



TAKE CONTROL OF

Backing Up Your Mac

by **JOE KISSELL**

\$14.99

5TH
EDITION

Table of Contents

Read Me First	5
Updates and More	5
Basics	6
Settings vs. Preferences	6
What's New in Version 5.2	7
What Was New in Version 5.1	7
What Was New in the Fifth Edition	8
Introduction	10
Quick Start.....	12
Plan a Backup Strategy	14
Understand Joe's Basic Backup Strategy	14
Why Create Versioned Backups?	16
Why Create Bootable Duplicates (or Not)?	19
Why Use External Storage?	32
Why Use Multiple Partitions (or Not)?	33
Why Automate Backups?	34
Why Keep Multiple Backups?	36
Why Store Backups Offsite?	37
Can Cloud Sync Simplify Backups?	38
Can You Reduce Your Backup Footprint?	41
Reassess Your Backup Strategy	43
What's New in Mac Backups	43
Factors to Reevaluate	45
Choose Local or Network Backups	52
Local Backups	53
Network Backups	53
Local vs. Network Backups: Joe's Recommendations	57
Choose Backup Software	60
Decide Whether Time Machine Is Best for You	60

Explore Versioned Backup Features	64
Choose Another Versioned Backup App	79
Choose a Duplicate App	83
Choose Backup Hardware	85
Choose Hard Drives, SSDs, or Both	85
Decide on Capacity	87
Decide on a Storage Configuration	91
Hardware You Should Probably Avoid	103
Prepare Your Backup Drive	106
Choose the Right Partition Map Scheme	106
Decide How Many Partitions and Volumes to Make	108
Decide How to Format Your Partitions	111
Configure Your Drive	113
Configure and Use Time Machine	118
Time Machine Basics	118
Configure a Destination	121
Exclude Files from Time Machine	126
Manage Your Time Machine Schedule	130
Restore Data with Time Machine	134
Delete Files from a Time Machine Backup	145
Use a Mac as a Time Machine Server	147
Use a Single Backup Disk with Multiple Macs	152
Use Power Nap	153
Migrate to a Larger Time Machine Disk	154
Avoid or Solve Time Machine Problems	156
Use Other Versioned Backup Software	159
Arq Tips	159
Carbon Copy Cloner Tips	161
ChronoSync Tips	165
QRecall Tips	169
Retrospect Tips	169
Test Your Versioned Backup	172

Create and Use a Duplicate	174
Give the Destination Volume a Unique Name	175
Create a Data-Only Duplicate	175
Create a Bootable Duplicate	180
Test a Bootable Duplicate	189
Store an Extra Backup Offsite	195
Use an Extra Hard Drive or SSD	195
Use a Cloud Backup Service	197
What to Do When Disaster Strikes	205
Restore Individual Files	205
Use Your Bootable Duplicate	207
Restore a Disk from a Bootable Duplicate	209
Restore a Disk from a Data-Only Duplicate	212
Manage Your Media	215
What to Do When Your Disks Fill Up	215
Consider Long-Term Archive Storage	217
Consider Special Backup Needs	220
Back Up and Restore Notes	220
Back Up Digital Photos	224
Deal with Huge Volumes of Data	227
Back Up a NAS	232
Back Up Data from the Cloud	234
Back Up While on the Road	236
Back Up an iPhone or iPad	240
Back Up Windows Files and Volumes	242
About This Book	250
Ebook Extras	250
About the Author and Publisher	251
Credits	251
Also by Joe Kissell	252
Copyright and Fine Print	254

Read Me First

Welcome to *Take Control of Backing Up Your Mac, Fifth Edition*, version 5.2, published in December 2025 by alt concepts. This book was written by Joe Kissell and edited by Caroline Rose.

The data on every Mac should be backed up to protect against theft, hardware failure, user error, and other catastrophes. This book helps you design a sensible backup strategy, choose and configure the best backup hardware and software for your needs, and understand how to make your backups as painless as possible.

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.

Copyright © 2025, Joe Kissell. All rights reserved.

Updates and More

You can access extras related to this ebook 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.

Basics

In this book, when I use the term *disk* by itself, I generally mean your Mac’s primary internal storage device—whether that’s a mechanical hard drive, an SSD, or other solid-state storage. (Apple, after all, still uses the term “Macintosh HD” as the default name for your Mac’s startup volume, even when it’s not stored on a hard drive.) A *drive* is a physical device for storing data; a single drive can comprise one or more *volumes*, or logical storage devices. The volume that contains the copy of macOS currently used to start up, or *boot*, your Mac is your *startup volume*, sometimes called the *boot volume* or *boot drive*. I’ll specify *hard drive* when I need to talk specifically about the little boxes with spinning platters, and I’ll occasionally use *hard disk* when talking about the logical storage space on a hard drive.

I also talk about duplicating your startup volume onto another disk in such a way that you can boot from the duplicate. The more formal name for such a disk is a *bootable duplicate*, but they’re commonly called *clones*, and I sometimes use that term too. Any volume can be cloned, even a non-boot volume, but the context should make clear when I’m talking about the sort of clone you can boot from.

This book covers both Intel-based Macs and Macs that use Apple silicon chips. I generally refer to the latter as “M-series Macs” since they use chips such as the M1, M2, M3, M4, and so on.

Settings vs. Preferences

In macOS 13 Ventura, Apple replaced System Preferences with System Settings, and in most apps what was formerly a Preferences window is now a Settings window. In this book, I sometimes use a shorthand like “go to Finder > Settings/Preferences” or “open System Settings/System Preferences” to reflect these two possibilities; when the details are significantly different, I spell them out separately for Ventura or later and for macOS 12 Monterey or earlier.

What's New in Version 5.2

Version 5.2 brings the book up to date with changes that occurred in macOS Sequoia 15.3, and is now completely current with macOS 26 Tahoe (even though Tahoe itself made no changes to the ways Mac backups work). Changes in this version include the following:

- Mentioned in several places that a bug affecting bootable duplicates in macOS Sequoia 15.2 was fixed in version 15.3; see, for example, [Why Create Bootable Duplicates \(or Not\)?](#)
- Made a clarification in [The Signed System Volume](#) about updating the Data volume on bootable duplicates
- Pointed out in [Decide Whether Time Machine Is Best for You](#) that support for Time Capsules will end with macOS 27
- Throughout [Create a Bootable Duplicate](#), added links to the Tahoe installer as necessary
- Added a brief mention of Parachute Backup in [Back Up Data from the Cloud](#)

What Was New in Version 5.1

Version 5.1 updated the book to cover recent changes in macOS 15 Sequoia. The most significant changes were:

- Rewrote much of [Why Create Bootable Duplicates \(or Not\)?](#), [Choose a Duplicate App](#), and [Create and Use a Duplicate](#) to revise my advice, since Apple made this process much more difficult in macOS 15.2
- Added mention of Thunderbolt 5 where appropriate throughout the book, but especially in [M-Series Mac Changes](#), [Choose an Interface](#), and [USB 3.x, USB4, USB-C, and Thunderbolt 3, 4, and 5](#)
- Added the sidebar [What Is Time Machine Cleaning Up?](#)

- Revised [Back Up and Restore Notes](#) to include additional details and techniques

What Was New in the Fifth Edition

This edition brought the book up to date with changes in macOS and third-party apps as of early 2024. It also dropped coverage of Mojave and Catalina, meaning it covered only macOS 11 Big Sur, macOS 12 Monterey, macOS 13 Ventura, and macOS 14 Sonoma. Those changes involved a fair amount of surgery throughout the book. In addition, I made the following changes:

