Books, and turned to using the Finder for syncing iOS/iPadOS devices. However, iTunes for Windows has stuck around as the all-purpose tool for dealing with Apple media on PCs. That's about to change, as Apple has developed Windows 11 versions of the Apple Music and Apple TV apps, as well as an Apple Devices app for syncing and backing up iOS/iPadOS devices. At publication time, preview versions were available in the Microsoft Store. (Apple had previously said they would release the software in 2023, but as of January 2024, they all still have the "preview" label.)

Once those apps are finalized, they'll take over their respective duties from the iTunes for Windows app. However, I haven't heard whether or how Apple will enable users to sync books or podcasts to a PC in the future, or whether iTunes for Windows will be discontinued—or simply remain as another option.

In any case, for the time being, I assume that Windows users will continue to use iTunes for Windows as they have done for years, so throughout this chapter I say things like "use Music (or iTunes for Windows) to do this or that."

Understand Apple's Music Services

iTunes Match and Apple Music are optional add-on services. With either service, you pay a fee to subscribe, and then activate the service on each of your devices. After you subscribe, there's one additional setup step:

- On a Mac, turn on the feature (open Music, go to Music > Settings/ Preferences > General and select Sync Library).
- On an iOS or iPadOS device, go to Settings > Music and turn on Sync Library.

After that, your device, the iTunes Store, and iCloud collaborate to make the following happen with both services:

- Music (or iTunes for Windows) scans the music library on your computer and compares what you have to Apple's vast iTunes Store selection—with tens of millions of tracks. This process should take just a few minutes unless you have a huge music library.
- Whenever Music (or iTunes for Windows) finds a track in your library that wasn't purchased from the iTunes Store but matches a track in Apple's library, it makes Apple's version available for download or streaming on all your devices (including your Apple TV and HomePod). The files aren't downloaded automatically.

  The music in Apple's library is stored as high-quality 256 Kbps AAC files. So, if the song already on your Mac was stored at a lower quality, the version now available to all your devices will be superior. Furthermore, any matched (i.e., previously owned) tracks that you download come without DRM (digital rights management), commonly known as copy protection. And you get to keep those upgraded, DRM-free tracks, even if you later cancel iTunes Match or Apple Music.

Note: When you download a higher-quality track from Apple, it maintains your existing metadata (such as play count).

- When Music (or iTunes for Windows) encounters a track it can't match—for example, a rare version of a song, or a track you recorded yourself, or music by an artist who's not in the iTunes Store—it uploads that track to iCloud, after which it's available to all your other devices for download or streaming. (This may take a while, depending on the quantity of music and the speed of your internet connection.) Unmatched tracks are uploaded at their existing quality, even if that's less than 256 Kbps AAC.
- Tracks stored in your library (whether purchased or uploaded) don't count against your iCloud storage quota.

Note: Apple limits you to 100,000 tracks, although tracks purchased from the iTunes Store don't count toward this limit.

Note: Once songs are matched, you can also opt to remove local copies of any of your music to free up space. Select one or more downloaded songs, and then in Music (or iTunes for Windows), choose Song > Remove Download. Don't choose Delete from Library or press the Delete key: that will prompt you to delete the song from your iCloud set and all your linked devices.

So far so good? OK. Now, here's where the two services differ:

- **iTunes Match:** iTunes Match costs $24.99 per year and includes *only the above features*. iTunes Match is especially useful for those without lots of storage space on their Macs or iOS/iPadOS devices as it lets you safely delete tracks from local storage—see the note above—while remain secure in the knowledge you can stream or download them from the cloud whenever needed (as long as you keep paying that annual fee).
- **Apple Music:** Apple Music is more expensive, at $10.99 per month for an individual, $5.99 per month for a college student, or $16.99 per month for a family. (A family plan requires that you first sign up for iCloud Family Sharing; see Use iCloud Family Sharing.) Apple Music is also available as part of all Apple One bundles. But in addition to all the iTunes Match features, it offers *unlimited*

streaming of *any* music from Apple's vast catalog, on any of your devices—including not only an Apple TV and HomePod but also a cellular-enabled Apple Watch—and you can download any of this music for later playback when you're offline. There's a small catch, however: downloaded tracks that were not matched (that is, tracks you didn't already own) are protected by DRM. This prevents you from sharing them with people who aren't Apple Music subscribers.

If you subscribe to Apple Music, you already have all the features of iTunes Match. However, if you have no use for an on-demand streaming service, and prefer to play *only* the music you deliberately purchase, rip, create, or otherwise acquire—but appreciate being able to access that music on any of your devices—iTunes Match is a better fit for you.

Use iTunes Match

If you've decided to use iTunes Match, read on to learn how to set it up.

Activate iTunes Match on a Mac or PC

To subscribe to iTunes Match on your computer (or add a computer to an existing subscription), follow these steps:

1. Open Music (macOS) or iTunes (Windows).
2. Select iTunes Store in the sidebar and click the iTunes Match link on the right. The main part of the window explains what you get if you subscribe. (After you subscribe, the link disappears.)

   In iTunes for Windows, click the Store link at the top of iTunes then scroll to the bottom and click iTunes Match under Features.
3. Click Subscribe for $24.99 per Year.

Note: If you've already subscribed on a different device (or if you signed out from iTunes Match for any reason), instead click Add This Computer and follow the prompts.

4. Enter your Apple ID and password, and click Subscribe.

The app verifies your purchase; you may need to confirm billing details and agree to the iTunes Match Terms and Conditions. It next gathers information about your Music library, and then begins matching your tracks. You can continue using Music (or iTunes for Windows) normally while that happens, but try not to quit the app: quitting interrupts the process until you open the app again.

5. In macOS, go to Music > Settings/Preferences > General and confirm that Sync Library is selected. There's no similar option in iTunes for Windows.

If you have another Mac or PC, you can follow the same process, with special attention to the note after step 3. (An iTunes Match subscription allows for up to ten devices that share an Apple ID.)

Activate iTunes Match on an iOS or iPadOS Device

To subscribe to iTunes Match on your iOS/iPadOS device (or add an iOS or iPadOS device to an existing subscription), follow these steps:

1. Tap Settings > Music.
2. If you see a Subscribe to iTunes Match link, tap it. Otherwise, turn on Sync Library.
3. You'll see an alert that iTunes Match will replace the music on this device, but that's misleading—any music already on the device that was previously synced to a library you've connected to iTunes Match stays in place. Tap Replace.

Note: After you connect to iTunes Match from this device, the Subscribe to iTunes Match link disappears from Settings > Music.

4. If you previously subscribed to iTunes Match on a Mac or a PC, all the music from that computer should appear as available to download or stream in the Music app within a few moments.
5. If you want to ensure that iTunes Match downloads music only when your iOS or iPadOS device is connected to the internet via Wi-

Fi (and not when it's using a cellular connection), tap Settings > Music > Cellular Data and turn Cellular Data off. (If you don't see this switch, your device doesn't have a cellular modem.)

You can now stream or download any of your tracks on this device using the Music app or through a connected HomePod. Repeat the above steps for any other iOS or iPadOS devices you use.

Tip: You can listen to all your iTunes Match tracks on an Apple TV; see Set Up iCloud on an Apple TV.

I could go on for quite a few pages about iTunes Match, but my colleague Kirk McElhearn has already done so in his book *Take Control of macOS Media Apps*, which I heartily recommend.

Manage Your Photos

As we've seen, iCloud's main modus operandi is "just put all my data everywhere," and you'll undoubtedly want to include your photos and videos among that data.

iCloud has three separate features you can use with your Photos library in iOS/iPadOS, macOS, and Windows:

- **iCloud Photos syncs media across devices.** iCloud Photos keeps your entire Photos library in sync automatically across your devices via the cloud. Synced photos and videos count against your iCloud or iCloud+ data storage quota.
- **iCloud Shared Photo Library lets you share a library with a small group.** Use this for your family or another group of up to six people (including yourself). The person sharing a Photo Library has its contents count against their iCloud storage.
- **Shared Albums shares and pools items with others.** Set up albums that contain media you share with other people. You can optionally let them comment or add their own images and videos. These items don't count against your or their iCloud storage, and you don't have to use iCloud Photos to use Shared Albums. (This feature was previously called iCloud Photo Sharing.)

This chapter helps you understand the advantages and limitations of iCloud Photos, and how best to use Shared Albums or iCloud Shared Photo Library to allow others to view media, add their own, or interact with your images and movies.

Sync with iCloud Photos

iCloud Photos synchronizes your photos, videos, albums, and people across all your devices as well as storing all of that in the cloud. The

cloud-stored version is available via your account on the iCloud web-site and accessible from an Apple TV HD or later.

Note: Smart albums, ones that have criteria that are matched to assemble at set of matching media, can be created and viewed only in Photos for Mac. You can't create or view them in iOS, iPadOS, or Windows, and they don't sync via iCloud Photos.

Apple always stores the full-resolution original versions of images and movies in the cloud no matter what option you choose in macOS, iOS, iPadOS, or Windows. But because Photos libraries can be enormous, Apple offers a choice in iOS/iPadOS and macOS between holding a full-resolution copy of everything or optimized versions.

If you choose optimization, your device retains thumbnails of every piece of media, which dramatically reduces the space required to hold the library. When you add items to Photos on other devices, only the thumbnail is retrieved to this device. Images added locally are uploaded to the cloud and the full-resolution version deleted as storage space on the drive is required. However, Photos always downloads the full-resolution version when you view, edit, or share a photo or video if only the thumbnail is currently stored locally.

Note: Edits to your photos and organizational changes to your library also sync across devices.

Even minimal use of the Camera app on an iPhone or iPad, or managing media you captured in the past in a Mac Photos library, may outstrip the free 5 GB tier of iCloud storage. You will almost certainly need to upgrade to iCloud+ at 50 GB, 200 GB, or 2 TB.

Tip: This is a great use of Family Sharing pooled storage, as each of you in a family might have over 200 GB of media and only need to pay $9.99 per month to get the pooled 2 TB of storage and all the other iCloud+ features.

Enable iCloud Photos on Your Devices

To enable iCloud Photos on a Mac, open Photos, go to Photos > Settings/Preferences > iCloud, and select iCloud. For local storage options, choose between:

- **Download Originals to this Mac:** If you have enough storage and want full-resolution local copies of all your images and videos, this option always retains all media you add and downloads all media added to other devices.
- **Optimize Mac Storage:** When you lack enough storage to hold your entire Photos library or prefer to not retain everything locally, let Photos automatically manage when full-resolution versions are downloaded or retained.

In iOS or iPadOS, tap Settings > *Account Name* > iCloud > Photos and make sure Sync this iPhone or Sync this iPad is turned on under iCloud Photos (**Figure 15**).

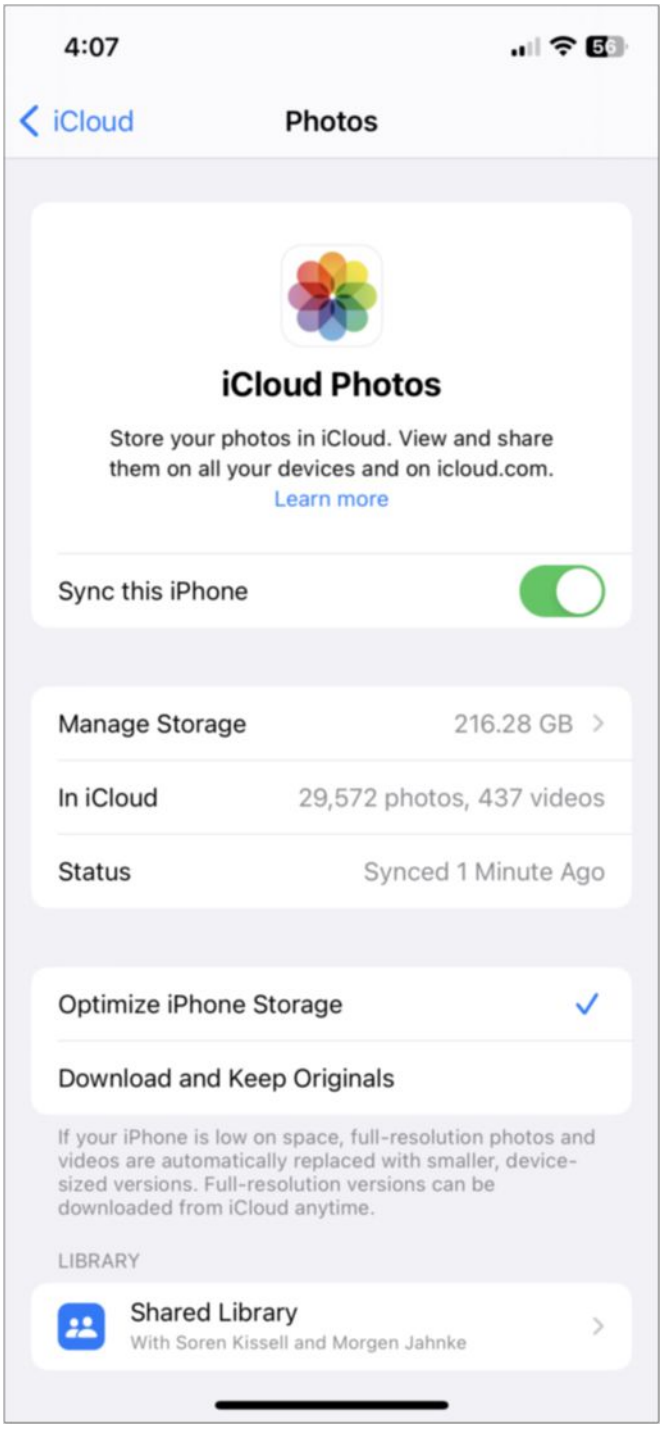


Figure 15: Turn on iCloud photo syncing options here.

If you want to keep your originals on the device (space permitting), leave Download and Keep Originals selected. Otherwise, pick Optimize *Device* Storage to keep just thumbnails.

Note: A few years ago, it seemed ridiculous to think about keeping a large Photos library at full resolution on an iPhone or iPad. Now Apple offers iPhones with up to 1 TB of storage and iPads with up to 2 TB.

In Windows 11 with iCloud for Windows installed, open the iCloud app, check the Photos box (if it isn't already checked), click Options to the right of Photos, and select iCloud Photos.

iCloud for Windows uses the Microsoft Photos app to display and manage photos in iCloud Photos. Open the Photos app and select iCloud Photos in the sidebar to see your iCloud photos. (If that sidebar entry does not appear, go to Settings and make sure Show iCloud Photos is turned on.)

Note: Microsoft Photos may prompt you to download and install HEIF and HEVC Extensions to be able to view and edit certain content from iCloud Photos. To do this, go to Settings, click the "Get Media Extensions bundle" button in the HEIF and HEVC Media Extensions section, and follow the prompts. (The bundle costs $0.99.)

Learn More About iCloud Photos

When you first enable iCloud Photos on each device, the device does a dance with iCloud to upload unique images, videos, albums, and other data stored locally and to download and merge anything it doesn't possess that's in your iCloud storehouse. From that point on, you don't have to do anything special after taking photos on an iOS or iPadOS device or importing them on a Mac or PC: they sync to iCloud automatically, and from there, to your other devices.

Tip: Remember that with iCloud Photos enabled, Camera Roll disappears from your iOS/iPadOS device. Go to All Photos to see what used to be in that album.

Theoretically, that should be all there is to it: things just work, all your photos automagically appear everywhere, and you no longer have to think about syncing or wonder where your photos are. But, of course, it's not quite that simple. You may have any number of questions. Here are the common ones and my answers, developed over several years:

- **Does iCloud Photos suck up bandwidth?** Yes: you might be uploading and downloading hundreds of gigabytes of media. When

first released, Photos absolutely hijacked broadband connections; Apple improved it to be a better network citizen over time.

Tip: Click or tap the Pause button at the bottom of the All Photos view in the Photos app to temporarily halt all syncing.

- **Can I have multiple iCloud Photos libraries on a Mac?** Sort of, but mostly no. While you can switch among Photos libraries with the Mac app, only one can be marked as the System Photo [sic] Library (in Photos > Settings/Preferences > General), and that's the only one used for iCloud Photos syncing. However, there's one exception: If you set up iCloud Shared Photo Library, you do get a second library that syncs via iCloud. See Share a Photo Library.

Note: You can use an external volume to hold your iCloud Photos library. However, the Live Text search in images in Ventura within Photos works with system-wide Spotlight searching only if the library is on the internal volume.

- **How does iCloud Photos handle duplicates?** It seems to figure out when an image or video is identical and stores just a single copy, merging metadata.
- **What happens when I delete a photo?** It will ultimately be deleted from all your devices. There's no way to keep an image or video in iCloud Photos on just some of your linked devices. However, Apple first shifts the media into the Recently Deleted special album, where it sits for about 30 days until its purged. You can recover media from there before that time is up or immediately delete it from within the album.
- **Is everything in my Mac Photos library uploaded?** The Mac version of Photos has an option that lets you import images without copying them into the library. If you have any so-called *referenced* images, iCloud Photos ignores those and provides information in small type at the bottom of the All Photos view about what it can't upload. You can also create a smart album that includes all referenced images or all images that iCloud Photos can't upload.

- **Can I merge libraries from two different Macs?** Yes. When you enable iCloud Photos on each device, it automatically syncs the local Photos library.
- **If I turn off iCloud Photos, does it delete all my media?** You're given a choice to download everything locally or remove all media before synchronization is disabled. If you want to retain your images and videos on the device, don't choose the remove option!
- **If I turn off iCloud Photos and turn it back on, does it re-download and re-upload everything?** At first blush, it seems like it, but in testing, it looks like iCloud checks each piece of media to see whether it's already in iCloud or downloaded rather than transferring it up or down again.

Tip: For more extensive help in using Photos, I recommend reading Jason Snell's book *Take Control of Photos*.

Share Photos, Videos, and Albums

With Shared Albums, you can set up one or more shared photo albums that contain a subset of your photos. You can then invite others to subscribe to those photo albums, which will be available on any of their devices. (Want to share an entire library? Skip ahead to Share a Photo Library.)

You can view and make changes to shared albums in Photos for macOS, iOS, and iPadOS, on the iCloud.com website, and in the iCloud Shared Albums app in Windows.

An album can also be optionally reachable as a public website. Likewise, you can subscribe to photo albums other people have shared with you. And, you can also share *individual* photos or videos. Images can be any size; videos are limited to 15 minutes.

Albums are limited to 5,000 photos or videos each. You can add up to 1,000 images per hour across all your shared albums, and up to 10,000

per day. You can also share up 200 albums and subscribe to up to 200 albums; each album can have up to 100 subscribers.

Note: For more tweaky limits, see Apple's article Shared Album limits for details.

None of this media counts towards your iCloud storage totals, whether you've shared the media or it's being shared with. Once you share media, it remains available until you delete the source media from your library or remove the shared photo album.

People who subscribe to a photo album you've shared can comment on (or simply "like") the photos, and can add their own photos and videos if you permit, up to that 5,000-item limit noted above. Up to 100 people can share an album. Comments associated with posting new images or comments on existing ones can be up to 200 characters.

For details about dealing with comments, likes, subscribers, and other aspects of shared photo albums beyond what I cover here, see Apple's article If Shared Albums aren't working.

Enable Shared Albums

If you have not already done so, enable Shared Albums:

- **macOS:** Open Photos, go to Photos > Settings/Preferences > iCloud, and select Shared Albums.
- **iOS/iPadOS:** Go to Settings > *Account Name* > iCloud > Photos, scroll to the very bottom, and turn on Shared Albums.
- **Windows:** Go to the iCloud app, check Photos, click Options, and select Shared Albums.

Note: Turning on this control is not required for sharing *individual* photos or videos.

Share Photos from an iOS or iPadOS Device

To share photos or videos individually:

1. Open the Photos or Camera app and then navigate to the photos or videos you want to use.
2. Tap Select, select the item(s) that you want to share, and tap the Share icon.
3. Tap Copy iCloud Link, and then paste the resulting URL into Messages, Mail, or anywhere else you'd like. (This link expires after 30 days.)

Tip: Apple removed the capability to make a shared iCloud link from the Mac version of Photos a few years ago. Rely on the iOS/iPadOS Photos app or the iCloud website to create a link.

To add items to a shared album, follow these steps:

1. Open the Photos or Camera app and then navigate to the photos or videos you want to use.
2. Tap Select, select the item(s) that you want to share, and tap the Share icon.
3. Tap Add to Shared Album. What happens next depends on your circumstances:
   - If you haven't created any shared albums on this device yet, you'll be prompted to enter the name for a new album; do so and tap Next. You can also opt to create a new album: tap Shared Album > New Shared Album, enter a name for the new album, and tap Next. Now enter the name or email address for each contact with whom you want to share and tap Next.

Note: Only iCloud members can join shared photo albums; if you want recipients who are not iCloud members to be able to view the photos on the web, you must enable the Public Website feature (described just ahead).

- If you've already set up shared photo albums, iCloud defaults to the most recently used album; to add items to this album, enter an optional comment and tap Post.
- To add items to a different existing album, tap Shared Album and select an album from the list.

4. Enter a comment (optional), and tap Post.

Photos and videos in shared albums then appear on all your devices that have Shared Albums enabled. iCloud notifies recipients by email of the newly available shared photo album. Once a recipient joins a shared album, that album appears on all devices that are signed in with that user's iCloud Apple ID.

To modify a shared album, open the Photos app and swipe up to find the Shared Albums section. Tap See All to view your list of shared photo albums. Then:

- To add more photos, tap a shared album, tap the plus + icon, select one or more photos, tap Done, and then optionally enter a comment and tap Post.
- To change an album's settings, tap the shared album and then tap the People icon. You'll then see the following options:
  - *Invite People:* Tap to invite more people.
  - *Subscribers Can Post:* Leave this on (the default) to let subscribers add their own photos and videos to the album; turn it off to make it read-only.
  - *Public Website:* This option is off by default. If you turn it on, iCloud creates a public webpage for the shared photo album that anyone with the URL can view—even people without any iCloud-compatible devices. Tap Share Link to send the link to others; the URL also appears on the screen.
  - *Notifications:* Leave this on (the default) to be notified when subscribers interact with the shared album—for example, commenting or adding photos.

Note: If you have iCloud Family Sharing enabled, you'll have a Family album with all family members listed at top and no Subscribers Can Post option.

- To delete a shared album, tap the People icon, tap the stream's Delete Delete Shared Album, and then tap Delete.

Share Albums from a Mac

To share an album from Photos on a Mac, follow these steps:

1. Select one or more images in any view.
2. Either right-click (or Control-click) and choose Share > Shared Albums, or click the plus icon to the right of Shared Albums in the sidebar.
3. In the dialog that appears, enter an optional comment, and click an existing shared album or New Shared Album.

   If you clicked New Shared Album, enter an album name, one or more addressees, and an optional comment, and click Create.

To adjust the settings for a shared photo album, enable web access for a shared photo album, or copy its URL, select the shared album in the sidebar and click the People icon on the toolbar.

When viewing a shared photo album, you can drag photos from it to your permanent Photos library to import them, just as with any other photo.

To delete a shared photo album, right-click (or Control-click) the shared album name in the sidebar and choose Delete Shared Album.

Note: If you are using iCloud Family Sharing and want to share photos with other members of your family, you may find the Family shared stream to be adequate. See Use iCloud Family Sharing.

Share Albums from Windows

Apple's iCloud installer for Windows adds the standalone iCloud Shared Albums app. (You must enable Shared Albums first in the iCloud app as described in Enable iCloud Photos on Your Devices.)

To share albums in Windows:

1. Launch iCloud Shared Albums.
2. Click the "New shared album" button in the upper-left corner.
3. Set up the album's details (**Figure 16**):
   - Name the album by typing a label in the Name field.
   - Check "Create a public website…" to share the images via an iCloud.com URL as described above.
   - Optionally start typing names in the To field to invite people. As you type, the app matches entries in your contacts you can select.

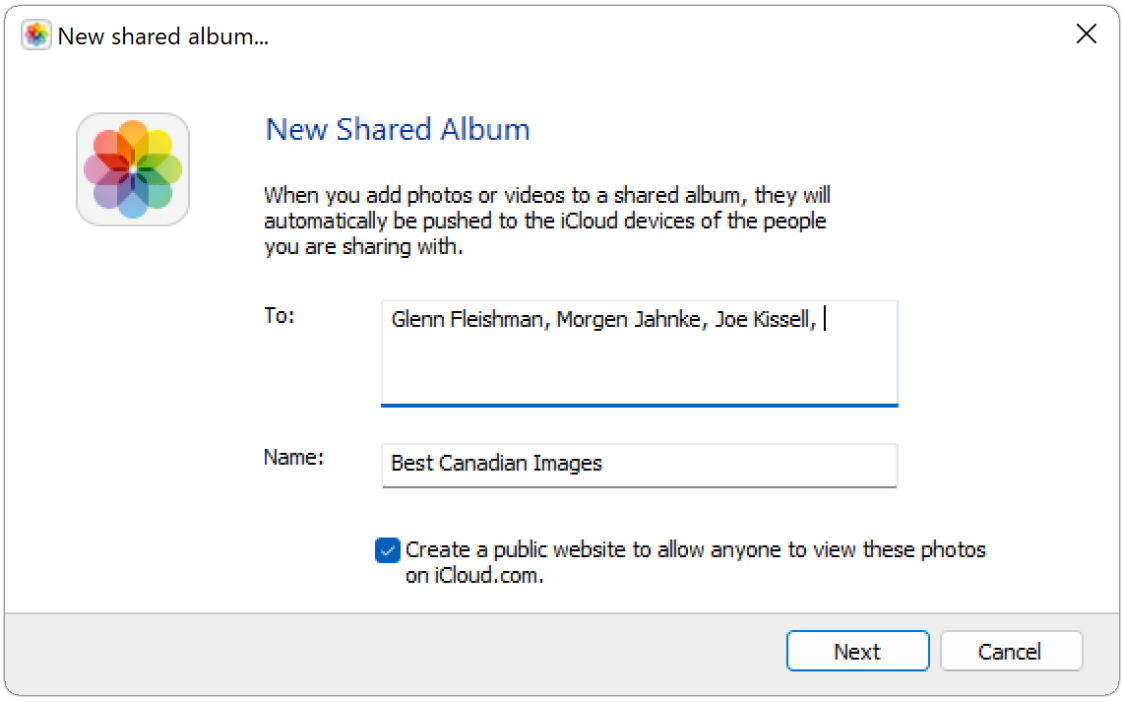


Figure 16: Create a New Shared Album in Windows.

4. Click Next.

5. Click “Choose photos or videos” to select media to add. In the dialog box that appears, choose a location from the “Look in” menu at the top, which can be iCloud Photos or anywhere else on your PC.
6. Select the photos you want to add and click Open.
7. When you’re finished, click Done.

Right-click an album in the main view and choose “Stream options” or double-click an album and click Options to access settings. You can change the name, modify subscribers, and toggle whether subscribers can add media to the album or whether the album is reachable via a public website.

The Windows app doesn’t let you directly copy the public URL of an album shared at iCloud.com. Instead, you have to right-click in the main album view or while viewing the contents of an album and choose “Open public web view.” You can then copy the URL from the browser for the page that opens.

Share a Photo Library

The Photos app has long included a special Family album that’s automatically available to all the members of a Family Sharing group (see Use iCloud Family Sharing). However, adding photos to this album is an entirely manual process, and, because it is such a bother, many families avoid it.

Ventura, iOS 16, and iPadOS 16 added an entirely new way for families—or other small groups of up to six people—to share photos: iCloud Shared Photo Library. That word *library* is key: this isn’t merely another album in your current library, but an entirely separate library, which gives it additional capabilities. Furthermore, you can designate any five people besides yourself as participants, and they don’t have to be in your Family Sharing group. (Indeed, Family Sharing isn’t required to use this feature.) But you can have only *one* shared library, so most of the time you’ll probably choose to share it only with family members.

One of the interesting features of this shared library is that when taking photos with your iPhone or iPad, you can have the Camera app automatically or manually send the photos directly to your shared library. (Configure this on your mobile device in Settings > Photos > Shared Library > Sharing from Camera.)

All participants in the shared library can add, delete, and edit photos, and their changes appear for everyone else too. Similarly, shared photos will be available to all in Memories, Featured Photos, and the Photos widget.

The process of setting up iCloud Shared Photo Library, moving photos to it, and working with it is somewhat involved. For details, see Apple's page How to use iCloud Shared Photo Library or Jason Snell's *Take Control of Photos*. But just to put you on the right path if you're interested in using this feature, go to Photos > Settings > Shared Library (**Figure 17**), click Get Started, and follow the prompts. You'll be able to move all your photos, only those photos matching certain criteria, or just manually selected photos to the shared library—or opt not to move anything right now and deal with it later.

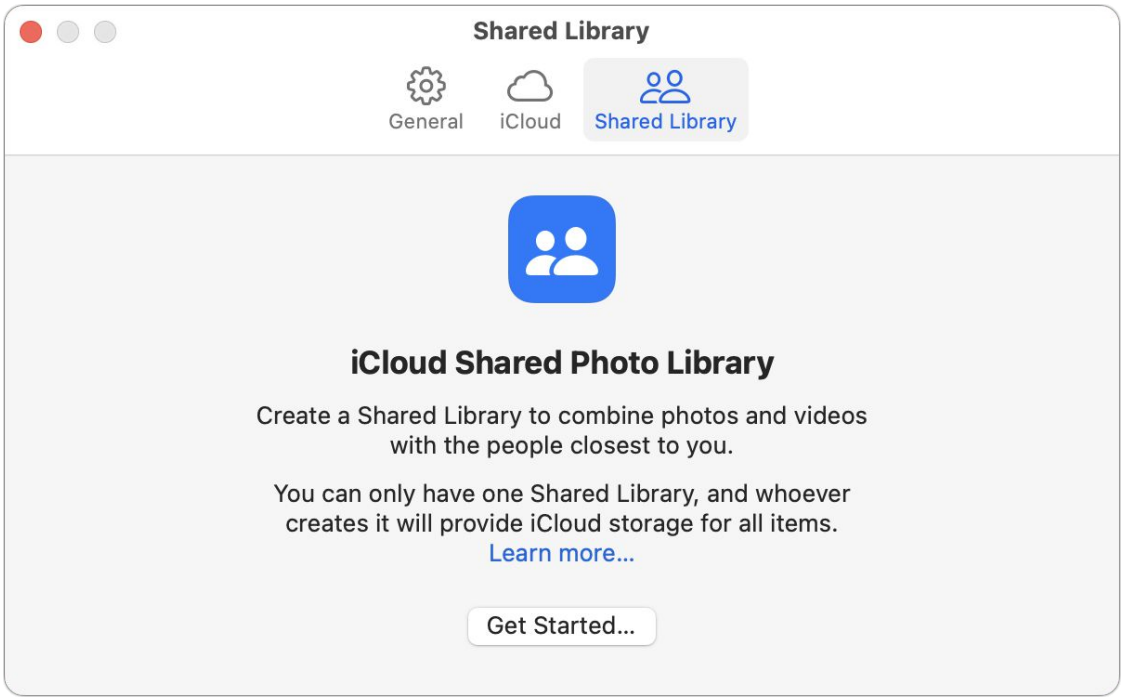


Figure 17: Here's where you enable iCloud Shared Photo Library.

Afterward, you can go back to the same spot to configure a variety of settings (**Figure 18**).

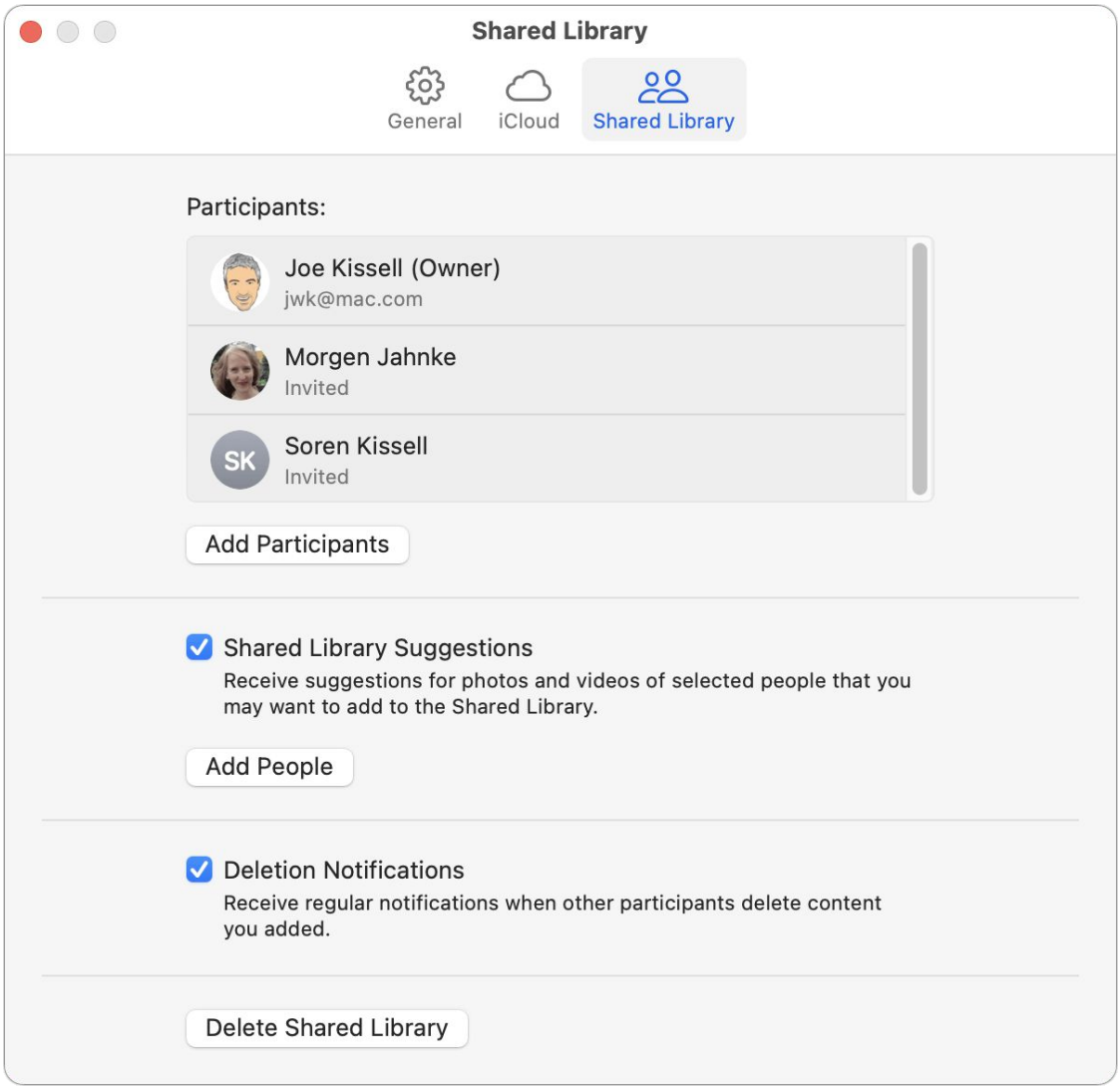


Figure 18: After you set up your shared library, the Settings pane in Photos may look something like this.

Your shared library is available within the Photos app in macOS, iOS, and iPadOS, as well as in the Photos web app at iCloud.com. You can use the menu in any of these places to display just your personal library, just the shared library, or both libraries combined.

Keep Documents and App Data in Sync

iCloud Drive is Cloud's online file storage component, which includes mechanisms to sync files and folders among your devices and apps.

