April 2021
Vol. XL, No 3

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

April Program

We plan to discuss anti-virus apps
and security for Mac users.

We have virtual meetings via Zoom
on the third Tuesday of each month
except for summer vacation.

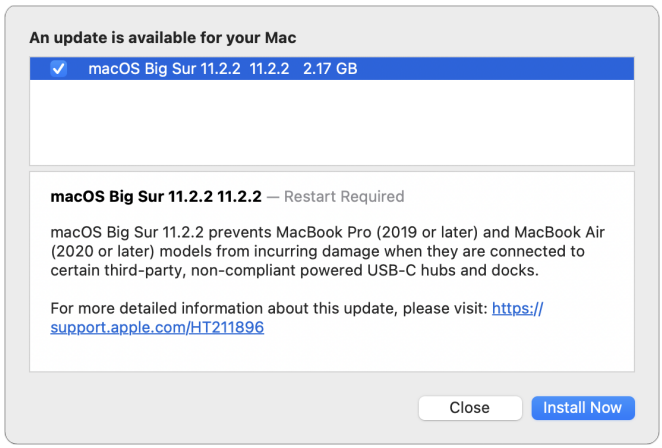
Emails will be sent out prior to each meeting.
Just follow the directions/invitations each month

Contents

By Adam Engst

macOS 11.2.2 Protects MacBook Pro and MacBook Air from Non-Compliant USB-C Hubs and Docks

Here's an unusual update. Apple has released macOS 11.2.2 Big Sur, saying that the update prevents MacBook Pro models from 2019 and later and MacBook Air models from 2020 and later from being damaged by "certain third-party, non-compliant, powered USB-C hubs and docks." Apple lists no other changes, even security fixes. It's a 2.17 GB download.



Apple makes no mention of a repair program, which implies that the company feels that any damage incurred is not its fault, although most of the bricked Macs appear to have been replaced under warranty or AppleCare.

Nor does Apple name names, so there's no way to know which USB-C hubs and docks might be dangerous here. The general advice is with power-carrying accessories is to stick with well-known and reputable manufacturers. Although there's no guarantee that they would have produced compliant peripherals, it's probably easier to ask such companies if their products are compliant.

That said, a Reddit thread collects reports from people who have experienced problems with particular devices, including those from Dodocool, HyperDrive, Satechi, and ZMUIPNG. If you're buying a USB-C hub or dock right now, it's probably safest to avoid powered ones for the moment.

Our initial take is that Apple engineers have evaluated enough damaged Macs to understand the problem—presumably too much or dirty power—and realized that they could prevent the problem by adjusting how the Mac interacts with the powered hub or dock. Hence macOS 11.2.2.

If you're running Big Sur on a recent MacBook Pro or MacBook Air and have a powered USB-C hub or dock, we recommend unplugging it immediately and installing this update before using it again. If you don't have such a hub or dock, or are using a different Mac, there's seemingly no reason to install this update. macOS 11.3 should be coming soon.

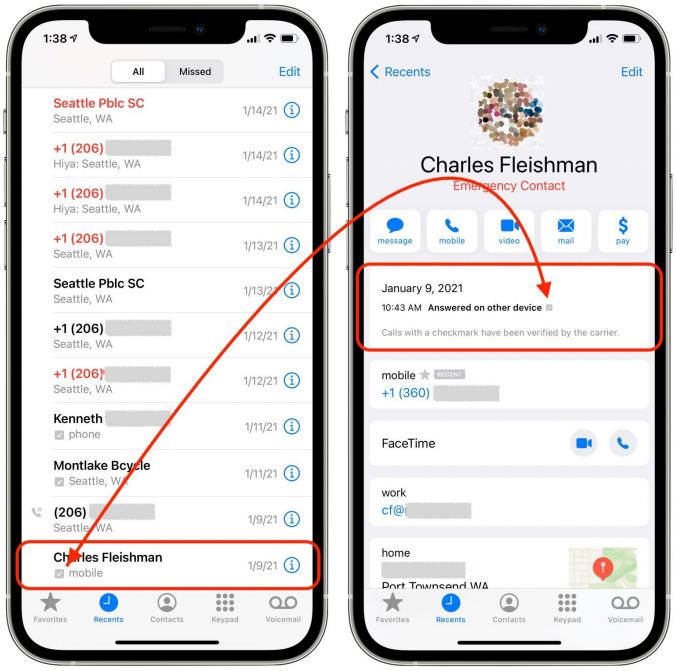
More concerning is what to do with a MacBook Pro or MacBook Air running an earlier version of macOS with a powered USB-C hub or dock. Perhaps Apple will release a supplemental update for 10.15 Catalina and 10.14 Mojave to address the problem. If that doesn't materialize, we'll never know if the problem was somehow specific to Big Sur or if Apple chose not to open the codebases for those older operating systems. Regardless, if you use a powered USB-C hub or dock with a recent MacBook Pro or MacBook Air, we recommend unplugging it and contacting the manufacturer to determine if it might cause this problem.