- Removed mentions of certain apps that are either no longer available or incompatible with recent versions of macOS, and apparently no longer being developed: Back-In-Time, Déjà Vu, and Mac Backup Guru
- Simplified the advice in [So, Should I Make a Bootable Duplicate?](#)
- Rewrote [Why Use Multiple Partitions \(or Not\)?](#) to clarify my current thinking
- Relocated and shortened the discussion of how what Dropbox does is almost, but not quite, like a backup; see the sidebar [Dropbox's Kinda-Sorta Backups](#)
- Rewrote [What's New in Mac Backups](#), and updated [Factors to Reevaluate](#), to reflect changes since the previous edition of the book
- Removed the discussion of Cubbit Cell devices, which are currently unavailable for sale
- Added a new topic, [Backing Up Cloud-Only Data with Carbon Copy Cloner](#), to [Carbon Copy Cloner Tips](#)
- In [ChronoSync Tips](#), added information on a new range of supported cloud storage services, revised advice on handling packages, and added instructions for using ChronoSync to back up files stored only in the cloud

- In [Option D: Create a One-Time Bootable Duplicate, Update the Data Volume Duplicate, and Create a Data-Only Duplicate](#), revised the instructions for Carbon Copy Cloner, SuperDuper!, and Chrono-Sync
- Added a new topic, [Back Up and Restore Notes](#), about Apple's Notes app
- Updated the [online appendixes](#) with the latest details, as needed

Introduction

The first time I thought seriously about backups was right after I lost a valuable, irreplaceable piece of data—an email message sent to me by a celebrity—as the result of a disk crash. That was nearly 30 years ago, and ever since, I’ve practiced and preached diligent Mac backups. After all, Macs may be fantastic computers, but they’re still subject to electronic and mechanical failure, theft, human error, and many other problems that could cause anyone to lose data.

My first book about Mac backups was published in 2004. Back then, I found that many readers still needed convincing that hard drives were better for backups than CDs, that backups ought to run without manual intervention, and even that backups were worth the bother in the first place. When Apple introduced Time Machine as a built-in backup feature in Mac OS X 10.5 Leopard in 2007, backups became easier to perform and harder to ignore. Although Time Machine isn’t the only way (or even, necessarily, the best way) to back up your Mac, it has done more to popularize the concept of Mac backups than anything that came before it, and it set a new standard for usability.

If you don’t back up your Mac at all, or if you do so only haphazardly, this book will help you over the initial hump of getting started with a solid backup plan. Having great backups no longer requires lots of money, time, or technical expertise. You can be up and running in a couple of hours, after which things will run mostly on their own, and the only time you’ll have to think about your backups is when it comes time to restore lost data—something you won’t have to fear anymore.

On the other hand, if you already have a backup system, it might be time for you to update it. Technology changes rapidly, and you could find that a different approach (or newer hardware, software, or cloud services) will serve your current needs better.

This book explains how to develop a solid backup strategy, what your hardware and software choices are, how to set everything up, what pitfalls you may encounter, and how to restore your data if disaster

strikes. Rather than explore every alternative, I guide you gently but firmly into a fairly narrow set of options that should yield excellent results for the vast majority of Mac users.

Before we get started, I need to mention a few qualifications:

- This book is primarily for people who need to back up either a single Mac or a small network—not for system administrators who need to back up dozens or hundreds of machines. As a result, I say little about the high-end equipment and enterprise-grade software used for backing up large networks.
- I don't cover command-line software such as `cp` or `rsync`. My goal is to make the process as simple as possible—ideally, without requiring you to know anything about Unix or using the Terminal utility to configure and interact with your backups.
- Although I provide basic guidance for performing backups with several popular apps, I can't give you foolproof, step-by-step instructions for setting up every backup app you might use. But by the end of this book, you should have enough information to determine, with the help of your software's documentation, the settings that will produce your desired outcome.
- The fourth edition of this book covered operating systems all the way back to OS X 10.14 Mojave, but since Mojave is now more than six years old—and extensive details for older versions made the book harder to read—I now include specific instructions only for macOS 11 Big Sur through macOS 12 Tahoe (although much of this material applies generally to Macs running older versions of macOS). Also, although I don't cover Windows extensively, [Back Up Windows Files and Volumes](#) discusses backing up Windows when it's running on your Mac.
- I've put certain information, like feature comparisons of Mac backup hardware and software, in [online appendixes](#).

Quick Start

First things first: most people do *not* need to read this entire book! There's a lot of detail here for those who want it, but if your backup needs are unexceptional, you can skim much of this material. Even so, don't skip [Plan a Backup Strategy](#), which outlines the basics and prepares you for the hardware, software, and setup advice I give later.

For all readers, the following points should help you understand what I cover where, and which parts you're most interested in.

Decide on a backup strategy:

- If you don't already have a backup system in place, start at the beginning, with the [Plan a Backup Strategy](#) chapter. You'll soon [Understand Joe's Basic Backup Strategy](#), which revolves around three key components: *versioned backups* (containing multiple copies of files as they existed at various points in time), an optional *bootable duplicate* (a complete, bootable copy of your startup volume), and *offsite storage* (in case something wipes out your Mac and the backup media sitting right next to it).
- If you're already backing up your Mac (even if your strategy is based on recommendations from an earlier version of this book), read [Reassess Your Backup Strategy](#) to find out what's new and which [Factors to Reevaluate](#) to determine whether any changes are in order.

Assemble the components:

- Consider whether the best approach for your situation is to store your backups on hard drives (or other devices) directly connected to your Mac(s), or on network servers or appliances. See [Choose Local or Network Backups](#).
- Decide whether Time Machine is a good match for your needs, and if not, select a different app to perform versioned backups. Read [Choose Backup Software](#) for a feature overview, then pick an option

noted in [Explore Versioned Backup Features](#) or consult the [online appendixes](#) for details and sources.

- [Choose Backup Hardware](#)—such as a hard drive or two, and/or a network storage device—to store your backups on.
- [Prepare Your Backup Drive](#) with the right number and type of partitions and volume formats for the types of backups you want to do.

Set up your backups:

- If you've chosen to use Time Machine for versioned backups, read [Configure and Use Time Machine](#). Otherwise, see [Use Other Versioned Backup Software](#) to learn how to configure a versioned backup and verify that you can retrieve stored files.
- Make a bootable copy of your startup volume, schedule it for regular updates, and test it to make sure it works with the advice in [Create and Use a Duplicate](#).
- One way or another, [Store an Extra Backup Offsite](#)—either by physically moving backup media or by signing up for an online backup service.

Address problems and unusual situations:

- If your disk dies, your Mac is stolen, or an important file goes missing, don't panic; read [What to Do When Disaster Strikes](#).
- After months or years of backing up your Mac, you may run out of space on your backup disks or become concerned about the long-term viability of your backup media. Discover what to do about this in [Manage Your Media](#).
- Find out how to deal with backup needs that don't fit neatly into the duplicate or versioned categories in [Consider Special Backup Needs](#). As appropriate, read [Back Up and Restore Notes](#), [Back Up Digital Photos](#), [Deal with Huge Volumes of Data](#), [Back Up While on the Road](#), and [Back Up Windows Files and Volumes](#).