To learn all about iCloud Drive, read the next topic, Use iCloud Drive. In addition, you'll want to read Use In-App Data Syncing, later in this chapter, for information on working with apps that don't rely on documents but do need to sync data across devices.

Use iCloud Drive

iCloud Drive is cloud-based storage you can access from any of your devices. That includes in the Finder in macOS, in the Files app on an iOS or iPadOS device, in Windows, on the iCloud website, and from within apps that support it.

With iCloud Drive, an authoritative copy of each of your documents—called the "truth" or the definitive version among multiple versions—is stored in the cloud. Your Mac normally maintains a local copy of each document, too, and any changes you make to the contents of your iCloud Drive on one device immediately sync to the others via Apple's servers so long as you have an internet connection.

Warning! When you're offline, you can make changes to locally cached copies. If changes are made to those files anywhere else—on other devices or at iCloud.com—you could wind up with conflicted copies. iCloud syncs conflicted copies and names the versions it thinks aren't the "truth" with the date of the problem. When you open a file that has conflicted versions, the app prompts you to select the correct version.

Note: Your Mac might delete the local copies of some files if you've enabled Optimize Mac Storage and your disk starts running low on free space. They always remain in iCloud.

That sounds simple enough, but iCloud Drive has quite a bit of hidden complexity and doesn't always make sense. You'll be able to use iCloud Drive more effectively if you understand at least some of Apple's logic. After I tell you how to turn on iCloud Drive (next), I'll give you a quick overview of what you'll see there (see Explore iCloud Drive on a Mac or PC). Later I delve into how you can use it in various environments, including within Mac and iOS/iPadOS apps.

Activate iCloud Drive

For most users, iCloud Drive was already activated at some point within the past few years, typically while upgrading to a new version of macOS, iOS, or iPadOS. If you deliberately skipped enabling iCloud Drive for some reason, you can activate it whenever you're ready by turning on iCloud Drive in System Settings > *Account Name* > iCloud (Ventura or later), System Preferences > Apple ID > iCloud (Monterey or earlier), or Settings > *Account Name* > iCloud (iOS/iPadOS). In Windows, open the iCloud app and check the iCloud Drive box.

There are a few other iCloud settings you can change. While the default settings are fine for almost anyone, you should be aware that they exist, just in case.

First, you can prevent a particular app in macOS, iOS, or iPadOS from using iCloud Drive (for added security or to save space):

- **Mac:** Go to System Settings > *Account Name* > iCloud > iCloud Drive and click the Options button (in Ventura or later) or go to System Preferences > Apple ID > iCloud and click the Options button next to iCloud Drive (in Monterey or earlier). Then uncheck any app you want to prevent from using iCloud and click Done. This hides that app's folder in iCloud Drive on this Mac, but does not affect the data already saved to iCloud Drive or its appearance on other devices. This setting doesn't prevent you from manually selecting iCloud Drive as a destination for unchecked apps.

Note that one of the items you can select or deselect is Desktop & Documents Folders, but that requires its own discussion; see Sync Your Desktop and Documents Folders (or Don't), ahead.

- **iOS/iPadOS:** Go to Settings > *Account Name* > iCloud > iCloud Drive. Then, in iOS/iPadOS, tap Show All. Turn off any app you want to disable on that device. That app loses in-app access to documents stored in iCloud Drive until you turn it back on. You can, however, still access that app's documents from the Files app.

Second, on a Mac you can enable or disable Optimize Mac Storage. That also requires a bit of explanation; see Optimize Mac Storage.

Note: Windows treats iCloud Drive more or less like Dropbox or another sync service: the files are available on demand—when opened or launched—and synced as needed.

Third, you can choose which apps let other people find you by your email address for the purpose of sharing documents. To enable this on a Mac, go to System Settings > *Account Name* > iCloud > iCloud Drive and click the Options button (in Ventura or later) or go to System Preferences > Apple ID > iCloud and click the Options button next to iCloud Drive (in Monterey or earlier); then click Look Me Up by Email. On an iOS or iPadOS device, go to Settings > *Account Name* > iCloud> Look Me Up.

Note: In all the years I've been using iCloud, I have never once encountered an app that supports this find-by-email feature.

Sync Your Desktop and Documents Folders (or Don't)

In macOS only, iCloud offers the option to sync your Desktop (`~/Desktop`) and Documents (`~/Documents`) folders using iCloud Drive. The idea sounds both simple and elegant: merely check a box, and everything in those two folders becomes available on all your Macs, *plus* on your iOS or iPadOS devices (via the Files app and within apps that directly support iCloud Drive) and on the iCloud website. That's

the vast majority of personal files for most users, apart from photos and music.

Add a file on one Mac, and it appears on the others; change a file in one place, and it changes on the rest. You'll never be without your important data, and never have to take manual steps to sync things among your devices. In other words, this feature is supposed to do for your files what iCloud's other features already do for your email, contacts, calendars, notes, keychains, and so on.

In a moment, I'll tell you how to turn this feature on (or off), and how to achieve a similar result *without* using iCloud if that's your preference. But first I want to offer a reality check. I don't use this feature myself, and I think it will prove problematic for lots of Mac users. Before you jump in (if you haven't already), I want you to be fully aware of how it works and what the consequences will be.

How Desktop & Documents Folder Syncing Works

When you turn on syncing for your Desktop and Documents folders, macOS *moves* those two folders from their original locations to your iCloud Drive folder. In most cases, the contents of any given Mac's Desktop folder actually move into a *subfolder* of the new Desktop folder in iCloud Drive called "Desktop - *Mac Name,*" and likewise the contents of the Documents folder goes into "Documents - Mac *Name*."

In other words, upon initially activating this feature, the Desktop folders and Documents folders from your various Macs don't merge with each other, but you can merge the files manually if you like—see Enable Desktop & Documents Folder Syncing for details.

Once macOS has performed the folder relocation, those folders, like everything else in iCloud Drive, begin syncing to Apple's servers, and from there, to your other devices.

Let me be clear on what syncing means for these folders and iCloud:

- If you lack enough available storage in iCloud Drive for all that new data, you'll be prompted to upgrade to a higher tier iCloud+ plan.

- Even if storage limits are not a concern, you'll have to wait for all that stuff to upload, and then download to your other devices with this sync also enabled. Depending on the amount of data you have and the speed of your broadband connection, this could take from minutes to weeks.

Note: Files sync only to other Macs. Your iOS and iPadOS devices will show the files uploaded from your Mac, but they won't be stored locally until you need to work with them.

Warning! If your ISP imposes a monthly data cap and then throttles or charges overage fees, using this feature could quickly hit that limit. You may be charged more, or have your service slowed down or limited in some way.

- Huge files sync poorly, because any tiny change can result in the entire file syncing once more across all your linked Macs, burning bandwidth as they go and remaining perpetually out of sync. For files that run into the gigabytes or larger, like virtual machines or database software, it's a huge problem.

  If you have such files but still want to use this feature, move them out of your Documents or Desktop folders before enabling syncing.

Tip: VMware Fusion gives you the option to split a virtual disk into smaller files, such that only the changed portions need to be re-uploaded. Enable this by going to the Settings window for each virtual machine. Click Hard Disk, click the disclosure triangle next to "Advanced options," and select "Split into multiple files." Parallels Desktop formerly offered a similar option, but it no longer exists.

- Although iCloud Drive encrypts your data in transit as well as on Apple's servers, this protects it only from malicious outside parties. Unless you Use Advanced Data Protection, nothing prevents Apple from accessing your data, and if a government agency demanded access to it, Apple would be both obligated and able to provide it.

- If you *also* enable Optimize Mac Storage—more on this in a moment—macOS can delete the *local* copies of any of your documents if your Mac starts running low on disk space, leaving only their icons behind. (Such files are marked with a badge to indicate that the originals are stored in iCloud Drive and, presumably, on your other Macs.)

  If you have one Mac with plenty of storage but another with much less room, the Optimize Mac Storage setting means you won't get stuck: both Macs will show all your files and folders. On the lower-capacity Mac, some files won't be stored locally, instead downloading only when you need them. However, if the moment you need them is one when you have no internet access or a slow connection, you could be up a creek.

Warning! Backup software, including Time Machine, can back up only those files for which there is a local copy. If something is stored solely on Apple's servers, it won't be included in your backups.

- With Desktop & Documents syncing enabled, you will no longer have folders located at `~/Desktop` or `~/Documents`. macOS transparently remaps those folders in the background, so apps, scripts, and other tools that are hard-coded to look in those locations should continue to work.
- You can't choose to sync *just* your Desktop folder or *just* your Documents folder, or to sync any additional folders. It's those two or nothing.
- If you decide to turn off Desktop & Documents syncing, macOS will *not* put everything back where it was! This has led some people to panic, unable to figure out how to restore their previous working system. Instead, macOS will recreate your Desktop and Documents folders in their original locations and leave them empty—it won't move the data from iCloud Drive to those folders; you'll have to do that manually.

This feature isn't for everyone. It works best for someone with multiple Macs, whose Documents folder has relatively few files that don't take

up a large amount of storage, and who isn't especially concerned about the privacy of any of that data.

If that's not you, simply leave the option disabled and carry on as if it never existed. (But, read Sync Desktop & Documents Folders Without iCloud Drive for what I consider a better path to essentially the same end result.)

Enable Desktop & Documents Folder Syncing

During setup of a new Mac or upgrading to a newer version of macOS, you should have been invited to enable syncing of your Desktop and Documents folders. This may have been a preselected checkbox you could easily have overlooked. If you left that box checked (intentionally or not), the feature is already on.

If you (wisely) deselected it during setup or an upgrade and want to turn it on now, go to System Settings > *Account Name* > iCloud > iCloud Drive and turn on Desktop & Documents Folders (in Ventura or later) or go to System Preferences > Apple ID > iCloud and click the Options button next to iCloud Drive (in Monterey or earlier). Select the Desktop & Documents Folders checkbox, and click Done.

The change is immediate, although syncing to Apple's servers may take quite a while.

As I mentioned earlier, if you use this feature on two or more Macs, iCloud moves those folders to Apple's servers but *does not merge them across your computers* by default. You'll have to do that manually, and thereafter, the files will sync as you expect.

To perform this manual, one-time merge for each folder:

1. Select iCloud Drive in the sidebar of a Finder window, and inside that, select one of the two "Desktop - *Mac Name*" folders.
2. Drag the stuff that's in that folder to your actual Desktop.
3. Repeat the above with each additional "Desktop - *Mac Name*" folder, but if there are duplicate files or folders already dragged to the Desktop, you'll have to sort those out manually.

4. Now delete all the empty "Desktop - *Mac Name*" folders from iCloud Drive.

5. Repeat steps 1–4 with two or more Documents folders.

Disable Desktop & Documents Folder Syncing

To disable this feature, go to System Settings > *Account Name* > iCloud > iCloud Drive and click the Options button (in Ventura or later) or go to System Preferences > Apple ID > iCloud and click the Options button next to iCloud Drive (in Monterey or earlier). Deselect the Desktop & Documents Folders checkbox, click Turn Off in the alert that appears, and click Done. Then click OK in the second alert confirming that the change has occurred.

Once you've done this, the items you'd stored in iCloud Drive *remain there*, and your local copies will disappear—which may sound like the opposite of what you were expecting: you want the contents of your Desktop and Documents folders back in those locations. To move them back, you drag and drop in the usual way. After dragging the files, click Move in the alert that asks if you really want to move them out of iCloud Drive. If optimization was enabled, the download time depends on the quantity of data you've stored in those two folders and your broadband speed.

Tip: For more on working with iCloud Drive in the Finder, see Explore iCloud Drive on a Mac or PC, ahead.

What I've just described is only for cases in which you leave iCloud Drive turned on, and simply disable Desktop & Documents. If, instead, you turn off iCloud Drive completely while Desktop & Documents is enabled—or if you sign out of iCloud altogether—iCloud prompts you to choose whether to keep a local copy of your files (**Figure 19**). Click Remove from Mac to remove the local copies; click Keep a Copy to create a folder called iCloud Drive (Archive) in your home folder, where a copy of *all* the contents of your iCloud Drive, including those two folders, will appear. (You'll have to move all those items to your preferred final destinations manually.) Either way, the originals

remain on Apple's servers, while new Desktop and Documents folders are recreated at their original locations within your home folder.

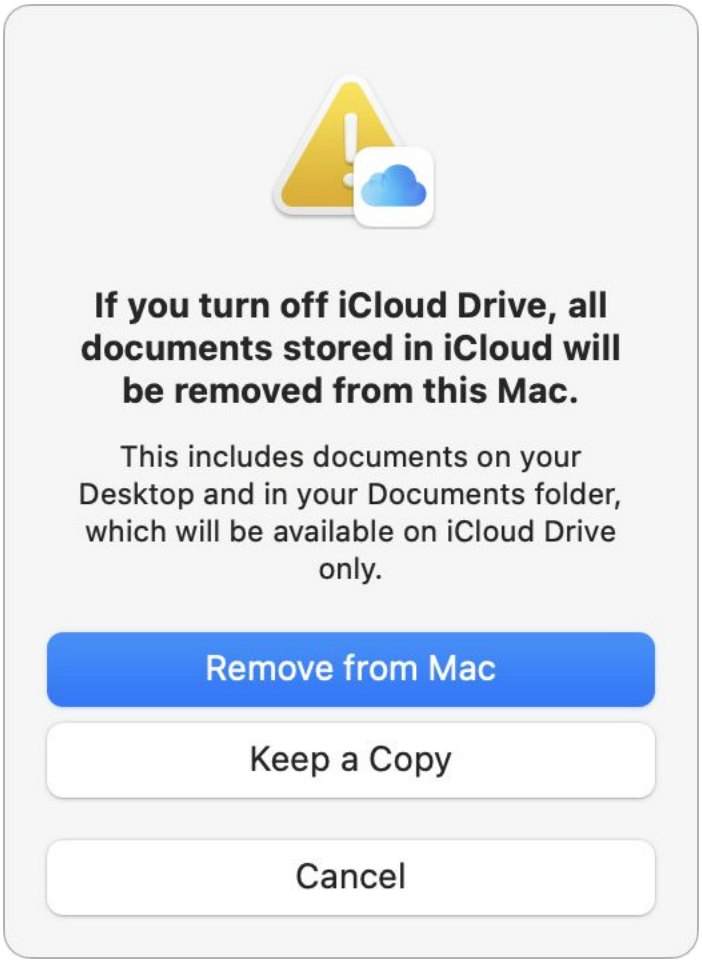


Figure 19: If you turn off iCloud Drive while Desktop & Documents is enabled, iCloud asks you what you want to do.

Sync Desktop & Documents Folders Without iCloud Drive

If you're concerned about using this iCloud feature but wish you could have its benefits, let me briefly share a different approach. I use an app called Resilio Sync Home (formerly known as BitTorrent Sync), which lets me sync any number of folders on my Mac with other devices I own, or share them with other people. (I use it only for my own devices, however.) The syncing uses the same underlying peer-to-peer technology as BitTorrent, which means that it does *not* rely on a central server, like iCloud Drive. Your devices talk directly to each other over an encrypted connection.

I can use this tool to sync folders across computers (Mac or PC) as well as a NAS device in my office, and I can access all my files from an iOS or iPadOS device. I can't reach them from the web—remember, they're not stored on a server. That's fine by me, because I don't have to pay anyone for storage or worry about file sizes. Changes are synced almost instantly, and I can opt to save old and deleted versions of each file. And, for files over 4 MB that are modified, only the *changed portions* are transferred during a sync, which saves lots of time and bandwidth.

Resilio Sync Home comes in both free and Pro (paid) versions. The Pro version costs $59.90 for personal use, and that's what I recommend—primarily because it lets you link all your devices, such that sharing a folder on one automatically syncs it to all of them. (Family and business plans are also available.)

The Pro version also offers Selective Sync, which approximates iCloud Drive's Optimized Storage feature and Dropbox's Smart Sync. If you enable Selective Sync in Resilio Pro for a folder, you'll see its contents on your other devices but the files themselves won't transfer until you try to open them (or explicitly request that they download). Note that with Selective Sync enabled, you won't see thumbnails of graphics that haven't been downloaded to your computer.

Optimize Mac Storage

If you go to System Settings > *Account Name* > iCloud (in Ventura or later), or go to System Preferences > Apple ID > iCloud and click the Options button next to iCloud Drive (in Monterey or earlier), you'll notice an Optimize Mac Storage switch or checkbox. When this is enabled (as it is by default), your Mac keeps a local copy of everything in your iCloud Drive folder—including your Desktop and Documents folders, if you enabled syncing for them—*unless* you start running low on disk space.

If your startup volume does start to get squeezed for space, iCloud Drive automatically deletes older documents from your Mac, leaving only their icons (and other metadata) behind, while the originals remain stored in iCloud Drive. When you try to open a document

whose content has been deleted from your Mac, macOS downloads it from iCloud Drive automatically. Other than taking a bit longer for such files to open, the process should be transparent.

If this sounds suspiciously like Music's Sync Library feature (see Use iCloud Music Features) or iCloud Photos (see Sync with iCloud Photos), that's no coincidence: it's Apple's way of applying roughly the same logic to the rest of your iCloud documents.

Note: Despite having both "optimize" and "storage" in its name, it's merely a small subset of your Mac's Optimized Storage capabilities, which I describe further in the sidebar About Optimized Storage.

Optimized storage is great—and possibly indispensable—for users with very little free storage on their Macs. But it's not risk-free. By enabling this feature, you're trusting that your data won't go missing from Apple's servers, that there won't be an iCloud outage (or problems with your internet connection) at the moment you need those files, that you have the bandwidth to retrieve files you need on demand, and that macOS will make intelligent choices about which old files to remove from your Mac and when.

Personally, I feel safer with this feature disabled.

Explore iCloud Drive on a Mac or PC

Once you've activated iCloud Drive, you can use it almost like any other folder on a Mac or PC. (A bit later in this chapter I cover using iCloud Drive in iOS/iPadOS.)

In the Mac Finder, iCloud Drive appears in the sidebar. Select this (or choose Go > iCloud Drive) to open iCloud Drive (**Figure 20**).

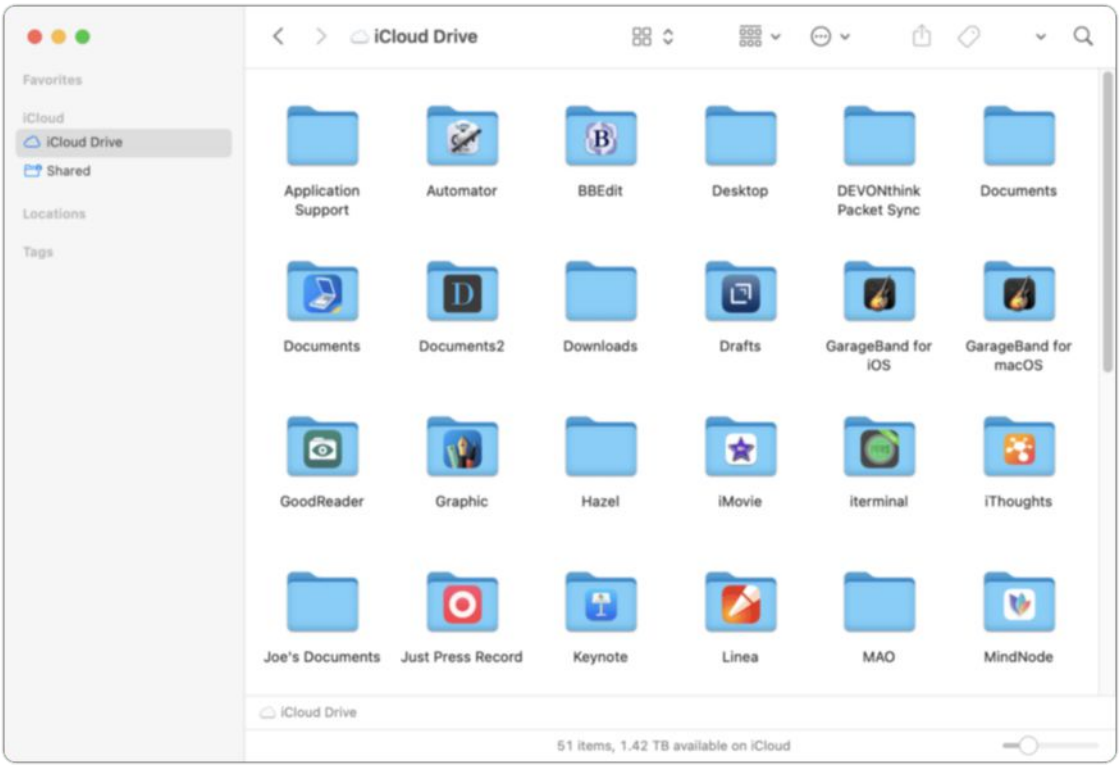


Figure 20: iCloud Drive in the Finder.

Tip: iCloud appears near the top if Desktop & Documents Folders is disabled. If it's enabled, you'll see iCloud Drive, Desktop, and Documents listed under an iCloud heading in the sidebar.

In Windows, iCloud Drive appears in the navigation pane of File Explorer and behaves just like any other folder.

If you need access to your documents in iCloud Drive on a computer that isn't signed in to your iCloud account—or if you want to engage in real-time collaboration in an iWork app—you can do so by visiting the iCloud website in a browser (see The iCloud Drive Web App). You can open documents from Pages, Numbers, and Keynote (see The iWork Web Apps), but otherwise, you can open a file only if the computer you're using has a compatible app.

Drag files into or out of the iCloud Drive folder to move them to or from iCloud; copying/cutting and pasting also works. You may see an alert asking if you're sure you want to remove an item from iCloud because moving it out of that folder really does remove the copy from Apple's servers as well. You can also use the usual methods to create folders and organize items within iCloud Drive.

Warning! I recommend against deleting any of the existing app-specific folders created by iCloud Drive, because doing so will remove all the synced data for that app from all your devices. Some iOS/iPadOS apps, for example, store data in these folders that you never directly interact with.

You may notice icons next to some filenames and folders within the iCloud Drive folder. These indicate the item's local or remote status:

- **macOS:** A download icon appears next to a file or folder in the Finder if it isn't fully downloaded; for a folder, that may mean some items in the folder aren't downloaded, even if others are. This includes anything temporarily removed from your Mac due to optimized Mac storage. To download a file or an entire folder without opening it, click the download icon; or, to download and open a file, double-click the *file's* icon. If an item has either a downloaded icon or no icon at all next to its name, you have a full local copy of it. Right-click (or Control-click) a file or folder and choose Remove Download to evict the locally stored copy from your Mac. Shared folders and items within them are identified by who shared or added an item: shared folders have gray text following their name that reads "Shared by *Name*"; within a shared folder, files and folders have the same gray text with "Added by *Name*."
- **Windows:** An icon next to the file or folder (or in the Status column, depending on your view) indicates whether the item is stored only in the cloud, is waiting to sync, has a local copy, or is designated as *always* having a local copy. To download and open a file that's in the cloud, double-click it. A person icon also appears next to shared folders. Similar to the optimized Mac storage feature, iCloud for Windows automatically removes the local copies of files if you begin to run low on disk space. To force a file to stay on your PC, whether already downloaded or not and even if you're low on disk space, right-click it and choose "Always keep on this device." Alternatively, to delete the local copy of a file, leaving the master copy in the cloud, right-click it and choose "Free up space."

As you explore iCloud Drive, be aware that you may not see a folder for every iCloud-enabled app you use (especially iOS and iPadOS apps), and some folders may not contain the files you think they should. (In fact, these items merely *look* like folders; they are actually called App Libraries, although I refer to them here as folders for simplicity.)

Prevent Items from Syncing

While the whole point of iCloud Drive is to keep files and folders in sync with the cloud and across your devices, you might encounter a situation where you need something to be inside your iCloud Drive folder on your Mac but *not* sync to the cloud. Fortunately, there's a hidden way to manually exclude it. To exclude an item:

- **For a file:** Add the extension `.nosync` within the filename before its extension:
  - If you haven't enabled "Show all filename extensions" in Finder > Settings > Advanced, add the extension at the end, so the file `MyFile` looks in the Finder like `MyFile.nosync`. (Behind the scenes, the Finder changes it to `MyFile.nosync.pdf`.)
  - If you have enabled "Show all filename extensions," add `.nosync` *before* any existing extension. For example, `MyFile.pdf` would become: `MyFile.nosync.pdf`.
- **For a folder:** Add the extension `.tmp` to the folder name. This prevents the folder and all its contents from syncing to the cloud.

Files and folders excluded from syncing in this way have a special "no cloud" icon next to the filename. To resume syncing, remove the `.nosync` or `.tmp` extension.

Share Files and Folders on a Mac or PC

Almost any file or folder you add to iCloud Drive yourself (whether within an app or otherwise) can be shared with other people. Apple conceptually divides sharing into two modes:

- **Collaborate:** By default, you share iCloud Drive folders and documents in Collaborate mode, which simply means that other people will see changes to whatever you're sharing as you make them. Optionally, those other people can also be given permission to change or delete the shared item. Collaborate mode is normally restricted to just the people you invite, though you can also open up the sharing to anyone who has a link.

  The people with whom you share files and folders in this way must have an Apple ID in order to access them, but if they don't have one already, they'll be prompted to create one (for free, naturally).

- **Send Copy:** This is the old-fashioned mode of sharing, in which you can send a file or folder to anyone via email, Messages, or other means. Because it's a static copy, the recipient gets only the current version, not any future changes you may make.

Although these two modes of sharing have been around for a while, Apple changed the interface and wording significantly in Ventura—for example, you won't see the word "Collaborate" in Monterey or earlier, even though the capability exists there.

Here's how to share files and folders on a Mac or PC. (Later, I discuss doing the same thing in iOS/iPadOS; see Use the Files App for iOS or iPadOS.)

Share Items on a Mac

Because the process changed so much in Ventura, I've divided the instructions into "Ventura or later" and "Monterey or earlier."

Share Items in macOS Ventura or Later

In the Finder, select a file or folder inside iCloud Drive. Click the Share icon on the toolbar. A popover (**Figure 21**) appears.

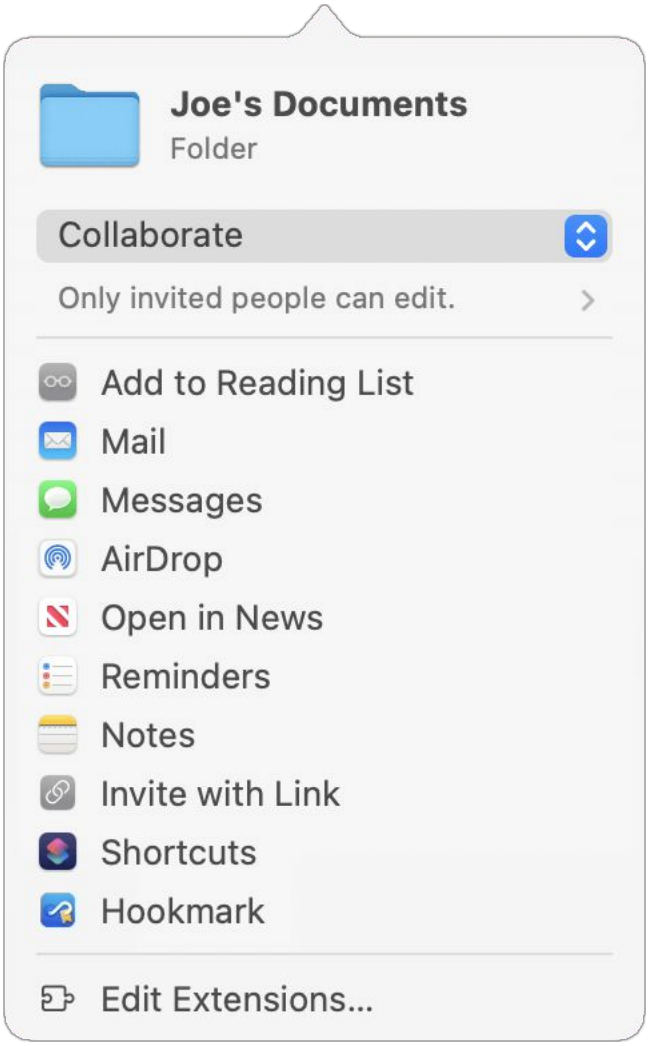


Figure 21: Use the controls in this popover to share iCloud items.

By default, sharing uses Collaborate mode (changes are synced with other people as you make them), *and* allows access only to people you invite. The remaining steps depend on which mode you choose from the top pop-up menu.

If you choose Collaborate:

1. To change any of the default sharing options, click "Only invited people can edit." Two more pop-up menus appear:

    a. **Who can access:** Choose "Only invited people" (the default) to restrict access to the shared item, or "Anyone with the link" for unrestricted access—use this with caution! If you're restricting the item only to invited people, leave "Allow others to invite" checked to enable people you're sharing the item with to extend that invitation to others, or uncheck it to prevent this.

b. **Permissions:** Choose “Can make changes” (the default) to permit those sharing the item to edit or delete it, or “View only” to prevent anyone but yourself from making changes.

2. Choose how you want to distribute the link to the shared file by selecting Mail, Messages, AirDrop, Invite with Link, or any app that supports iCloud Drive sharing links. (You can always share items in another way later.)

   If you chose “Only invited people,” you must next enter the email addresses or phone numbers of the people who will have access to the shared item.

   Depending on the delivery method, optionally add a subject and/or message, then send it in the usual way.

3. Click Send, Send Link, Share Link, or whichever button serves a similar purpose (wording varies by app).

   For all but Messages and Invite with Link, the link is sent through the selected method. With Invite with Link, the link is copied to the Clipboard; you’re now responsible for distributing it. With Messages, the Messages app opens, with a share link prefilled in a new message. Fill in the desired recipients, customize the message and other details, and click Send.

If you choose Send Copy:

1. The list of sharing options shortens, as fewer of them are applicable (**Figure 22**).

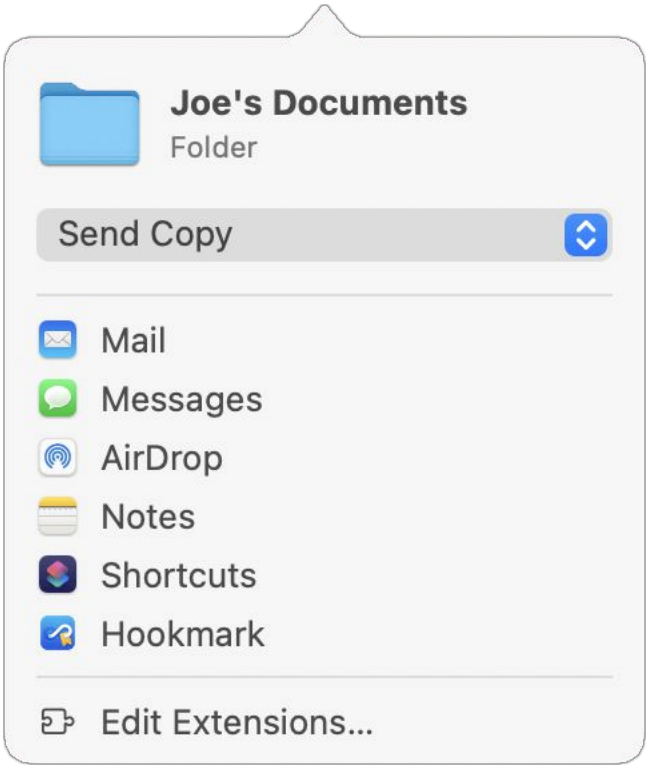


Figure 22: Sending a copy of a file or folder involves fewer steps.

2. Choose a sharing method for sending the copy—in most cases, one of the first three (Mail, Messages, or AirDrop) are what you want.
3. Depending on the delivery method, optionally add a subject and/or message, then send it in the usual way.

To change sharing options later, select the shared item, which should now be labeled "Shared by Me." Right-click/Control-click the item and choose Manage Shared File/Folder. A dialog appears in which you can add people, remove people, or change individual permissions (by hovering over someone's name and then clicking the More ••• icon that appears), or click Stop Sharing to stop sharing the item.

Share Items in macOS Monterey or Earlier

The process for sharing items in iCloud Drive is a bit different in Monterey or earlier:

1. In the Finder, select a file or folder inside iCloud Drive. Click the Share icon on the toolbar and choose Share File or Share Folder (**Figure 23**).

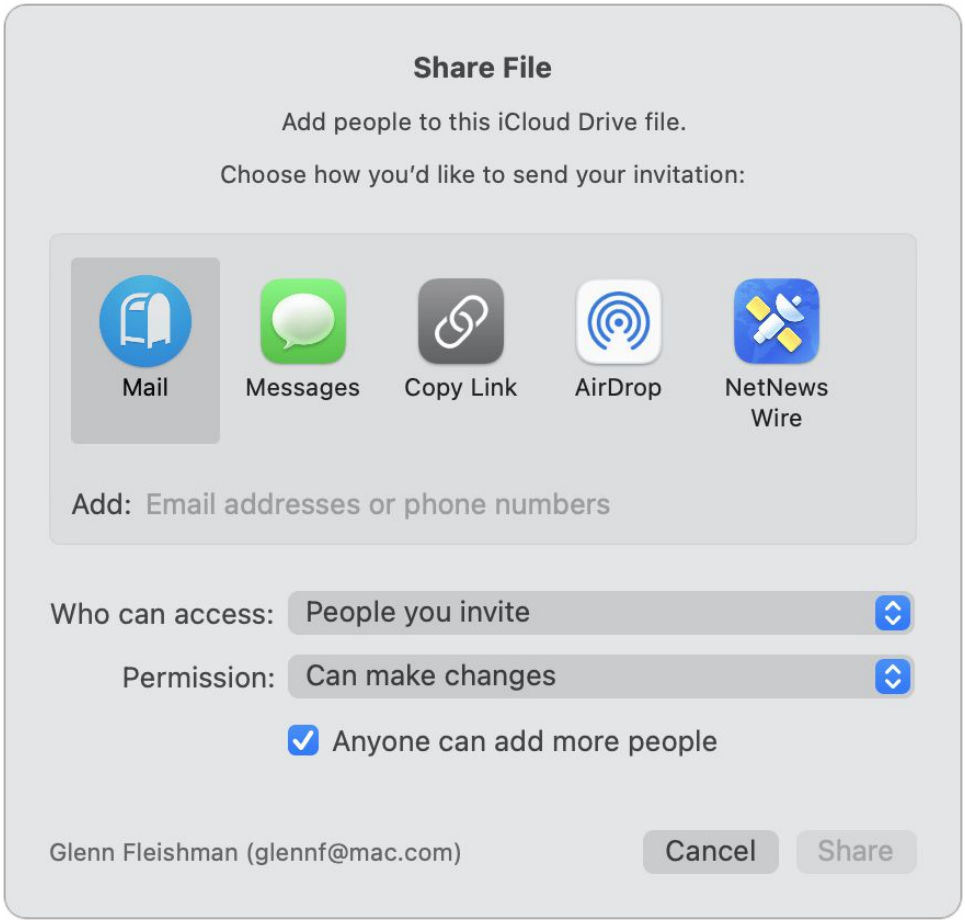


Figure 23: Control iCloud Drive file sharing with Share File options.

2. In the dialog that appears, you can set access and permission:

   - From the "Who can access" pop-up menu, choose "People you invite" to restrict access to people you specify, or "Anyone with the link" to make it available to anyone with the link.
   - From the Permission pop-up menu, choose "View only" to make the item read-only for others, or "Can make changes" to enable the people sharing the item to make changes.
   - Select the "Anyone can add more people" checkbox to allow those invited to expand shared access.