By Glenn Fleishman

Caller ID Authentication May Tame the Scourge of Spam Calls

This morning, my iPhone rang five times. Because I pay Hiya for reverse Caller ID lookups, each number lit up with a name I didn't know, along with the originating city and state: three from Florida and two from Connecticut. I didn't answer any of the calls because I didn't recognize any of the names. When I checked later, I found they lacked a relatively new indicator that I watch out for: a tell-tale checkmark. While tiny, it's a harbinger of better things to come, particularly with a looming deadline in June 2021 for major phone carriers and Internet telephony providers.

You may not even notice this checkmark—it's truly very tiny—but it appears in the Recents list in the Phone app on an iPhone and in call details. On some Android phones, a verified indicator appears on the incoming call screen, and telephone carriers have asked Apple to add it there on iPhones, too. Only in the call detail do you get an explanation from Apple: "Calls with a checkmark have been verified by the carrier."



What Are Those Tiny Checkmarks?

These marks started to appear in iOS 13 in the third quarter of 2019, but usage has accelerated as carriers want to block spam calls from ever reaching their customers. Spam calls cause huge headaches for those who run phone networks. They consume network resources, don't produce revenue (spammers don't pay a receiving phone network for the calls they place), and irritate the heck out of a carrier's customers. Those customers, in turn, spend a lot of time complaining to customer-service operators, on forums, and to the US Federal Communications Commission and Federal Trade Commission.

Those two federal agencies have targeted these spam calls, as they want to reduce the number of people who lose money to scams. These calls might waste a moment of your time, but scammers can exploit vulnerable people in cognitive decline or those with too much trust in others to the tune of hundreds or even tens of thousands of dollars. It's a rare regulatory initiative that started under the previous hands-off presidential administration.

These tiny checkmarks appear on calls that pass through a new standard implemented on major telephone networks starting in 2019 and gradually being rolled out by smaller ones since. The standard, known as SHAKEN, is an amusingly named expansion of an earlier plan called STIR, and the two are often spoken of together as STIR/SHAKEN. (Best said with a James Bond intonation.) What they do is establish a cryptographic chain of trust for the originating number that you see as a Caller ID message. (If you want to know what they stand for, take a deep breath: STIR is Secure Telephony Identity Revisited; SHAKEN is quite absurdly squeezed into its acronym from Signature-based Handling of Asserted Information Using toKENs.)

Larger companies involved in plain old telephone service (POTS), a loose term for the network that handles phone numbers for calling, must implement STIR/SHAKEN by 30 June 2021. There are a lot of exceptions, as noted in this industry briefing article, but any carrier with 100,000 or more

lines has to be ready to go by then. (Smaller carriers have until 30 June 2023.) As we approach that date, we should see a few effects at varying levels:

- **Fewer spam and scam calls:** Pundits often predict this desirable result whenever there's a major enforcement action or carriers make changes. But in the past, fraudsters just adapted because call-based financial crimes are low-hanging fruit with little risk. STIR/SHAKEN will bump up the cost of doing business, so crime won't pay as well.
- **More checkmarks:** We can train ourselves and vulnerable members of our families, friends, and colleagues to identify recent calls with no checkmark. Apple might not yet put the mark on the incoming call screen, but we can check in the Recents list before treating the source as eventually legitimate. About one-third of my regular incoming calls already have a checkmark.
- **Better automated call-blocking:** With STIR/SHAKEN as a signal, carrier software—like T-Mobile's free tier of ScamShield—and third-party apps could more accurately predict unwanted calls. Carriers normally are required to pass all calls placed through to a recipient, but the FCC made clear a few years ago that as long as a telco is appropriately looking for spam signals, they can block these. STIR/SHAKEN provides even more data for that purpose. (Verizon claims it has blocked nine billion unwanted calls as of December 2020 through various techniques that include STIR/SHAKEN.)
- **Greater accountability:** Because STIR/SHAKEN will force spammers who keep plying their trade to rely more heavily on legitimate originating phone numbers, it will make them (or their providers) a lot more vulnerable, trackable, and arrestable. It could help authorities shut down boiler-room operations much more quickly, too.

How STIR/SHAKEN Will Help

STIR/SHAKEN essentially rectifies a historical failure that resulted from extending phone system technology that assumed few participants who trusted one another, much like email. It's harder to forge Caller ID than the return address on an email, but Caller ID has been spoofable for decades. You probably already knew that, because you've received so many illegitimate calls. In recent years, scammers would even engage in "prefix spam," calling your number with a fake Caller ID number that used the same three-digit prefix that follows the area code. (That prefix remains tied to local phone exchanges with wireline numbers and regional assignments with wireless carriers.)

Originally, businesses and other institutions could set Caller ID via a PBX (corporate phone exchange), which made sense first when companies were managing oodles of internal lines and later when they started using Voice over IP (VoIP). Back in the late 1990s and early 2000s, when I freelanced for the New York Times, I knew I was getting a call from an editor there when Caller ID reported 1 (111) 111-1111, the number the Times spoofed to protect their internal phone numbers. (The Times changed that a decade ago.)

VoIP carriers have long had the broader capability to set a unique phone number for any outgoing call because their calls don't originate in the plain old telephone system, and carriers had to offer that flexibility to allow Caller ID to work for VoIP calls at all. While hundreds of millions of VoIP-based calls made with correct identification occur every day, spammers also make a reported 100 million-plus illegitimate calls daily. How do you avoid throwing the baby out with the bathwater?

A call may need to make multiple hops across different carrier and third-party networks from the caller to the person answering. STIR and SHAKEN —the latter technically an implementable and broader version of the former—use public-key cryptography to identify which phone numbers are assigned to which originating parts of the phone network. When a call is placed, it has to pass cryptographic tests that are checked at each hop and that can validate that the number identified from Caller ID originated from the right point in the phone system. (For more technical details, see my 2019 *Fast Company* article on the early stages of STIR/SHAKEN.)

While STIR/SHAKEN should allow carriers to block the passage of calls that lie about their originating numbers, questions remain unanswered about other elements of the system. How will it

affect calls that aren't properly tagged? How should carriers and smartphone manufacturers present such calls to the dialing public? Although Apple's display is tremendously subtle right now, I expect more prominent marking and signaling over time, including adding a verified message to the incoming call screen. Validated Caller ID should eventually help legitimate calls evade blocking techniques that snag the unproven.

How long will this take? We can probably draw a lesson from the Web's fairly rapid switchover from mostly non-secured HTTP sites to nearly all HTTPS-secured ones. While the transition started slowly, once browser makers decided on schedules, they began to identify sites without HTTPS with increasingly aggressive labeling that warned of the lack of security. That changeover was combined with significantly easier and cheaper systems for creating and managing the necessary security certificates, like Let's Encrypt. Having both the carrot of easy upgrades and the stick of browser warnings prompted site owners to upgrade their security.

Ultimately, companies and carriers will find their calls dropped or blocked unless they fully embrace STIR/SHAKEN as it's adopted by mobile phone operating systems and the rest of the phone network. For those who have built businesses on unethical practices, we hope STIR/SHAKEN will spell the end for them. Good riddance, and we look forward to the day when we can once again answer the phone without worrying that we're being targeted by a scammer.