Plan a Backup Strategy

This book focuses on the strategies, hardware, and software I can most heartily recommend based on extensive personal and professional experience. I'm going to give you my expert advice, and although that will include areas in which you can choose among several options, in this book I'm framing the decision simply: I'll be telling you, "Today's choices are lasagna, fried rice, and ratatouille (and by the way, my lasagna is pretty darn good)" instead of saying, "Choose anything from the *Joy of Cooking*."

If you follow my suggestions, you can rest easy knowing that your data is safe—and you won't break the bank or waste days of work setting things up. And even if you opt out of any of the three main components I recommend in my basic backup strategy, you'll do so with both eyes open.

Understand Joe's Basic Backup Strategy

Since I started writing about Mac backups in 2004, the basic strategy I've followed and recommended has consisted of three main components. Now, for the first time, I'm altering my practices and recommendations. There are still three components, but one of them is now optional, and carried out differently than before:

- **Versioned backups:** Use Time Machine or another backup app to store *versioned backups*—multiple copies of each file, so you have both the latest version and numerous previous versions. Update your versioned backups incrementally (copying only new or changed data each time) at least daily, and preferably more often.
- **Bootable duplicate:** *Optionally*, depending on your circumstances, create a bootable duplicate of your startup volume on an external SSD or hard drive, and update it regularly. (I explain my reasoning in [Why Create Bootable Duplicates \(or Not\)?](#).) If you

choose not to create a bootable duplicate, you might want to add something else in its place or make other alterations to your strategy; see [Alternatives to Bootable Duplicates](#).

- **Offsite copies:** Keep at least one backup copy of your important data somewhere safely away from your Mac—in another building, at least, and perhaps even in another part of the world (in the latter case, by using a cloud backup service).

Tip: Later in this chapter I also talk about how cloud-based file *syncing* services (which are different from backup services) can supplement your backup strategy. See [Can Cloud Sync Simplify Backups?](#).

In some cases, you might be able to use a single backup drive for both versioned backups and a bootable duplicate—for example, by dividing it into two partitions (see [Why Use Multiple Partitions \(or Not\)?](#)) or by using backup software that creates a *versioned* bootable duplicate (see [Bootable Duplicates with Versioning](#)). Otherwise, you'll want a separate drive for each type of backup, though even if you use a combined drive, you might choose to add a second drive for extra peace of mind. I also discuss using online storage for versioned backups, which counts as an offsite copy and could reduce the amount of hardware you must buy.

Furthermore, my goal is to automate nearly all of this so that, to the extent possible, backups happen in the background without your having to remember anything, press buttons, run apps, or intervene in any other way. And I'll try to make even the setup process as painless as possible.

Because I want you to understand why I make the recommendations I do and how the whole process works, I spend just a few pages describing my suggested backup strategy in more detail and outlining what choices you'll make along the way. (If you're already on board with my basic strategy, you can skip these details and go straight to [Choose Backup Software](#).) As you read, I suggest that you jot down a few notes about hardware that you may want to purchase, software features that seem important to you, or special questions relating to your circumstances to keep in mind as you continue reading the book.

Reassess Your Backup Strategy

If you're reading this book for the first time, you may not already have a backup strategy, in which case feel free to skip this chapter for now and move on to [Choose Backup Software](#). But I suggest returning to this chapter in a year or so, by which time you may benefit from its recommendations. If you already have a backup strategy, though, read on to learn the best way to proceed.

Just as I reevaluate my own stance every so often, you too should periodically reassess your backup strategy in light of new information. If you read an earlier incarnation of one of my books and set up your backup system based on what I said years ago, I'd like you to reassess your strategy right now. In any case, put a reminder on your calendar for one year from now to come back and (re)read this chapter, then reassess your strategy again!

I want to begin with a brief “state of the union” look at what has changed in the last two years or so (as I write this in early 2025), and then say a few words about [Factors to Reevaluate](#) as you reconsider your backup strategy, both now and every year. Feel free to skim this chapter to see which topics are applicable to you; you might want to jot down a few notes about those topics to help you identify items to concentrate on as you reformulate your backup approach.

What's New in Mac Backups

In the past few revisions of this book, I used this space to talk about changes in hardware and software that could affect the way you think about and perform backups—things like the Mac's transition to the APFS file system, split system volumes, and M-series processors, plus changes in third-party backup offerings. Now all those things seem like old news, and although any of them may require you to rethink parts of

your strategy if you're just now moving from much older hardware to a new Mac (or a much older version of macOS to a newer one), that material is already integrated into other parts of the book, so I won't repeat it here.

Instead, I want to mention a few notable changes since the fourth edition of this book was published in 2023:

- **SSD prices continue to drop.** It wasn't so long ago that I dismissed the idea of using SSDs as backup destinations on the grounds that they were far too expensive. As of early 2025, the cost for lower-capacity models tended to run about \$50–75 per terabyte; I've seen 2 TB external drives for under \$100 and 4 TB drives for under \$200. (For that matter, I've seen a 16 TB external SSD for about \$1,100—or \$68.75 per terabyte. Even larger SSDs exist, up to [100 TB](#), but at those sizes the per-terabyte cost goes way back up; the 100 TB drive, for instance, costs around \$40,000, or \$400 per terabyte.)

Note: As of late 2025, prices for SSDs have risen significantly, due to high demand for the chips they use. I expect that before long the market will sort itself out and prices will drop again.

To be sure, even at \$100, a 2 TB SSD costs far more than a hard drive of similar capacity, but seeing prices drop roughly in half over the course of a year is certainly encouraging.

- **You have more and better options for backing up stuff *from the cloud*.** I've remarked in earlier versions of this book that when you store stuff in a folder that syncs to the cloud (using, for example, iCloud Drive or Dropbox) and you permit the service to offload from your Mac local copies of items you're not actively using, you run into a backup problem. Apps like Time Machine can't back up those files because they aren't actually on your Mac, even though you may still see icons for them. This can put users in a bind: either avoid features like Optimize Mac Storage (iCloud Drive) and “online-only” (Dropbox) and risk running out of disk space, or turn them on and risk being unable to back up some of your files.

Choose Local or Network Backups

Before you go too far in designing a backup plan, you should take a moment to ponder whether you'll back up to a local storage device (that is, one connected *directly* to a Mac with a cable) or to a device located somewhere else on your (wired or wireless) network—or both.

Note: In recent years, a new term has sprung up: *DAS* (direct-attached storage), to contrast with *NAS* (network-attached storage). Any storage device that plugs directly into your Mac via Thunderbolt or USB (a single hard drive or SSD, a RAID, or another multi-drive enclosure) is a DAS; any storage device you access over a wired or wireless network in your home or office is a NAS.

In years past, I assumed that in most cases each Mac would have one or more backup drives of its own, and that network backups were mainly for locations with more than a few Macs or with exceptional backup needs of some sort. Now, however, network-based backups of one sort or another seem like a good fit for a wider range of people.

In this brief chapter, I help you think through the pros and cons of both local (DAS) and network (NAS and server-based) backups. Whichever approach (or combination of approaches) you choose, your decision will help inform which software and hardware you use; I discuss those choices in the next two chapters.

Note: This decision affects only the backups in your home and office and is thus independent of whether to use a cloud backup service (see [Use a Cloud Backup Service](#), later).

Local Backups

With a local backup, you plug your hard drive or other storage device into a Mac and let your backup software run. (Time Machine starts automatically, as do some third-party backup apps; other software requires either an explicit schedule or that you manually run backups after attaching a drive.) When it's done, you can disconnect the storage device and hook it up to another Mac if you have one.