3. Choose how you want to distribute the link to the shared file by selecting Mail, Messages, Copy Link, AirDrop, or third-party apps that support iCloud Drive sharing links. (You can always share items in another way later.)

For Mail, AirDrop, and third-party apps, an Add field appears; fill in the email addresses or phone numbers of people who should have access to the shared item.

With Messages and Copy Link, that step happens next.

Note: Copy Link requires that you enter at least one phone number or email address—and only those people will have access to the shared item (after accepting your invitation).

4. Click Share. For all but Messages and Copy Link, the link is sent through the selected method.

   With Copy Link, the link is copied to the Clipboard. You're now responsible for distributing it.

   With Messages, a Message dialog appears. Fill in the desired recipients, customize the message and other details, and click Send.

Tip: You can grab the link by itself later by clicking the Share button on the toolbar or right-clicking/Control-clicking the item and choosing Share > Managed Shared File/Folder, and then choosing Copy Link.

To change sharing options later, select the shared item, which should now be labeled "Shared by Me." Click the Share icon on the toolbar or right-click/Control-click the item and choose Share > Manage Shared File/Folder. A dialog appears in which you can add people, remove people or change individual permissions (by hovering over someone's name and then clicking the More ··· icon that appears), or click Stop Sharing to stop sharing the item.

Share Items on a PC

To share iCloud Drive files and folders in Windows:

1. Right-click (or Control-click) a file or folder in iCloud Drive and choose Share with iCloud Drive > Share File or Share Folder.

2. In the dialog box that appears, decide on your initial sharing options:
    - From the “Who can access” pop-up menu, choose “Only people you invite” to restrict access to people you specify, or “Anyone with the link” to make it available to anyone with the link.
    - From the Permission pop-up menu, choose “View only” to make the item read-only for others, or “Can make changes” to enable the people sharing the item to make changes.
    - Select the “Anyone can add more people” checkbox to allow those invited to expand shared access.
3. If you selected “Only people you invite,” click in the People box and type an email address or phone number. Repeat as needed. You can also change any individual person’s permissions by clicking the More ··· icon next to that person’s name in the list and choosing a different option from the pop-up menu.
4. Click Apply to begin sharing. A “Share link” dialog appears. You can click to email listed contacts or click “Copy link” to copy the link to your clipboard. You can then share it with others by email, instant messaging, or whatever other method you like.

To change sharing options later, right-click the shared item again and choose Share with iCloud Drive > Manage Shared File or Folder. The same dialog box appears, in which you can add or remove people, modify permissions, or click Stop Sharing to stop sharing the item altogether.

Tip: To learn more about sharing folders, see Apple’s support article Share files and folders in iCloud Drive on iCloud.com.

Use iCloud Drive Within Mac Apps

Every Mac app’s Open and Save dialogs show iCloud Drive in the sidebar, which means you can navigate manually to any spot in iCloud Drive to open or save a document. (If you don’t see the sidebar in a

Save dialog, click the disclosure button next to the filename field, or choose Other from the Where pop-up menu, to expand the dialog.)

However, those with explicit support for iCloud Drive show an extra entry, bearing the app's name, under iCloud in the sidebar of that app's Open and Save dialogs (**Figure 24**).

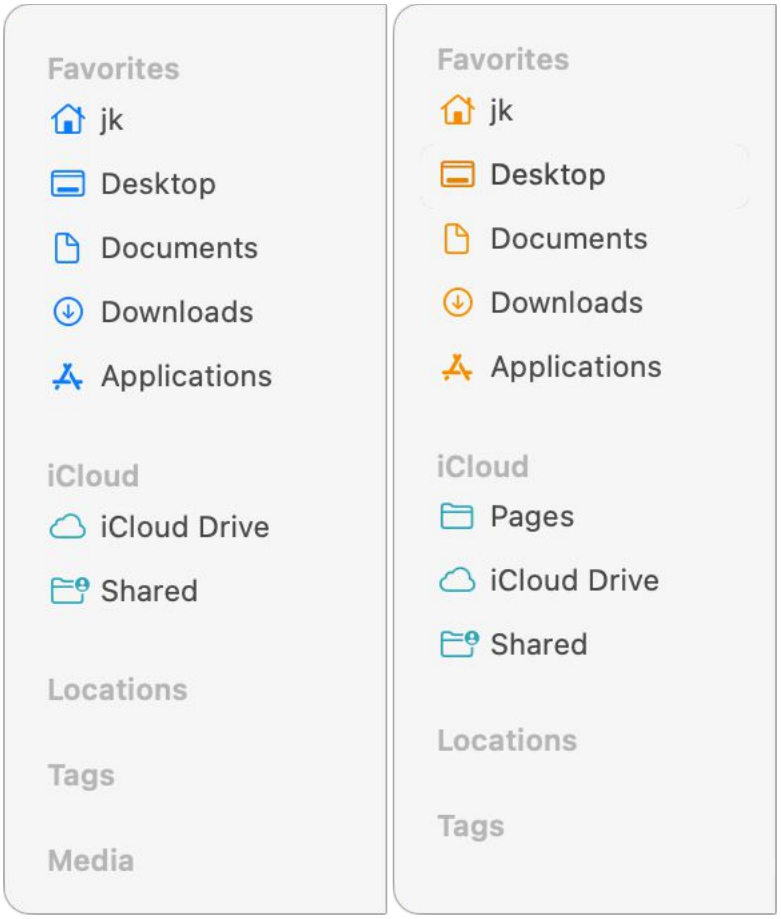


Figure 24: Apps *without* explicit iCloud support (left) have an iCloud Drive entry in Open and Save dialogs. Those with iCloud support (right) also have their own entry at the top of the iCloud section. (If Desktop & Documents Folders is enabled, iCloud Drive, Desktop, and Documents appear under the iCloud heading.)

When you see an entry like this, it's a shortcut to that app's iCloud Drive folder. But individual app developers can choose to hide their app's folder on one or more platforms, which means—depending on the app—that sidebar entry may be the *only* way to see that app's documents. The folder may not show up in the Finder, on the iCloud website, and so on.

Developers can also determine which file types their app-specific folder may contain. So, if App X can't open Pages documents, for example, it may not permit you to put a Pages document in its folder (even by dragging it in the Finder), and the folder for Pages won't be available in that app's document picker in iOS/iPadOS.

Autosave and iCloud

Apps that have built-in support for both autosave and iCloud Drive may automatically save copies of newly created documents in iCloud. These are documents that you haven't explicitly stored anywhere yet. This is apparently necessary for Handoff, which makes in-progress documents available to your other devices.

If this behavior is a concern to you (for privacy reasons, say), try one of these two remedies:

- Turn off iCloud Drive—either completely (meaning you won't be able to take advantage of its other benefits), or only for a specific app. (Disable iCloud Drive in Ventura or later via System Settings > *Account Name* > iCloud > iCloud Drive and click the Options button in Ventura or later; in Monterey or earlier, go to System Preferences > iCloud and click the Options button next to iCloud Drive. In all cases, then deselect the app).
- Immediately save new files locally, rather than to iCloud. For more privacy considerations, see Manage iCloud Security and Privacy.

Use the Files App for iOS or iPadOS

The Files app, which is installed automatically with iOS and iPadOS, gives you access to all your iCloud Drive files, as well as data from a variety of other apps and cloud service providers. We'll begin by looking at iCloud Drive, since that's most germane to this book.

When you open the app on an iPhone or iPod touch, you may see something like **Figure 25**, in which the top view shows recently added or modified files, and the bottom view shows a list of locations you can browse. (Tap Recents or Browse, respectively, to switch between these views.) iPads, with their larger screens, instead show a sidebar with

categories that include Recents and Locations; if you don't see it, tap the Sidebar icon at the top.

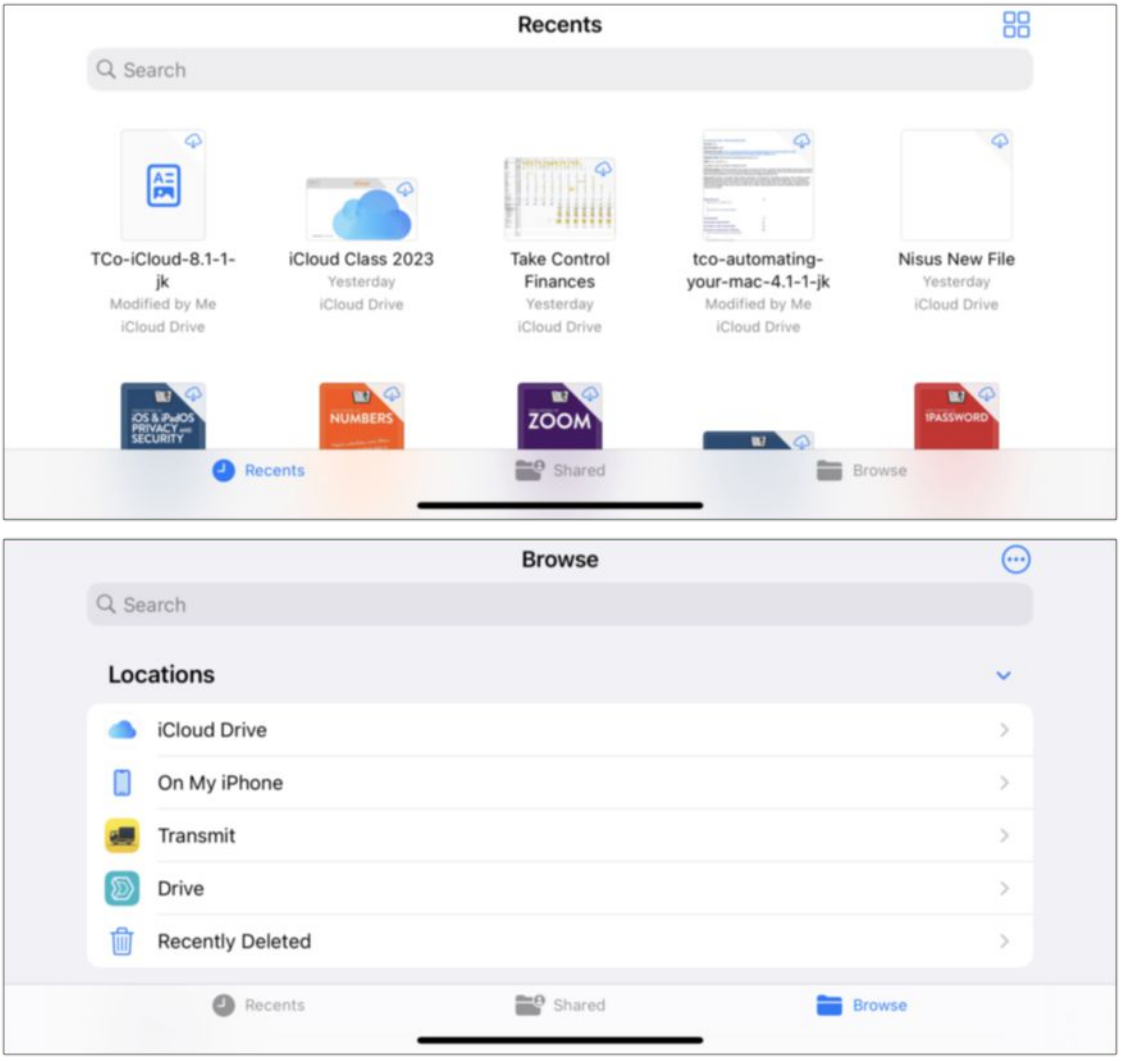


Figure 25: The Files app for iOS has a Recents view (top) and a Browse view (bottom). The Browse view lets you navigate to iCloud Drive and other locations.

If you see a list of locations in the Browse view on an iPhone or iPod touch, tap iCloud Drive to see what's there (**Figure 26**). If you're already in another location, you may need to tap whatever label appears in the upper-left corner of the screen to move up a level, and continue as necessary to get to the Locations list. Then tap iCloud Drive.

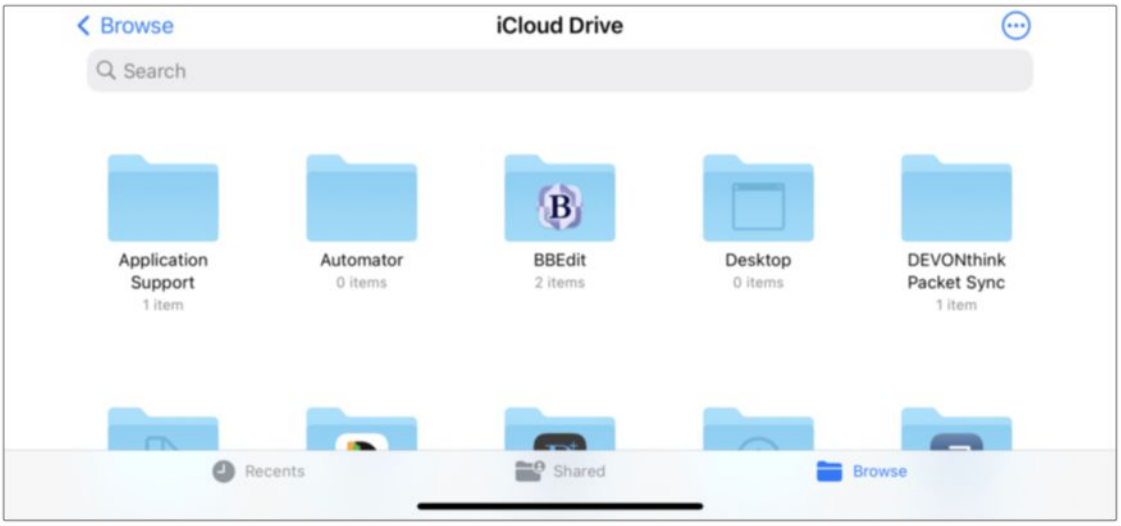


Figure 26: The iCloud Drive location in the Files app.

On an iPhone, you can tap the More icon to display additional commands, such as New Folder, as well as switch between Icons and List and adjust the sort order. On an iPad, you can tap the View (or or) icon to display a pop-up menu of view options, including Icons, List, and Columns (as well as sorting options), and tap the New Folder icon to create a new folder.

In the Files app, as in the iCloud Drive folder in macOS or Windows, you can navigate, view, or move files and folders in iCloud Drive. Here are some of the more interesting things you can do with a file or folder:

- **Open it:** Tap the file to open it with its default app.
- **Rename it:** Touch and hold the file, and tap Rename on the popover. (Note that you can't rename certain folders, including those belonging to specific apps.)
- **Delete it:** Tap Select, select the file, and tap the Trash icon or the word Delete.

Note: If you delete something stored on iCloud Drive, it appears in the Trash on your Mac, and in the Recently Deleted location on all your iOS and iPadOS devices.

- **Move it:** Tap Select, select the file, tap the Folder icon or the word Move, navigate to a new location, and tap Move. Not all

locations are valid destinations, and I have not yet been able to discern how Files decides where you can and can't move things.

- **Share it:** Tap Select, select the file or folder, and tap the Share icon. Then, on the share sheet, choose Send Copy (the default) or Collaborate from the pop-up menu. If Collaborate is chosen, tap "Only invited people can edit" to specify other sharing options (identical to those covered in Share Items in macOS Ventura or Later). Tap a destination (such as Message or Mail), fill in the recipient(s), and send the message. Refer back to Share Files and Folders on a Mac or PC for more information on sharing.
- **Zip or unzip it:** Tap Select, select the file, tap the word More or the More icon, and tap Compress or Uncompress.

You can also use the Search field at the top to search for files anywhere on your iCloud Drive.

Note: Some files and folders may be dimmed and thus inaccessible. This happens, for example, when the app in question is Mac-only and there's no iOS or iPadOS app that can open its files.

Tip: Files downloaded from Safari (including…*cough*…Take Control ebooks) go straight into the Files app. To find files downloaded from Safari, open Files and, if they're not immediately visible, open the Downloads folder.

Just as you can navigate iCloud Drive and open, delete, or save documents in the Files app, you can do the same with a wide variety of cloud-connected apps—as long as they're installed on your iOS or iPadOS device. That includes Dropbox, Google Drive, OneDrive, Transmit, Resilio Sync, DEVONthink To Go, and numerous others. It also sweeps in any Macs on your local network with file sharing enabled. There's even an On My *Device* category for files stored locally on your iOS or iPadOS device and not in the cloud.

To view and navigate to these locations, start on the Browse screen and then tap Locations in the upper-left corner, followed by a location. (You may need to sign in the first time you use a new location.) To add

new locations from supported apps on your iOS or iPadOS device, or disable existing locations, tap the More icon followed by Edit or Edit Sidebar (**Figure 27**) and then turn switches on or off; you can also drag the handle to reorder them.

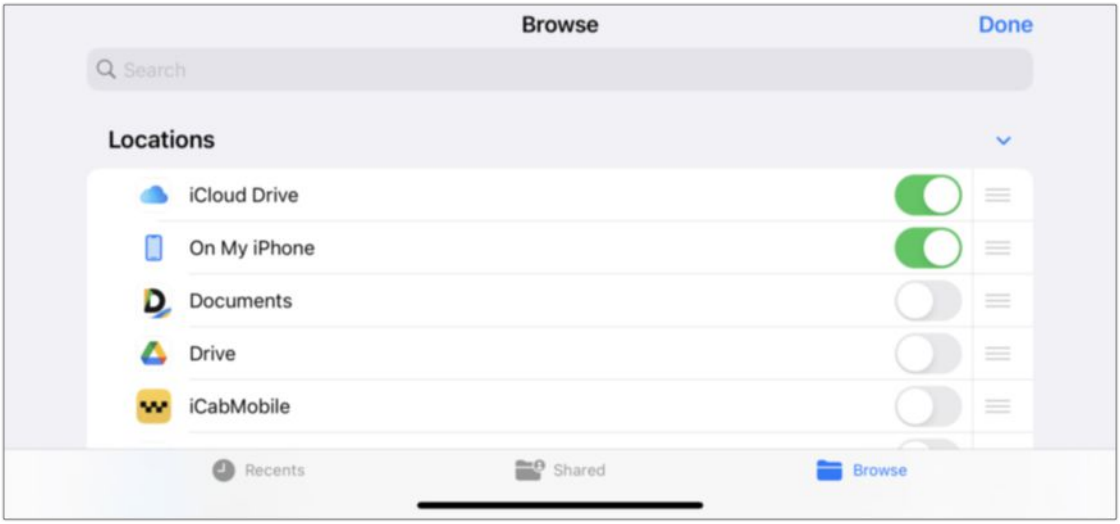


Figure 27: Enable, disable, or reorder locations in this view.

Each location in the Files app has its own interface and features, so what you see when you tap Dropbox, for example, will look much different from what you see when you tap OneDrive. However, they should be similar enough to the stand-alone apps that you'll be able to figure them out easily.

Use iCloud Drive Within iOS and iPadOS Apps

Long before the Files app existed, it was possible to access iCloud Drive from within iOS and iPadOS apps. At first, apps could access only their own files, then later the entire Files interface became available from within supported apps, so that they could directly access files from other locations as well. This means that most of what you can do in Files, you can also do within most apps. However, apps aren't entirely consistent when it comes to iCloud Drive. So I want to offer some broad guidance and then give a few specific examples.

Somewhere within most iOS/iPadOS apps that support iCloud Drive is a document picker that looks something like **Figure 28**, which is to say almost exactly like the Files app.)

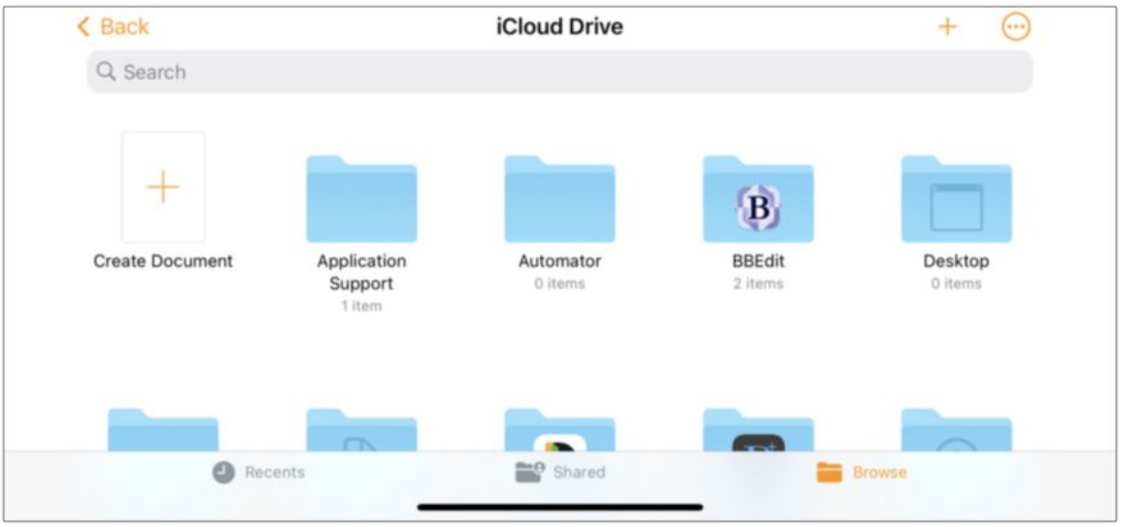


Figure 28: The document picker in a typical iOS or iPadOS app.

For simplicity, many apps show you only their own documents by default—that is, what's in the folder with that app's name—rather than this top-level iCloud Drive view. (Indeed, some iOS/iPadOS apps use iCloud Drive exclusively for their own documents and provide no access to documents outside that folder.) You may have to dig a bit to find iCloud Drive.

For example:

- In Pages, Numbers, and Keynote, the iCloud Drive document picker is the first thing you see, by default, when you open the app. It may, however, initially be set to show Recents (recently modified documents); to browse through all your files, tap Browse at the bottom. If you already have a document open, tap the word or icon in the upper-left corner of the screen to see the app's documents; to navigate up to the top level of iCloud Drive, tap iCloud Drive in the upper-left corner.
- In GoodReader, tap the Manage Files icon and then tap Import Files followed by Open from Files or Import from Files.

- In Documents by Readdle, tap My Files > Files > Browse and then navigate to the top level of iCloud Drive.

If you can't find iCloud Drive, it may mean the app doesn't fully support it—or the document picker might just be in an unexpected place. Check with the developer for guidance.

iCloud Drive and Backups

Although iCloud includes a feature for backing up iOS/iPadOS devices (see Back Up and Restore iOS/iPadOS Data), it does *not* include a way to back up Macs. Lots of people have asked me whether iCloud Drive can be used for that purpose, but it can't.

iCloud Drive is designed for syncing, not for backup. Space permitting, it keeps a local copy of all your files, too, though you can manually remove local copies of files and folders by right-clicking (or Control-clicking) them and choosing Remove Download(s). It also retains deleted files for only 30 days (see Data Recovery), and it doesn't necessarily retain old *versions* of files (although some individual apps may store old versions). This means that *copying* data to iCloud Drive wastes disk space, while *moving* data there relocates it but doesn't back it up. If you delete a file in iCloud Drive on your Mac, the cloud copy disappears too (after 30 days).

Looking at things from another angle, however, you should absolutely back up everything in iCloud Drive, along with the rest of your files, to one or more other drives or external locations. Thus, with whatever backup apps you may use—Time Machine, Backblaze, Carbon Copy Cloner, or whatever—make sure it includes the directory `~/Library/Mobile Documents/`, which is where iCloud Drive stores its local copies of your files. If something goes missing from your iCloud Drive for any reason, you'll want another way to recover your data.

Troubleshoot iCloud Drive

If files aren't syncing to or from your Mac at all, confirm that you're signed in to System Settings > *Account Name* or System Preferences > Apple ID with the same Apple ID you use on your other devices.

A more frequent problem is iCloud Drive getting "stuck" indefinitely during a sync, with seemingly no progress. If you look in the sidebar of a

Finder window under the iCloud heading, you'll see an iCloud Drive entry. If any files are actively being synced, a circular progress icon appears next to it that indicates what portion of the sync is finished (**Figure 29**). Click that icon to show a more detailed display (**Figure 30**) with the number and size of items being uploaded or downloaded.

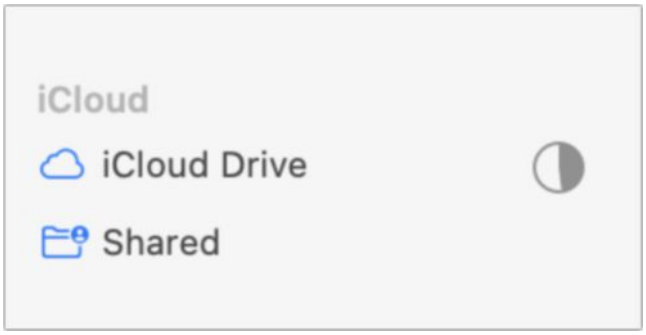


Figure 29: The iCloud Drive item in the sidebar displays a circularly filled icon when items are actively syncing.

Figure 30: Here's what iCloud Drive thinks it's syncing right now.

If you see no progress at all in this display after many minutes, or if files mysteriously stop syncing after a while, rebooting often helps. But I've found an even quicker way to "nudge" iCloud Drive, by stopping two background processes (which then automatically restart themselves). To do this, open Terminal and type the following:

```
killall bird; killall cloudd
```

Then press Return. In a moment, iCloud Drive syncing should resume.

Note: Glenn Fleishman describes a more involved syncing problem he had, and the steps he went through to address it, in the TidBITS article Cloudy with a Chance of Insanity: Unsticking iCloud Drive.

For other problems, it's always worth trying The All-Purpose iCloud Troubleshooting Procedure, which begins with checking Apple's status

page. You might also want to check out the free Cirrus app, which provides access to logs and status information on iCloud processes, but requires significant technical chops to make sense of.

I should also mention two Apple support articles on the web that may help you with iCloud Drive problems and questions:

- iCloud Drive FAQ
- Set Up iCloud Drive on iPhone

Other Syncing Issues

iCloud might encounter syncing issues for data besides what's in iCloud Drive. When it does, you may find a Some iCloud Data Isn't Syncing item near the top of System Settings (**Figure 31**).

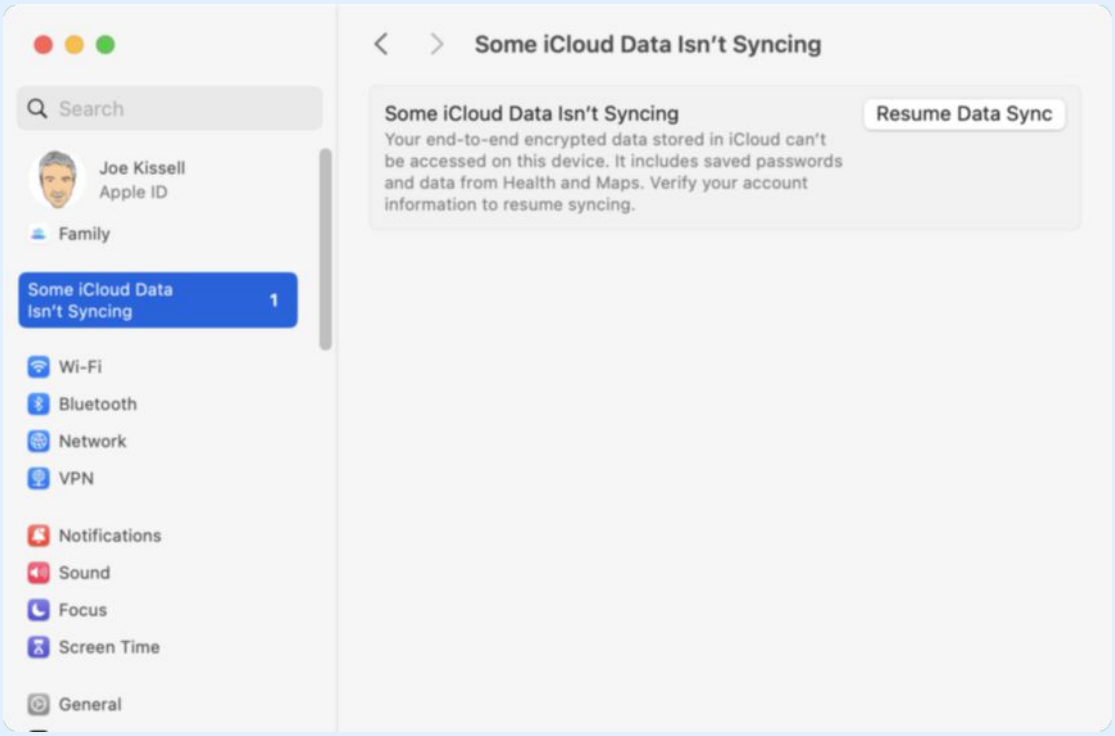


Figure 31: *In some situations, iCloud alerts you to sync issues in System Settings.*

As the dialog says, you may need to verify your account information, which means clicking your name at the top of the sidebar in System Settings and following any instructions shown there (such as reentering your iCloud password). Then click the Resume Data Sync button shown above.

Use In-App Data Syncing

Not all apps are based on documents, but even those that aren't can use iCloud to synchronize other kinds of data. The easiest way to explain what I mean is by way of a few examples:

- BBEdit can synchronize its settings, scripts, plugins, and other data across multiple Macs via iCloud.
- Hazel, which automatically performs user-created actions on the contents of folders you specify, can use iCloud to synchronize its rules across your Macs.
- Apple's Podcasts app uses iCloud to synchronize custom stations and playback positions. This lets you start listening to a podcast on one device and continue on another.

In addition, when iCloud Drive is enabled, iCloud syncs a few other bits of data across your devices, including text abbreviations (from System Settings > Keyboard > Text Replacements or System Preferences > Keyboard > Text on a Mac, or from Settings > General > Keyboard > Text Replacement on an iOS or iPadOS device) and several types of settings and data for Apple Mail: signatures, flag names (see this article for how to change the names), blocked senders and muted conversations, and (only on Macs) rules and smart mailboxes. And, to be clear, this syncing occurs even if Mail is unchecked in the list of apps syncing with iCloud Drive! (Mail rules also sync, but their enabled/disabled state does not, since you might want different rules enabled on each Mac.)

Note: Although iCloud also syncs Mail's VIPs and previous recipients, that data is part of the Contacts category, not iCloud Drive. Go figure.

Developers must explicitly add iCloud syncing support to their apps, and not all apps are good candidates for this type of syncing. In general, iCloud syncing is turned off by default for third-party apps; you'll have to look through each app's preferences to see if it's supported and how to turn it on. More often than not, it's as simple as flipping a

switch or choosing iCloud from a pop-up menu. On the other hand, Apple apps that use in-app syncing (such as Podcasts and Game Center) usually have iCloud syncing turned on automatically with no way to disable it.

But remember, iCloud syncing is for Macs and iOS/iPadOS devices only. If you use an app that also has a version for Windows, Linux, or Android, you may be better off with an alternative syncing method, such as Dropbox, if it's offered.

About Optimized Storage

Optimized Storage is the term Apple uses for a collection of features, all of which are designed to reduce the amount of disk space occupied on your Mac. Although Apple isn't crystal clear about which features are and are not considered part of Optimized Storage, the list appears to include at least the following:

- macOS automatically purges certain caches, logs, and duplicate downloads. None of this is user-configurable, as far as I can tell.
- In the Storage Management window of the System Information utility, macOS shows you how much storage various apps and files use, and gives you a way to delete anything you consider clutter.
- If you like, macOS can automatically remove any file from your Trash after it's been there for 30 days.
- You can instruct Music (or iTunes for Windows) to delete purchased movies and TV shows you've already watched. (You can re-download them if needed.)
- Apple Mail includes a preference that lets you specify whether to download all attachments, no attachments, or only recent attachments.
- You can enable the Optimize Mac Storage setting for iCloud Photos in Photos to replace full-resolution local copies of your photos with lower-resolution versions if you start running low on disk space (see Sync with iCloud Photos).
- iCloud Drive can store your Desktop and Documents folders (see Sync Your Desktop and Documents Folders (or Don't)).
- An optional iCloud Drive setting, Optimize Mac Storage, works much like the feature of the same name in Photos, except that it applies to files stored in iCloud Drive.

Significantly, however, only the last three of these features involve iCloud (and thus are the only ones I cover in this book).

Keep Mail, Contacts, and Calendars in Sync

Email, contact, and calendar data work together to help you with many day-to-day tasks, and those sets of details are the ones you'll most likely want to keep in sync across your Macs and iOS and iPadOS devices. Behind the scenes, they rely on different technologies to do their work. But the end result is that when you change email, contact, or calendar data on one device, iCloud immediately pushes those changes to your other devices.

This chapter discusses these three data types. In the interest of simplicity, I've left out most of the boring instructions for tasks you already know how to carry out or can figure out easily, as well as anything for which Apple offers detailed instructions via the Help menu on your Mac or visiting the iCloud User Guide).

In this chapter, I also explain how to Use Mail Drop, an iCloud feature that simplifies sending large attachments.

Work with iCloud Mail

An iCloud account includes an email address in the icloud.com domain, at least 5 GB of storage (shared with other iCloud services), and a lovely web interface for checking your email (see The Mail Web App).

Note: Apple also lets you still use *account*@me.com if your Apple ID account dates back to MobileMe; and *account*@mac.com if it dates back even further. These addresses are all interchangeable, though you can use filtering at the iCloud website or in Mail to distinguish among messages sent to them.

In most respects, iCloud Mail is a conventional IMAP account. (For more on what that means, read my article FlippedBITS: IMAP Miscon-

ceptions.) Your email host's mail server stores all the messages in your inbox, messages you've filed in folders, and your sent mail. The server also tracks which messages you've read, replied to, or forwarded. Because mail is stored remotely, you can access your email on any device (even with a third-party email client) or in a web browser, and see exactly the same messages, in the same locations, with the same status. (iCloud offers no POP support at all.)

Note: You can choose to move any messages out of the server's folders in any macOS mail client and some iOS/iPadOS ones to store them just on a single device, removing them from the server.

With default settings, as soon as you enable Mail in iCloud's settings on each device, your iCloud Mail stays in sync across devices without any manual intervention—not because iCloud does anything special but because that's the way IMAP works. However, iCloud Mail differs from run-of-the-mill IMAP accounts in several respects:

- Setting up an iCloud Mail account on any Apple device is as easy as it gets: all you have to do is make sure Mail is turned on after entering your iCloud username and password.
- When used with iOS and iPadOS devices, you can choose *push* updates, which send messages to your device the instant they come in, rather than having to wait for the next scheduled check.
- iCloud Mail has a good webmail interface that supports searching message contents, setting up auto-responses, forwarding email to another account, uploading attachments with Mail Drop (see Use Mail Drop), and creating rules that automatically sort messages.
- Apple's mail servers provide basic spam and malware filtering. *However,* when iCloud Mail encounters an incoming message that matches certain criteria that Apple doesn't disclose, it doesn't merely label the message as Junk or move it to a Spam mailbox; instead, the iCloud server summarily deletes it without any notice to the sender or recipient. (You can read about this in Silent email filtering makes iCloud an unreliable option at Macworld.) I disagree with this approach because all spam filters make mistakes.

Note: The iCloud mail servers don't seem to get smarter over time regarding what is spam and what isn't, unlike the spam filter built into Mail for macOS.