By Tim Sullivan

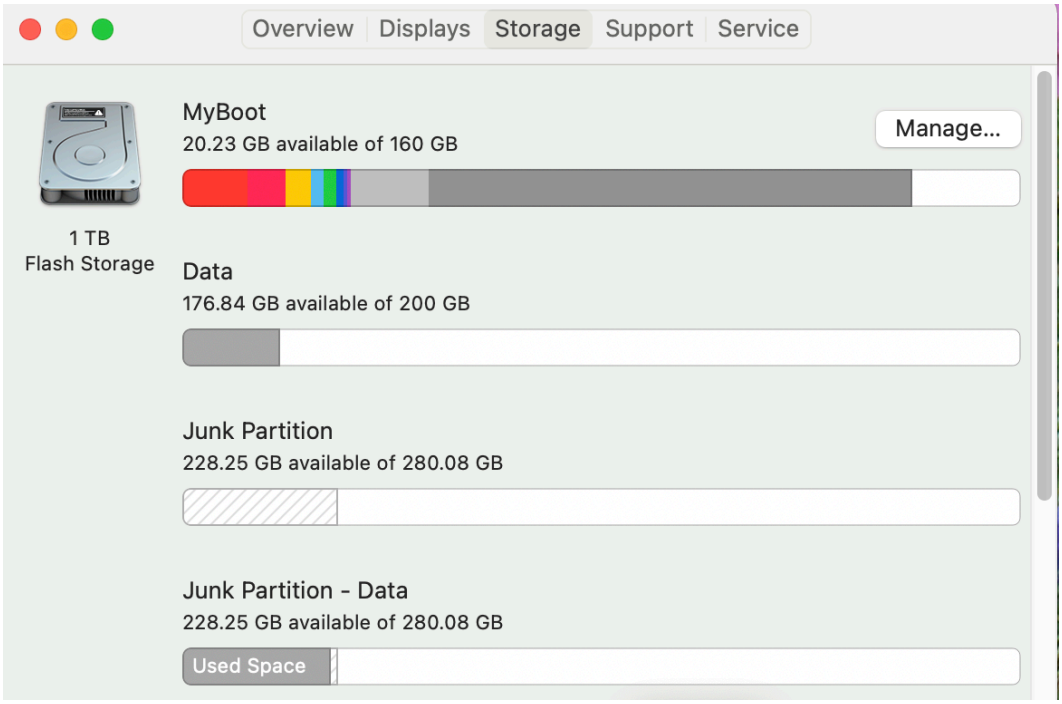
Where Did All My Disc Space Go?

Apple uses APFS (Apple File System) with solid state drives. APFS replaces the HFS+ file system. APFS replaced the concept of 'partitions' with 'containers'. That began with High Sierra 10.12. In APFS parlance, a container refers to the basic storage unit. Each APFS container holds one or more volumes.

My disc space has been partitioned into over 5 partitions to make backups easier. It's been this way for several generations of Macs. Over a year ago I got a new laptop that uses a SSD rather than a disc.

Each morning when I boot up I run a script that checks disc size — 80% full being a practical upper limit for discs. For this laptop the My Boot partition has been sized at 160 GB. The system files (Big Sur) take up a little over 15 GB. Yet the partition is pushing 90% full.

I can get a graphic representation by going to the Apple menu, then About the Mac, and finally the Storage tab.



Reading from left to right, I have
- 12.73 GB of iOS files (orange)
- 7.28 GB of Apps (red)
- 4.86 GB of Photos
- 2.34 GB of Music Creation
- 2.27 GB of Documents
- 1.39 GB of Mail
- 936.2 MB of TV
- 15.05 GB of System (light gray)

That adds up to about 47 GB of stuff and then at almost twice the size there's
- 92.07 GB of Other (dark gray)

This Other space has been steadily increasing in size recently.