If you want to make a bootable duplicate, you'll need a local storage device (preferably an SSD). For versioned backups, meanwhile, the main advantage of a local storage device is speed, at least if you're using a fast interface (such as Thunderbolt 4). However, as I explain just ahead, nowadays the speed difference versus a fast network is small enough that most people won't notice it.

The downside to local storage is that backups and restorations can occur for a given computer only while the drive is connected, and if you forget to connect the drive, you won't have a backup at all. You may end up doing a lot of plugging and unplugging—and more so if you're moving a single drive between computers. And, if you have a laptop and you actually use it on your lap (as opposed to a desk), having an external drive attached can be a real hassle.

Keep in mind that local storage need not be a single external hard drive or SSD; it could be a RAID or other multi-drive assembly—any type of DAS. See [Decide on a Storage Configuration](#) for further details.

Network Backups

In a network backup, one computer (or other device) typically functions as the backup server—the machine to which your backup drive(s) are physically connected. Files from your other computers (which function as clients) are copied over the network onto each backup drive.

If you have multiple computers—especially if one or more of them is a laptop that gets moved around a lot—network backups can be far more

Choose Backup Software

In this chapter, I help you decide which backup software to use for versioned backups and which to use for bootable duplicates. (You might choose the same app for both purposes, but as we'll see, the best app for one type of backup isn't necessarily best for the other.)

Decide Whether Time Machine Is Best for You

Time Machine is the backup software built into macOS starting with OS X 10.5 Leopard. Apple's goal was to make backups as easy as possible, and compared to anything that came before it, Time Machine is certainly much simpler to set up and use. Anything that makes backups easier and thereby encourages more people to use them gets a gold star in my book.

Tip: Howard Oakley at The Eclectic Light Company has written a number of [articles about Time Machine](#), taking readers deep into its inner workings. If you're curious about how Time Machine works (and doesn't work) in extensive technical detail, check out Howard's site.

However, Time Machine is not ideal for everyone. Before getting into the details about setting up and using it (see [Configure and Use Time Machine](#)), I tell you what I like and dislike about it and look at a few situations in which it may be the wrong solution. For those people who need different software, I point you in the right direction with a discussion of features to look for and examples of other versioned backup apps I can recommend.

Without a doubt, Apple got a lot of things right about Time Machine:

- The user interface is elegant, if unusual.
- I love how I can restore files right in the Finder, without opening a separate app.

- I appreciate the fact that my MacBook Pro can back up files even when I'm away from my desk and a Time Machine volume (see [Local Snapshots](#), later in this book).
- Time Machine supports encryption for both local and network backups, and also lets me choose multiple destination disks (which it rotates among automatically).
- You can back up either to a locally attached hard drive or to any of several kinds of network destinations (including a NAS device and another Mac), whatever you find most convenient.
- Starting in Big Sur, Time Machine can back up to either Mac OS Extended (HFS Plus) or APFS destinations—and both performance and disk usage under APFS are way better. (For help deciding which is best, see [Decide How to Format Your Partitions](#).)

All that is fantastic, and in many respects better than the competition. And yet, having used Time Machine since day one, I'm less than fully enthusiastic about it, for several reasons:

- When using Mac OS Extended destination disks, Time Machine's approach doesn't scale well to large amounts of data. For one thing, backing up lots of large files takes far longer than it should, because with Mac OS Extended, Time Machine always copies entire files rather than use delta encoding as many other backup apps do (see [Delta Encoding](#), ahead). And, even if your Time Machine drive has plenty of storage space, by the time you have several months' worth of backups the sheer number of files seems to bog down Time Machine and make simple operations unreasonably sluggish. Using APFS for your backup disk solves many of these problems, while creating some new ones; see [Decide How to Format Your Partitions](#).
- Although Time Machine is supposed to be almost invisible in ordinary use, it sometimes uses up far too many system resources—again, most often when the destination is Mac OS Extended. If I notice the fan on my wife's MacBook Pro start to wail, it's usually because Time Machine happens to be running.

Choose Backup Hardware

Depending on what you decided in [Choose Local or Network Backups](#), you're likely going to need one or more external hard drives or SSDs for your backups. (Even if you use network storage or a cloud backup service, you'll need a separate external drive if you want to store a bootable duplicate.) You can find hard drives and SSDs with every imaginable combination of capacity, speed, interface, and case design—as well as devices that incorporate more than one hard drive or SSD in a single unit—and the selection changes constantly.

In this chapter, I start by addressing the increasingly important question of hard drives versus SSDs. Then I walk you through the calculations of how much storage capacity you'll need for backups (see [Decide on Capacity](#)). Next, in [Decide on a Storage Configuration](#), I help you understand whether you should be looking for standalone drives, a RAID or other multi-drive DAS enclosure, a NAS or similar network storage device, or drives you'll hook up to another computer on your network that will function as a backup server. I end the chapter with a few thoughts on [Hardware You Should Probably Avoid](#).

Tip: In this chapter I'm concerned exclusively with hardware for storing backups, but if you want to know about storage devices more generally—or if you want far more information than I can provide here about file systems, RAIDs, and other storage topics—I recommend reading Jeff Carlson's [Take Control of Your Digital Storage](#).

Choose Hard Drives, SSDs, or Both

In previous editions of this book, I took it for granted that almost all readers would use external hard drives for local backups. But the landscape is changing, and that's no longer the obvious default. As I explained in [The APFS File System](#) and elsewhere, changes in macOS now make SSDs all but obligatory for bootable duplicates. And, al-

though prices are still quite high for larger SSD capacities, some people may even consider SSDs reasonable choices for versioned backups.

The nice thing about using hard drives was that most people could purchase a single, inexpensive, high-capacity drive and partition it to use for both bootable duplicates and versioned backups (see [Decide How Many Drives to Buy](#), later in this chapter). But because APFS is now mandatory, and booting from an APFS-formatted hard drive is excruciatingly slow, that approach no longer makes sense. Instead, the approaches you should now consider are the following:

- **Hard drive(s) only:** If you've read [Why Create Bootable Duplicates \(or Not\)?](#) and determined that bootable duplicates aren't sufficiently important to you to merit the additional cost of SSDs and the hassle of using multiple drives for your backups, you can choose one or more hard drives to hold your versioned backups and call it a day. Even if they're formatted as APFS, mechanical hard drives are generally fast enough for backing up and restoring files; you just don't want to *boot* from them.
- **SSD(s) only:** If you do want to make bootable duplicates, if speed and convenience are your top priorities, and if you can afford it given the amount of data you have (see [Decide on Capacity](#), next), you can buy one or more high-capacity external SSDs and partition them for both bootable duplicates and versioned backups. (Or, if you prefer, buy one SSD for duplicates and another for versioned backups.) Note that if you ever intend to boot an M-series Mac from your SSD, you should buy a Thunderbolt 3, 4, or 5 SSD and not just a USB 3.x model, even though both use the USB-C connector.

Note: If you need more capacity than you can get from a single SSD, consider a RAID or other multi-disk enclosure designed for SSDs rather than hard drives. See [Consider RAIDs and RAID-Like Tech](#).

- **Hard drive(s) plus SSD(s):** If you want to make bootable duplicates but can't quite afford enough SSD storage to cover versioned duplicates, you can buy a smaller-capacity SSD plus a smaller-capacity hard drive.