- You can add up to three *aliases*—extra email addresses ending in @icloud.com—that forward incoming messages to your main Inbox. You can build rules around these aliases, just like your main email address, if you want to file, forward, or process them distinctly.
- With an iCloud+ account, you can use Hide My Email to create an anonymized alias that Apple manages directly in a message you're composing. See Hide Your Email Address.
- iCloud Mail lets you use a custom domain name if you subscribe to iCloud+. With a custom domain enabled, you can use up to three addresses at that domain just like you would iCloud aliases. See Configure a Custom Domain.
- Although turning on Mail in System Settings > *Account Name* > iCloud or System Preferences > Apple ID > iCloud (Mac), or Settings > *Account Name* > iCloud (iOS/iPadOS) syncs your messages and mailboxes, several other types of Mail settings and data sync *only* when iCloud Drive is enabled and Mail is selected in iCloud Drive > Options: signatures, flag names, blocked senders and muted conversations, and (only on Macs) rules and smart mailboxes. (VIPs and previous recipients are synced as part of Contacts.)

On the whole, iCloud Mail is not bad as email services go, although you may prefer more customizability or need additional features. If so, keep in mind that email providers are a dime (or less) a dozen—anyone can get a free account from Gmail, Outlook.com, Yahoo, and numerous other sources, and paid options with more services, security, or storage abound. So, if you find the limitations of iCloud Mail a turnoff, you're free to ignore it, or to use it only as a secondary account.

Syncing Mail Rules and Settings

As I mentioned above, as long as you have iCloud Drive enabled (and Mail enabled within iCloud Drive > Options), iCloud also syncs Apple Mail rules, smart mailboxes, signatures, flag names, blocked senders, and muted conversations across your devices. There's nothing to configure—it just happens. However, note the following qualifications:

- This feature has nothing to do with iCloud Mail—it works even if you have iCloud Mail disabled on all your devices and rely instead on other email providers.
- Although Mail rules sync across Macs, their state (enabled/disabled) does not, because you may want different rules to be enabled on different computers.
- iCloud does *not* sync rules with the Mail web app on the iCloud website, only with the Apple Mail app.

Access iCloud Mail with Other Email Clients

If you're unsatisfied with the iCloud webmail interface, but can't or don't want to use Mail on your Mac, you can use the email client of your choice on any platform, including Windows and Linux.

Just set up a new account using IMAP, with these settings:

- **Incoming mail (IMAP) server:** `imap.mail.me.com`
- **Username:** Your (full) Apple ID
- **Password:** An app-specific password (see Use App-Specific Passwords)
- **IMAP authentication method:** Use "password" if your email client provides multiple authentication options
- **SSL for incoming mail:** Yes
- **Port:** 993
- **Outgoing (or SMTP) mail server:** `smtp.mail.me.com`
- **SMTP Authentication:** Yes; use "password" if your email client provides multiple options
- **SSL for outgoing mail:** Yes
- **SMTP port:** 587

Use Mail Drop

Email servers often handle large attachments awkwardly. To avoid aggravation, you can send a *link* instead: copy a file to cloud storage, follow the service's steps to get a URL for the file, and then email that URL. But that's an inconvenient, multi-step process.

A better way, available in Mail on all platforms (macOS, iOS, iPadOS, and web), is an iCloud feature called Mail Drop. In iOS and iPadOS it's always enabled. On a Mac, it's enabled by default for iCloud email accounts; for other IMAP and Exchange accounts (but not POP accounts, which don't support Mail Drop), go to Mail > Settings/Preferences > Accounts > *Account Name* > Account Information and select "Send large attachments with Mail Drop" (**Figure 32**). In the Mail web app on the iCloud website, enable it by clicking the gear ⚙ icon in the sidebar, choosing Preferences, and clicking Composing. Then check "Use Mail Drop when sending large attachments."

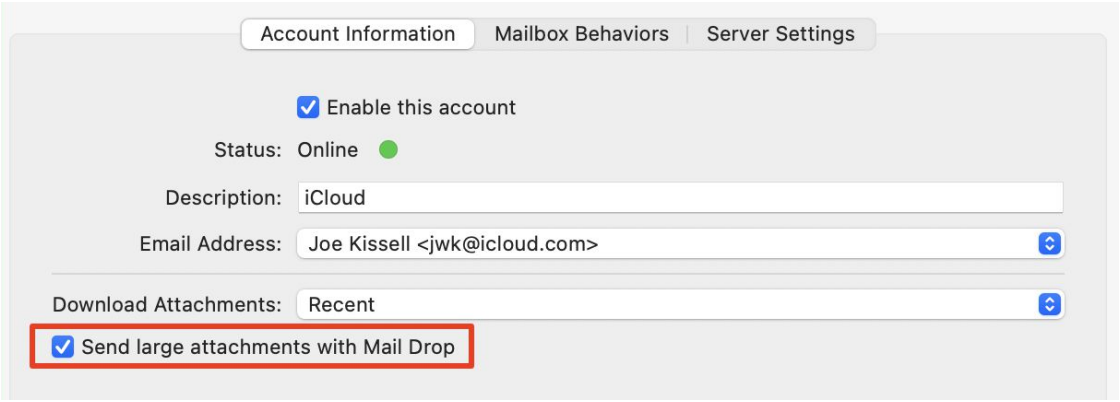


Figure 32: Enable Mail Drop for each of your accounts to eliminate the pain of emailing large attachments.

With Mail Drop, you compose a message and drag files in to attach them, just as you normally would. But when you click the Send button, if the message and its attachments are over 20 MB or so, Mail uploads the attachments to iCloud, and inserts a link to the files in the message. Mail Drop attachments don't count towards your iCloud storage quota.

When the message arrives, the recipient sees a link that can be used to download the attachments. iCloud stores sent attachments for 30 days and then deletes them.

Note: Mail Drop limits the total size of a single message sent to 5 GB including its attachments, and you can have no more than 1 TB in outstanding, unexpired attachments at any given time.

Sync Your Contacts

iCloud's Contacts feature lets you create, search, and organize an address book of the people and companies you interact with often. As you make additions and changes, the contact data synchronizes immediately among your various devices. Depending on which device you're using at the moment, the Contacts app may give you options to dial a phone number, compose an email message, map an address, and perform other tasks relevant to the contact you're currently viewing.

When you turn on Contacts in iCloud's settings, syncing begins at once and continues in the background. In some situations you may be asked if you want to merge contacts on your device with contacts already in iCloud—nearly always, the answer is yes. (Similarly, if you turn off iCloud Contacts on a device, you'll be asked whether you want to delete the local copy of those contacts; the answer to that is usually no.)

Note: Behind the scenes, the Contacts category also syncs VIPs and previous recipients from Mail.

Most of the things you'll need to do with contacts are self-explanatory. But two aspects of iCloud's contact syncing have always struck me as a bit weird and annoying, so I want to say a few words about those here. (I also offer problem-solving pointers for contacts at the end of the chapter, in Troubleshoot Contact and Calendar Problems.)

Work with Contact Groups

Groups are nothing more or less than lists of contacts. If you create a group in the Contacts app on the iCloud website or in the Contacts app—say, all the members of your volleyball team or the coworkers in your department—then you can later send a message to everyone in the group simply by typing the group's name into the To, Cc, or Bcc field

when you compose a new message in Mail. That's the obvious use for groups—in fact, it's the whole point. Putting contacts in a group does give you the secondary benefit of being able to quickly narrow searches to just group members, but there are other ways to accomplish that.

Create Groups on your iPhone or iPad

To manage groups—also called *lists*—on your iPhone or iPad, open the Contacts app and make sure you're at the top level, where the label is Lists. Tap Add List and select an account name if you have more than one. Type a name for your list and tap Done. Then tap the list, tap Add Contacts, select the people you want to include in the group, and tap Done.

Groups in iOS and iPadOS do have one limitation compared to macOS: Because Contacts for iOS and iPadOS has no concept of smart groups, any smart groups you created on your Mac won't appear in Contacts on your iOS or iPadOS devices and thus won't be available to Mail on those devices either.

Share Your Contacts with Someone Else

Although iCloud offers calendar sharing (described later in this chapter), it includes no comparable feature for contacts—not even with Family Sharing (see Use iCloud Family Sharing). Sure, you can export one or more contacts in industry-standard vCard format and email them to someone else, but there's no way to keep contacts in sync between users. Apple apparently expects each iCloud user to maintain an independent list of contacts, but lots of people want to share a list of contacts with a family member, so additions and updates can happen just once instead of duplicating all that effort.

One way to *sort of* work around this problem is to create a new iCloud account (see What If I Share an Apple ID with Someone?). On each device of yours and of the family members with whom you will share contacts, add that iCloud account as a secondary account (see Work with Multiple iCloud Accounts) and turn *off* all services for that account except Contacts. Then put all the contacts you want to share in

that account; to minimize confusion, delete them from your individual accounts.

(As a variation, say I want to share all my contacts with my wife. Since I trust her with my iCloud credentials, we could skip the third iCloud account—I could add my own account on her devices as a secondary account, but leave only Contacts enabled.)

If you add this additional shared account, be sure to check which iCloud account is the default account for contacts on your iOS/iPadOS devices (Settings > Contacts > Default Account) so newly added contacts go where you expect them to.

However, this workaround is just that: a hack, not a solution. One downside to this approach involves your "me" card, which is the contact record that represents you. You can't have two separate "me" cards on any device, even if you have more than one iCloud account set up. So, if you designate a certain card as "me" in your personal iCloud account and the shared account has a card for you too, that change propagates to your shared account—meaning that all the people sharing those contacts have the same "me" card!

Tip: To designate a card as "me" in Contacts for Mac, select the card and choose Card > Make This My Card. You can't set a "me" card in iOS or iPadOS.

To avoid this problem, make sure your *shared* account doesn't have cards for yourself or for anyone you'll be sharing the account with.

iCloud and Other Contact/Calendar Services

If you have an iCloud account as well as an Exchange account, you can access your Exchange and iCloud contacts and calendars through Outlook on a Windows PC and through Contacts and Calendars on a Mac or iOS device. Likewise, you can access Google Calendar accounts in Calendar and Google Contacts in Contacts. The same is true for other contact and calendar providers.

The fact that a single app can show contacts and calendars for both iCloud and another provider has led some people to assume that somehow your iCloud account shares data with your Exchange, Google, or other account. But it doesn't! For example, if you make a change to your iCloud calendar on your Mac, that won't show up in your Exchange calendar when you view it in Outlook on a PC. The accounts are entirely separate; they're merely displayed in the same place.

I have heard of various complicated workarounds that claim to sync contacts and calendars across services. But in my opinion, they're more trouble than they're worth. Let your iCloud account hold the data that belongs there; let your Exchange, Google, or other account hold its own data; and simply set up each of your devices to access all your accounts. Attempting to sync various cloud-based accounts with each other is a recipe for frustration—or duplication.

Sync Your Calendars

iCloud's Calendar feature stores events and appointments of all sorts, pushes updates to all your devices automatically, and lets you access your calendar data in a web browser. You can also share calendars with other iCloud users, send and receive meeting invitations, and perform quite a few other scheduling tasks.

As with contacts, most calendar activities are straightforward, but I want to explain a bit more about handling meeting invitations and shared calendars. (For tips on solving problems with calendars, see Troubleshoot Contact and Calendar Problems.)

Better Calendars with BusyCal
Although Calendar has gotten better in recent years, I still prefer BusyMac's BusyCal for Mac for managing my calendars because it's more customizable and easier to use. It works great with iCloud, as well as Exchange, Google Calendar, and CalDAV. As with other third-party apps, if you use two-factor authentication with your iCloud account, you'll have to Use App-Specific Passwords in BusyCal.

Invite Others to a Meeting

You can invite other people to join any event on your calendar. This lets you keep track of who has agreed to come (or turned down the meeting), and to send out updates if the event changes.

When you create an event, enter a name or email address in the invitees field to invite someone. As you type, Calendar looks for matching contacts in your Contacts list and offers a menu of possible matches. Select a contact from this list to accept it, or keep typing. After you add an invitee, you can repeat the procedure to add more.

After adding an invitee, click the person's name to open a pop-up menu with options such as Edit and Remove (or, in iOS/iPadOS, swipe to the left on a name to remove it). If you remove an invitee, the event is deleted from that person's calendar; if you remove everyone after sending an invitation, a cancellation notice is sent.

For invitees who use iCloud, the invitation appears in Calendar's notification box on the iCloud website, as well as in Calendar on a Mac or iOS/iPadOS device. For other invitees, invitation messages include buttons (or links) for Accept, Decline, and Maybe. After clicking one of these, the invitee sees a confirmation page with a downloadable `.ics` file that can be used to add the event to Calendar or a third-party calendar app.

In addition, the event on your own calendar is updated with icons reflecting each invitee's status, and any responses also appear in your notification box.

Work with Shared Calendars

iCloud can share any calendar, either publicly or privately, using the industry-standard CalDAV protocol. When you share a calendar privately, you can assign read-only or read-write privileges on a per-user basis. This mechanism makes it practical for families, coworkers, and other groups to use iCloud for calendars that apply to multiple people without jumping through lots of hoops or buying extra software. (Note, however, that families who Use iCloud Family Sharing get a shared Family calendar automatically and can skip this topic.)

Shared calendars can be viewed in iCloud Calendar, the Calendar app for Mac or iOS/iPadOS, or third-party calendar apps such as BusyCal and Microsoft Outlook.

> **Note:** Behind the scenes, reminder lists (covered in the next chapter) are stored and synced exactly as calendars are, and can be shared in much the same way other calendars can—but only privately.

To share a calendar on a Mac, click the Share icon that appears when you hover over the calendar's name in the sidebar. In the popover, you can share the calendar privately with only people you select—and also decide who is allowed to edit the calendar—or you can share it publicly for anyone with the address to view (but not edit).

> **Note:** The people with whom you share private calendars must be iCloud users. You can't share calendars between iCloud and Google Calendar or other services.

Troubleshoot Contact and Calendar Problems

iCloud Contacts and Calendar have been astonishingly problem-free for me over the past few years, but I've heard from a number of users who have experienced problems, especially duplication of entries when moving from another provider or app.

Because of the sheer number of variables involved, I can't offer specific solutions to every problem, but I can recommend *Take Control of Calendar and Reminders* by Scholle McFarland and Glenn Fleishman, which includes a troubleshooting chapter. I can also point you to Apple's extensive and helpful support articles:

Contacts troubleshooting:

- If your iCloud Contacts, Calendars, or Reminders won't sync
- If you see duplicate contacts after setting up iCloud Contacts

Calendar troubleshooting:

- If your iCloud Contacts, Calendars, or Reminders won't sync
- If you have duplicate events on your iCloud Calendar

Sync Other iCloud Data

In much the same way that iCloud delivers immediate push updates to your email, contacts, and calendars, it syncs numerous other types of information, among which are Safari bookmarks, iCloud Tabs, and your Reading List; data from the iPhone's Health app; Siri data; Reminders (a.k.a. tasks or to-do items); Notes; iMessage conversations; and data from built-in Apple apps such as News, Stocks, Home, and Voice Memos.

Note: I discuss yet another type of data syncing in the next chapter, Work with iCloud Keychain.

These features aren't at all flashy and there's not a great deal to say about them, but in this chapter, I give you an overview of how they work—and point out a few cool things you may not have noticed.

Work with Browser Bookmarks, Tabs, and Reading List

The list of iCloud services on your Mac, PC, or iOS/iPadOS device includes either Safari (Mac, iOS, and iPadOS) or Bookmarks (Windows). Either way, this item, when enabled, syncs the following items.

Note: Apple enables end-to-end encryption for Safari history, tab groups, and iCloud Tabs. No one—even Apple—can inspect those synced items except with access to your devices. Bookmarks lack this extra protection, however.

Bookmarks and History

When Safari enabled, iCloud syncs Safari bookmarks and your browser history among your Apple devices. In Windows, iCloud syncs bookmarks with Edge, Google Chrome, or Firefox.

Note: iCloud won't sync Edge, Google Chrome, or Firefox bookmarks on a Mac.

Reading List

For Macs and iOS/iPadOS devices, iCloud syncs the Reading List, which comprises webpages you've saved to read later by choosing Bookmarks > Add to Reading List (Mac) or by tapping the Share icon and then Add to Reading List (iOS/iPadOS).

Tab Groups and iCloud Tabs

Safari lets you create *tab groups*, essentially browser "desktops." A tab group is a named set of tabs, each open to a given webpage or the Start Page. You can switch any open Safari window among available tab groups. With Safari syncing enabled, tab groups sync across all applicable devices. Apple explains how to use these features on their Group tabs in Safari page.

Unrelated to tab groups are iCloud Tabs, Apple's name for a list of all tabs in open windows that syncs across all your Macs and iOS/iPadOS devices. (The feature has sported various names, but it dates back several years.) You can find iCloud Tabs in macOS in two places:

- **Show the Start Page:** Choose File > New Window or New Tab (if the option in Safari > Settings/Preferences > General for "New windows open with" or "New tabs open with" is set to Start Page), or choose Bookmarks > Start Page on any page. iCloud Tabs appears as a popup menu listing your device names and the tabs open on that device. If it doesn't appear, click the Start Page customize button in the lower-right corner and select iCloud Tabs. Use the popup menu to switch among your devices.
- **Add an icon to the toolbar in Safari for macOS:** Choose View > Customize and drag iCloud Tabs onto the toolbar. You can now click that to reveal a popover that shows a list of tabs with favicon and the window title under headings for each of your devices (**Figure 33**). Click an item in the list to open it.

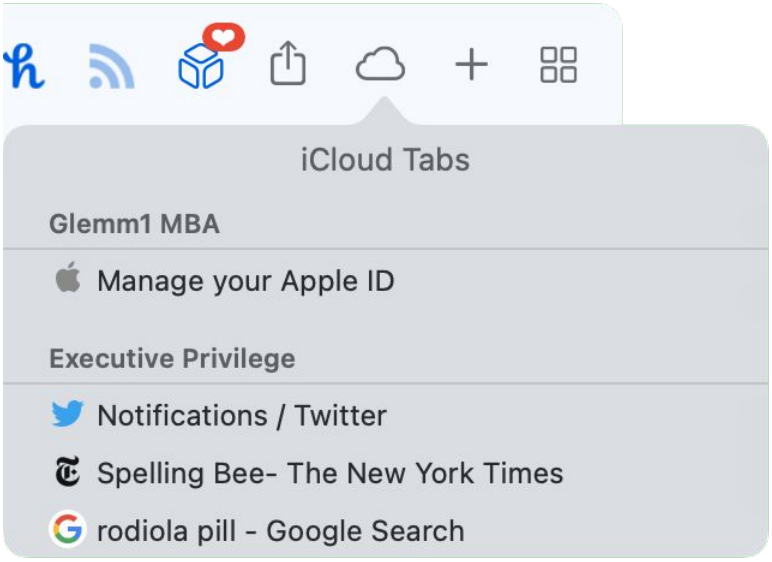


Figure 33: See open Safari tabs on your other devices in this view.

To close an open tab on another device:

- On the Start Page, right-click (or Control-click) the tab name and choose Close Tab.
- In the iCloud Tabs popover, hover over the tab name and then click the close icon.

In Safari for iOS and iPadOS, open a new Start Page (tap the Tabs icon and then tap the plus + icon), and then swipe down to find a popup menu (just like the one in Safari for macOS) listing your other devices, with opens tabs appearing below the currently selected device name. Tap to open. Touch and hold, and then select Close to close the tab.

Note: You might be surprised to find that pinned Safari tabs *don't* sync through iCloud, although they do appear in all Safari windows on a given Mac. That means you'll have to set up your pinned tabs how you like them on each of your Macs.

Sync Messages

A feature called Messages in iCloud enables you to keep all your iMessage and SMS exchanges from the Messages app in sync across all

your devices. This feature can also take advantage of optimized storage by removing old messages and their attachments from a device if it runs low on space, but continuing to store them in the cloud.

To use Messages in iCloud, you must have iCloud Keychain (see Work with iCloud Keychain) enabled on your devices, along with two-factor authentication (see Enable Two-Factor Authentication). Then you can enable Messages in iCloud on each device.

How Private Are Your Messages?

There's a weird contradiction with Messages in iCloud and iCloud Backup. Apple doesn't provide access on the iCloud website to Messages in iCloud, as the contents are too private for that—just like your iCloud Keychain items can be accessed only from individual devices. Apple requires two-factor authentication as an extra measure to preserve your messages' privacy.

But if you have iCloud Backup enabled *and* Messages in iCloud, an encryption key necessary to decrypt your synced messages is stored in your iCloud Backup—which lacks end-to-end encryption! So if someone (a thief, enemy, government, etc.) obtained your backup, they could then decrypt your archived messages! The way to avoid this is to Use Advanced Data Protection, which applies end-to-end encryption to (among other things) your iCloud Backup.

To enable Messages in iCloud on a Mac:

1. Open Messages.
2. Go to Messages > Settings/Preferences > iMessage > Settings.
3. Select Enable Messages in iCloud.

You can then optionally click Sync Now to force an immediate sync.

To enable Messages in iCloud in iOS or iPadOS:

1. Go to Settings > *Account Name* > iCloud; then tap Show All.
2. Turn on Sync this iPhone or Sync this iPad.

Once you've turned on Messages in iCloud on all your devices, your messages should begin syncing almost immediately; how long they take to finish will depend on the quantity of message data you have and the speed of your internet connection.

Use Reminders

Reminders (also known as tasks or to-do items) can be accessed in the Reminders app on most Apple devices, which includes the Mac, iPad, iPhone, iPod touch, Apple Watch, and HomePod; and the Reminders web app on the iCloud website. Reminders consist of text (the thing you want to remember) with a circle you can select to show the task has been completed, as well as optional alerts based on time or location.

Tip: The HomePod lets you complete various Reminders-related tasks with your voice, such as adding an item to a list or hearing a list.

Note: Outlook for Windows also syncs what appear to be iCloud reminder lists, but it does so in a way that Apple's Reminders app can't see them on any platform. If you happen to use BusyCal, however, you can see and edit those lists!

You can turn Reminders on or off in the iCloud settings on an iOS or iPadOS device or a Mac. Behind the scenes, reminders are stored in special calendar files called reminder lists, and they can be shared much like calendars. But unlike calendar events, reminders don't have to be tied to a particular date or time.

Here are a few aspects of Reminders that deserve a more thorough discussion.

Share a Reminder List

You can share a reminder list in much the same way as a calendar, but only privately. A great use for shared reminder lists is family shopping lists. My wife and I share a shopping list so if either of us is at the store,

we can see what's needed and mark off items as we pick them up. And since it would be rare for either of us to be out of reach of a Mac, iOS/iPadOS device, or Apple Watch, we can easily add things to the list wherever we may be.

Note: If you enable Family Sharing, you get a shared reminder list called Family automatically. You can use this for any purpose you like, or ignore it. See Use iCloud Family Sharing.

To share a reminder list:

- **In the Mac Reminders app or on the web:** Hover to the right of a reminder list name to display the Share icon; then, click that icon. Enter the name or email address of the person with whom you want to share and press Return to confirm; repeat if needed to add more people. Then click Done. iCloud notifies the other person, and the shared list appears in their Reminders apps.
- **In the Reminders app in iOS/iPadOS:** Open the list in Reminders. Then tap the Share icon, tap an app name, fill in the email addresses or phone numbers of the people you want to share the list with, and send it.

iCloud notifies the other people, and the shared list appears in their Reminders apps.

Use Location-Based Reminders

Reminders can alert you when you leave or arrive at a location. For example, you could ask to be reminded to pick up milk only when you walk by the grocery store, or have a reminder to set out the trash that appears when you get home.

Location-based reminders require a Mac, an iPhone, or an iPad with a cellular radio (and an active data plan). The device must have Location Services enabled, too; if it's not, the first time you set up a location-based reminder, you'll be prompted to turn it on (or to approve Reminders, if Location Services is already on but Reminders isn't yet approved).

To add a location to a reminder, select it and click or tap its Info icon (**Figure 34**). Then select At a Location (Mac) or Remind Me at a Location (iOS/iPadOS). Enter the address you want to trigger the reminder, type in a contact's name to use the contact's address, or choose Current Location from the pop-up menu. Then select whether you want to receive the alert when Arriving or Leaving and click or tap Done.

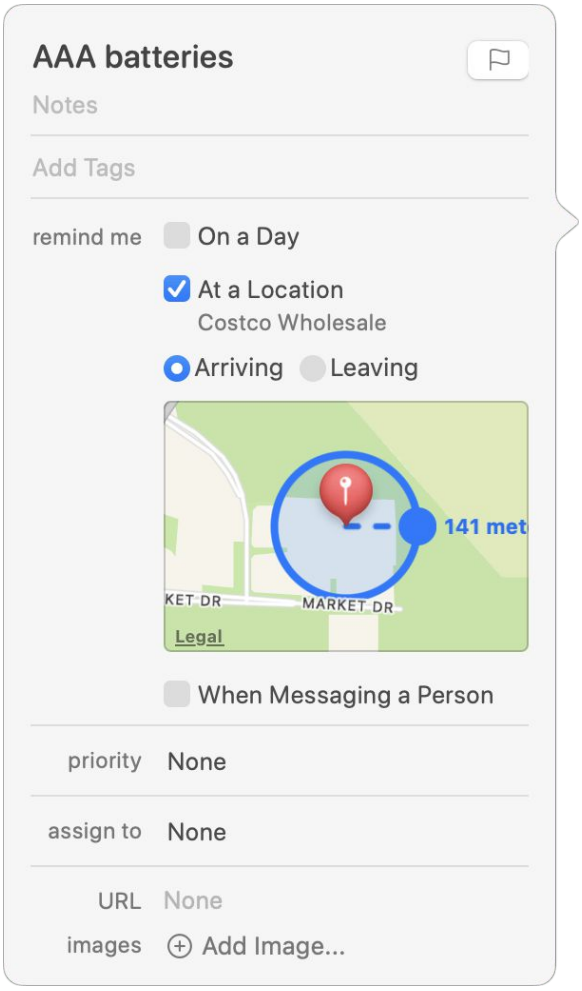


Figure 34: Set up a location-based reminder in Reminders on a Mac.

Tip: You can also use Siri to create a reminder like this. For example: "Siri, remind me to take out the trash when I get home."

When you arrive at or leave the location specified, your device should alert you with the text of this reminder. However, bear in mind that network conditions and other variables may prevent location-based alerts from appearing at precisely the right place.

Note: For more on location-based reminders, see *Take Control of Calendar and Reminders*.

Work with Notes

If you need to store lists, text snippets, or other notes, and sync them between your devices, Notes gives you an easy way to do so. For the most part, you simply type or paste whatever you want into the Notes app on a Mac, iOS or iPadOS device, or the iCloud website, and your notes sync automatically among all these devices.

Tip: To learn all about the hidden power of Notes, read *Take Control of Notes* by Josh Centers.

Notes was once a pretty boring app. But over the past few years, Apple has enhanced the Notes app on all platforms with more capabilities. Here are some of the many things you can do with Notes:

- Enter plain or styled text, which can now include headings; bulleted, dashed, and numbered lists; checklists; tables; a limited selection of paragraph styles; various levels of indentation; and bold, italic, or underline. In the Mac version of Notes, you can also change attributes such as font and color. The Notes web app offers more limited formatting options, but it does display attributes you added or changed on a Mac or iOS/iPadOS device.
- Attach files, such as photos, movies, sounds, and PDFs.
- Include URLs (such as those shared from a browser).
- On an iOS or iPadOS device, draw a sketch with your finger or a stylus in a note. (You can even use an iOS or iPadOS device to insert a sketch into a note on your Mac.) You can also use an iOS or iPadOS device's built-in camera to "scan" a document; Notes helpfully crops and deskews it for you.
- Intersperse sketches and typing in the same note.

- Search for text that you wrote when sketching—pull down on the Notes list to see the Search field.
- Use the Share menu in supported Mac apps, or the share sheet in supported iOS/iPadOS apps, to send data directly to Notes, such as text, webpages, videos, and photos, as well as maps and routes from the Maps app.
- On an iOS or iPadOS device, record your voice using the Voice Memos app and then tap the Share icon to send the clip to Notes.
- Let other people collaborate in editing a note by clicking or tapping the Add People button.
- Set a password and you can lock individual notes (click the Lock button). This feature is an oddball: it's not automatically linked to Touch ID or Face ID; if you forget or lose the password, any note locked with it is irretrievable forever. You can reset the password, but old notes remain locked with the old passwords and subsequent notes with the new one.
- Use the Instant Notes feature to start a note by tapping your iPad's Lock screen with your Apple Pencil or by tapping the Notes button in Control Center. (To add the Notes button to Control Center, go to Settings > Control Center.) You can customize how this feature works in Settings > Notes > Access Notes from Lock Screen.

Note: Notes don't sync with any desktop app in Windows, so the only way to access your notes in Windows is on the iCloud website.

Sync Data from Other Apps

iCloud optionally syncs data from Health and Siri plus the several other built-in apps:

- **Health:** The iOS Health app, which appears only on iPhones, can use iCloud to save its data to Apple's servers and also sync it to other iPhones. This isn't terribly useful for most people—it would be

quite nice if you could view that data on the web or on your Mac, for instance—but if you want to sync the data, just go to Settings > *Account Name* > iCloud on your iPhone and turn on Health.

Tip: Health does let you export—but not sync—your recorded data in an XML format, which third-party apps can import and analyze.

- **Siri:** Macs and iOS/iPadOS devices can sync Siri data too. As you use Siri, it learns about you—your data, your preferences, and your behavior—in order to customize its responses and make them more useful. Previously, this information was confined to each individual device: Siri on your Mac couldn't benefit from what Siri on your iPhone knew and so on. But, if you like, you can use iCloud to sync Siri data across all your devices, so that what it learns in one place is useful everywhere. To enable this feature on a Mac, go to System Settings > *Account Name* > iCloud (Ventura or later) or System Preferences > Apple ID > iCloud (Monterey or earlier) and enable Siri. On an iOS/iPadOS device, go to Settings > *Account Name* > iCloud and turn on Siri.
- **Other built-in apps:** iCloud can sync data from several additional built-in Apple apps across your devices: Freeform, Game Center, Home, News, Stocks, Voice Memos, and Wallet. Most of these have their own switches or checkboxes in the main part of the iCloud pane. Voice Memos appears only after you record your first one. After that, you can enable or disable syncing by going to back to the iCloud settings, clicking the Options button for iCloud Drive, and checking or unchecking Voice Memos.

Use Universal Clipboard

Universal Clipboard is a simple yet incredibly useful feature: anything you copy or cut to the clipboard on one device is immediately synced to the clipboard on your other nearby devices. You can copy text from your iPhone and paste it into an or app on your Mac, copy a photo from your iPad and paste it somewhere on your iPhone, and so on.

This capability works with pretty much any type of data that's supported on both devices.

Note: After a brief but unspecified period of time, Apple clears the copied data from your other devices' clipboards.

Universal Clipboard has no explicit user interface—that is, there's no switch to turn it on or off, no settings to adjust. It's enabled automatically as long as the devices you're using for copying and pasting have the following attributes:

- For a Mac, its model must have been introduced in 2012 or later (or, in the case of the Mac Pro, 2013 or later).
- They are all running 10.12 Sierra or later, iOS 10 or later, or iPadOS 13 or later.
- They are on the same Wi-Fi network.
- They have Bluetooth enabled and are within Bluetooth range of each other (roughly speaking, in the same room).
- They are signed in to the same iCloud account, and that account is the primary iCloud account on each device.
- They have Handoff enabled. In Ventura or later, go to System Settings > AirDrop & Handoff; in Monterey or earlier, go to System Preferences > General on a Mac; or in iOS/iPadOS, go to Settings > General > AirPlay & Handoff.

Work with iCloud Keychain

iCloud Keychain allows you to sync a *keychain* containing passwords, credit card numbers, and other sensitive data across your Apple devices securely via the cloud. This lets Safari autofill usernames and passwords on any of your devices no matter which device you initially created the login with. It also syncs Wi-Fi passwords among all your devices, avoiding the need to reenter them.

Apple's keychain lets you do the following on any single device:

- Store and enter credit card information in web forms.
- Create multiple sets of credentials per site and credentials that can be used across subdomains of the same site.
- View and remove passwords within Safari for macOS, System Settings/System Preferences on a Mac, and the Settings app for iOS/iPadOS.
- Enable and use one-time codes that are used for second-factor authentication and have them available from all your devices.
- Create private notes you add to password entries.

Note: Apple also offers to generate strong passwords within Safari.

That's great, but you don't want to re-enter information and keep it up to date across your equipment. When iCloud Keychain is enabled, that information is synced across your devices and available within Safari and other locations. iCloud keychain can also sync the history of your iMessage and SMS communications (see Sync Messages).

In addition, the following items sync automatically amongst your other Macs (but not, alas, iOS or iPadOS devices):

- Settings for the accounts listed in the Internet Accounts pane of System Settings/System Preferences, such as email accounts

- Signatures you scanned or wrote in Preview (see *Take Control of Preview*, by Josh Centers and Adam Engst), or using the Markup feature of Mail
- Entries in the default macOS login keychain—viewable via the Keychain Manager app—that can be used across Macs but aren't relevant to iPhones or iPads

iCloud Keychain offers great utility to those who use Apple devices exclusively, and who use only Safari in macOS—you can't access iCloud Keychain entries in other browsers in macOS. However, iCloud Keychain entries can also be accessed from several places across apps and operating systems:

- Apple and third-party apps on a Mac and iOS/iPadOS devices
- Settings > Passwords in iOS/iPadOS
- System Settings/System Preferences > Passwords in Monterey or later
- iCloud Passwords in Windows
- Cloud extension for Edge or Google Chrome in Windows (even though you can't do this with Edge or Chrome in macOS)

Go Beyond iCloud Keychain Features

Some third-party password managers, including my favorite, 1Password, offer additional features such as greater flexibility in password creation; rich support for web browsers other than Safari on a Mac and support for Android, Linux, and Windows; password vaults you can share with family members or within a company; and storage of other types of information, like bank accounts, Social Security numbers, and software licenses.

If you're interested in using 1Password instead of, or in addition to, iCloud Keychain, start with Use iCloud Keychain with Another Password Manager, at the end of this chapter. To look more deeply at 1Password, you might enjoy reading my book *Take Control of 1Password*. For a thorough introduction to password security, read *Take Control of Your Passwords*.

Enable and Configure iCloud Keychain

iCloud Keychain isn't very useful if you set it up on only one device; since syncing passwords is the main point of the features, you'll want to enable it on each of your Macs and iOS/iPadOS devices.

Set Up iCloud Keychain if Two-Factor Authentication Is On

If you have already turned on two-factor authentication for your Apple ID (see Enable Two-Factor Authentication)—as most people likely have, by this point—setting up iCloud Keychain is simple. You simply enable it on each device.

> **Tip:** If you haven't turned on two-factor authentication, now is a great time to do so. It'll increase your security and save you many steps in setting up iCloud Keychain!

On a Mac running Ventura or later, go to System Settings > *Account Name* > iCloud and turn on Password & Keychain. In Monterey or earlier, go to System Preferences > Apple ID > iCloud and select iCloud Keychain. In iOS/iPadOS, go to Settings > *Account Name* > iCloud > Passwords & Keychain and turn on Sync this iPhone or Sync this iPad.

You may be prompted to enter a previously created iCloud Security Code or the passcode for another device that's already using iCloud Keychain.

That's it! You can now skip ahead to Use iCloud Keychain in Safari.