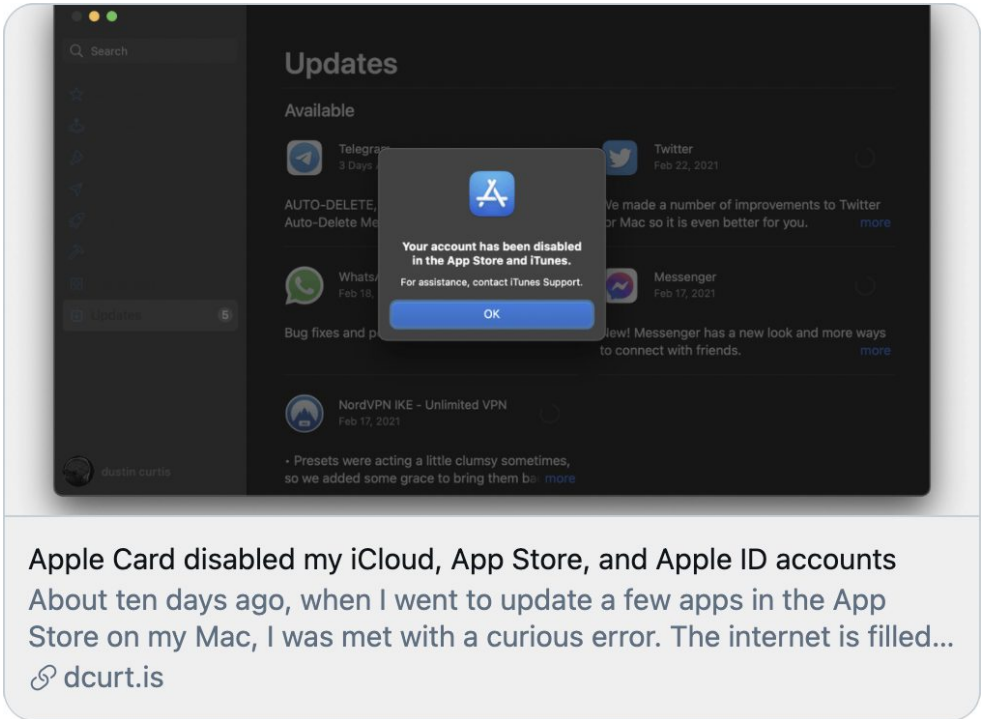
The iOS files would most likely be backups of our iPhones.

Some research indicates that Apple is using APFS startup containers to store what Apple calls "Other Volumes". This is where Preboot, VM/Virtual Machine, Recovery, and Macintosh HD data are stored. So far my limited research dictates that the only way reduce the size of My Boot is to delete the volume. I'm still looking for a better a better solution.

By Josh Centers

The Mystery of Dustin Curtis's Locked Apple ID

There has been a lot of buzz in the Apple world lately about designer Dustin Curtis and his locked Apple ID. It's a long and winding tale, but one that's disturbing for those of us who are heavily invested in the Apple ecosystem. In short, Dustin's Apple ID ended up locked such that he couldn't download or update apps, nor could he use Apple Music. His iCloud calendar stopped syncing, and even Handoff stopped working. However, iMessage and Photos continued to work.



Apple Card disabled my iCloud, App Store, and Apple ID accounts

About ten days ago, when I went to update a few apps in the App Store on my Mac, I was met with a curious error. The internet is filled...

dcurt.is

How It Happened

The good news is that Apple has reactivated Dustin's account, but the concerns remain. Let's try to piece together a timeline of the story:

1. **Sometime in January:** The bank account number tied to Dustin's Apple Card account changed, causing autopay to fail.
2. **Mid-January:** Dustin bought an M1-based MacBook Pro with his Apple Card. Apple offered a trade-in credit for an old MacBook Pro, and Dustin was told he would receive a trade-in kit and would have two weeks to send it in.
3. The trade-in kit never arrived.
4. Apple apparently tried to charge the Apple Card.
5. **Mid-February:** Apple sent Dustin an email asking about the trade-in. Dustin replied that he never received the kit but didn't receive a response from Apple.
6. **February 15th:** Apple sent another email saying that it was unable to collect full payment for a new iPhone (that was erroneous, and was presumably an automated message) and that Dustin's iTunes and Mac App Store accounts would be disabled until he resolved the situation with an Apple Card specialist at Goldman Sachs. Dustin missed this email initially, finding it only in a search after Apple locked his account.
7. **Late February:** Dustin discovered that his account had been locked. He immediately called Apple Support and was told that they could do nothing except escalate the issue and that he should hopefully get a call within a day.
8. Two days later, Dustin called Apple Support again. The representative said something about Apple Card but couldn't help because Apple ID was a different department. The support rep emailed that department—email was apparently the only way to contact them.
9. Dustin found the email he missed earlier and corrected his Apple Card info. However, when he tried to reply to that email, he received an automated "Address not found" bounce.
10. Dustin used Apple Business Chat to contact Goldman Sachs support, who said they would email the Apple ID support department.