Prepare Your Backup Drive

You’ve just unpacked your brand-new hard drive(s) and/or SSD(s), and you’re ready to get busy backing up. You might be able to plug in a drive and start working with it immediately, but that depends. Some hard drives and SSDs come formatted for Windows computers, for example, while others might be formatted for a Mac—or not at all. Some come preloaded with utilities and demo software. Some might use the wrong partition map scheme for your computer, possibly preventing Time Machine from being able to see or use the drive. And if you’re not going to plug a hard drive directly into your Mac, but rather put it inside, or attach it to, a network storage device, still other considerations apply.

In short, because each situation is different, you should take a few minutes, before you do anything else, to make sure any new drives you’ve obtained are configured correctly for your needs.

If you have a NAS, its built-in drive(s) should come preconfigured as needed, and it should also be able to format any external drives you connect to it, so you don’t have to follow the configuration steps in this chapter for that device (but skip ahead to [Network Backups](#) for additional factors to consider). However, you must still follow the steps outlined here for the external drive you use to store your bootable duplicate, if any.

Note: For a RAID or other locally attached, multi-drive enclosure, the rules are highly variable; consult the manufacturer’s instructions or website to learn whether or how you must format the drives.

Choose the Right Partition Map Scheme

Your external drive contains a tiny block of information called a *partition map* or *partition table* that describes things like how many volumes the drive has, how large they are, and where they’re located. The way information is stored in this little block of data is called the *parti-*

tion map scheme, and the choice of scheme is crucial to how the drive can be used. Windows PCs generally use a scheme called the Master Boot Record (MBR) Partition Table; pre-Intel Macs used a scheme called Apple Partition Map; and Intel-based and M-series Macs by default use a newer and more advanced scheme, GUID Partition Map. The partition map scheme affects the entire drive, regardless of how many partitions it has or how those partitions are formatted.

Some hard drives and SSDs are configured at the factory to use the MBR scheme, because that's common in Windows. In some cases, if you plug such a drive into your Mac, it will work as a backup drive without any intervention. However, Time Machine may be unable to use volumes larger than 512 GB on an MBR-partitioned drive, you can't create APFS partitions on an MBR-partitioned drive, and MBR also gives you less flexibility in partition sizes.

Therefore, I recommend that, just to be on the safe side, you manually repartition any new disk *before* handing it over to Time Machine or otherwise using it for backup purposes. As you do, you should check the partition map scheme to make sure it's GUID Partition Map, and change it to that if not, because changing the scheme requires erasing all the data on the disk; that's obviously something best done before you've copied any of your personal files onto the drive.

Although there are a couple of ways to check your drive's partition map scheme, I recommend using Disk Utility (and then just leaving it open, because you'll be using it to format your drives in just a moment; see [Configure Your Drive](#)). Follow these steps:

1. Open Disk Utility (in [/Applications/Utilities](#)).
2. Choose View > Show All Devices.
3. In the list on the left, select your external drive. (The drive name may have icons indented beneath it for one or more volumes; if so, be sure to select the drive as a whole, at the topmost level.)
4. Look near the bottom of the window next to "Partition Map" (**Figure 3**). It should say GUID Partition Map or Master Boot Record.

Configure and Use Time Machine

If you've decided to use Time Machine for versioned backups, read this chapter to learn everything you need to know about that. (If you've chosen other software for versioned backups, skip ahead to [Use Other Versioned Backup Software](#).) We'll walk through the details of setting up Time Machine, backing up and restoring files, and other activities.

As I explained in [Decide Whether Time Machine Is Best for You](#), my enthusiasm for Time Machine is not what it once was. I still use it, but not as my only form of versioned backups, and not on all my Macs. Therefore, even though this chapter is fairly long, I make no attempt to be comprehensive here, especially when it comes to troubleshooting.

Time Machine Basics

Time Machine has three visible components:

- A pane in System Settings (Ventura or later; **Figure 7**) or System Preferences (Monterey or earlier; **Figure 8**).
- An app found in the Applications folder, in Launchpad, and, optionally, in the Dock (**Figure 9**).
- A Time Machine  menu in the main menu bar.

Note: You can enable or disable this menu. In Ventura or later, go to System Settings > Control Center, scroll to the bottom, and, under Menu Bar Only, choose Show in Menu Bar or Don't Show in Menu Bar from the Time Machine pop-up menu. In Monterey or earlier, use the "Show Time Machine in menu bar" checkbox in System Preferences > Time Machine.

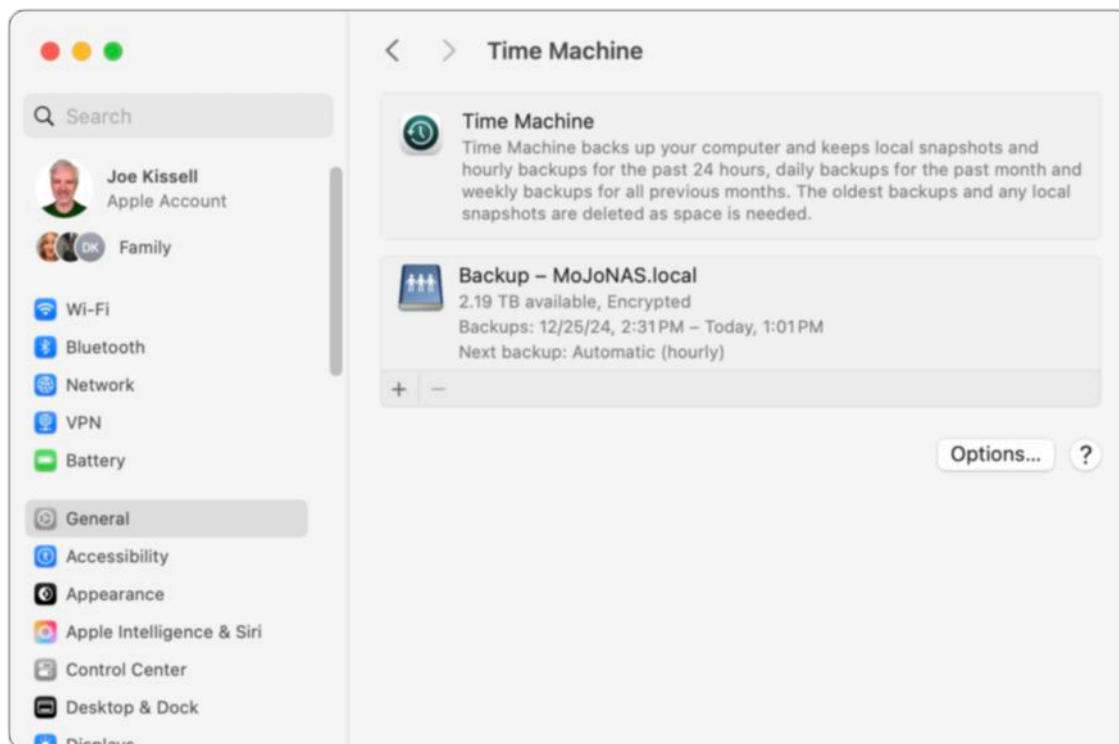


Figure 7: In Ventura or later, configure Time Machine in System Settings > General > Time Machine.