Only You Have Access to iCloud Keychain's Contents

Apple has zero knowledge of the encryption keys used to secure your iCloud Keychain. Those keys are created and reside only on each of your devices, and are protected by the password/passcode of one of your devices when two-factor authentication is turned on and by an iCloud Security Code when it's not. Apple can't retrieve them or decrypt your keychain's entries.

Thus, Apple asks for a secret only you know when setting up iCloud Keychain, because they need *you* to prove you know that secret in order to enable sync.

Set Up iCloud Keychain if Two-Factor Authentication Is Off

If you have *not* enabled two-factor authentication, you can't simply flip a switch and turn iCloud Keychain on. The initial setup process is considerably more involved. In addition, the steps you follow with whichever device you set up first will be different from the steps for setting up all subsequent devices.

If you've already set up at least one device to use iCloud Keychain, skip ahead to Approve Additional Devices; if all your devices are already set up, move right on to Use iCloud Keychain in Safari. Otherwise, keep reading.

Set Up iCloud Keychain on Your First Device

When you set up your first device to use iCloud Keychain, you may also be prompted to perform a one-time procedure to choose a security code, which can be used to approve additional devices. (There are other ways to approve additional devices, too, as we'll see.)

I suggest setting up a Mac before an iOS or iPadOS device. I say this because when you first set up iCloud Keychain, it copies most of the contents of your existing login keychain to the new iCloud keychain. Because your Mac almost certainly has more items in its login keychain than your iOS or iPadOS device does, your new iCloud keychain will be more useful, more quickly.

Note: You may be prompted to set up iCloud Keychain while installing macOS, but if not, you can set it up afterward. The instructions here are for an after-the-fact setup, although the steps to configure iCloud Keychain during installation are similar enough that you should be able to follow along.

Set up iCloud Keychain on a Mac

To set up iCloud Keychain for the first time on a Mac, follow these steps:

1. *Optional but recommended:* Go to System Settings > Lock Screen or System Preferences > Security & Privacy > General. In Ventura or later, make sure "Require password after screen saver begins or display is turned off" is set to something other than Never; in Monterey or earlier, make sure the first checkbox (Require Password ____ after Sleep or Screen Saver Begins) is selected, and choose a time period from the pop-up menu to fill in the blank. You can skip this step, but if you do, the Apple ID pane will complain about it later—and for good reason, because if your Mac is unlocked, someone else can access all your iCloud Keychain passwords.

2. Go to System Settings > *Account Name* > iCloud (Ventura or later) or System Preferences > Apple ID > iCloud (Monterey or earlier). If you haven't previously signed in to your iCloud account, do so now.

3. Turn on Passwords & Keychain (Ventura or later) or select the Keychain checkbox (Monterey or earlier).

4. When prompted, enter your Apple ID password and click OK.

5. Since this is the first of your devices on which you're setting up iCloud Keychain, you may be prompted to create an iCloud Security Code, which you can use later, with your password, to set up other devices.

   You can either enter a 6-digit numeric code or, for greater security, click Advanced and select one of the following:

- *Use a Complex Security Code:* Enter a random password, a phrase, or another arbitrary code that you devise yourself or with the help of a third-party password generator.
- *Get a Random Security Code:* Have Apple generate a long, random string for you, in the format `XXXX-XXXX-XXXX-XXXX-XXXX-XXXX`, where each `X` is a digit or uppercase letter.
- *Don't Create Security Code:* Skip this step, with the consequence that when you set up iCloud Keychain on another device, you'll have to approve it from a different device. (For example, you can use Mac A to approve a request from Mac B, as long as both are signed in to your iCloud account.) See the Note just ahead for more details.

After entering the code in whichever form or opting out, click Next. Re-enter your code if prompted and click Next again. Then, assuming that you didn't skip setting up an iCloud Security Code, enter a mobile phone number, which can be used as a secondary means of verifying your identity via an SMS message, and click Done.

Omit a Security Code and Risk Hijacking

Skipping the iCloud Security Code lets you sync keychains among devices *without* storing them on Apple's servers; it also avoids the need to enter an SMS number, which can be risky, given how readily cellular numbers can be hijacked (or "SIM swapped"). However, it also means Apple will be unable to recover your iCloud Keychain if you forget your password, and you'll be out of luck if you lose access to all your approved devices. See the FAQ on this page for details.

macOS copies most of the items from your login keychain (Wi-Fi network passwords, application passwords, internet passwords, and web form passwords) to a new keychain called iCloud, and that's what syncs. You can edit this keychain using either Keychain Access (found in `/Applications/Utilities`) or Safari (choose Safari > Settings/Preferences > Passwords). However, bear in mind that it's a separate entity from your login keychain: changes in one keychain won't affect the other.

Set up iCloud Keychain on an iOS or iPadOS Device

If the first device you set up for iCloud Keychain runs iOS or iPadOS, follow these steps:

1. In iOS/iPadOS, tap Settings > *Account Name* > iCloud > Passwords & Keychain and turn on Sync this iPhone or Sync this iPad.
2. When prompted, enter your Apple ID password and tap OK.
3. Follow the prompts (similar to those from step 5 in the instructions for setting up a Mac, just previously) to pick an iCloud Security Code—or skip it, if you prefer.

Your iOS or iPadOS device creates a new keychain called iCloud, containing any keychain information (such as Wi-Fi passwords or passwords saved from Safari) that were stored on the device. (You can't directly interact with that keychain on your iOS or iPadOS device, but it'll appear in Keychain Access on a Mac synced via iCloud.)

Approve Additional Devices

After you've set up your first device, and optionally set up an iCloud Security Code, you can add your remaining devices. Begin by enabling Passwords & Keychain (or Keychain) in System Settings/System Preferences or Settings, just as you did when you set up your first device.

> **Note:** As a reminder, if you Enable Two-Factor Authentication, you don't have to jump through any extra hoops: just check the box or flip the switch to enable iCloud Keychain on your other devices.

If you don't use two-factor authentication, you must now *approve* each additional device in one of two ways:

- **Use Your iCloud Security Code:** If you choose this option (phrased as "Use Code" in iOS/iPadOS), you'll be prompted to enter your iCloud Security Code—and, in some cases, a verification number sent to your mobile phone via SMS.
- **Approve from Other Device:** If you choose this option (phrased as "Request Approval" in iOS/iPadOS), iCloud sends a request to all your other devices using iCloud Keychain with the same Apple ID.

On each of those devices, a notification (**Figure 35**) appears; follow the prompts to approve the request.

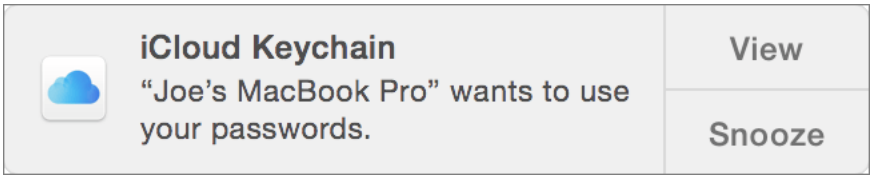


Figure 35: Your Mac notifies you that another of your devices wants to access your iCloud Keychain.

Then, and only then, will your iCloud Keychain begin syncing.

Note: If you use the Quick Start feature in iOS or iPadOS to set up a new device automatically based on settings of an existing device, that setup will include transferring your iCloud Keychain data.

Use iCloud Keychain in Safari

Safari makes best use of iCloud Keychain across macOS, iOS, and iPadOS, and it’s the place you’re likely to use it most. It works quite similarly in each operating system, too.

Note: Windows can use iCloud Keychain in a browser, too: with Apple’s iCloud software installed, you can enable an extension for Microsoft’s Edge browser or Google Chrome. See Set Up iCloud for Windows.

Enable iCloud Keychain Features in Safari

Make sure Safari is set up to use all of iCloud Keychain’s features:

- **Mac:** Go to Safari > Settings/Preferences > AutoFill and make sure the checkboxes are selected for each type of data you want to autofill—the two options relevant to iCloud Keychain are “User names and passwords” and “Credit cards.” Then click Passwords at the top and, if the screen says “Passwords are locked,” fill in the password for your macOS user account and press Return.

- **iOS/iPadOS:** First tap Settings > Passwords > Password Options, and make sure AutoFill Passwords is turned on and iCloud Passwords & Keychain is selected. Then go to Settings > Safari > AutoFill, and turn on the Credit Cards switch.

Autofill Secrets

Apple provides support for two intertwined account validation secrets: passwords and verification codes. Nearly all sites require passwords for login; an increasing number allow or require a verification code.

Note: One trend I've seen is sites that avoid a password as the method proffered for logging in. Instead, they suggest you enter your email address and click to "send a magic link." This link arrives via email if your account is in their records, and you click to log in. It validates your email and access to email on each login.

Autofill Passwords

After you load a login page for which you've already stored credentials in your iCloud Keychain, click or tap in the Username or Password field and then:

- Click the credentials you want to use on the pop-up menu that appears (Mac)
- Tap the credentials you want to use on the QuickType bar (iOS/iPadOS)

Tip: You can also opt on a Mac to choose Edit > AutoFill Form or press ⌘-Shift-A (Mac).

Safari fills in the username and password fields for you—all you need to do then is click or tap the Log In (or equivalent) button.

Tip: Sometimes Safari doesn't recognize that a password is required when you tap in a username field; or a website has you enter a username or email address, tap a button, and then enter the password. In those cases, you may only be able to get the autofill option to appear when you tap in the password field.

On a Mac, if you've stored more than one set of credentials for a site—for example, if you have two different accounts for Microsoft or Google—first delete the credentials Safari has autofilled, if any. You can then click in the username field to display a pop-up menu (**Figure 36**). If the login shown is not the one you want to use, click "Other Passwords for *URL*" and then choose the one you want to fill in your credentials.

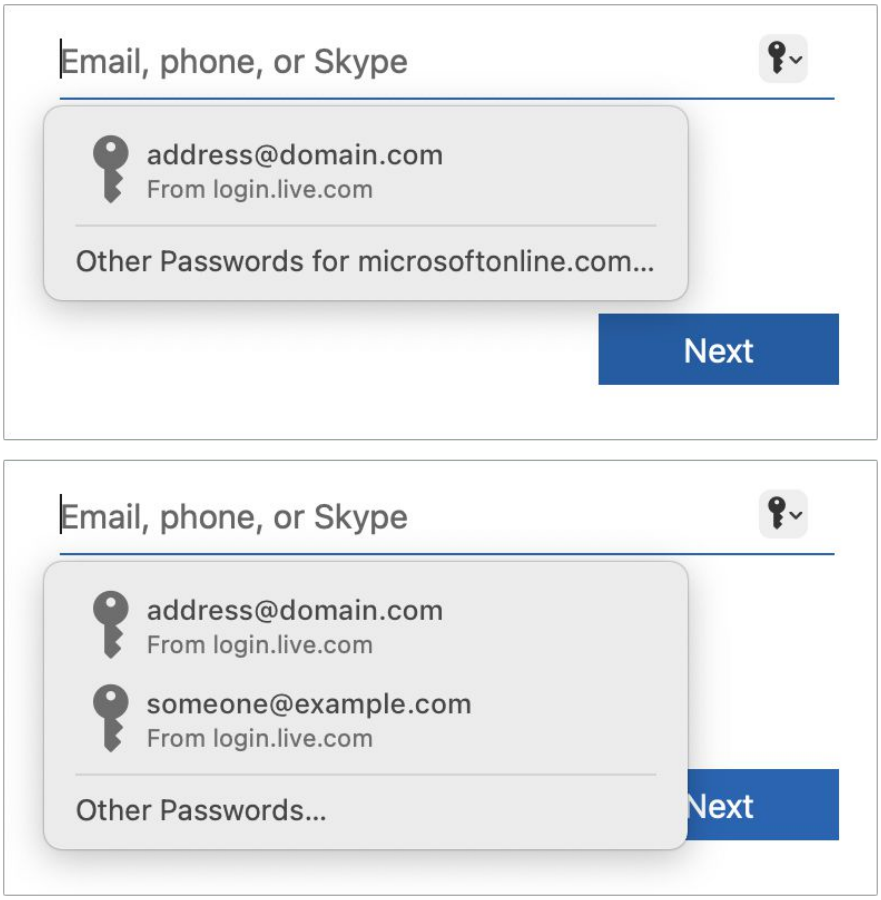


Figure 36: If you have multiple credentials for a site, click or tap in the username field, then click the "Other Passwords for…" option to display other matches.

On an iOS or iPadOS device, websites for which you have multiple sets of credentials show a single option by default, or two options on the QuickType bar (**Figure 37**) if it's visible; tap one of these to fill in both the username and password fields. To use a different set of credentials, tap the key icon or the word Passwords to display a popover with all available credentials for that site.

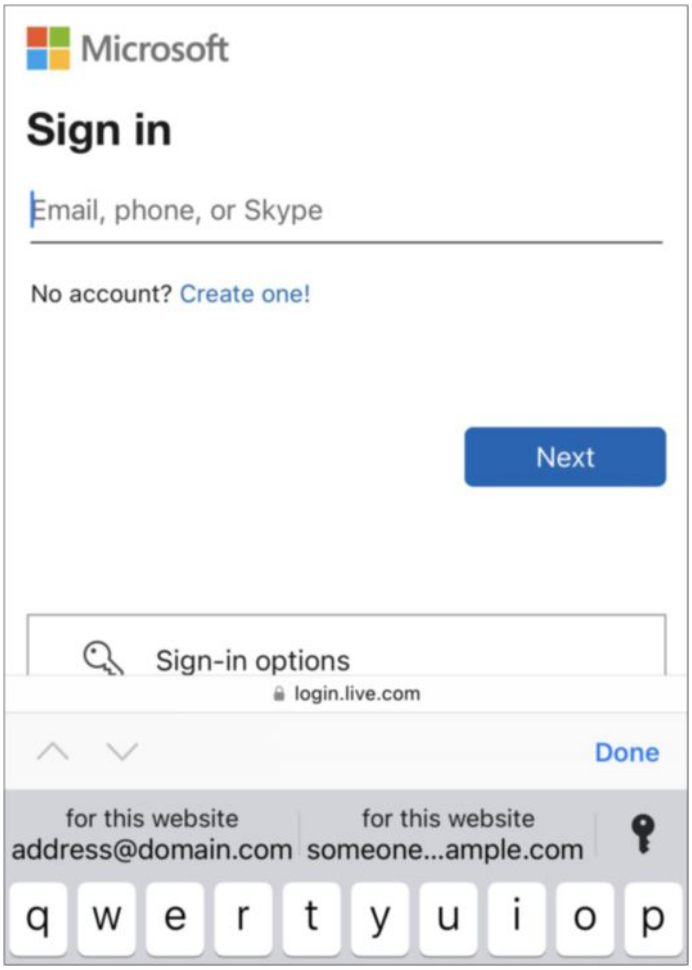


Figure 37: Safari for iOS/iPadOS shows multiple password options when you have at least two sets of credentials for a particular site.

If Safari autofills a set of credentials and it's not what you want, delete them and try clicking or tapping the username field again. If they still don't appear (for example, because the domain names don't match exactly), do the following:

- **Mac:** Click Other Passwords. Locate the account you want (manually or using the Search field). Select it and click Fill.
- **iOS/iPadOS:** Tap the key icon or the word Passwords and type your passcode or use Touch ID or Face ID when prompted, then locate the account you want (manually or using the Search field) and tap it.

Some websites deliberately block browsers and password managers from saving passwords you enter there, in a misguided attempt at greater security. Safari can either accept or attempt to bypass any site's restrictions, but unfortunately, you can't control that behavior.

Tip: Starting in iOS 17/iPadOS 17 and Safari 17 for macOS 12 Monterey and later, if you tap or Control-click/right-click in a field, an Autofill option appears that lets you navigate to fill in passwords and verification codes (described next).

Autofill Verification Codes

Starting in iOS/iPadOS 15 and Safari 15 for macOS 10.15 Catalina and later, Apple also lets you work with a popular second-factor element for account verification. A standard algorithm takes a seed offered up when you enroll your account at a website or in an app for second-factor authentication and generates a unique time-based code that only a device possessing the secret seed could provide.

Glenn Fleishman explains the process of setting up these codes (for iOS, iPadOS, and macOS) in the TidBITS article Add Two-Factor Codes to Password Entries in iOS 15, iPadOS 15, and Safari 15.

To use verification codes as part of logging in, after providing your user name and password, tap a field or click in a field that prompts for the code. Safari automatically generates a code tied to the website's address and lets you fill it in as Safari does for passwords.

If a code prompt doesn't appear in macOS or as a QuickType bar entry in iOS/iPadOS, you can use the same tools above to search for the iCloud Keychain entry and copy the code from that entry to paste into a webpage form field.

Store New Passwords

If you arrive at a login page for which iCloud Keychain does not yet contain your credentials, enter them (or fill them in with your third-party password manager) and log in. Safari should then display a prompt asking if you want to save the password in your iCloud Keychain. Click or tap Save Password to store your credentials for that site.

Note: Again, if a site offers two-step verification via one-time codes, see this article for instructions on setting that up.

If you already have credentials stored for the site and you want to store an additional username/password combination, first delete the credentials Safari has autofilled. Then enter the new credentials, log in, and click or tap Save Password when prompted.

Generate a Random Password

When you're asked to register on a website and create a new password, iCloud Keychain can generate one for you and store it automatically. Follow these steps:

1. Make sure the Password field is completely empty.
2. Click or tap in the field. The next steps vary by platform.

   On a Mac:

   a. If a suggested password isn't automatically filled in—usually, it will be—click the key icon and choose Suggest New Password from the pop-up menu.

   b. Safari fills in a suggested password (highlighted in yellow), but displays only the first few characters, along with the label "Strong Password." A popover with additional details may appear on its own; if not, click the field to display it (**Figure 38**). (The same password appears in a "verify" or "enter your password again" field, if the website offers one.)

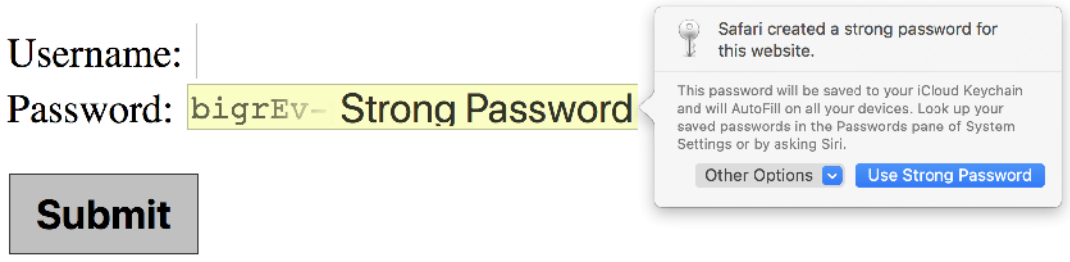


Figure 38: Click a suggested password to see this popover.

   c. To use Safari's suggested password (without even seeing the whole thing), click Use Strong Password. To use an alternative password without special characters, choose No Special Charac-

ters from the Other Options pop-up menu. Or, to fill in your own password instead (perhaps using a third-party password generator), choose Choose My Own Password from the Other Options pop-up menu.

On an iOS or iPadOS device:

a. If a suggested password isn't automatically filled in—usually, it will be—tap the key icon or the word Passwords, and then tap Suggest New Password.

b. Safari displays a suggested password in a popover. To use it, tap Use Suggested Password. Safari also puts that password in a second verification field—to confirm you "typed" it accurately—if a website requires it. To use an alternative password without special characters, tap Other Options followed by No Special Characters. Or, to fill in your own password instead, tap Other Options followed by Choose My Own Password.

3. Fill in any remaining fields (such as Username) and submit the form.

When you submit the form, Safari saves your credentials for the site without any additional steps.

Note: Some sites reject the high-strength passwords that Apple's algorithm generates because those sites insist on ridiculous formulas for passwords that, conversely, make it more likely someone picks a less-secure password out of frustration.

Store and Enter Credit Card Numbers

Credit cards work much like passwords: if you type or paste a credit card number and its expiration date into form fields and submit the form, Safari prompts you to save the credit card number in your iCloud Keychain.

When it's time to fill in a stored credit card number, click or tap in the Credit Card Number field and choose the desired credit card from the pop-up menu or from the QuickType bar in iOS/iPadOS. If you have more than one credit card stored, Safari displays a pop-up menu from

which you can choose the one you want to use, just as when filling in your username and password on a site for which you have multiple sets of credentials.

About Card Verification Numbers or CVVs

Your physical and virtual credit or debit cards each have a numeric code called a CVV (card verification value). On a physical card, it's a three-digit number on its back for Discover, MasterCard, and Visa; it's a four-digit code printed on the front for American Express. (Some card issuers refer to it as a CVC or card verification code.) When making a purchase online, you nearly always have to enter this code along with the card number and expiration date. It's considered a physical verification step. But, for a long time, Safari couldn't fill in these codes automatically, even as many third-party password managers could.

This changed with the release of Big Sur and iOS 14/iPadOS 14, but neither editor Glenn Fleishman nor I noticed it at the time. Now, Safari (for macOS, iOS, or iPadOS) *can* fill in the CVV, as long as you've recorded it. You may have filled it in when you added a card to Apple Pay (in System Settings/System Preferences > Wallet & Apple Pay). For cards not in Apple Pay, you can add the CVV by going to Safari > Settings/Preferences > AutoFill, clicking Edit next to "Credit cards," selecting a card, and filling in the Security Code field.

Use iCloud Keychain in Other Mac Browsers

When you use Safari's built-in features to remember the usernames and passwords you enter on a website, those credentials are stored in your keychain. Later, if you visit the same site, Safari can autofill those credentials by retrieving that information from your keychain. And, ever since OS X 10.9 Mavericks, iCloud Keychain has been able to sync all those credentials across your Apple devices, so you can, for example, open Safari on your iPhone and log in to a site whose password was saved on your Mac.

Note: This text in this section was adapted from my book *Take Control of Sonoma*.

However, before Sonoma, access to the keychain on your Mac was restricted to Safari. You could use password management tools built into other browsers, but those passwords would remain completely separate from the ones in your keychain. Or, you could use a third-party password manager such as 1Password, which is compatible with nearly every browser on nearly every platform and syncs its data across devices. But no other app could read from or write to your keychain.

Sonoma changed that by allowing third-party browsers access to your keychain—but with a significant list of qualifications.

Note: You can also use iCloud Keychain in Chrome or Edge for Windows; refer to Set Up iCloud for Windows and Use iCloud Keychain in Windows.

Use Passwords from Your Keychain

macOS uses different methods to support *passwords* and *passkeys* from your keychain in other browsers. Let's talk about passwords first.

To enable another browser to access passwords in your keychain, the first thing you need is the free iCloud Passwords extension, available at present only for Google Chrome and other browsers that using the Chromium engine (such as Microsoft Edge, Brave, and Vivaldi). As of publication time, there's no Firefox extension, and Apple hasn't announced whether one is planned. I've seen some third-party attempts to make a Firefox extension, but they don't seem fully baked.

After you install and activate the extension in your other browser(s), follow these steps:

1. Look for a (dimmed, locked) iCloud Passwords icon on your toolbar. If you don't see it—which is likely because most browsers hide extension icons by default—figure out how to display it on your toolbar, because you'll need to click it frequently. Each browser has its own way of doing this. In Chrome, for example, click the Exten-

sions icon on the toolbar to display a pop-up list of extensions, and then click the gray pin icon next to iCloud Passwords. The pin turns blue and the extension's icon then appears on your toolbar.

2. Optional but recommended: turn off any other password-filling features in that browser, whether built in or supplied by a third-party password manager, because having multiple apps trying to fill in the same set of credentials at once can cause confusing, overlapping pop-ups.

3. You must explicitly enable password autofill. To do this, click the iCloud Passwords icon. You'll see two pop-up windows, the locations and appearance of which may vary between browsers. One, created by the extension, asks for a six-digit verification code; the other, prompted by macOS, supplies that code (**Figure 39**). Type the code into the field.

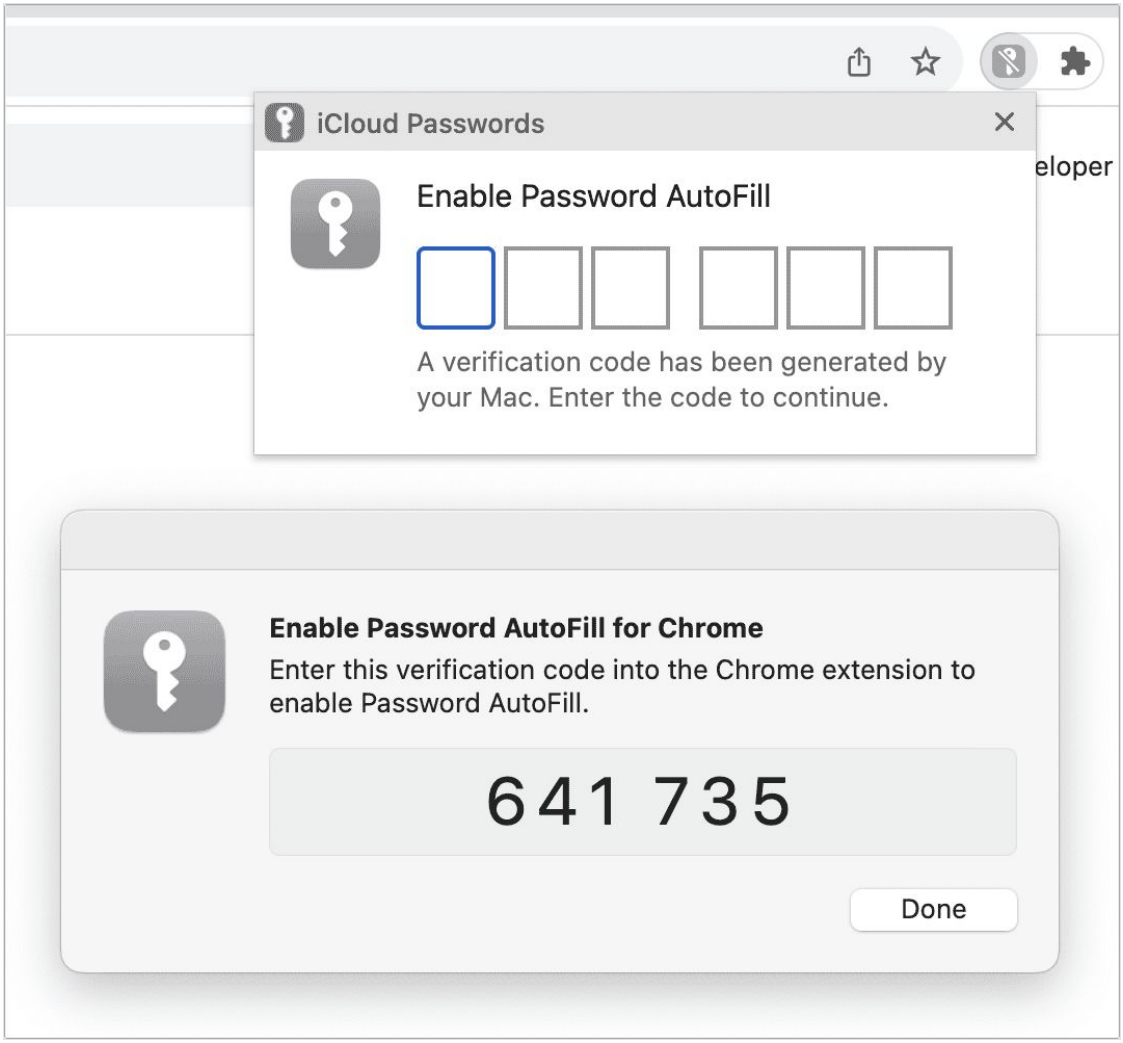


Figure 39: You must enter a verification code into your browser to use the iCloud Passwords extension.

Note: You must repeat this process every single time you quit and reopen your third-party browser. Every. Single. Time.

4. Navigate to the login page of a website for which you have a password stored in your keychain. Click in the username or password field. A pop-up menu (**Figure 40**) shows any matching credentials from your keychain plus a Manage Passwords command, which takes you to System Settings > Passwords. If you have more than one account, there may be multiple entries. Click the credentials you want to use.

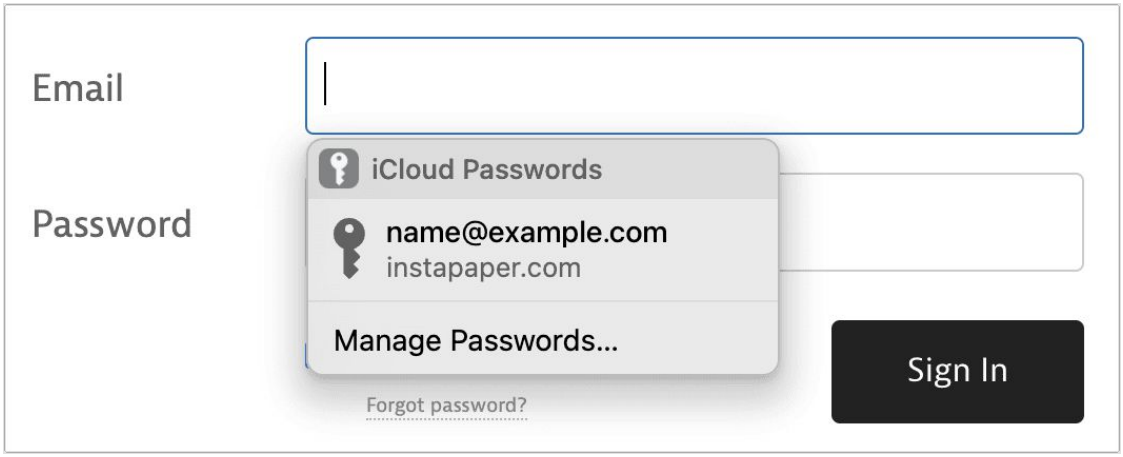


Figure 40: Use this pop-up menu to enter your credentials.

Note: If you skipped step 3 earlier, an Enable Password AutoFill alert appears here. Follow the prompts and then try logging in again.

5. An alert appears asking you to unlock your passwords (**Figure 41**). Depending on your Mac and its configuration, you can do this with Touch ID, double-pressing the side button on your Apple Watch, or entering your Mac's login password.

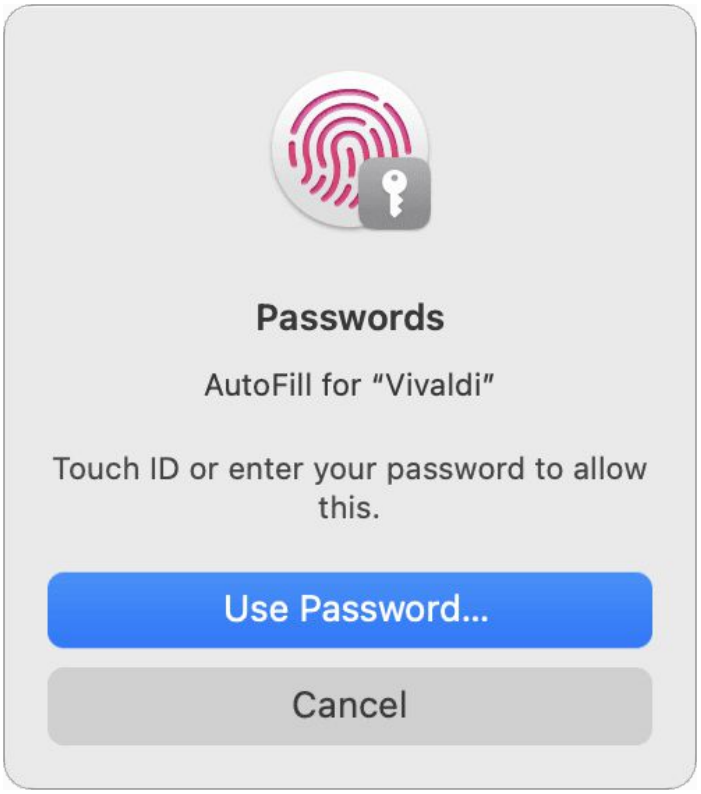


Figure 41: Authorize your browser to access your passwords.

Now, at long last, iCloud Passwords fills in your password!

Is it just me, or does that sound like a rather exhausting, roundabout procedure compared to how Safari handles AutoFill and how most third-party password managers work? It's almost as if Apple is trying to convince you that you should just use Safari after all!

iCloud Passwords does have a few other cross-browser capabilities beyond filling credentials, which I'll list here but not describe in detail:

- It can store newly entered usernames and passwords.
- It can enter one-time verification codes you've previously set up in Safari.
- It can enroll in a site's verification code system. To do this, navigate to the page where the site displays a QR code for two-step verification. Right-click (or Control-click) that code, choose Set Up Verification Code from the contextual menu, and follow the prompts.

Given the awkwardness of iCloud Passwords as it currently exists, I think it's still better to use a third-party app to manage passwords. With an app such as 1Password, the user experience is much smoother, while platform and browser support is broader. Nevertheless, I'm glad Apple has finally admitted that Safari isn't the only browser people use, and has taken the first steps toward making keychain contents available outside the Apple ecosystem.

Use Passcodes from Your Keychain

Although the process for accessing passwords from your keychain in other browsers is pretty cumbersome, as I described above, it's much simpler to access passkeys, the simplified secure multi-factor login system Apple and Google support and Microsoft has committed to rolling out fully. (For more background on passkeys, see *Take Control of Your Passwords*.)

Suppose you visited a site in Safari and enrolled in passkey logins. As part of upgrading your account to use a passkey, Safari stores the necessary secure login information in your keychain. In Sonoma, it's now possible to use the very same passkey in another browser.

Crucially, unlike the situation with passwords, this capability does *not* depend on a browser extension. All you need is the right browser and configuration. However, as of January 2024, the only third-party browsers I've found that can use passkeys from my keychain are Brave and Google Chrome; other browsers (such as Vivaldi and Microsoft Edge) resorted to displaying a QR code for me to scan with my iPhone—it works, but it's awkward. This is likely to change.

To use a passkey from your keychain in another supported browser:

1. In that browser, go to a site that offers passkeys (for example, www.passkeys.io), and click the link or button to sign in with a passkey. If prompted to choose a source for the passkey, select iCloud Keychain.

2. The first time you use this feature in a given browser, an alert appears, prompting you to allow the browser to see the list of accounts with passkeys in your keychain (**Figure 42**). Click Allow.

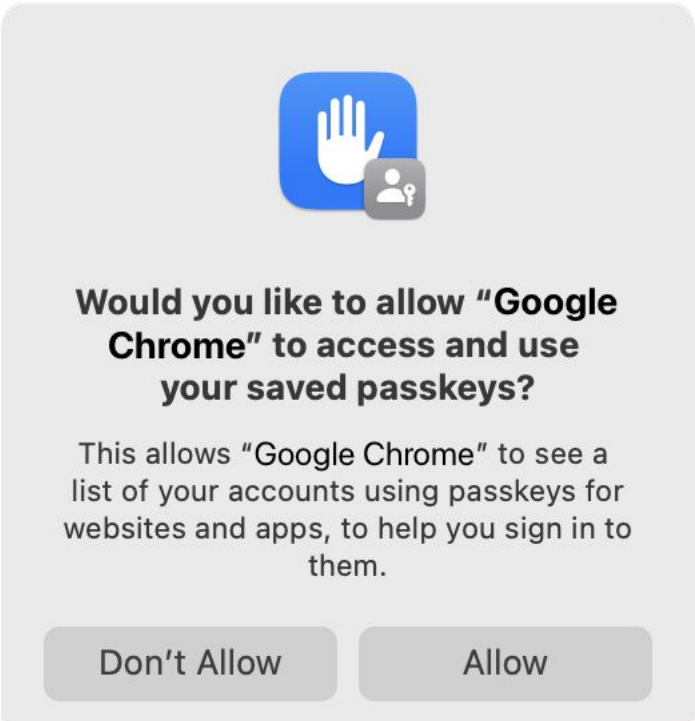


Figure 42: Click Allow to let your third-party browser see which accounts in your keychain have passkeys.