11. An Apple ID support rep called Dustin to tell him that his accounts would be restored in 3–5 days. That happened, and all is back to normal.

In a statement to 9to5Mac, Apple denied that the issue was at all related to Apple Card:

We apologize for any confusion or inconvenience we may have caused for this customer. The issue in question involved a restriction on the customer's Apple ID that disabled App Store and iTunes purchases and subscription services, excluding iCloud. Apple provided an instant credit for the purchase of a new MacBook Pro, and as part of that agreement, the customer was to return their current unit to us. No matter what payment method was used, the ability to transact on the associated Apple ID was disabled because Apple could not collect funds. This is entirely unrelated to Apple Card.

However, developer and blogger Michael Tsai questions Apple's explanation:

As far as I can tell, it really is an Apple Card-specific issue. With a regular credit card, you can imagine that Apple would have pre-authorized a charge for the trade-in in case it didn't arrive. And if the bank account linked to the card changed, that would not be Apple's concern. Apple would add the additional charge, which would go on the card account, the issuer would pay Apple, and then from Apple's point of view there would be no debt.

Many commentators have suggested that this situation was Dustin's fault, and while that's at least partially true, it also exposes some problems at Apple's end.

Dave Mark at The Loop said:

And to be clear, I think I am less concerned that Apple disabled Dustin's account as I am that it took so long to address the issue. If the call to Apple customer support had made the issue clear immediately, a couple of clicks would have resolved this. As is, and if true, looks like the left hand didn't know what the right hand was doing.

At the very least, it seems that Apple has fallen prey to what happens to so many large companies: entire departments don't communicate with each other, aren't aware of broader company policies, and can't resolve problems outside of their direct sphere of influence.

For the rest of us, Dustin's story throws a spotlight on the danger of doing too much business with a single company. When you buy your hardware from Apple, purchase your software through the App Store, and rely on subscriptions to Apple cloud services, paying for it all with an Apple credit card, you're signing up for both great convenience and a certain level of risk. That's not necessarily a bad strategy, but as the 19th-century industrialist and philanthropist Andrew Carnegie recommended, "Put all your eggs in one basket and then watch that basket."

In this case, watching the basket would entail paying attention to the effect that bank account numbers changing might have, making calendar reminders for known deadlines (like the trade-in kit arriving and its two-week return period), and creating an email strategy that reduces the chance of missing an important message.

It's also worth putting some thought into how you would work around such a problem if it happened to you. Most Apple services aren't mission-critical—you could probably go without Apple TV+ or Apple Fitness+ for a while—but what about iCloud Mail and iCloud Drive? Would the loss of iCloud Calendar syncing be problematic? Ensuring the continuity of certain services is yet another facet of a modern backup strategy (see "The Role of Bootable Duplicates in a Modern Backup Strategy," 23 February 2021).

By Adam Engst

Is It Safe to Upgrade to macOS 11 Big Sur?

"Is it safe to upgrade yet?" That's the question I've been asked repeatedly since Apple first released macOS 11 Big Sur in November 2020. It's a hard question to answer because everyone's situation is different—I can't know if you might rely on an app that doesn't work perfectly in Big Sur. Worse, emotions often run high when it comes to macOS upgrades, with some people viewing "different" as "bad" on principle, and Big Sur's visual redesign is quite different. So I won't tell you that you *should* upgrade to Big Sur—if you choose not to, that's entirely your prerogative. But I will say that I have upgraded with no real problems, and if you wish to upgrade, it's generally safe to do so.