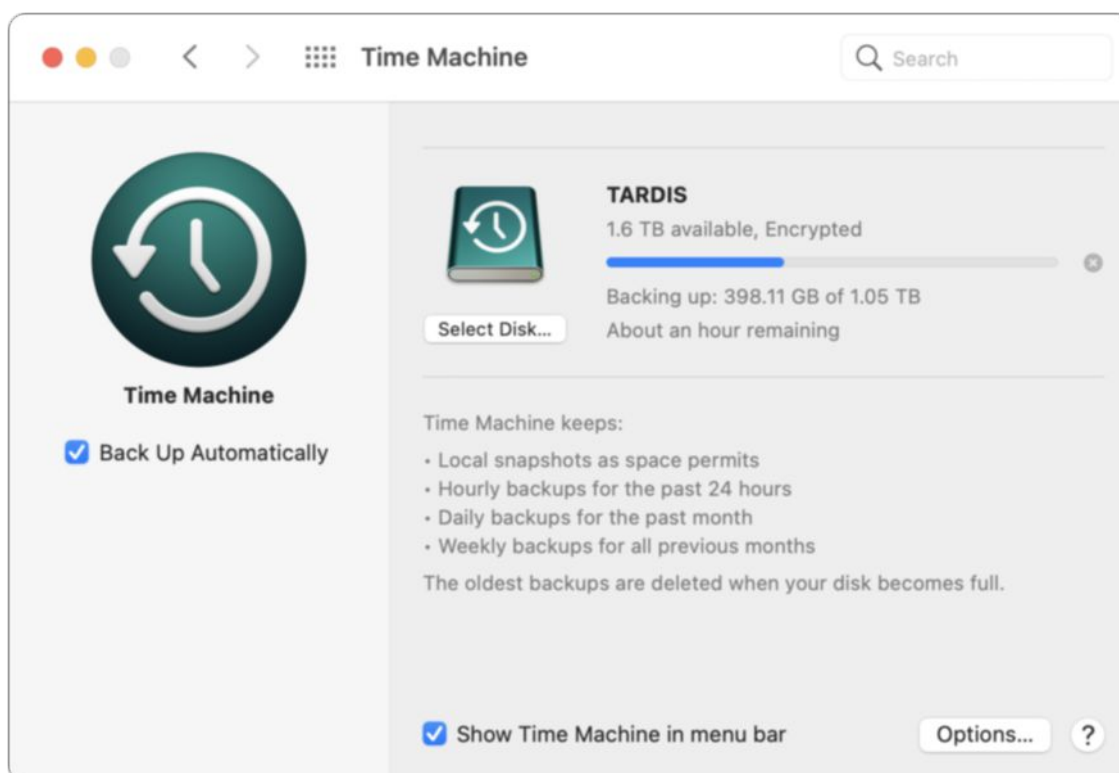


Figure 8: In Monterey or earlier, configure Time Machine in System Preferences > Time Machine.

Use Other Versioned Backup Software

If you’ve decided to create versioned backups using an app other than (or in addition to) Time Machine, set that up now. I wish I could give you step-by-step instructions for using each one of those apps, but that would take too many pages (and you can read the app’s documentation for help). Instead, I want to give you a few tips for each of several good choices, all of which I mentioned back in [Choose Another Versioned Backup App](#). Although I’ve used and can recommend each of the apps I mention here, I don’t pretend that this is an exhaustive list. There are many other excellent options, and you can read about them in the [online appendixes](#).

Later in the chapter, I also give several general pointers about things like power management and testing versioned backups.

Arq Tips

Arq is a popular choice for people who want the benefits of cloud storage but also want greater control over their data than cloud backup providers offer—and the freedom to choose inexpensive cloud storage. If you use Arq for your versioned backups (or are considering doing so), keep the following in mind:

- **All cloud storage is not created equal.** Arq supports lots of different cloud storage providers, some of which are so inexpensive that they seem almost too good to be true. As I point out later, in BYOS (Bring Your Own Software) Internet Backups, some cloud storage services limit your upload rate—perhaps only after you’ve transferred a given amount of data or number of files in a certain month. The result can be that backups are disappointingly slow. So read your provider’s fine print and try some speed tests with a few gigabytes of data before you start to upload files by the millions.

- **Backups run on fixed schedules.** Compared to, say, Backblaze, which backs up your data continuously, Arq can run any given backup no more often than once per hour. So, if you're moving to Arq from a competitor that backs up files as often as you save them, you might need to adapt your thinking and behavior, because Arq won't make such frequent copies. (In addition, running less frequently means each backup is likely to take longer.) You can, however, work around this somewhat by setting up multiple backups to the same destination; make them identical except for the time. (For example, make the first one hourly on the hour and the second one hourly on the half hour.)
- **Mind your settings.** Arq helps you avoid unexpected expenses by pruning old backups according to your preferences and letting you set a budget (the maximum amount of storage space your backups can occupy, or the maximum price you're willing to pay for storage). So review the settings carefully for each destination (pruning and budget options are on the Retention tab) and make sure you're taking advantage of Arq's money-saving features.
- **Arq supports local backups too.** Although Arq is best known as a backup app to be used with cloud destinations, you can also choose local hard drives, network volumes, or NAS devices as destinations. That makes it much more versatile than most cloud backup apps and lets you use the same app for both local and cloud-based versioned backups. Alas, Arq lacks the capability to make bootable duplicates, so you'll still need a separate app for that.

Note: Although I haven't tested them in any detail, a number of newer backup apps are broadly similar to Arq (in the sense of focusing on versioned backups to user-supplied cloud storage, but with the option to do local backups too). If that's the general path you want to take, you might also consider looking into [Duplicacy](#) and [Duplicati](#).

Create and Use a Duplicate

For many years I used the term *duplicate* as a shortened form of “bootable duplicate,” since the whole point of a duplicate used to be that you could boot from it. Now, however, considering the numerous reasons one might have a duplicate that’s *not* bootable, I’ve broadened my use of the term to include non-bootable duplicates (which, when speaking of startup disks, include only the read/write Data volume). This chapter covers both types. We begin with the non-bootable variety, and then (in [Create a Bootable Duplicate](#)) talk about the bootable sort.

To review:

- *Bootable* duplicates stored on an external SSD let you get back to work quickly if your internal storage fails, give you a useful troubleshooting tool, and make upgrading to a new version of macOS safer, *but* they’re a real pain to create, especially in recent versions of macOS, and even more of a pain to update. (Remember, too, that if the internal SSD on an M-series Mac dies completely, you’ll be unable to start up the Mac, even from an external, bootable SSD.) You can’t make a bootable duplicate by copying files in the Finder; you need a special utility, of which I describe a few options in this chapter.

Warning! You cannot store duplicates of two drives on the same volume, even if you put them in separate folders; the result will not be bootable. They must be on separate partitions or on entirely separate drives.

- *Non-bootable*, or *data-only*, duplicates are exact copies of everything on your disk *except* macOS itself. They can still be used to restore a full disk from a backup or to migrate to a new Mac; you just can’t start your Mac from them (though, as I explain ahead, it is possible to turn a data-only duplicate into a bootable duplicate after the fact).

Carbon Copy Cloner, ChronoSync, and SuperDuper! can make one-off duplicates or run automatically on a schedule, updating the duplicate with just the files that are new or changed since the last run and deleting files on the destination that are no longer on the source disk. (In Big Sur and later, these updates are limited to the Data volume, while a separate procedure is needed to update macOS on a bootable duplicate.) I recommend scheduling duplicates to update at least once a week (daily is even better).