3. If Safari is not already configured to autofill passwords from your keychain, another alert appears (**Figure 43**). Click Open "Password

Options” or manually go to Settings > Passwords, sign in, and click Password Options. Then turn on AutoFill Passwords and Passkeys and make sure iCloud Keychain is turned on below it.

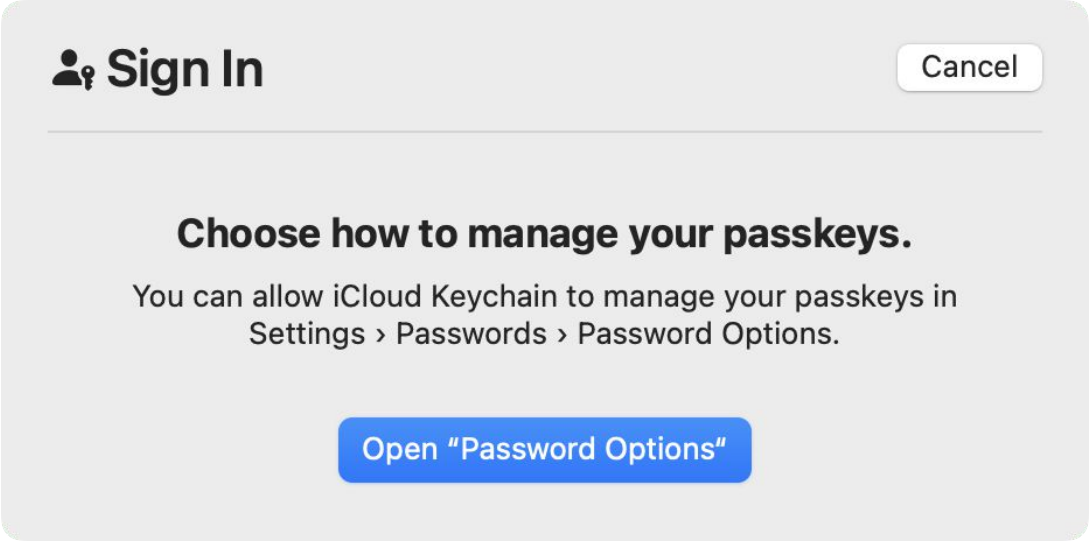


Figure 43: This alert prompts you to enable AutoFill.

4. When prompted, use Touch ID or your login password, as prompted, to sign in.

Use iCloud Keychain in Other iOS/iPadOS Apps

Third-party apps for iOS and iPadOS can also access items in your iCloud Keychain. To use this feature in an app, go to the app’s Sign In (or similar) screen. Tap in the username or password field. If iOS/iPadOS can identify which of the credentials in your keychain goes with the app in question, it displays them on the QuickType bar (**Figure 44**); tap your credentials to fill them in, and then tap Log In (or an equivalent button). If iOS/iPadOS can’t find your credentials, or if the ones it displays are the wrong ones, tap the key icon or the word Passwords, and then find and tap your credentials in the list that appears.

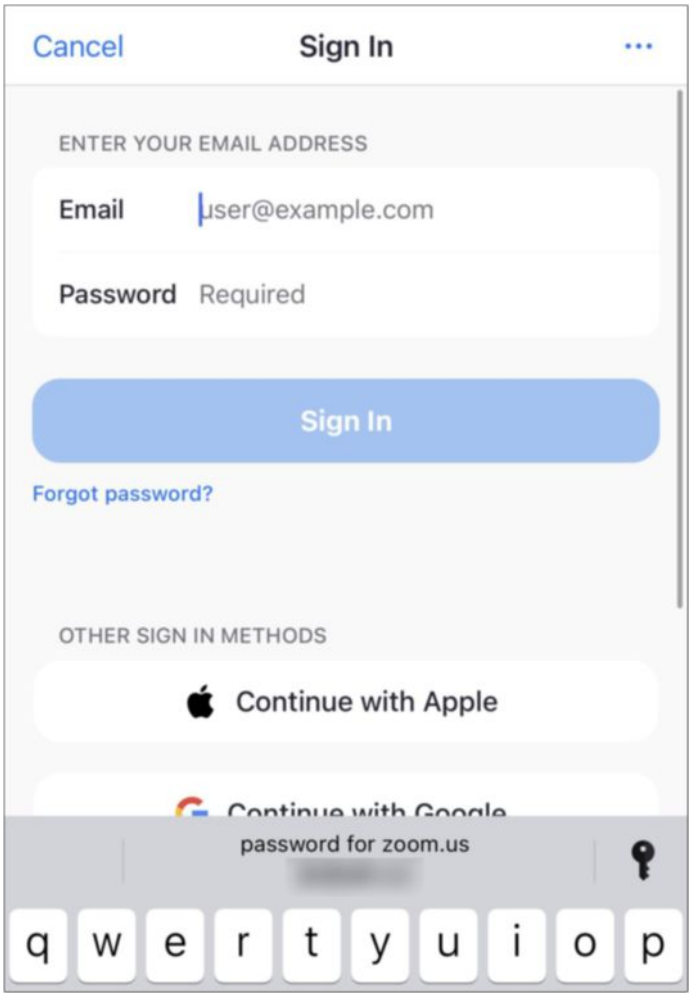


Figure 44: Tap a username on the QuickType bar to enter your credentials, or tap the key icon to choose different credentials.

Use iCloud Keychain in Windows

iCloud for Windows includes two methods for accessing and modifying iCloud Keychain entries: the standalone iCloud Passwords app and extensions for Microsoft Edge and Google Chrome. I explained the extensions earlier in Set Up iCloud for Windows.

The standalone app requires that you set up Windows Hello on your Windows machine. Windows Hello in turn requires a Trusted Platform Module, something akin to Apple's Secure Enclave. You can set up a PIN or biometric ID, but one or more of the three available methods must be enabled to use iCloud Passwords. See Microsoft's instructions to set up Windows Hello in Windows 11.

iCloud Passwords is similar to the Passwords view in Safari > Settings/Preferences in macOS, providing a searchable list of passwords, but omitting nearly everything else. In iCloud Passwords, you can select a password from the list and then click the copy icon to choose Copy User Name, Copy Password, or Copy Web Site (if any are associated with the entry).

In the upper-left corner, you can click the plus + icon to create a new password entry. With an entry select, you can click the edit icon to edit the stored information or generate a new password. When you save, the details are synced back to iCloud Keychain.

Warning! iCloud Passwords does not support verification codes. If you need a verification code for a log in, you will have to have access to another one of your devices that can generate it for you.

View and Edit iCloud Keychain Contents

To see what's in your iCloud Keychain without entering it in a form—or to edit or delete anything from your keychain, you have a few options:

- In Safari for Mac, choose Safari > Settings/Preferences and click Passwords. The same information is also available in Monterey or later via System Settings/System Preferences > Passwords. If prompted, authenticate with Touch ID (if available) or enter your user account password and press Return. You can then browse or search your web login items. Select an entry to see the password. To remove an item, select it and click Remove. To add a new item, click Add, fill in the fields, and press Return.
- In iOS or iPadOS, tap Settings > Passwords and enter your passcode (or use Touch ID or Face ID). For credit cards, tap Settings > Safari > AutoFill > Saved Credit Cards and then enter your passcode (or use Touch ID or Face ID). You can swipe left on a keychain entry to delete it.
- You can also view or edit your passwords in Keychain Access in macOS (found in `/Applications/Utilities`) by selecting iCloud in

the list of keychains in the upper-left corner of the window. (If you don't see the list of keychains, choose View > Show Keychains.) Keychain Access can also store and display secure notes in your iCloud Keychain, but those are visible only on a Mac, not on an iOS or iPadOS device. Unfortunately, Apple hasn't improved the awful interface that Keychain Access has had from day one, so I suggest avoiding it if you can.

Tip: Having trouble with iCloud Keychain? Check out these two Apple support articles: Set up iCloud Keychain and If iCloud Keychain won't turn on or sync.

Use iCloud Keychain with Another Password Manager

What if you already use 1Password, Dashlane, or another password manager? Does iCloud Keychain replace it?

In a word, no. iCloud Keychain is great for what it does—especially the way it handles Wi-Fi passwords so seamlessly—but third-party managers offer additional features.

For example:

- If you need to sync passwords with Windows, Android, or Linux, iCloud Keychain won't help you, but numerous third-party password managers can.
- Likewise, iCloud Keychain is currently unavailable in Mac browsers other than Safari, so unless or until such support exists, you'll need something else if you want to use a different browser.
- You can store your credit card's number, expiration date, and CVV (security code) in Safari for macOS (in Safari > Settings/Preferences > AutoFill > Credit Cards), and iCloud Keychain syncs that data among your devices.

Apple Pay, Safari-Stored Cards, and Safari Settings

Apple has a complicated relationship between Apple Pay and Safari. If you store a payment card in Safari, they don't also have to be available via Apple Pay. However, all credit and debit cards added via Apple Pay are always made available to Safari as well as an Apple Card if you have one. (See About Card Verification Numbers or CVVs earlier this chapter, too.)

Safari can either autofill card information from stored cards or, if you have the feature enabled on a Mac, use Apple Pay when you verify via Touch ID on a Mac or a nearby iPhone, iPad, or Watch that's logged in to the same Apple ID account. (You can disable Apple Pay in Safari in macOS at Safari > Preferences/Settings > Privacy by unchecking "Allow websites to check for Apple Pay and Apple Card." This used to be called Apple Pay in Safari; now it's labeled Apple Pay and Apple Card.)

When you use Apple Pay directly or via Safari in macOS, Apple generates a unique cryptographic transaction for the credit-card network. When you use Safari-stored cards that aren't set up in Apple Pay in macOS, iOS, or iPadOS, you're just allowing Safari to enter the information from your card automatically.

- Some password managers, such as 1Password, can store additional types of secure information, including software licenses and even arbitrary documents, in a safely encrypted form. If you need to store more types of information than iCloud Keychain can handle, another app may suit your needs better.
- iCloud Keychain offers no secure way to share specific passwords with other people, like coworkers or family members, while that's a feature of a number of third-party password managers.

It's possible in iOS, iPadOS, and macOS for third-party password managers to fill in your credentials in most of the same places that iCloud Keychain can. As a result, it's easy to rely on an app like 1Password or Dashlane (almost) exclusively.

It is nevertheless possible to have both iCloud Keychain and another password manager enabled at the same time. You should, however, be aware of a few issues:

- When credentials for a given site are stored both in iCloud Keychain and in another password manager, it's easy to get confused as to which tool you're using when filling forms, and you'll have to put up with extra visual clutter, too.
- Because Apple strictly limits access to Keychain data, there's no easy way to import existing keychain entries into a third-party password manager or vice versa.
- Although iCloud Keychain syncs among your devices—and another app may also sync its passwords among devices—iCloud Keychain won't sync with any third-party password managers. So, for example, if you change a password in 1Password, you'll have to change it again in iCloud Keychain.

Use the iCloud Website

iCloud is mostly about keeping data in sync across all your devices, but several key types of data can also be viewed and edited on the iCloud website in robust web apps—Mail, Contacts, Calendar, Photos, iCloud Drive, Notes, Reminders, Pages, Numbers, Keynote, and Find Devices. (If you've enabled it, there's also a News Publisher web app, which appears only on the iCloud website, with no Mac or iOS/iPadOS version.)

The native apps running on the Mac and in iOS/iPadOS are more powerful and convenient. But there are several reasons you may want to use the iCloud website:

- **Non-Apple platforms:** If you use Windows, Linux, Android, or other operating systems where these apps aren't available natively, the iCloud site can make crucial features available to you. (iCloud Drive is the only exception: you can use it in Windows.)
- **On someone else's computer:** When you use someone else's computer (or a public computer), the iCloud website is the best way to access your iCloud data.
- **Exclusive settings:** A few features are exclusively available only in the website's iCloud Settings (notably, the option to Data Recovery.) These options are not found in any native app.
- **Find My for a lost device:** If you lose your iPhone or other devices or they're stolen, you may have to use Find Devices app on the iCloud website—on someone else's mobile device or computer, even—to report it lost, trigger a sound, or erase it.

Because Apple updates the iCloud website features and user interface regularly and on no fixed schedule, I can't provide detailed instructions for each of the ever-changing iCloud web apps. Instead, this chapter offers a general overview of what's on the site as of January 2024 and how to navigate it. I then offer a few tips for getting the most out of the web apps and locating obscure features.

Check Your Website Access

Before you can do much on the iCloud website, make sure you haven't turned off your own access. To check, go to System Settings > *Account Name* > iCloud (macOS) or Settings (iOS/iPadOS) > *Account Name* > iCloud, scroll to the bottom, and make sure Access iCloud Data on the Web is on. If you Use Advanced Data Protection you will need to take additional steps described in that section.

Navigate the iCloud Website

When you visit the iCloud website and click Sign In, you can enter your Apple ID, press Return, and enter your password. There's also an optional "Keep me signed in" checkbox, and a few informational links.

Note: If you visit the site on a Mac with Touch ID configured, you'll instead see a Touch ID authentication dialog.

Once you are signed in, keep in mind just a few things:

- **Opening and switching apps:** On the home screen is a tile with app names (**Figure 45**); click an icon to go to that app.

Figure 45: Click an icon on the home page to go to the web app.

Or, you can click the always-visible menu icon and then click the app you want to use in the popover that appears (**Figure 46**).

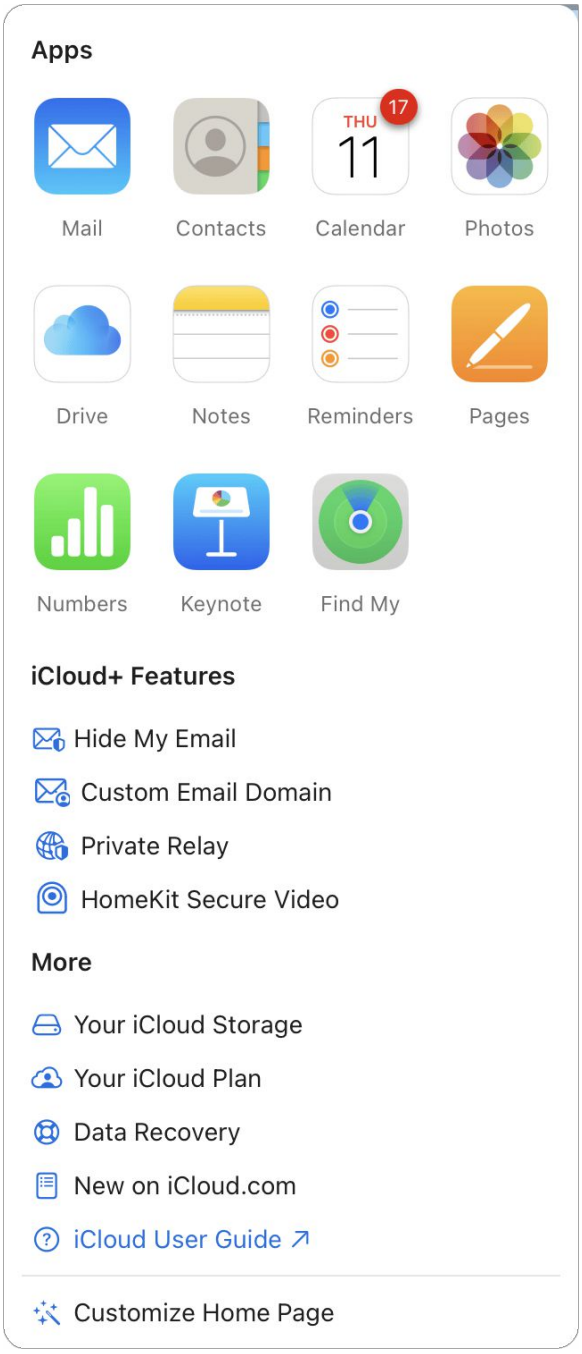


Figure 46: This popover appears when you click the menu icon.

- **Settings and signing out:** Click your picture at the top to display a pop-up menu that lets you view account settings or sign out.
- **Finding help:** Click the menu icon and choose iCloud User Guide. A separate tab with help appears. This help is actually *helpful*. I mean, it's no Take Control book, but seriously, it's not bad.

Click “Table of Contents” to display the table of contents. Or, to search the help, click the Search icon at the top.

- **Customizing the Home Page:** You can now personalize the display by clicking the menu icon and choosing Customize Home Page. You can then click Edit to change the app used for a tile, click Add Tile to add a tile for a single app or a large tile with icons for every app, delete a tile, or drag a tile to a new location. Click Done to exit customization.

That introduction out of the way, let’s take a quick spin through each of the web apps.

The Mail Web App

The Mail web app doesn’t approach the full capabilities of Apple Mail in macOS, but it’s quite similar to Mail in iOS/iPadOS—and it’s even *more* powerful in some respects.

iCloud Mail’s sidebar lists the containers for your messages. For reasons I can’t comprehend, iCloud Mail labels the Apple-managed items as Mailboxes at the top of the sidebar, for Inbox, Sent, Trash, and others; it labels any mailboxes you create as Folders.

You can add, delete, or rename your folders as needed, and drag them in and out of other folders to change their nested levels. To move a nested folder back to the top level, drag it on to the Folders label. Folders are always sorted alphabetically.

With an item in the sidebar selected, its contents are shown in the column next to it. Select an item in the mailbox or folder, and its contents appear in a preview on the right. If you hover over the line dividing the sidebar from the selected item’s contents or the item and its preview, you can drag the column dividers to make columns wider or narrower. Refresh the contents if you believe they’re out of date by clicking the refresh icon at the top of the sidebar.

Tip: To toggle showing and hiding the sidebar, click the sidebar icon at the top of the mailbox/folder contents panel.

iCloud Mail has many preferences you can adjust, including managing aliases and setting rules. To do so, click the gear icon in the sidebar, choose Preferences, and click a category such as General or Composing.

Note: One of the preferences you can enable is Mail Drop, which works much like its macOS and iOS/iPadOS counterparts. For details, see Use Mail Drop.

Here are more things you can do in the iCloud mail app:

- **View a message:** Click any message in the list; its contents appear in the preview pane. Or double-click a message in the list to open it in a separate window.
- **Message actions:** The icons at the top of the screen can be used to compose, reply, flag, delete, and move messages. (Click the Reply icon, or right-click/Control-click a message, to display a popover with even more options.) You can also drag messages to other mailboxes to move them.
- **Keyboard shortcuts:** iCloud Mail has many keyboard shortcuts; to see a list, visit this help page.
- **Aliases:** Your iCloud account comes with an icloud.com email address, but you can also configure up to three *aliases*—extra icloud.com email addresses that deliver messages to your main account. To set these up, click the gear icon in the sidebar, choose Settings, and click Accounts. The right side of the Settings display lists any aliases you've already set up. To add one, click Add an Alias. To disable one, select it and check Disable Alias, or you can delete it irrevocably by clicking Delete Alias.

Note: iCloud+ users can also add custom domains that let them use up to three additional email addresses with iCloud Mail, iMessage, and other services. See Configure a Custom Domain.

- **Rules:** iCloud can run server-based rules on incoming messages. To set up rules, click the gear icon in the sidebar and choose Rules. Even though that's a feature of most desktop clients, iCloud Mail's rules can sort messages *before* they appear on your iOS or iPadOS device—which overcomes, to some extent, the lack of a rules feature on these devices. iCloud Mail's rules are far less powerful than, say, Gmail's, but they're still quite useful.

Tip: Rules let you file, mark, or forward emails based on their sender, recipient, or subject. Because it can examine recipients, you can sort email based on whether someone has sent a message to your main iCloud address, an iCloud alias, or a custom domain alias.

The Contacts Web App

The simple Contacts app is straightforward, but Apple recently re-arranged some controls:

- **Gear menu:** Click the gear icon at the top of the sidebar to display the Settings window (where you can adjust sort order, address layout, and the like).
- **Plus menu (contact card):** Click the plus icon in the upper-right corner of a contact card to display a menu with Create New Contact and Import Contact commands.
- **Plus menu (sidebar):** Yes, there's another plus icon at the top of the sidebar, which you can use to add a list (group) of contacts.
- **More menu:** Click the more icon at the top of the contact list to display a menu with Select All Contacts, Make This My Card, and Delete Contact commands.

The Calendar Web App

You can manage appointments, meetings, and other events in the Calendar web app, which looks and acts much like Calendar on a Mac or iOS/iPadOS device. I want to point out a handful of controls that have changed since the previous version of this book:

- **Sharing:** To share a calendar or change the settings for an already-shared calendar, click the Share icon next to it. (I say more about this in Sync Your Calendars.)
- **More menu:** Click the more icon at the top of the sidebar to display a menu with important controls, such as Settings, Show Declined Events, Go to Date, and Delete Event.
- **Calendar list:** Click the Calendar List icon in the upper-left corner of the window to show or hide the sidebar containing a list of your calendars.
- **Notifications:** Click the Notifications icon at the top to display notifications, such as events added by someone else sharing your calendar and meeting replies. (The icon may show a number 5, representing how many notifications you have.)

The Photos Web App

Use the Photos web app to view and work with the items in iCloud Photos, albeit to a more limited extent than in the Photos app for macOS or iOS/iPadOS. Some of the key actions you can take are:

- **Download photos or videos, add them to an album, or delete them.** Select one photo or video—or hold down ⌘ to select multiple media items—and then click an icon at the top of the window, such as Download or Delete.
- **Mark a photo or video as a favorite.** Hover over the item's thumbnail, and click the heart icon that appears in its lower-left corner. Or click the heart icon at the top of the screen.

- **Upload a photo.** You can upload new photos (in JPEG format only) by clicking Upload at the top of the window. (You can't upload videos to the web app.)
- **View your albums, favorites, and memories.** If the sidebar is visible, find your albums there (as well as other categories of photos, including Memories); if not, click the sidebar icon at the top of the window.
- **Find additional controls.** Click the More icon to display a menu with additional controls, including Play Slideshow, Share, and Add to Album. If you have more than one item selected when you display this menu, the controls there apply to all selected items.

The Notes Web App

Like the Notes app in macOS and iOS/iPadOS (see Work with Notes), the Notes web app offers these capabilities:

- Use the sidebar to select a folder or tag, or create or delete a folder. You can also drag notes into a folder in the sidebar.
- To create a new note, click the New Note icon.
- To apply a style, click the Style icon to display a popover with style controls. Your choices are Title, Heading, Subheading, Body, Monospaced, Bulleted List, Dashed List, Numbered List, Bold, Italic, Underline, and Strikethrough.
- To create a table, click the Table icon.
- To turn the selected paragraph(s) into a checklist, click the Checklist icon.
- You can add other people to a note (allowing them to collaborate in editing the note) by clicking the Share icon.

Although the Notes web app can display attachments, URLs, and other text styles created with the Notes app on other platforms, it currently offers no way to add those attributes. It also offers no way to lock notes

with a password, as you can in the macOS and iOS/iPadOS versions of Notes, though you can use the web app to unlock notes that you locked on another platform.

The Reminders Web App

The simple Reminders app is easy to work in and mostly self-explanatory. Oddly, you can't add, remove, or share reminder lists in the web app; for those tasks, you must use a Mac or iOS/iPadOS device.

The iWork Web Apps

The three iWork for iCloud apps (Pages, Numbers, and Keynote) represent a remarkable piece of engineering, because they include the majority of the capabilities of the iOS/iPadOS and Mac versions of the apps—and all inside a web browser. If you've used iWork on any of the other platforms, you'll find the web app versions similar.

To learn more about any of these apps, click the menu  icon, choose iCloud User Guide, and then click Table of Contents.

Tip: For more about Pages, read Michael Cohen's *Take Control of Pages*.

The iCloud Drive Web App

The iCloud Drive web app lets you view your files and folders. You can use the icons at the top of the page to create folders and to upload, download, delete, and share items; you can also rearrange items using drag and drop. Double-clicking a Pages, Numbers, or Keynote document opens it in the corresponding web app.

Tip: Only a few icons are available for working with files and folders when Recents is selected in the sidebar (as it is by default). Click Browse to get full access to everything.

You can now view the contents of your iCloud Drive as either a grid of icons or a list. To switch views, choose either Grid or List from the pop-up menu at the top of the window. You can also select a file and press Space to see a Quick Look-style preview.

The Find Devices Web App

Find My helps you locate your devices, which Apple defines as a Mac, iPhone, iPad, AirPods, Beats (certain models of headphones or ear buds), or Apple Watch. It works when you've just misplaced them or know they're lost—or stolen. If the device (iPhone, iPad, or Mac) had Find My *Device* activated or its paired iPhone or iPad did (audio devices, Apple Watch), you can use Find My to locate it. You can also play a sound on the wayward item, lock it, or even wipe its contents.

The Find Devices web app can't locate Find My items such as AirTags, which rely on device pairing and end-to-end encryption. For more information, see Find Your Hardware with an App, later.

iCloud Settings

Although not quite a web app like the other items discussed here, the iCloud Settings page (which you display by clicking your picture in the upper-right corner and then choosing iCloud Settings) lets you view (and in some cases manage) your Apple ID, language, time zone, storage, devices, Family Sharing, and other iCloud features. It also lets you restore certain items you may have deleted from iCloud. I discuss all this later, in Use the iCloud Website Settings Page.

Find My Nouns

Apple offers three overlapping services that let you find hardware and people in varying combinations and with varying degrees of permission and consent.

Loosely, these can be categorized in the way that Apple breaks them out as views in the native Find My apps for iOS, iPadOS, and macOS:

- **People:** You can share your location with friends, family, and others, and view the location of people who have shared theirs.
- **Devices:** All your iCloud-linked computing and audio hardware appears here, as well as all the devices logged in by members of your Family Sharing group (if any). You can track any iPhone, iPad, iPod touch, Mac, or Watch, and AirPods (nearly, via Bluetooth only), AirPods Pro, AirPods Max, and a variety of Beats audio hardware.
- **Items:** AirTags and other items paired with an iPhone or iPad that make use of the crowdsourced Find My network appear in this view. This includes third-party licensed devices, such as Pebblebee and Chipolo's trackers and Knog's bike tracker. This also includes shared items starting in iOS 17/iPadOS 17 and Sonoma.

For people, devices, and items, you can view or ask Siri for their current location. For all devices and some items, you can cause a sound to play. With a Mac, Watch, iPad, iPhone, or iPod touch, you can lock the device (to keep it from being used) and display a message with a phone number (or reward!), or erase it, rendering its data inaccessible. You can even see your wayward hardware's battery level.

For devices, tracking works more reliably when they have an active cellular connection. That works with all iPhones, iPads with cellular modems, and Series 3 or later cellular Apple Watch models. These devices are likely to have a network connection at all times—cellular access is pretty ubiquitous—whereas Wi-Fi is spotty, and may require a login and even payment.

Note: Series 2 and later Apple Watch models, iOS devices, and iPadOS devices (only those with cellular support) also have GPS receivers, so their reported location over Wi-Fi is more precise than for Macs and for earlier iOS or iPadOS devices that lack satellite positioning circuitry.

Apple has increasingly made device "sleep" more of a "nap with one eye open." The iPhone, iPad, iPod touch, and Watch maintain their mobile connections even when seemingly in a standby mode. Macs with SSDs—most of them these days—send updates even while ostensibly asleep.

Most newer Apple hardware also uses a clever technique to rely on nearby Apple devices to securely pass along their location by broadcasting a special Bluetooth signal if they have no internet connection.

In this chapter, I explain how iCloud acts as the pivot around which location information, actions, privacy, and security rotate.

Tip: For vastly more detail on Find My and Apple's AirTags and third-party trackers that use the Find My network, see Glenn Fleishman's *Take Control of Find My and AirTags*.

Activate Find My

Find My *Device* and Find My *Item* can track a broad array of devices and items, but the service works only when that device or item has Location Services enabled and then Find My *Device* or the Find My network is also turned on.

To enable Location Services:

- **macOS:** In Ventura or later, go to System Settings > Privacy & Security > Location Services (Ventura or later) and turn Location Services on if necessary; you may be prompted to authenticate when you do this. Then scroll down to the bottom, click Details next to

System Services, and make sure Find My Mac is also turned on. Click Done.

In Monterey or earlier, go to System Preferences > Security & Privacy > Privacy > Location Services, click the lock icon and authenticate, and select Enable Location Services. Next, scroll down to System Services, click the Details button, and then ensure that Find My Mac is selected in the set of items under "Allow System Services to determine your location." If it's not, you can enable Find My Mac, but your Mac won't share its location.

- **iOS/iPadOS:** Go to Settings > Privacy & Security > Location Services and make sure Location Services is turned on at the top.

As noted earlier, Find My *Device* and Find My *Item* track hardware in slightly different ways. That extends to how you ensure that each form of location updates is enabled.

Turn on Find My Device

Find My *Device* can track an iPhone, iPad, or iPod touch running iOS 5 or later or iPadOS, an Apple Watch, AirPods, or a Mac running 10.7.2 Lion or later.

You might find that Find My *Device* is already active, because Apple aggressively encourages enabling it during setting up a device from scratch and during upgrades, but to make sure:

- **macOS:** Go to System Settings > *Account Name* > iCloud (Ventura or later) or System Preferences > Apple ID > iCloud (Monterey or earlier and make sure Find My Mac is turned on.
- **iOS/iPadOS:** In iOS/iPadOS, tap Settings > *Account Name*, and make sure Find My *Device* is on; if not, tap Find My *Device,* tap the switch to turn it on, and optionally turn on Send Last Location, which sends the location automatically when the battery is nearly depleted.
- **AirPods, Beats devices, and Apple Watches:** Audio hardware and Apple Watches can be discovered through Find My *Device* if

Find My iPhone is enabled on the iPhone to which they are paired. Depending on the model, your earbuds and charging case may be separately trackable.

Apple tracks a device with Find My enabled even when it's ostensibly "turned off"—really in a sort of mild sleep mode—or after it's been erased.

Check for Find My Network

I recommend also using the Find My network (once called "offline finding"), explained just below. It's on by default. To check whether Find My network is enabled:

- **macOS:** In Ventura or later, go to System Settings > *Account Name* > iCloud, click Find My Mac, and confirm that "Find My network" is turned on. In Monterey or earlier, go to System Preferences > Apple ID > iCloud, click the Options button next to Find My Mac, and confirm that "Find My network" is set to On.
- **iOS/iPadOS:** Go to Settings > Privacy & Security > Location Services > Share My Location > Find My *Device* and ensure that "Find My network" is turned on. (Send Last Location should also be turned on.)

How Crowdsourced Find My Works

The Find My network provides a secure and anonymous way for devices and tracking items to report their whereabouts using crowdsourcing. Any nearby iOS 13/iPadOS 13 or later device or Mac running macOS 10.14 Mojave or later acts as a relay for secure Bluetooth broadcasts from Apple hardware owned by other people that can't reach the internet or lacks internet networking.

Whenever a Mac or iOS/iPadOS device with the feature enabled cannot reach the internet, it begins to broadcast a Bluetooth identifier that's anonymous and contains encrypted information about the device's identity. Most Apple audio hardware, Beats audio hardware, and AirTags and third-party Find My items continuously broadcast a Find My network signal, as they have no way to reach the internet.

A nearby qualifying device with an active internet connection automatically identifies this special Bluetooth broadcast, determines its own location, pairs it with the Bluetooth ID, and uploads it to Apple.

From Find My on an iPhone, iPad, or Mac logged in to your iCloud account, your device sends cryptographically secured identifying information to Apple, which then matches and downloads only Bluetooth IDs that your devices can decrypt to extract the location.

It's a one-way data street, so you can't activate Find My *Device* features on your missing Apple devices—like wiping its contents—just because other people's equipment has managed to locate it.

Understand Device and Item Locks

Enabling Find My *Device* also enables Activation Lock on any device with a screen. This lock is a theft deterrent that prevents erasing or setting up a device that's been erased without the iCloud account password that originally locked it. As noted above, even if a thief, criminal, or unintentional buyer of stolen goods manages to erase a device, Find My can be used to track it.

However, this adds a step that buyers and sellers of used devices must be aware of. See Check Activation Lock, later in this book, for details.

Note: Although you can set up more than one iCloud account on a Mac or iOS/iPadOS device, Find My *Device* can be enabled for only one of the accounts—the first one you set up.

With your device properly configured, you can then find it using the Find My app on a Mac, iOS/iPadOS device, or the iCloud website. I describe all these options in the pages ahead.

Find My *items* lack a screen or internet connection, and Apple created the distinct Find My Lock for them (formerly called Pairing Lock). They remain locked to the iPhone or iPad they associate with until they are unpaired, which requires physical proximity and the ability to unlock the iPhone or iPad.

The only way to remove the Find My Lock and disable tracking without the iPhone or iPad is to remove the battery or otherwise disable Find My on the item. However, without unpairing the item, it may never be used with another iPhone or iPad again.

Deactivate Find My Device

Like most iCloud features, you can turn off Find My *Device* by unchecking a box (Mac) or flipping a switch (iOS/iPadOS)—the same one you used to turn it on. You might do this if you want the device's location to remain private; if you're about to sell, give away, or recycle the device; or if you're signing out of iCloud altogether. (In fact, it's rather critical when selling: see Check Activation Lock above.)

After you uncheck that box or flip that switch, you will be asked for your Apple ID password and confirmation that you want to disable the Find My network. At the very least, your device will ask you to be extra sure this is something you want to do, because turning off this feature can increase your risk if the device is ever lost or stolen.

Deactivate Find My Items

AirTags lack a physical interface, and other Find My items have limited interactivity. You can turn off Find My network on devices with which Find My items are paired or unpair those items from devices.

With AirTags, unscrew the battery cap and remove the battery; see Apple's instructions. Consult the websites for makers of third-party items, as the instructions vary tremendously!

Find Your Hardware with an App

The easiest way to find your iCloud-enabled iOS/iPadOS device, Mac, Apple Watch, or AirPod is to use the Find My app for macOS, iOS, or iPadOS. The *only* way to locate a Find My item or use the crowd-sourced Find My network is via one of those apps.

Apple Lets Find My Web Apps Lag Behind

While Apple still offers Find Devices for any Apple device on the iCloud.com website, it's out of parity with the native apps. It lacks any of the notification options and can't be used with the Find My network at all. That's because Apple built the Find My network around end-to-end encryption, requiring a device that can store secret keys in a highly secure way.

To use the Find My app, open it and authenticate if prompted to do so. Apple divides People, Devices, and Items into separate views available through tabs in the upper-left corner of the macOS app and icons at the bottom of the iOS/iPadOS app. Click or tap Devices or Items to see your hardware on a map tracked in one of those two methods.

Initially, both views show a map on which iCloud tries to locate all your devices or items (**Figure 47**). If you're a member of a Family Group, the Devices view shows all the other members' tracked devices, too, divided up by person below your devices in the list.