Why might you want to upgrade? For many people, it's the thrill of exploring all the changes—technology should be fun. The user interface changes in Big Sur are a makeover the likes of which we haven't seen in years, with Apple adding whitespace and trying to prevent the interface from distracting from your content. Some changes will be more successful than others, but in a year or two, older versions of macOS will look dated.

Technology should also make life easier and support our work. Big Sur's new Control Center does a good job of consolidating numerous menu bar items into a single interface. With its single column for notifications and widgets, the redesigned Notification Center may work better for you, especially with grouped notifications using space more efficiently. Safari provides a customizable start page and translation capabilities. In Messages, you can pin favorite conversations to the top, reply directly to messages in group conversations, and search more effectively. Maps gains city guides, cycling routes in a few major cities, and indoor maps of major airports and shopping centers. And thanks in part to Apple's acquisition of Dark Sky, the Weather widgets provide next-hour precipitation charts, severe weather alerts, and warnings of significant weather shifts.

Honestly, though, the main reason to upgrade eventually is to stay current. The security threats that Apple addresses with updates are real, and developers continually enhance their apps to take advantage of new core capabilities that Apple builds into macOS. You don't have to upgrade right away, but you will have to do so at some point, even if just as part of the purchase of a new Mac.

External Evidence

I will say that I think Big Sur has proven itself more solid than 10.15 Catalina. I never officially recommended an upgrade to Catalina because it never felt entirely baked, even after Apple announced Big Sur. When forced by circumstance, I did upgrade my primary Mac to Catalina last April with no real problems (see "Six Lessons Learned from Dealing with an iMac's Dead SSD," 27 April 2020), but Apple's chaotic updates early in the cycle had poisoned the well for many people. By this point last year, Catalina was on its sixth update, with a seventh supplemental update coming soon.

In contrast, Big Sur has so far received only five updates, with only 11 non-security bugs explicitly addressed. A sixth update is due soon. They include:

- **11.1:** Largely a feature release, version 11.1 kept macOS in feature parity with iOS 14.3. Apple's release notes listed only five bug fixes, although we heard it also addressed problems in Rosetta 2 for M1-based Macs. See "Apple Releases Apple Fitness+, macOS 11.1 Big Sur, iOS 14.3, iPadOS 14.3, watchOS 7.2, and tvOS 14.3" (14 December 2020).
- **11.2:** Despite the version number suggesting new features, version 11.2 focused on bug and security fixes. It addressed just five bugs again, but 43 security fixes. See "macOS 11.2 Big Sur Improves Bluetooth, Squashes Bugs" (1 February 2021).

- **11.2.1:** A focused release, version 11.2.1 addressed a rare but nasty bug affecting some 2016 and 2017 MacBook Pro models. It also fixed three important security vulnerabilities. See "macOS 11.2.1 Big Sur Fixes MacBook Pro Charging Bug and sudo Vulnerability" (9 February 2021).
- **11.2.2:** Apple released version 11.2.2 purely to protect recent MacBook Pro and MacBook Air models from dangerous USB-C hubs and docks. See "macOS 11.2.2 Protects MacBook Pro and MacBook Air from Non-Compliant USB-C Hubs and Docks" (26 February 2021).
- **11.2.3:** Another one-trick pony update, version 11.2.3 addressed a presumably serious WebKit vulnerability common to all of Apple's operating systems, including Catalina and Mojave. See "iOS 14.4.1, iPadOS 14.4.1, macOS 11.2.3 Big Sur, and watchOS 7.3.2 Address WebKit Security Vulnerability" (8 March 2021).
- **11.3:** Undoubtedly due out soon, version 11.3 will likely fix a few bugs and address newly discovered security vulnerabilities, but it is also slated to add new features and enhance existing capabilities.

The conspiracy-minded might say that Apple could be fixing vast numbers of bugs without acknowledging them in its release notes. However, based on my experience with the Big Sur public beta, with running it on my M1-based MacBook Air, and now having upgraded my primary Mac—a 2020 27-inch iMac—I can say that Big Sur feels stable and predictable. Informally, that sentiment seems to be echoed by many professionals and consultants in the Apple world.