Give the Destination Volume a Unique Name

If you didn't do so when partitioning the drive (see [Configure Your Drive](#)), rename the destination volume for your bootable duplicate so that it's different from your Mac's regular startup volume. This will help eliminate confusion later on, especially when you're testing your duplicate and restoring files. To change the name, select the volume in the Finder, right-click (or Control-click) it, choose Rename "*volume name*" from the contextual menu, type a new name, and press Return.

Tip: I suggest that you *label* the drive with its name and the date you last updated it. Use a sticker, a piece of tape, or another physical label, so you can tell what's what without connecting the drive. (And note, it can be very difficult to tell which of several clones is the most recent, even if you do connect it!)

Create a Data-Only Duplicate

macOS has a split system volume (see [The Split System Volume](#) for details), in which a read-only system volume holds macOS itself and a read/write Data volume holds everything else, and macOS makes it appear as though these two are a single startup volume. Due to the increased difficulties in creating and maintaining bootable duplicates that encompass both of these sub-volumes, I suggest cloning only the Data volume; that duplicate won't be bootable, because it won't contain

Store an Extra Backup Offsite

No matter how many backups you have or how often you update them, they do you no good if they disappear along with your Mac—as they likely will in the case of theft, fire, or any other serious disaster. I urge everyone to take the precautionary step of keeping a second copy of their backups safely away from their Mac, preferably in another building altogether. You can do this with a second hard drive—or, more easily and economically, with a cloud backup service.

Which type(s) of backup should you store offsite? As you'll recall, the main purpose of a bootable duplicate is to get you back up and running immediately after a disk failure or other crisis, and it can't perform that function if it's offsite. So, although you're welcome to store an extra duplicate offsite if you like, I think of offsite storage as being more appropriate for versioned backups.

Use an Extra Hard Drive or SSD

If you purchase two or more hard drives or SSDs, you can set each of them up the same way. Then back up to one drive for a week, switch to the other one, and take the first offsite. Repeat this rotation every week or so, and you'll be safe in the knowledge that if you lose your first backup, a second one is still available that's no more than a week out of date.

Although you can use this process with just two drives, having three is more convenient (although, of course, more expensive). At any time, you'll have one drive (A) in use, your next-most-recent one (B) onsite, and your oldest one (C) offsite. When you rotate the drives, you bring your oldest one (C) back onsite and make it active, while taking what has now become the oldest drive (B) offsite—and so on.

The safest way to keep multiple backup drives is to set them up separately. Configure one drive with partitions for duplicate and versioned backups. Set up Time Machine (or another versioned backup app) and let it run. Then disconnect the drive and repeat the entire procedure with a second drive. If you use Time Machine, you can configure multiple destination drives, and Time Machine switches between them automatically (see [Configure a Destination](#)).

You may be wondering where exactly “offsite” could be in your case. Here are some suggestions:

- Your place of work
- A neighbor’s or relative’s home
- A storage unit
- A safe deposit box

Don’t keep an offsite backup in your car (or your garage!), which is, if anything, more susceptible to damage and theft than your home. Heat and cold extremes in your car can also hasten data corruption. If you want as much security as possible with a trade-off of less convenience, keep the drive in a safe deposit box at your local bank.

Taking care of your media is just as important as making proper backups in the first place. If your backup disk is lost or damaged, it does you no good. So whatever else you do, be sure to store your backup media in a cool, dry place away from significant sources of light, static electricity, vibration, and other hazards (such as inquisitive pets or children). This may seem obvious, but it pays to remember that you’re doing backups in the first place because your data is valuable—perhaps even irreplaceable.

Tip: For extra safety, when your media isn’t actively in use, store it in a container that’s rated fireproof for media.

What to Do When Disaster Strikes

You've diligently performed the backups recommended in this book, and then, one fateful day, disaster strikes. It might be a small disaster (one important file is missing) or a large one (your whole computer is missing). In any case, the very first thing you should do is take a deep breath and remind yourself that everything is going to be fine. Once you're finished not panicking, proceed with the instructions here, depending on the nature of your disaster.

Restore Individual Files

The easiest problem to recover from is a small number of files that are missing, or for which you need an older version. Follow these steps:

1. If you backed up the files using Time Machine, try restoring them using the steps in [Restore Data with Time Machine](#); or, if you used another versioned backup app, follow the developer's instructions (check the Help menu) for restoring your files.
2. If the files are missing from your backup, check your duplicate if you have one. Connect the drive (if it's not already attached) and navigate to the location on the disk where the file should be. If it's there, copy it to your main disk.
3. If steps 1 and 2 don't work—for example, if your entire backup drive is missing—move on to your secondary backup. That may mean fetching an extra backup drive from another location and following steps 1 and 2 again, or using your internet backup app to find the file in your online backup.

Warning! If you need to restore data from a photo management app (such as Photos), virtualization software, or any app that uses a database-like structure, restore the *entire* data unit (photo library, virtual machine, or whatever) rather than individual files within it, or data corruption may result. You might prefer to restore these from a duplicate; see [Create a Data-Only Duplicate](#).

Restoring Email from a Backup

I've said that with IMAP accounts your Mac has its own local copy of the messages in your email account. Those messages, in turn, should be backed up by whatever backup software you use. But if a message goes missing, the nature of IMAP means it will almost certainly be gone from both the server and your Mac. Even worse, if you do manage to restore it, the IMAP server might immediately instruct your client to delete it again, since the restored copy doesn't match its master record!

How do you retrieve such a message from a backup and get it back into your email account?

It was once possible to use Time Machine to restore messages from within Mail, though the process was notoriously flaky. There is, however, a manual method you can try.

First, determine where your email app stores individual messages. (For Mail in Ventura, they're in a series of subfolders within `~/Library/Mail/V10`, each with the extension `.emlx`; some digging is required!) Go to the corresponding spot in your backups, use the date to find likely matches to the missing message(s), then restore the entire `.mbox` folder containing them to a different location (such as your desktop).

Finally, use your email app's import feature (in Mail, use File > Import Mailboxes) to import the `.mbox` folder. Then you can sort through the messages, tossing those you don't need and moving the ones you do to a new location.

Manage Your Media

For many people, a backup drive may sit on a desk for years, quietly doing its thing without any intervention. For others, two or more drives may be shuttled between locations to provide offsite storage. But in either case, your backup drive won't last forever. So, in this brief chapter, I look at [What to Do When Your Disks Fill Up](#) and explain why you should [Consider Long-Term Archive Storage](#).

What to Do When Your Disks Fill Up

Your bootable duplicates (if any) and versioned backups should continue updating themselves happily for some time. But sooner or later, the drives you use for backups will fill up. (Whether this takes a few months or a few years depends on the rate at which you accumulate new data and the size of your backup disks.) When this happens, you have two options: buy new drives and start over, or recycle. By “recycle” I don't mean throw your drives in a blue bin; I mean erase them and reuse them for a new set of backups.

One argument for starting fresh is that new drives are virtually always more reliable than old ones. Another is that you can save your old drives as a long-term archive, in case you need to see what you backed up a few years ago (assuming the drive continues to work after all that time). On the other hand, recycling media saves money, not to mention physical storage space. And most people have little need for backups stretching back more than a couple of years.

The choice is entirely yours, but I can give you some tips either way.

If You Recycle Old Backups

For versioned backups, you may want to recycle your drives on a regular basis, *before* they fill up. By periodically erasing them and starting over with a full backup—instead of relying indefinitely on incremental additions since a single full backup long ago—you reduce

the risk of data loss due to file corruption or misbehaving backup software. How often you recycle your media is up to you, but in general I'd suggest recycling mechanical hard drives every one to two years, and SSDs every three to four years.