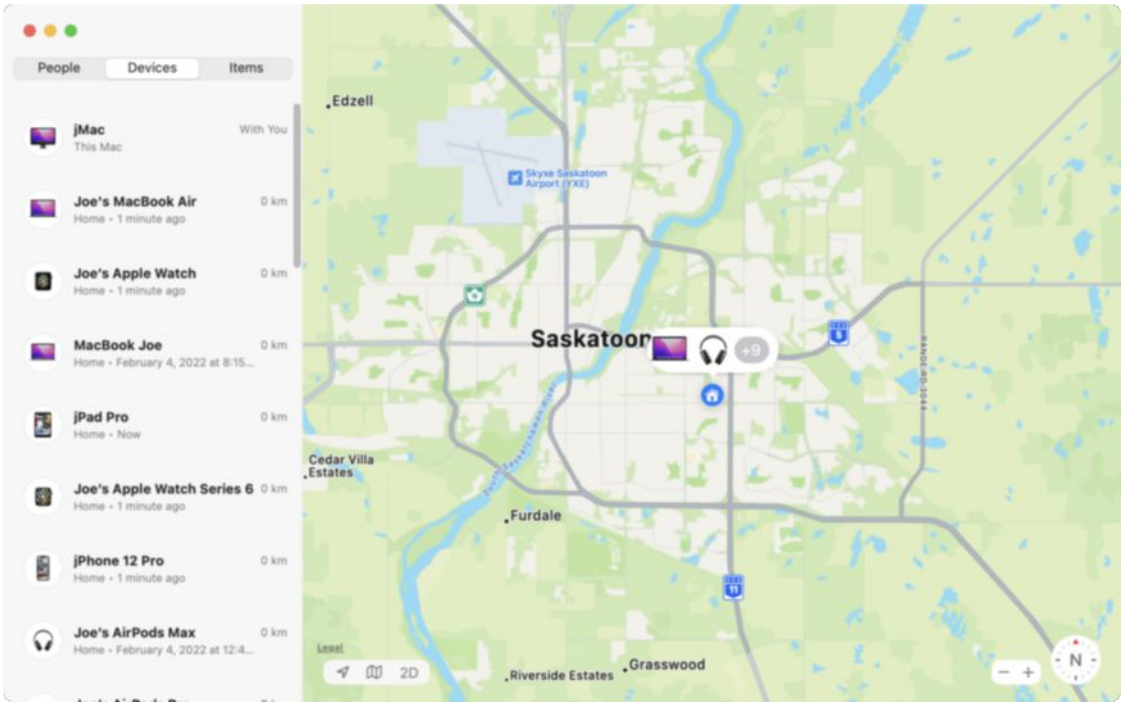


Figure 47: The Find My app (shown here on a Mac) lists all your devices. Select a device to zoom in on its location on the map.

Devices and items show their current location and distance below their name in their respective lists. Select a device or item to isolate its location on the map.

Location Not Found?

Devices and items that aren't powered on, haven't been powered on recently, or cannot send their location or be picked up the crowd-sourced network, appear as "No location found." If that hardware had a recent-enough connection, its last location should be shown along with the time when that was captured.

The location may show as a point with a shaded circle of confidence around it: the point is the best guess at the exact location and the shaded area the potential for error. For some devices and items, you may first see a broadly defined area which becomes smaller and zooms in as more location data is received.

Note: A device determines its location using a combination of cell tower trilateration, Wi-Fi network positioning, and GPS, depending on which of these are available. An item or an offline device using the Find My network relies on the same coordination sources as gathered by the device through which it relays.

A control panel for the selected device or item appears automatically in macOS, iOS, and iPadOS (**Figure 48**). (To see the control panel in the Find My iPhone for the web, click or tap the Info ⓘ icon.)

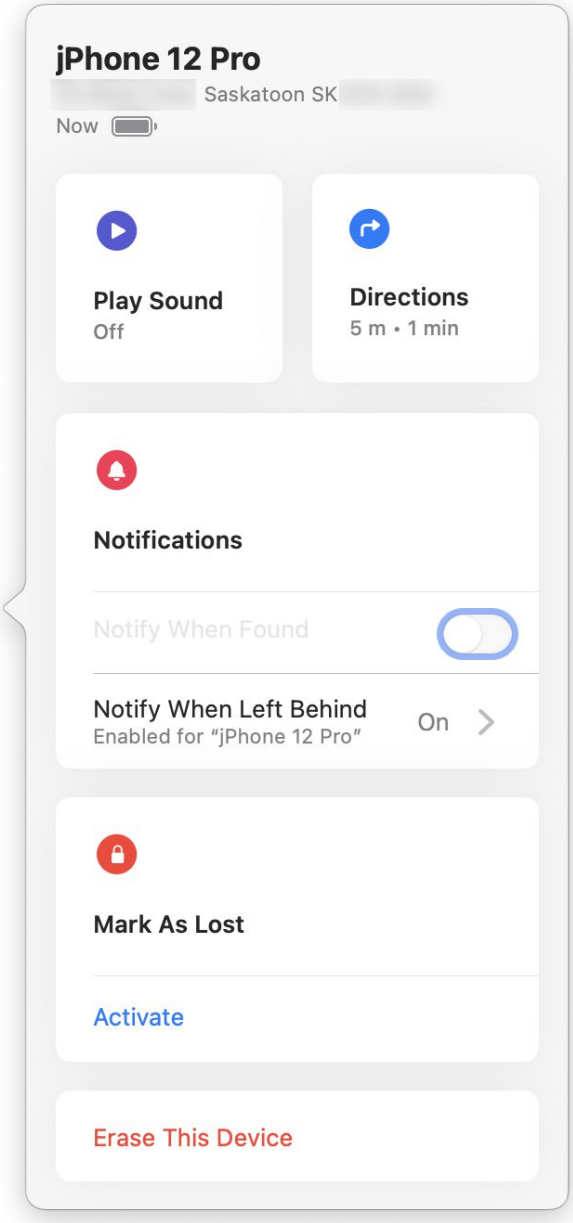


Figure 48: This control panel (shown here for an iPhone) lets you select various Find My *Device* actions.

Beyond merely locating the device, you can take any or all of several other steps depending on the device type. To do so, use these options in the control panel:

- **Play Sound:** If the device is online, clicking or tapping this button will play a pinging sound at full volume, even if the device is locked, has its ringer switch turned off, or is in Do Not Disturb mode. This can help you locate it if you misplaced it in your home or office. If the device is offline, the sound plays when it comes back online.

  On the wayward device, you can turn off the sound or dismiss the message by unlocking the device (if necessary) and then clicking or tapping a button. If the sound has been played or the message sent, iCloud sends you an email message to confirm this, which helps let you know it was online if you can't find it.

Note: If you're within Bluetooth range of your AirPods or AirPods Pro, you can tap the Left and Right buttons adjacent to the Stop Playing button to mute one or the other earbud in a pair selectively, allowing you to better hear the other one. This doesn't work over the Find My network, which only tracks one in a pair.

- **Directions (devices):** As with any other location on a map, you can click or tap Directions to get walking, driving, or transit directions to your device's location.
- **Find (AirTags):** When an AirTag is paired with an iPhone 11 or later model, and is within about 30 feet (10 meters), it can be pinpointed by direction and within feet using ultrawideband radios found in the AirTag and the iPhones. Because the iPhone uses augmented reality to help position itself relative to the UWB signals, you must have sufficient light; you're prompted if that's not the case.
- **Notifications:** Apple offers two kinds of notifications, depending on the device or item:

  - If a device cannot be located and was most recently located more than an hour ago, you can turn on Notify When Found. When the

device next comes online, iCloud will alert you by email so you can return to Find My and take the next step.

  - You can help stop yourself from walking away from stuff you own by enabling Notify When Left Behind on devices that allow it. You can choose locations to ignore, too, so you're not being warned that you left your home computer at home, for instance.

- **Mark As Lost:** Mark As Lost lets you not only lock your device, but also put a telephone number and message on the screen to help a finder return it to you. If your device wasn't already locked with a passcode when you click or tap Mark As Lost, you'll be prompted to choose one. When the device becomes available online, it will be locked, the message you sent will appear on the screen, and you'll get an email confirmation.

  Marking a device as lost also disables Apple Pay on that device, which suspends any credit, debit, or other cards. If you recover your device, you can re-enable Apple Pay with your Apple ID password, and if you sync cards with iCloud, they will be restored to and reactivated on the device.

How To Lock a Mac via the Web App

If you have to resort to the Find My iPhone web app to mark a Mac as lost, you'll find it's labeled Lost Mode and it appears only for newer Macs. For older Macs, you'll instead see a Lock command. Here's how to use it.

Click Lock and click Lock again to confirm. Enter and repeat a numeric passcode, enter an optional message, and click Lock. On receiving the command, your Mac will shut down and lock itself so that no one else can use it or see its data. Only entering the code you chose will unlock it. A locked Mac can't be erased remotely, as explained next.

- **Erase This Device:** If your device has been stolen or is otherwise unrecoverable, you can tell iCloud to securely erase all its data—your email messages, address book, photos, apps, documents, and everything else—so that at least whoever has the device can't access your personal information.

To do this, click or tap Erase This Device, read the warning, and click Erase. If the device you're erasing is a Mac, you must also enter and confirm a numeric passcode that can be used to unlock the device (although not to recover the erased data), and enter a message that will be displayed on the screen if the Mac is ever found. The data is wiped immediately if the device is online, or as soon as it comes back online if not.

Erasure is almost immediate on all modern Apple hardware: an iOS/iPadOS device of the last decade, any Apple Watch, any Intel Mac with either FileVault enabled or with a T2 chip, and any M-series Mac. (Macs with neither a T2 chip nor FileVault enabled could take as long as a day to erase.)

Once you've triggered erasure with an iOS/iPadOS device or Apple Watch, the Find My *Device* features are no longer available with watchOS. However, devices running iOS 15/iPadOS 15 or later remain findable.

If you wipe a Mac's data remotely, you may be able to locate it later with Find My *Device*. Some components used by Find My Mac are kept on the hidden recovery volume that the macOS installer creates—and that's not included in the data that's wiped.

Warning! According to Apple's online help, if you remotely erase a Mac that had a firmware password set, you may not be able to unlock it yourself—even with the passcode—if and when you recover it. If you can't, you must take it to an Apple Store or authorized repair center to be unlocked, and be able to demonstrate you were the legitimate and *first* purchaser with a dated sales receipt that shows its serial number.

- **Remove This Device:** If you no longer use the device, you remove it via Find My. Apple recommends first erasing the device, as above, and then clicking or tapping Remove This Device. Once you confirm removal, Apple disables the device's Activation Lock the next time it connects to the internet.

Why Erase and Then Remove?

The reason for this two-step procedure? If you don't have your hands on the device, ostensibly you want to wipe its contents before someone else uses it. The device must connect to the internet to receive that erasure instruction, and then you receive confirmation that the erase operation occurred. At that point, you know this remotely reachable device no longer has any useful data of yours on it. Then you can remove Activation Lock via Find My without worrying about your data being in someone else's hands, however benign they are.

Always Use a Passcode or Password

A passcode protects the data on an iOS or iPadOS device from prying eyes and buys you time to use Find My *Device*, especially with a stolen device, where a thief might quickly try to disable its ability to send its location or be erased. It's a must for anyone concerned about security. While you can set a passcode via Find My *Device*, that should be a last resort.

To set a passcode, tap Settings > Touch ID & Passcode (or Face ID & Passcode; or, on devices with neither Touch ID nor Face ID, Settings > Passcode). If your device does not have Touch ID or Face ID enabled, you can set the amount of time before the device automatically locks—the shorter that time is, the less chance someone will have to disable the passcode. (With Touch ID or Face ID enabled, the only option is "Immediately.") Also disable Control Center on the iOS/iPadOS lock screen (in Settings > Touch ID & Passcode), so a thief can't swipe to turn on Airplane Mode or disable Wi-Fi and Cellular.

Similarly, you should have a password on all Mac user accounts that appear at the startup screen. (If you have FileVault enabled, only password-protected accounts allowed to start up the machine appear, anyway.) You can additionally set your Mac to require a password after a period of inactivity. In Ventura or later, go to System Settings > Lock Screen and set "Require password after screen saver begins or display is turned off" to anything other than Never; then authenticate when prompted. In Monterey or earlier, go to System Preferences > Security & Privacy, click the lock  icon, and enter your credentials to unlock it. Click General, and if present, select the Require Password checkbox. Then choose a time (such as 5 Minutes) from the pop-up menu.

Find Your Device with Siri

On any recent Apple device, including a HomePod or an Apple TV with a Siri remote, you can activate Siri in any of the usual ways, and then say something like "Find my Mac" or "Where's my iPad?" and the device in question plays a sound. If you want to do anything more than play a sound, however, you'll have to use an app or the iCloud website.

Find People

Just as Find My *Device* lets you find devices of your own, Find My *People* lets you see the location of friends, family members, and others who have given you permission to know their whereabouts. Apple derives their location from their primary device, which can be an iPhone, iPad, iPod touch, or cellular model of the Apple Watch.

Note: Using one of these devices to identify one's "presence" appears to be based on the theory that those are items most likely to be carried on one's person and that also have sufficient network connectivity to advertise their locations.

On a Mac or iOS/iPadOS device, use the Find My app to find your friends. I describe steps in the iOS/iPadOS app below, but the macOS version is nearly identical.

To find a friend who has already given you access:

1. Open the Find My app.
2. Tap People to display a list of people whose location you're tracking.
3. Tap a person's name.

The app shows the person's location on a map, along with a panel with controls to contact them, get directions to their location, and add notifications, which come in two flavors:

- To notify *yourself* of either a change in the *other person's* location or the fact that the other person is *not* in a specified location when expected, tap Add under Notifications followed by Notify Me. Then:
  - **To know when someone arrives or leaves:** Tap When *Name* Arrives, and then select the location under *Name*'s Location; or When *Name* Leaves to be notified when the person leaves their current location or one you define. You can tap Every Time beneath Frequency to make it a recurring notification. Tap Add to complete the process.
  - **To be notified when your friend is not at a certain location at a given time:** Tap Person Is Not At, enter From and To times, and select a time period and one or more days of the week when you want to know about that. Tap Create Notification to complete the process. (This can be useful for keeping tabs that your child remains at school or at home.)

Note: Find My will inform you that the other person will be notified that you created the notification. If you proceed, sure enough, the other person is informed. This affirmative notification is part of Apple's efforts to deter stalking with Find My.

- To notify *that person* of a change in *your* location, tap Add under Notifications followed by Notify *Person's Name*. Select either I Arrive or I Leave under the When label, and either use your current location, another one you set, or create a new one. You can set this to recur as well by tapping Every Time or leave it as Only once. Tap Add to complete.

To give a friend permission to know your whereabouts, go back to the People view in the Find My app and tap the plus + icon and then tap Share My Location. Enter an email address and tap Send. To change the permissions one of your friends has, tap their name and then tap Stop Sharing My Location (which allows you to continue to know your friend's location, if they've authorized it) or Remove *Name* to remove that person altogether from both sides of the equation.

Note: To create a temporary authorization for other people to see your location, use Messages. In Messages, tap a person's name and then tap Share My Location. You can choose among Share for One Hour, Share Until End of Day, or Share Indefinitely.

For more information, you may find it useful to read Apple's Find people and share your location with Find My page.

Back Up and Restore iOS/iPadOS Data

iCloud can automatically back up most of the important data from your iOS or iPadOS device to Apple's servers. This feature is usually invisible once you've set it up, but there are a few options you may want to adjust, and you'll want to know how to Restore an iOS or iPadOS Device from a Backup should the need arise.

Note: As I mentioned in the sidebar iCloud Drive and Backups, iCloud is *not* designed to back up data from Macs. For that, you should use a local option (such as Time Machine or Carbon Copy Cloner) or a cloud service such as Backblaze. For more details, see my book *Take Control of Backing Up Your Mac*.

Understand How iCloud Backup Works

Backups are as important on an iOS or iPadOS device as on your computer—after all, your mobile device stores lots of crucial personal data, including photos and videos that may be irreplaceable. If it dies or needs replacing, backups can also save you time and aggravation.

But backing up an iOS or iPadOS device is a lot different from backing up a Mac or PC. Conventional backups methods won't work, because each app is *sandboxed*—prevented from interacting with other apps' data—and because iOS/iPadOS devices have no browsable file system. (Yes, there's the Files app, but that app only provides access to a small portion of all the data on your device.)

It's possible to back up your iOS or iPadOS device by connecting it to your Mac or PC via Wi-Fi or with a USB cable and clicking Back Up Now in the Finder (or iTunes for Windows). But with iCloud, you can back up over Wi-Fi directly to Apple's servers.

This means:

- **Back up on the go:** You can back up your data while away from any computer; you're not tethered to a machine for backups.
- **Restore without a computer:** You can restore an iOS or iPadOS device—such as one whose data was corrupted, or that had its data wiped as part of a repair—or set up a new device to use your existing data without a computer.
- **Differential backups:** When you back up via iCloud, only the first backup copies *all* your personal data. Subsequent backups upload only information that's new or different since last time, making iCloud backups faster on subsequent backup runs.

For all these reasons, I generally recommend using iCloud Backup. But, as I said in About iCloud Storage, backups can consume lots of space. To solve this problem, you can buy more storage, limit which types of data are backed up (as I describe ahead), or delete old backups. But if you're short on space and unwilling to buy more, you might stick with backups using the Finder (or iTunes for Windows).

Note: For the privacy implications of iCloud Backup, flip ahead to Protect Your Privacy.

What does iCloud Backup back up, anyway? It covers the following:

- The photos and videos you've taken on your iOS or iPadOS device if you haven't enabled iCloud Photos
- Photo albums you've created *on the iOS or iPadOS device* (but not those created on and synced from your computer)
- Documents and app settings, including Health (on an iPhone)
- All account data and iOS/iPadOS settings, which includes those configured in the Settings app, HomeKit configuration, and your Home screen and folder organization
- Conversations in the Messages app (iMessage, SMS, and MMS) if Messages in iCloud is not enabled

- Your call history, ringtones, and Visual Voicemail password
- Apple Watch backups
- Your purchase history from Apple

Note: This list changes from time to time, and some items require qualifications. For the latest details, see What does iCloud back up?.

This list doesn't include anything that's already stored in the cloud thanks to some other aspect of iCloud—purchased music, TV shows, movies, apps, and books; photos and videos synced via iCloud Photos; plus your contacts, calendars, reminders, email, notes, bookmarks, and any documents handled by iCloud Drive.

Activate and Configure iCloud Backup

To set up iCloud Backup for your iOS or iPadOS device, tap Settings > *Account Name* > iCloud > iCloud Backup, and turn on Back Up This iPhone or Back Up This iPad. Tap OK if prompted to confirm.

I also recommend the optional step of starting your first backup manually so that it begins immediately: Go to the Backup screen on your iOS or iPadOS device as above and tap Back Up Now.

Your initial backup may take several hours or more, but subsequent backups should be speedy. Backups occur automatically, once per day, as long as your iOS or iPadOS device is connected to power, has an active Wi-Fi connection, and is locked. Other than backups you initiate by tapping Back Up Now, you'll never see a backup in progress. (However, you can see when your last backup occurred at the bottom of the Settings > *Account Name* > iCloud > iCloud Backup screen.)

After your initial backup is complete, you can see how much space various types of data occupy, and you can selectively delete backups of individual data types:

1. Tap Settings > *Account Name* > iCloud. The screen (**Figure 49**, left) displays overall statistics for your iCloud account at the top.

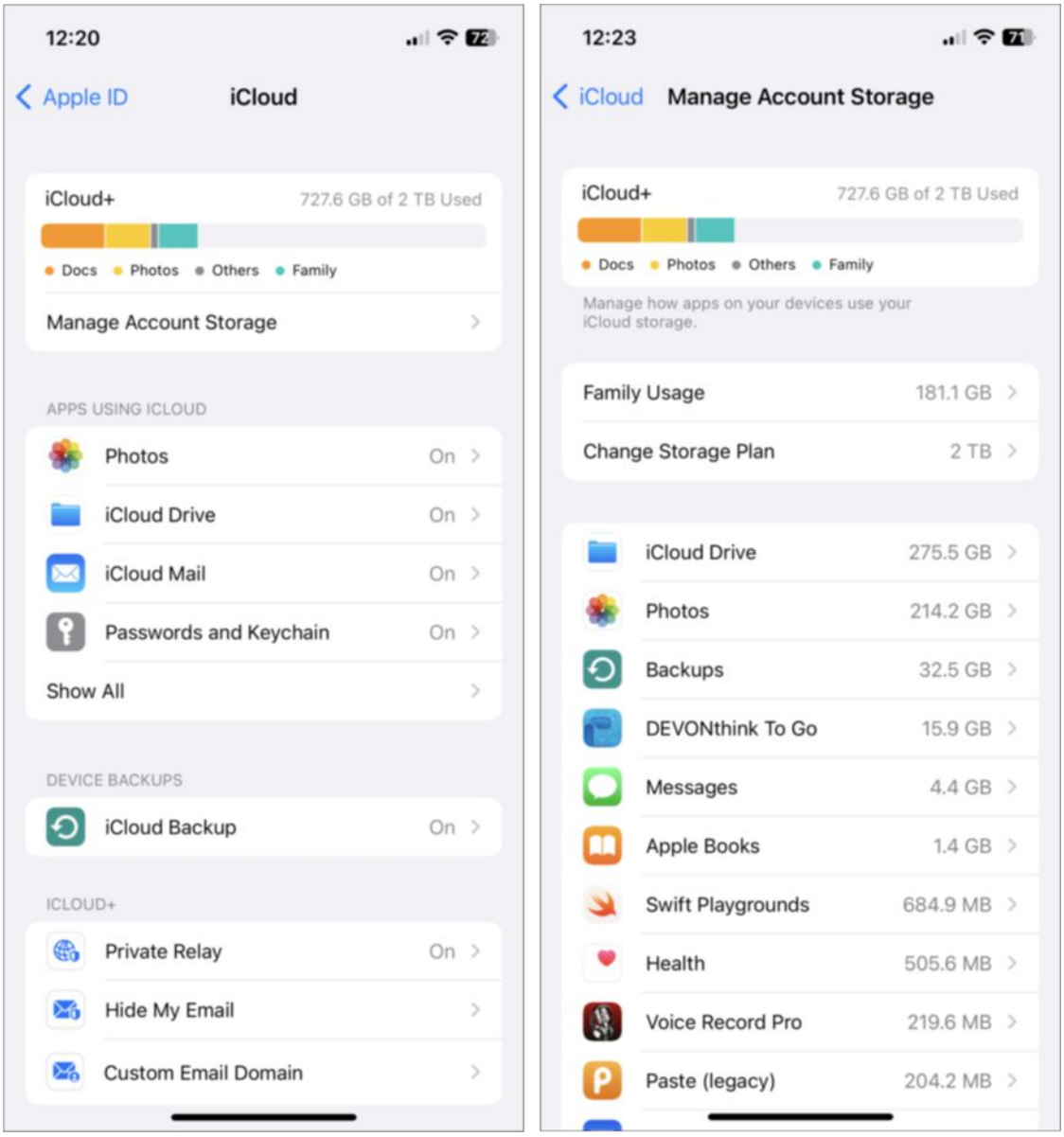


Figure 49: Left, top: The Storage section of the iCloud screen shows an overview of what is consuming space in your iCloud Drive account, including any iCloud backups. Right: From this screen, tap Backups to see and delete backups of particular kinds of data from this device.

2. Tap Manage Account Storage, and you'll see something like the screen on the right in **Figure 49**. The Backups category indicates the total size of backups for all your iOS and iPadOS devices. Tap Backups to see how this breaks down by device. Tap the name of the device you're holding to delete its entire backup or enable or disable backups of particular data types. To turn off future backups of a data type and delete its existing backups, tap it, tap Delete Documents & Data (or Delete Data), and tap Delete to confirm.

Note: Although you can turn off backups of data for specific apps, you can't turn off backups of other device data without turning off iCloud Backup altogether.

Tip: You'll have more room for backups if you aren't using so much space in your iCloud storage allotment for other things. For help with handling your storage, read Check and Modify Your Storage Usage, later.

Restore an iOS or iPadOS Device from a Backup

Let's say you've backed up your iOS or iPadOS device to iCloud. Now, you want to restore that backup to a new device—or your device is missing crucial data and you want to restore that data from a backup. What do you do?

If you need to restore your data to a new iOS/iPadOS device, you'll get a chance to select it while you set up the device. But restoring data to an existing device is not so obvious. Curiously, there's no Restore button anywhere in the Settings app, and no apparent way to get your data back! Furthermore, restoring is an all-or-nothing affair: you must restore *all* your data from a backup—you can't restore just your photos, or just data from a particular app.

To get your iOS or iPadOS device to a state where you can restore a backup, first, if possible, verify that you have a backup that you want to restore from, as described earlier in this chapter. With your device connected via USB to your computer, the General tab in the Finder (or the Summary pane in iTunes for Windows) lists your latest backups to both iCloud and "this computer" in the Backups section. You can check on iCloud backups on the device by tapping Settings > *Account Name* > iCloud > Manage Storage > Backups.

Now that you've confirmed that you have a backup to restore from, tap Settings > General > Transfer or Reset *Device* > Erase All Content and

Settings, enter your passcode if prompted, and then tap Erase *Device* (twice) to confirm. (If Find My *Device* was active, you may also be prompted for your iCloud password.)

This resets your iOS or iPadOS device to "factory fresh" status. When you next turn it on—or if you're setting up a new device—you'll go through these steps:

1. Follow the prompts to answer a few questions, such as your default language, country, and Wi-Fi network (entering its password, if necessary), and Location Services preference.
2. Tap Restore from iCloud Backup.
3. Enter your Apple ID and password.
4. Tap the backup you want to restore (likely your most recent one), and tap Restore.

iCloud backups tend to be quite slow to restore (typically, much slower than restoring local backups), so be prepared for a bit of a wait. After the backup has been downloaded, your device restarts and applies the backup.

That's not the end of the process, though. When your device finishes restarting, you will see when you unlock it that many apps are unavailable, and your media libraries—like iCloud Photos—are incomplete.

iOS and iPadOS make your device available for use even as apps, music, photos, and other items download, which could take from tens of minutes to several hours to complete, depending on your bandwidth and unknown factors that seem to hold up Apple's end.

Under apps that aren't yet downloaded, the label "Waiting…" appears; as they load, they display the circle-filling pattern you see with App Store downloads. Tap an app to bump it up in the queue to download sooner than it's unknown current position (which appears to be the order of installation, whenever you installed).

There's no prompt when these post-restart downloads are done.

Warning! iCloud backups don’t last forever, and are not intended for long-term archiving. If you disable iCloud backups or if your device is unable to back up for an extended period of time, Apple deletes the backed-up data for your device 180 days after its last backup.

Use iCloud on an Apple TV

The Apple TV is a small box that gives your TV access to media from Apple and other providers, Apple Arcade and third-party games, media stored on other Apple devices on your network, and other categories of apps. It also acts as a hub for HomeKit-connected devices, extending certain features and adding remote access.

Note: Although the third-generation Apple TV supports several iCloud features, this chapter covers HD and 4K models only.

In this chapter I talk briefly about Apple TV features that involve iCloud, but not about the rest of Apple TV. For a full look at Apple TV, consult *Take Control of Apple TV* by Josh Centers.

Set Up iCloud on an Apple TV

There are two main places to configure iCloud-related settings on your Apple TV. Depending on the choices you made when you set up the Apple TV, either or both of these may already be set, but it doesn't hurt to check.

Set Up iCloud Account Features

To configure an Apple TV to work with iCloud Photos, Family Sharing, and the AirPods paired with your iPhone (if you have them), navigate to Settings > Users and Accounts > *Account Name* > iCloud. If your Apple ID isn't already listed, select Sign In.

If you've already entered your Apple ID for the iTunes Store, you may be asked if you want to use that same Apple ID for these other features. If you do, select Yes (and enter your password); if not, select No, Use a Different Apple ID (and enter both the Apple ID and password for a different iCloud account).

The Users and Accounts screen shows two additional options related to iCloud:

- **One Home Screen:** When enabled, your Home screen will be the same on every Apple TV signed in to your iCloud account.
- **Photos:** Turn this on to provide access to your personal iCloud Photos library via an Apple TV. You can also separately enable or disable Show Memories and Shared Albums.

After that one-time setup procedure, to view your photos, follow the steps ahead in Use iCloud Photos on an Apple TV.

Set Up iTunes Store and iTunes Match

To set up your Apple TV to stream purchased media from iCloud, navigate to Settings > Users and Accounts > *Account Name* > Store. If your Apple ID isn't already listed, select Sign In and enter your credentials. Then select Yes, if prompted, to remember your password for rentals and purchases.

> **Tip:** You may want to avoid storing your password if your Apple TV is accessible by kids or guests who might rent or buy things on your account without your permission.

You may enter more than one Apple ID (for example, if multiple people in your household have purchased content from the iTunes Store that you want to view), and switch between them easily. To enter an additional account, once again go to Settings > Users and Accounts, select Add New User, and follow the prompts. (To switch between accounts, return to the Users and Accounts screen and select a different account.)

If you subscribe to iTunes Match, it's automatically enabled when you add your iCloud account, though you will need to turn on Sync Library in the Music app the first time you use it.

View Shared Purchases on an Apple TV

If you've enabled Family Sharing, you can't access other family members' music on an Apple TV, but you can view movies and TV shows purchased by other family members. Go to the tv app, swipe left on your remote to display the menu, and select Library > Family Sharing. Then select a family member to see that person's purchased content.

Use iTunes Match on an Apple TV

If you've set up iTunes Match on your Apple TV, navigate to the Music app to listen to matched or uploaded tracks from your Music library. You can then navigate through your entire Music library, including your playlists.

Use iCloud Photos on an Apple TV

After setting up iCloud Photos in the Settings app, you can select Photos on the home screen to display your photos and videos, shared albums, or personal albums. You may be prompted to turn on iCloud Photos the first time you use it. If iCloud Photos is enabled, you can also see Memories (automatically generated collections of photos and videos based on time, location, or faces).

Use AirPlay from iCloud

If you have an iOS or iPadOS device, you probably already know you can use AirPlay to send audio and video from it to your Apple TV, which essentially turns your TV into a much bigger display for your iOS/iPadOS device. AirPlay from iCloud alters this behavior in a subtle way: after you initiate playback in iOS/iPadOS, your Apple TV streams any media purchased from Apple or stored via iTunes Match directly from the iCloud servers instead of from your iOS/iPadOS device.

One benefit of this approach is that you preserve your iOS/iPadOS device's battery charge, since the device doesn't have to stream and transmit the media. Another is that you can use someone else's Apple TV (that is, one that's not signed in to your iCloud account) to display purchased content from *your* iCloud account, simply by virtue of your iOS or iPadOS device being within range.

For example, if you have a season pass to a TV show I want to see, I can invite you to my house and feed you popcorn in exchange for using your iOS/iPadOS device to play shows on my TV—without any changes in settings for either of us.

To enable AirPlay from iCloud, on the Apple TV, go to Settings > AirPlay and HomeKit and make sure AirPlay is set to On.

After you do that, whenever an iOS or iPadOS device sends content to your Apple TV, the Apple TV attempts to stream it from iCloud if it's stored there; if it can't for any reason, it falls back to streaming from the iOS/iPadOS device.

Manage Your Account

Your iCloud account has a handful of settings you may want to adjust, including your photo, default language, and time zone. And, if you've inadvertently deleted something from Bookmarks, Contacts, Calendar, or iCloud Drive within the last 30 days, you can restore it using the Settings app on the iCloud website; see Data Recovery. You can also use account-level controls to Increase Your Storage.

Use the iCloud Website Settings Page

The iCloud Settings page shows you a few settings related to your use of the iCloud website as a whole, as well as data recovery tools and links to other Apple ID resources. To use these features, log in to the iCloud website, click your name at the top, and choose iCloud Settings from the menu. The iCloud Settings page includes a navigation bar at the top, and you should be in the Settings category by default. You can now change settings in any of several categories. Any changes you make take effect immediately.

Settings

The Settings category is the main place for making changes.

Change Personal Information

You can adjust certain pieces of personal information:

- **Photo:** Your iCloud account can have a photo or picture associated with it, which other iCloud members will see in certain contexts (such as in email messages). To add or change a photo, first click Change Apple ID Photo under the Photo heading. Then, to replace the image, click "Browse your device for a new image," locate the graphic you want, and click Upload. You can also drag the slider to adjust the zoom level, drag the photo around to reposition it, or change the rotation in 90° increments. When satisfied, click Save.

- **Manage your Apple ID:** To make changes to your Apple ID settings (such as choosing a new password or changing the security settings), click the appleid.apple.com link under Apple ID Settings. This opens the Apple ID site in a new tab or window.

Sign Out of All Browsers

If you think you may still be signed in to iCloud on another browser and you want to be sure all browser sessions (including the current one) are closed, click Sign Out of All Browsers.

Manage Apps That Can Look You Up

You can use the Settings category to choose which apps let other people find you by your email address for the purpose of sharing documents. (This is just like the iCloud settings/preference pane in macOS after clicking the iCloud Drive Options button). To do so, click Manage Apps under the Look Me Up by Email heading.

Your iCloud Storage

Click Your iCloud Storage in the navigation bar at the top to view a multicolored graph, as well as a high-level breakdown of major storage categories. That graph's color corresponds to a breakdown by major storage category below it. Apple provides more information when you view your storage details from a desktop computer or iOS/iPadOS device, and I talk about that in Check and Modify Your Storage Usage, later in this chapter.

Data Recovery

iCloud keeps a copy for 30 days of several kinds of data: Contacts entries, Calendar events, Safari bookmarks, and iCloud Drive files. If you deleted a create item in one of those categories, you can recover it within that period.

Click Data Recovery in the navigation bar at the top of the iCloud Settings page, then click a tile: Restore Files, Restore Contacts, Restore Calendars, or Restore Bookmarks.

Next, follow these steps:

- **For files:** Select the checkbox next to each file you want to restore (or Select All to select everything). Then click Restore.
- **For other data:** Unfortunately, you can't restore an individual contact, event, or bookmark—or even an individual calendar. You can only restore your Contacts data as a whole, your combined Calendar data as a whole, or your bookmark data as a whole, to one of its previously archived states. To do so, locate the item you want to restore and click the Restore link to its right.

The selected item(s) will be restored to all your devices where that data type is enabled. For contacts, calendars, reminders, and bookmarks, iCloud archives your current data (as it exists before restoration) so you can return to your current state later if need be.

Change Payment Settings

If you subscribe to either of iCloud's optional paid add-ons (iTunes Match and additional storage), you may need to change your billing address and credit card information at some point.

- **On a Mac:** In Ventura or later, open the App Store app, choose Store > Account, click Account Settings at the top, and then click the Manage Payments link. In Monterey or earlier, go to System Preferences > Apple ID (Monterey or earlier) and click Payment & Shipping.
- **On an iOS or iPadOS device:** Tap Settings > *Account Name* > Payment & Shipping.

Check and Modify Your Storage Usage

I cover both free iCloud accounts and paid iCloud+ subscription tiers in iCloud Feature Changes and Use iCloud+, among other places. But regardless of your account type, there's one more element to highlight here about managing storage and data. iCloud lets you check how

much storage you're using and delete certain data from the cloud on a Mac, PC, or iOS/iPadOS device.

To check and modify storage usage on a Mac or PC:

1. In Ventura or later, go to System Settings > *Account Name* > iCloud and click Manage at the top; in Monterey or earlier, go to System Preferences > Apple ID > iCloud and click Manage; or in Windows, open the iCloud app and click Storage.

   In the dialog that appears (**Figure 50**), each category on the left shows how much data it's storing online; to see how that data breaks down, select the category. The Backups category shows the total storage consumed by backups for all your mobile devices, while an app that uses iCloud Drive displays the total amount of cloud storage that it uses.