Do, however, be aware that when you recycle media, you lose all the versioned backups stored since you started that particular cycle. In addition, if you recycle more than one set of media (for example, two or three hard drives), stagger them: do one, wait a week or two, then do the next one, and so on. That way, if you suddenly discover that you've erased the media containing an old file you need, you'll still have a chance to recover it easily from another set of backup media.

For bootable duplicates, as long as there's enough free space on your destination disk, you can simply erase the disk and start over from scratch. But if you're running out of space on the disk you use for duplicates, your only option is to erase the disk, use it for something else, and buy a new, larger drive to use for bootable duplicates from now on.

Tip: If you're erasing a disk anyway, this is a good time to reassess partition sizes (see [Decide on Capacity](#)). If your disk or home folder is significantly larger than before, consider changing the partition sizes to better accommodate your current needs.

If You Archive Old Backups

When you see that your backup media is close to being full—or when your drive's warranty has run out and you start losing faith in it—you can set it aside, buy new drives, and start new sets of backups.

Unfortunately, as I discuss just ahead in [Consider Long-Term Archive Storage](#), hard drives and SSDs alike make poor choices for long-term storage (though an older hard drive that you wouldn't trust for backups may be fine for casual, noncritical uses). In other words, do buy new drives but don't put too much faith in being able to retrieve backups from your old drives years from now.

Consider Special Backup Needs

Although duplicates, versioned backups, and offsite storage cover most situations the typical user will encounter, some people have special backup needs that don't quite fit the mold.

I'm thinking, for example, of users with vast numbers of digital photos and those who [Deal with Huge Volumes of Data](#) because they work extensively with the gigantic files required for digital video or pro audio apps. In other special cases, you may need to [Back Up While on the Road](#) (especially photos) or [Back Up Windows Files and Volumes](#).

Each of these situations may require additional steps beyond conventional duplicates and versioned backups.

Back Up and Restore Notes

Here's a puzzler for you: if you use Apple's Notes app, where can you find its data, and how might you back it up and restore it if necessary?

Depending on how you have Notes configured, individual notes may be stored only on your Mac, in iCloud (the default location), in other email accounts, or in some combination of these places. If you use iCloud, even though the data technically lives on Apple's mail servers, it's hidden in such a way that neither Mail nor any other email app can display it.

Your Mac does have copies of all this data. The folder `~/Library/Group Containers/group.com.apple.notes` contains local copies of all the Notes data currently stored in iCloud, and several other folders, whose names begin with `com.apple.Notes` in `~/Library/Containers`, contain any "On My Mac" Notes data. But notes aren't stored as individual files; rather, they're stored in an SQLite database that you will find it difficult if not impossible to extract data from using any app but Notes itself.

Since you know where your local Notes data is on your Mac, you can presumably back it up, simply by making sure the folder mentioned above is included in your backups. But *restoring* that data becomes a problem. You definitely can't restore individual notes; your only option would be to restore the entire folders in question, overwriting what was there before. But that means you'd lose any changes to Notes you made since your backup.

Even if you didn't care about that, your Mac might immediately replace that restored data with whatever happens to be stored in iCloud at the moment, because from Apple's point of view, what's stored in iCloud is the Truth—the primary version of any data, should a conflict ever arise. (You could presumably avoid this problem by turning off Notes syncing in System Settings > *your name* > iCloud or System Preferences > iCloud before restoring the data, but once you turn Notes syncing back on, you'll be right back where you started unless you go through a lot of manual copying.)

I've tried a couple of procedures I read about online that claimed to solve this problem, but they didn't work for me. It may be that they worked with older versions of macOS but then broke at some point when Apple made changes.

So, as I say, it's a puzzler. But a reader of this book wondered about this, and it is an excellent question. So, let me offer a few options, all of which require advance planning, and all of which involve some downsides:

- **Store notes on your Mac.** As I said above, Notes can store data locally (in the On My Mac category), in an iCloud account, or in an IMAP account. If you opt to store notes in the On My Mac category, they won't sync to your other devices—a distinct negative—and you won't be able to add collaborators to them. Plus, restoring them still means overwriting the entire folder containing all your notes. But, because the data is local, at least you wouldn't risk having it immediately replaced by a copy from the cloud.

To store notes locally, first go to Notes > Settings/Preferences and check "Enable the On My Mac account." Then, in that category in the

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.

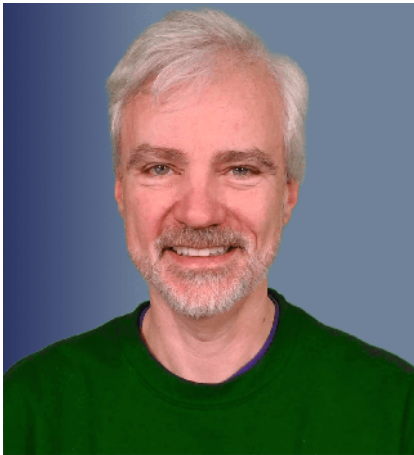
More Take Control Books

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on Macs and other Apple products.

You can buy Take Control books from the [Take Control online catalog](#) as well as from venues such as Amazon and the Apple Books Store. But it's a better user experience and our authors earn more when you buy directly from us. Just saying...

Our ebooks are available in two formats, PDF and EPUB, which are viewable on any computer, smartphone, tablet, or e-reader. All are DRM-free.

About the Author and Publisher



Joe Kissell is the author of more than 75 books about technology. In 2017, he also became the publisher of Take Control Books, when alt concepts—the company he runs with his wife, Morgen Jahnke—acquired the Take Control imprint from TidBITS Publishing Inc.’s owners, Adam and Tonya Engst. Before he began writing full-time in 2003, Joe managed software development, a *totally normal* profession for someone with degrees in philosophy and linguistics.

In his rare non-work hours, Joe likes to walk, cook, read, and practice tai 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 Backing Up Your Mac](#) in the subject. You can follow him on Mastodon ([@joekissell](#)) or Bluesky ([@joekissell.com](#)), or visit his personal website, [JoeKissell.com](#).

Credits

- Publisher: Joe Kissell
- Editor: Caroline Rose
- Cover design: Sam Schick of [Neversink](#)
- Logo design: 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!

[*Mac Basics*](#): Get to know your Mac inside and out with this detailed guide.

[*Take Control of 1Password*](#): Use this powerful password manager to create, store, enter, and sync personal data on all your devices.

[*Take Control of Apple Mail*](#): Learn the ins and outs of Apple's email app on your Mac, iPhone, or iPad.

[*Take Control of Automating Your Mac*](#): Work more efficiently on your Mac with time-saving shortcuts of all kinds.

[*Take Control of DEVONthink 4*](#): Master this powerful information management tool.

[*Take Control of iCloud*](#): Make the most of Apple's online service for storing, syncing, and sharing data.

[*Take Control of MailMaven*](#): Discover how to use this powerful Mac email app from SmallCubed.

[*Take Control of Solving Mac Problems*](#): Learn how to maintain, troubleshoot, and speed up your Mac.

[*Take Control of the Mac Command Line with Terminal*](#): Master your Mac's command-line interface and learn basic Unix skills.

[*Take Control of Tahoe*](#): Discover what's new in macOS 26, 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, a scanner, and this ebook, 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 Backing Up Your Mac, Fifth Edition

ISBN: 978-1-990783-48-7

Copyright © 2025, Joe Kissell. All rights reserved.

[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.