2. To delete any item (such as the backups of a particular iOS or iPadOS device), select it and click the Delete button; or, to delete all the data stored in the cloud for a particular app, select it and click Delete All Data, Delete All Files, Turn Off and Delete, or Delete from iCloud and All Devices.

   Read the warning that the data will be immediately deleted from *all* your devices (including this one), and click Delete to confirm.

Note: Deleting app-specific data is unavailable in iCloud for Windows.

Deleting items here removes the corresponding items from iCloud, which means they become almost immediately unavailable on all your devices.

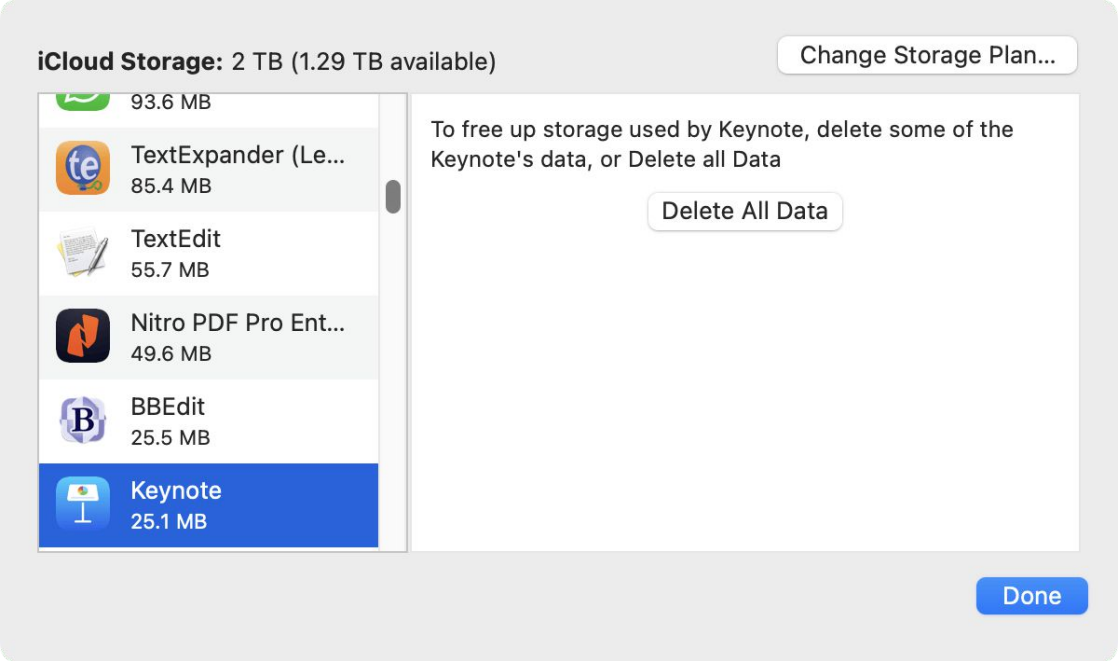


Figure 50: This dialog shows all the types of data you're storing and lets you delete specific items.

To check and modify storage usage on an iOS or iPadOS device:

1. Tap Settings > *Account Name* > iCloud.

   Figure 51: To stop any app on this device from using iCloud for storage, tap Show All if necessary, and turn off the switch next to that app.

2. To delete data already stored in iCloud for an app, tap Manage Account Storage followed by the app's name. Then, for apps where the Manage Storage screen is listing individual items, swipe left on an item and tap Delete to remove just that one item. Or, to delete *all* the data from that app, tap Delete Documents & Data, Delete Data, or Turn Off & Delete from iCloud.

Note: To read about deleting existing backups and turning off backups of certain data types, see Activate and Configure iCloud Backup.

Manage Account Recovery

Apple provides three separate ways to assist when you lose access to your Apple ID, threatening access to your synced iCloud data among other things.

The first, the Apple ID Recovery Key (covered next), doesn't tie in closely with iCloud—it's about your own ability to maintain access to your Apple ID account and, by extension, any iCloud data stored or synced that linked to. The second and third are about other people:

- iCloud Data Recovery Service lets you appoint trusted people who can help you recover access only to your iCloud data if you can't regain access to your Apple ID account. See Set Up Account Recovery Contacts, ahead.
- Digital Legacy allows people you choose to gain access to your iCloud after you are dead. Some people may find this desirable; others may want their data to be buried with them. See Set Up Digital Legacy Contacts, later in this chapter.

Decide on Using an Apple ID Recovery Key

The Apple ID Recovery Key provides a more secure and alternative path to standard "account recovery"—Apple's lowercase term—to regain access to an Apple ID if your account is locked or a password changed without your involvement.

Standard account recovery can be triggered if you can't log in to your Apple ID account and don't have the devices or other information necessary to reset the password. Apple relies on a combination of time, people, and information: they delay access to deter identity theft, have humans involved in the process, and require details like the credit card number associated with your Apple ID account.

Switching to the Recovery Key method allows you to reset your password immediately—as long as you possess the Recovery Key set at the time you enrolled via your Mac or iOS/iPadOS device and one or more elements associated with two-factor authentication.

You need either:

- Your Recovery Key and a passcode-protected trusted device (as enrolled in two-factor authentication), *or*
- Your Recovery Key, a trusted phone number, and any Apple device (not necessarily your own)

The advantage to a Recovery Key is that you can reset your account instantly and don't need to involve Apple.

The disadvantage? If you lose the 28-digit key or don't have a trusted device or access to a trusted phone number, your Apple ID is unrecoverable forever.

Apple provides general details in this support document on setting up and using a Recovery Key. For far more details on setting up, removing, and other parameters around the Recovery Key, see Glenn Fleishman's book, *Take Control of Your Apple ID*.

Set Up Account Recovery Contacts

Apple recognizes that not everybody is a technical expert. The addition of Recovery Assistance (previously called iCloud Data Recovery Service) acknowledges that and makes it easy for you to pick trusted people—family, friends, colleagues, or an attorney, say—to provide an additional way to recover access to iCloud data if you're in a pickle.

The scenario Apple describes is if you forget your password or "get locked out of your account," a rather passive description. Your account can be locked for several reasons, including if someone with no connection to you attempts to log in and enters the wrong password too many times. If you can't reset your password or prove to Apple that your account should be unlocked, you might otherwise permanently lose access to your synced iCloud data.

While this might be an issue for contacts, calendar entries, and email, it's probable you have a full copy of them on one or more of your devices. But with iCloud Photos, you might have optimized storage turned on for all your devices, and the only full-resolution copies are

stored in your iCloud.com account—that would be a real and permanent loss.

When you add people as recovery contacts, they receive information (after accepting an invitation if they're not in your Family Sharing group) that they can store digital or print as a sheet of paper providing details they would need to help you recover later. They should treat this information as secret and privileged—so choose wisely.

Note: Your recovery contacts cannot obtain access to your data with the information you give them. They can only provide a form of confirmation to you that you provide to Apple in order to regain access to your data.

Setting up this recovery method requires all your devices to running at least these versions of Apple's operating systems: iOS 15, iPadOS 15, watchOS 8, and macOS 12 Monterey. You also have to be 13 or older (or 14, 15, or 16 or older in some countries) and have two-factor authentication enabled on your Apple ID account.

To enroll in iCloud Data Recovery Service, follow the steps Apple provides in this support document.

Set Up Digital Legacy Contacts

Similar to iCloud Data Recovery Service, Digital Legacy lets you choose people as legacy contacts who could later gain access to most of your iCloud data—but not your media purchases, subscriptions, payment information, or keychain contents. Apple provides a full list of what will be available and what won't. The process is identical for inviting people to be a contact. They likewise receive information that they would have to present to Apple later—along with an image of the death certificate.

Note: Apple doesn't say whether a legacy contact can access extra data types that are encrypted end-to-end if you Use Advanced Data Protection. Apple may still be updating the relevant support pages.

A legacy contact visits a special Digital Legacy website to notify Apple of your demise and provide documentation. Apple creates a special legacy Apple ID and makes all data available through that account. Access to the legacy account remains in place for three years after the first legacy contact sets it up.

Warning! Consult with your prospective legacy contacts about your intent. Apple notes any legacy contact can opt to delete your data permanently at any time without coordinating with other contacts.

To enable digital legacy, you need at least iOS 15.2/iPadOS 15.2 or macOS 12.1 Monterey installed on the device you use to enroll; all devices don't have to be up to date. You also need two-factor authentication enabled on the Apple ID account. Digital Legacy is available to people at least 13 years old (or at least 14, 15, or 16 in certain countries).

For full details on setting up your digital bequeathal, see Apple's support document.

Manage iCloud Security and Privacy

Throughout this book I've mentioned security and privacy issues connected to iCloud. But because of high-profile incidents involving data theft from iCloud users and increasing privacy concerns overall, I want to end the book with some advice about protecting your data.

In the digital world, the words security and privacy are often used interchangeably, but even though they're related, they're not the same. *Security* is freedom from danger or harm, whereas *privacy* is freedom from observation or attention. Someone can harm you by impersonating you, taking over your account, stealing or deleting data, and so on; security makes such harm less likely to occur. On the other hand, if someone reads your email messages, sees your photos, or learns your location without your permission, you've lost your privacy.

It's possible to have security without privacy and vice versa. But when it comes to a service like iCloud, it turns out that all the steps you might take to improve your security also protect your privacy. For example, choosing an excellent password reduces the likelihood that a stranger might log in to your account and thereby obtain access to your private data.

Start by enhancing your security with a good password and two-factor authentication, discussed just ahead. If you plan to buy a used Mac or iOS/iPadOS device, read Check Activation Lock first to make sure you aren't buying a locked device—potentially one that was stolen. And you can take additional steps to Protect Your Privacy, such as turning off syncing for sensitive data and using a passcode on your iOS and iPadOS devices.

Tip: Although I hit the main points about iCloud security and privacy here, you'll get a more complete story in Glenn Fleishman's *Take Control of Your Apple ID*. Two other books Glenn wrote also address privacy and security on Apple platforms: *Take Control of Securing Your Mac* and *Take Control of iOS & iPadOS Privacy and Security*.

Choose a Good Password

The password associated with the Apple ID you use for iCloud is incredibly valuable. With your username and that password, someone can see all your email, contacts, calendar events, backed up photos—even your current location. And, using Find My *Device,* anyone with your password can remotely lock or wipe your Macs and iOS/iPadOS devices!

So, choosing a good password is a big deal. You don't want a password that any other person can guess, or that an automated cracking tool could uncover by brute force. For complete details on what makes one password stronger than another, how an attacker might go about guessing your password, and techniques for increasing password strength while not overtaxing your memory, read my book *Take Control of Your Passwords*. If you don't have time to read that whole book, at least follow these tips:

- **Make your iCloud password unique.** Don't use your iCloud password for any other site or service, because if your password for one site is compromised through a database breach or other leak, every account that uses the same password is at risk.
- **Choose a good password.** Apple requires that your iCloud password be *at least* eight characters long and include uppercase and lowercase letters and at least one digit. But I strongly suggest choosing a password that improves upon the minimum requirements: pick either a long, memorable one with dashes or punctuation between words, or a randomly generated one that has a lot of variation, including some punctuation. Better still, use a password

manager—see the next bullet—to create and store a long, random one that you never have to enter by hand (or finger).

- **Use a password manager.** Apps such as 1Password, Dashlane, and Bitwarden can create strong, random passwords for you, store them, sync them across your devices, and fill them in automatically. That takes most of the effort and pain out of using good passwords.

If you want to change your password now, go to appleid.apple.com, click Manage Your Apple ID, and follow the instructions.

Use Two-Factor Authentication

Even the longest, strongest, most random password provides no security if someone else finds out what it is. Perhaps someone watches over your shoulder as you type your password at your local coffee shop. Or maybe a spam email message persuades you to enter your password on a phishing site that looks almost exactly like the Apple site. Or an as-yet-undiscovered security bug or exploit exposes your password to an attacker.

In fact, it gets worse—an attacker may not need your password at all! When you set up your Apple ID, you were likely prompted to choose a few security questions and enter their answers. These questions (like "What was the name of your first pet?" or "What is the name of your oldest niece?") are supposed to be easy for you to remember but hard for an attacker to guess—so that if you forget your password, Apple can ask you these questions as a secondary means of verifying your identity. Answer correctly, and you can reset your password.

Trouble is, someone *pretending* to be you can claim to have forgotten your password—and if that person calls Apple and correctly answers your security questions, your account could be compromised. And (assuming you answer the security questions truthfully) it's surprisingly easy for a skilled attacker to find or guess the answers.

Apple, like many other companies (including Dropbox, Facebook, and Google) offers an optional method to bolster your security by adding a

verification step that requires a piece of information tied to a device you own. Called a second factor, this code or proof of possession of something prevents someone from gaining access to your stuff solely with a password.

Max the Factors

In the security world, each kind of verification is a *factor*, which can be something you know (like a password), something you have (like a hardware token or mobile device), or something you are (a biometric marker, like a fingerprint, face, or retina scan). In most consumer forms, like Apple's, your account login with a password is one factor; a verification code sent via an app, operating system, text, or automated voice call is the second.

In Apple's version, you first log in with your user name and password in any place your Apple ID is required. After successfully entering that information, you're prompted twice: first to allow login attempts and then to enter a code. Any Apple device associated with your iCloud account can display both the prompt and the code.

Apple used to make two-factor authentication optional, but they have increasingly tightened the screws, requiring it for many services and features. It's hard to avoid enabling now, and once you do, it can never be turned off for your Apple ID account after a two-week grace period.

Apart from the enhanced security two-factor authentication provides, Apple offers a carrot and a stick for enabling it:

- **The carrot:** Setting up two-factor authentication eliminates the security questions from your Apple ID—an attacker can no longer use them to break in to your account. So that's a lovely bonus.
- **The stick:** You must activate two-factor authentication in order to Use App-Specific Passwords, and Apple *requires* app-specific passwords for third-party apps (such as Outlook and BusyCal) that connect to your iCloud account.

Enable Two-Factor Authentication

Two-factor authentication for your Apple ID is available to all iCloud subscribers who have at least one device running iOS 9 or later or 10.11 El Capitan or later. It was probably automatically enabled on your account during an operating system upgrade or when setting up a new Apple ID account over the last few years.

With two-factor authentication feature enabled, here's what you'll see:

- The device you use initially to enable two-factor authentication becomes a *trusted device*. That means you'll use this device (along with your password) to authenticate your next device, which then also becomes trusted. You can have several trusted devices.
- When you sign in on a device that isn't yet trusted, you enter your username and password as usual, but then two things happen:
    - You must click or tap an Allow button that appears automatically on all your existing trusted devices and shows the area from which the new device is trying to sign in. (Once you click or tap it on one device, the alert disappears on the rest.)
    - On the new device, you must enter a six-digit verification code that's displayed automatically on the trusted device on which you just tapped Allow. (If you don't have access to a trusted device, you can receive your verification code via SMS or an automated spoken voice phone call instead.)
- Apps that access your iCloud account's email, contacts, and calendars must Use App-Specific Passwords.

In case you don't have two-factor authentication already turned on, here's how to enable it:

- **On a Mac:** In Sonoma or later, go to System Settings > *Account Name* > Sign-In & Security, or in Ventura, go to System Settings > *Account Name* > Password & Security, click Password & Security; then click "Turn on." In Monterey or earlier, go to System Preferences > Apple ID > Password & Security, click Security, enter your

password, and click Continue, then click Turn On Two-Factor Authentication.

- **On an iOS or iPadOS device:** In iOS 17/iPadOS 17 or later, go to Settings > *Account Name* > Sign-In & Security, or in iOS 16/iPadOS 16, go to Settings > *Account Name* > Password & Security. Then tap Turn On Two-Factor Authentication.

On all operating systems, follow the prompts. These may include answering two of your three security questions and supplying your date of birth and a phone number; you can select either "Text message" (for SMS) or "Phone call" (for an automated voice call).

Once you complete these steps, two-factor authentication is on, which means that in various situations you may be prompted for your password and verification code (or, in some cases, an app-specific password) on devices already signed in to your iCloud account.

The same is also true in Safari when you log in to the Apple ID site or iCloud.com, with the notification alert appearing even on the device that you're using to log in. If you have Touch ID enabled on any equipped device or Face ID on an iPhone, Apple often relies on the enhanced security of that biometric factor to bypass sending a verification code.

Why Your Browser Can Be Verified from the Same Device

I know it's counterintuitive to how it seems security works: why is it OK for the *same trusted device* on which you're logging in to an Apple service via a browser to also deliver you an alert and even provide a verification code? Because you've proven the chain of custody.

If you're logged in to a trusted device, then you have physical proximity (in most cases) and demonstrated you have the password or biometrics to access it. The browser, however, is untrusted by Apple when you visit one of their sites. You establish trust for the browser connection "out of band," by using Apple's method to contact one of your trusted devices to show you have custody of the device! That's also why Apple can bypass the code with Touch ID or Face ID, because you've demonstrated you must have physical possession (something you have) and are a human who can unlock it (something you are)—two factors!

After you complete this step, you're signed in to your iCloud account; and, if the process took place outside a browser, your new device also becomes trusted.

To learn more about Apple's two-factor authentication system, read:

- Apple's support articles Two-factor authentication for Apple ID and Availability of two-factor authentication for Apple ID.
- *Take Control of Your Apple ID*, by Glenn Fleishman, which contains detailed, practical steps for setting up and using this feature, along with a look at what to do if you lose a device or forget your password.

Use a Security Key

A security key is usually a little hardware dongle that connects via USB—though some may use NFC or Lightning—that you use as a second factor in lieu of a numeric code to prove your identity. Security keys rely on public-key cryptography linked with a particular site you enrolled the key at. This can provide greater security than a text code, though with added inconvenience (and the risk of losing it). Security keys can be purchased inexpensively from a variety of vendors.

Although security keys are only for people with exceptional needs—and thus beyond the scope of this book—Apple provides instructions for choosing and using such a key with your Apple ID account in About Security Keys for Apple ID. Glenn Fleishman provides even more details in *Take Control of Your Apple ID*.

Use App-Specific Passwords

Enabling two-factor authentication also activates another security feature: app-specific passwords. This feature applies to all third-party apps that access your iCloud account's email, contacts, and calendars, such as Outlook, Thunderbird, BusyCal, and BusyContacts. (No other kinds of data can be accessed by third-party apps or services.) It does not apply to Apple apps, like Mail, Safari, and Find My, although it was once required for FaceTime, Game Center, and iMessage accounts in Messages.

Your ordinary iCloud password no longer works for these apps when two-factor authentication is active. Instead, you have to create unique passwords for each of them.

Apple makes you go through the two-factor authentication process before you can create app-specific passwords, so you're still protected by both steps. And once you've created such a password for a given app on a given device, you're never prompted to do so again for that app on that device—unless you change your security settings.

To generate an app-specific password:

1. Open a third-party app that connects to your iCloud account. (If you're doing this for the first time after enabling two-factor authentication, you may see an error message stating that your password wasn't accepted.)
2. Locate the app's settings for username and password (often in the Preferences window). Leave the window open.
3. Visit appleid.apple.com in your browser, sign in, and verify your identity or use Touch ID or Face ID to validate your login.

4. Click Sign-In and Security in the sidebar and then click App-Specific Passwords.
5. Click the plus + icon to generate a password.
6. Label the entry with something descriptive, so you can later figure out which app it belongs to (such as `BusyCal iMac`) and click Create.
7. The new password appears on screen. Copy it and paste it (or type it) into the window you opened in step 2.
8. Click Done to dismiss the dialog.

> **App-Specific Passwords Appear Once Ever**
> Apple provides no way to view your app-specific passwords after you dismiss the window in which it's shown—you can see their *descriptive names,* but not the actual passwords. So you might want to record the password in a safe place, such as your password manager, to avoid the extra step of regenerating a new password for this app if you need to enter it again later.
>
> Apple doesn't retain the unencrypted form of these passwords, either; they store only a cryptographic transformation of the password it created.

If a device is lost or stolen, you may later want to revoke an app's password. Doing so prevents that app, on that device, from accessing your iCloud account. Follow the same steps, but when you get to step 4, instead click Edit and then click View History. You can then click the minus ⊖ icon and click Revoke to delete a single password. Click "Revoke all" and confirm it to wipe them all.

> **Note:** See the Apple support article Sign in to apps with your Apple ID using app-specific passwords for further details.

Check Activation Lock

iOS and iPadOS devices, Intel Macs with T2 chips (see list here), Macs with M-series processors, and Apple Watches can use a feature called

Activation Lock, which means no one can turn off Find My *Device*, erase the device, or reactivate it under a different account without the owner's iCloud username and password. The intention of Activation Lock is to make devices unattractive to thieves by preventing anyone but the rightful owner from setting it up for their own use.

You won't see a separate switch for enabling Activation Lock on supported devices; rather, it's a side-effect of having Find My *Device* turned on (see Activate Find My).

Warning! For Activation Lock to work on a Mac, the computer must also be running Catalina or later. An Intel Mac must have both Secure Boot enabled and "Disallow booting from external media" set. An M-series Mac must be set to Full Security; two-factor authentication has to be enabled as well. Full details appear on this Apple support page.

If you're thinking of selling or donating a device that may have Activation Lock enabled, be sure to turn off Find My *Device* first in order to disable Activation Lock. If you're thinking of buying a used Apple device that supports Activation Lock, make absolutely sure you follow the instructions on these pages, or you may wind up with an expensive metal brick:

- Apple Watch
- iOS and iPadOS devices
- Mac

Disable Activation Lock with Apple's Help

Apple can disable Activation Lock if you go to an Apple Store or certified third-party resellers and repair shops with a receipt from the original purchase that shows your name and the serial number of the device along with some form of acceptable ID that shows you are that person. They don't advertise this fact, but you can find the information in oodles of first-hand forum postings and articles.

However, the key issue here is that you have to both have that receipt and *be* the original purchaser. Apple apparently won't provide assistance for one of their hardware devices that's been sold.

Protect Your Privacy

At the risk of stating the obvious, any data you sync or share via iCloud travels over the internet and (with a few exceptions) is stored on Apple's servers. All your data is encrypted while in transit, most of it is also encrypted while on Apple's servers, and some of it is encrypted end-to-end—meaning that no one, not even Apple, can read it without access to one of your devices that you've unlocked. (For complete details, read Apple's article iCloud data security overview.)

Apple always uses end-to-end encryption for the contents of iMessage conversations, iCloud Keychain, Health data, the contents of the People & Pets album, Safari history, and some other items—no matter what, they're quite safe by being essentially locked to keys stored on your devices and nowhere else.

At the other extreme, a few kinds of iCloud data—namely, email, contacts, and calendars—can't be encrypted on the server at all using interoperable standards, because that would prevent them from working with the existing worldwide infrastructure for those services.

In the middle are several types of data that Apple encrypts, by default, only on the server, but not end-to-end: iCloud Backup, iCloud Drive, Photos, Notes, Reminders, Safari Bookmarks, Siri Shortcuts, Voice Memos, and Wallet passes.

The problem with "only on the server" encryption is that on your end, it's protected only by your password, and Apple holds the key to decrypt it on their end. So, that encryption is irrelevant if:

- Someone guesses or discovers your password, and you don't have two-factor authentication enabled
- Due to a security breach, a disgruntled employee, or other factor, data from your account is exposed
- Apple is legally obligated to provide your data to law enforcement or a government agency (read Apple's Privacy page, and in particu-

lar the Transparency Report that's linked from that article, for details)

You can and should take steps to avoid the first problem, as I explain next. But as for the second and third, the only solution (short of avoiding the use of iCloud altogether) is to use only those services for which end-to-end encryption is enabled.

Fortunately, you can now opt to expand the list of your iCloud data types that use end-to-end encryption to everything except email, contacts and calendars, making *almost* of your iCloud data incredibly secure. For that, you need a new feature called Advanced Data Protection; see Use Advanced Data Protection, ahead.

Take Basic Privacy Steps

Everyone can and should take several simple, concrete steps to protect the privacy of their iCloud data from everyone else—including hackers, thieves, and snoops. Here's what I recommend:

- **Use a good password.** I already counseled you to Choose a Good Password as a security measure, but I wanted to reiterate that point for the benefit of anyone not reading linearly.
- **Enable two-factor authentication.** Likewise, if you Enable Two-Factor Authentication, you'll make it much harder for anyone to obtain your private data. They have to steal not just your password, but also either steal a device (and be able to unlock it) or hijack your phone number (to get an SMS or voice verification token).
- **Use a passcode on iOS/iPadOS devices.** If your iOS or iPadOS device is locked with a passcode, anyone who steals or finds the device won't be able to access its contents. You can even configure your iOS or iPadOS device to erase its contents after 10 unsuccessful passcode attempts. Turn on a passcode in Settings > Face ID & Passcode (or Touch ID & Passcode).
- **Use FileVault.** The Mac's built-in FileVault feature protects your Mac by preventing any access to your Mac without having an ac-

count password. On old Intel Macs and external startup drives, FileVault also adds drive encryption.

Note: Intel Macs with a T2 security chip and all M-series Macs automatically encrypt the startup volume at a hardware level whether FileVault is turned on or not, but the drive is automatically decrypted when the Mac powers up. FileVault adds login protection before decryption occurs, protecting the drive's contents at that stage.

Beyond that, you have a couple of choices. If your situation permits, enable Advanced Data Protection as I describe ahead in Use Advanced Data Protection. If for any reason you can't or don't want to do that, yet you have extremely sensitive data that you want to keep entirely out of iCloud, turn off the relevant feature(s) in System Settings/System Preferences > Apple ID > iCloud (Mac), Settings > *Account Name* > iCloud on an iOS or iPadOS device, and the iCloud app in Windows. There are two parts to this:

- **Disable syncing of sensitive data.** You might want to disable any or all of the following categories if they contain potentially sensitive data:
  - *Contacts:* This includes the personal contact information for the people in your address book, plus the VIPs and previous recipients from Mail.
  - *iCloud Drive:* Data in this category includes documents (including automatically saved new documents in iCloud-enabled apps), Mail settings (signatures, flag names, rules, smart mailboxes, blocked senders, and muted conversations), and text abbreviations (see Use In-App Data Syncing).
  - *Photos:* This includes iCloud Photos and any shared albums.

Note: You'll notice that email is not in this list. That's because email is inherently insecure, and disabling Mail for iCloud won't change that. Although end-to-end email encryption does exist, it's not a feature offered in iCloud at this time.

- **Consider local backups for iOS and iPadOS devices.** Although iCloud Backup is handy (see Back Up and Restore iOS/iPadOS Data), if someone obtains your iCloud username and password, that person can restore your backed-up data to another device and thus obtain all your photos, email, contacts, iMessages, and so on. (The risk is greatly decreased, of course, if you use two-factor authentication.)

Note: iMessages sent among Apple devices using the Messages app are encrypted by the devices. But if you use Messages in iCloud, a password to decrypt archived messages are stored as part of your iCloud backup, making them vulnerable unless you enable Advanced Data Protection as described ahead.

As a less-convenient but more-secure alternative, you can turn *off* iCloud Backup and instead back up your iOS/iPadOS device to a Mac or PC using the Finder (or iTunes for Windows). See How to back up your iPhone, iPad, and iPod touch for details.

Tip: Although I haven't tried it and thus can't vouch for it, IDrive Online Backup claims to back up your iOS or iPadOS device's contacts, calendars, photos, and videos securely—all without going through iCloud.

Use Advanced Data Protection

If you want the convenience of cloud syncing, storage, and backup for more types of iCloud data, you have another option: a feature called Advanced Data Protection (ADP). Simply put, when you enable this feature, Apple uses end-to-end encryption for nearly all the data that would otherwise have been encrypted only at rest on the servers: iCloud backups, Find My *Nouns*, iCloud Drive, Messages in iCloud, Notes, Photos, Reminders, Siri Shortcuts, Voice Memos, and Wallet passes. (As I mentioned earlier, email, contacts, and calendars remain unencrypted, even with this feature enabled.)

If that arrangement sounds great—and it does!—why wouldn't Apple just make it the new default? Why shouldn't everyone just turn it on immediately?

Well, it does introduce a couple of issues. First, you have to meet quite a few requirements to be able to use ADP; many of us don't. Second, even if you do meet the requirements *and* enable it, some of your data will become harder for *you* to access when using the iCloud website. If you can meet the prerequisites and don't care about that extra bother, *by all means* turn on this feature!

Before you can enable ADP, all of the following must be true:

- Every device signed in to your iCloud account must be running a fairly recent version of its operating system: at least macOS 13.1 Ventura, iOS 16.2, iPadOS 16.2, tvOS 16.2, watchOS 9.2, and HomePod 16.2. If a device is too old to be updated to one of these operating systems, you must either remove it from your iCloud account or forgo enabling ADP.
- You must have two-factor authentication enabled for your Apple ID (refer back to Use Two-Factor Authentication).
- Passcodes or passwords must be set for all your Macs and iOS, iPadOS, and watchOS devices.
- Initially, ADP was available only for people whose iCloud account was based in the United States, although it has now rolled out to other countries.
- You must have a recovery key or a recovery contact—or both. (See Decide on Using an Apple ID Recovery Key and Set Up Account Recovery Contacts.)

Once you've met all those criteria, you can enable ADP. But read ahead first in Use ADP-Protected Data on the iCloud Website, to understand how this will affect accessing your data on the iCloud website.

Enable Advanced Data Protection

To enable ADP, go to System Settings (macOS) or Settings (iOS/iPadOS) > *Account Name* > iCloud > Advanced Data Protection. Click Turn On (macOS) or tap Turn On Advanced Data Protection (iOS/iPadOS). If you have any devices signed in to your iCloud account that don't meet Apple's criteria, a message tells you, for each of those devices, whether you can update it or must remove it from your account.

Assuming that's all good, Apple next verifies your account recovery setup:

1. A message reminds you that Apple will no longer be able to recover any of the data you're about to protect—that's your responsibility now. (And if you haven't already set up one or more recovery methods, you're prompted to do so now; you can't proceed otherwise.) Click or tap Review Recovery Methods.
2. If you have a recovery key, enter it, click or tap Next, and enter your device's password or passcode when prompted.
3. When you see the message "Advanced data Protection is On," click Done.

Apple also sends email to your iCloud.com address confirming that ADP is now enabled.

Note: If you ever want to disable ADP (for example, to enable an older device to connect to your account), go back to System Settings (macOS) or Settings (iOS/iPadOS) > *Account Name* > iCloud > Advanced Data Protection. Click Turn Off (macOS) or tap Turn Off Advanced Data Protection (iOS/iPadOS) and follow the prompts.

Use ADP-Protected Data on the iCloud Website

Since Apple is always able to decrypt information like email, contacts, and calendars, it's not a problem to display that data for you when you log in to the iCloud website. The same is true, with iCloud's default account settings with ADP disabled, for data in iCloud Drive, iCloud Photos, Notes, and Reminders.

But when you turn on ADP, those kinds of data become encrypted end-to-end. Apple no longer has the encryption key, so how can you access them in a browser?

Fortunately, Apple offers a method that provides temporary access by relying on a combination of in-browser encryption and one of your trusted devices (which holds your private encryption key).

To enable temporary access to ADP-protected data on the iCloud website, follow these steps:

1. In your browser, go to www.icloud.com and log in. A banner appears explaining that ADP is enabled and what to do.
2. Click the menu  icon and then click the app you want to use. When you do this, Apple sends all your trusted devices a request to access that app's data.
3. On one of your trusted devices, click or tap Allow Access. An alert then appears on all your trusted devices telling you that you've enabled access to that data type *for one hour*.

Although Apple says you must repeat this procedure for each app protected by ADP, I found in testing that it didn't always prompt me for each kind of additional data. However, you have to request access again if you continue using any of the apps for longer than an hour.

Note: If you turned off Access iCloud Data on the Web in System Settings (macOS)/Settings (iOS/iPadOS)> *Account Name* > iCloud, you won't be able to access any of your data on the iCloud website, whether or not ADP is enabled.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

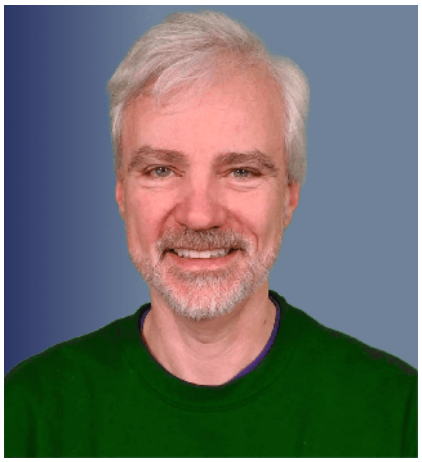
Ebook Extras

You can access extras related to this ebook on the web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Access the book in both PDF and EPUB formats. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook

If you bought this ebook from the Take Control website, it has been automatically added to your account, where you can download it in other formats and access any future updates.

About the Author and Publisher



Joe Kissell is the author of more than 60 books and hundreds of articles about technology. In 2017, he also became the publisher of Take Control Books, when alt concepts—the company he runs along with his wife, Morgen Jahnke—acquired the Take Control series from TidBITS Publishing Inc.'s owners, Adam and Tonya Engst. Before he began writing full-time in 2003, Joe managed software development for a living. He holds a bachelor's degree in Philosophy and a master's degree in Linguistics.

In his hypothetical spare time, Joe likes to walk, cook, eat, and practice t'ai chi. He lives in Saskatoon, Saskatchewan, Canada, with Morgen and their sons. To contact Joe about this book, send him email and *please* include `Take Control of iCloud` in the subject. You can also sign up for joeMail, his low-volume mailing list, follow him on Mastodon (@joekissell), or visit his blog at JoeKissell.com.

Credits

- Publisher: Joe Kissell
- Editor: Glenn Fleishman (seventh through ninth editions); Tonya Engst (earlier editions)
- Cover design: Sam Schick of Neversink
- Take Control Logo: Geoff Allen of FUN is OK

Also by Joe Kissell

Click any book title below or visit our web catalog to add more ebooks to your Take Control collection!

Take Control of 1Password: Slowed down by entering passwords repeatedly? Learn how to let 1Password do the heavy lifting.

Take Control of Apple Mail: Learn the ins and outs of Apple's email app in macOS, iOS, and iPadOS.

Take Control of Automating Your Mac: Work more efficiently on your Mac with time-saving shortcuts of all kinds.

Take Control of Backing Up Your Mac: Protect your valuable data with a complete, bulletproof backup strategy.

Take Control of DEVONthink 3: Master this powerful information management tool.

Take Control of the Mac Command Line with Terminal: Master your Mac's command-line interface and learn basic Unix skills.

Take Control of Ventura: Discover what's new in macOS 13, and get all the information you need to upgrade safely.

Take Control of Your Digital Legacy: Make sure your important digital information is preserved for future generations.

Take Control of Your Online Privacy: Learn what's private online (not much)—and what to do about it.

Take Control of Your Paperless Office: With your Mac and scanner, you'll clear the chaos of an office overflowing with paper.

Take Control of Your Passwords: Overcome password overload without losing your cool.

Copyright and Fine Print

Take Control of iCloud, Ninth Edition
ISBN: 978-1-990783-25-8

alt concepts, 419 8B-3110 8th St. East, Saskatoon, SK S7H 0W2 Canada

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, they should buy a copy. Your support makes it possible for future Take Control ebooks to hit the internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and alt concepts have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither alt concepts nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It's just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren't Apple: This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are registered trademarks or service marks of Apple Inc. If you're into that sort of thing, you can view a complete list of Apple Inc.'s registered trademarks and service marks.