However, if my Web analytics are anything to go by, many users are waiting on the sidelines. I compared the first 100 days after the release of each of the last three versions of macOS, focusing on how many people had upgraded to the latest versus staying on the previous release.

First 100 days	11 Big Sur	10.15 Catalina	10.14 Mojave	10.13 High Sierra
10.13 → 10.14			39%	38%
10.14 → 10.15		49%	33%	10%
10.15 → 11	13%	65%	11%	7%

You can see that, in the first 100 days after the release of Mojave, 39% of people visiting tidbits.com had upgraded, with 38% remaining on High Sierra. That upgrade was positive enough that the first 100 days after the release of Catalina showed that 49% of people had upgraded to Catalina, with 33% staying on Mojave. That's despite all the bad press Catalina received early on.

In contrast, the first 100 days of Big Sur show that a mere 13% of tidbits.com visitors have upgraded or bought an M1-based Mac, with a whopping 65% remaining on Catalina. It's tempting to attribute the extremely low upgrade rate to users rendered gun-shy by Catalina's troubles or to people scared off by the significant user interface changes in Big Sur.

However, when Tonya and I discussed these numbers, she rightly pointed out that the pandemic is likely the prime factor in upgrade hesitancy. People who are working or taking classes from home or who rely on their Macs for lifeline communications with friends and family will be extremely cautious when it comes to a significant macOS upgrade that's unlikely to improve the experience of using third-party apps. (Interestingly, 90% of our iOS/iPadOS traffic now comes from some version of iOS/iPadOS 14, showing that people are much quicker to upgrade their iPhones and iPads.)

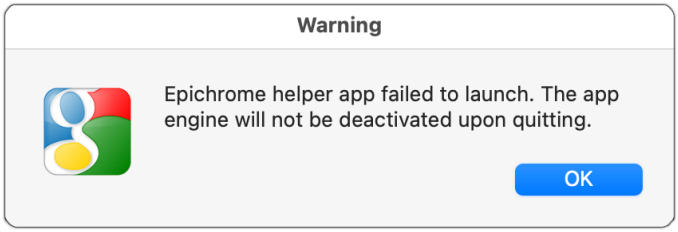
There's still no shame in delaying, and at this point, I would encourage anyone who isn't champing at the bit to wait until version 11.3 has been out for a week or two. However, as I noted, I bit the bullet a few weeks back for my primary Mac, making sure,

as always, to follow Joe Kissell's upgrading advice, now in *Take Control of Big Sur*.

As a broad outline, I recommend that you make at least one backup right before you upgrade, ensure you have a bare minimum of 36 GB free, and plan for your Mac to be inaccessible for at least half a day. The upgrade might go faster, but between the huge download, the long installation time (coupled with a conversion to APFS for drives still using HFS+), and getting everything reconfigured afterward, it's best to allow plenty of time.

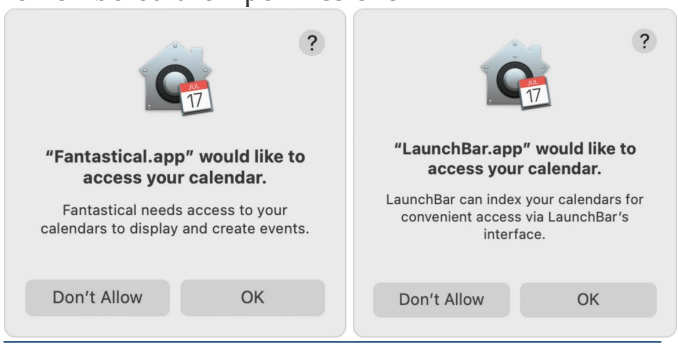
My Immediate Post-Upgrade Experiences

The quick summary of my upgrade is that, after a short time of fiddling with things that needed resetting, I returned to work with no significant interruption or productivity hit. Nearly every app I've needed to use—even the elderly ScreenFlow 7.3 from 2017, which I pulled out for a project last weekend—has worked just as it did before I upgraded. One slight exception is the site-specific browser Epichrome, which says it was not developed or fully tested with Big Sur and whose helper app crashed on first launch, although my site-specific browsers work fine in daily usage.

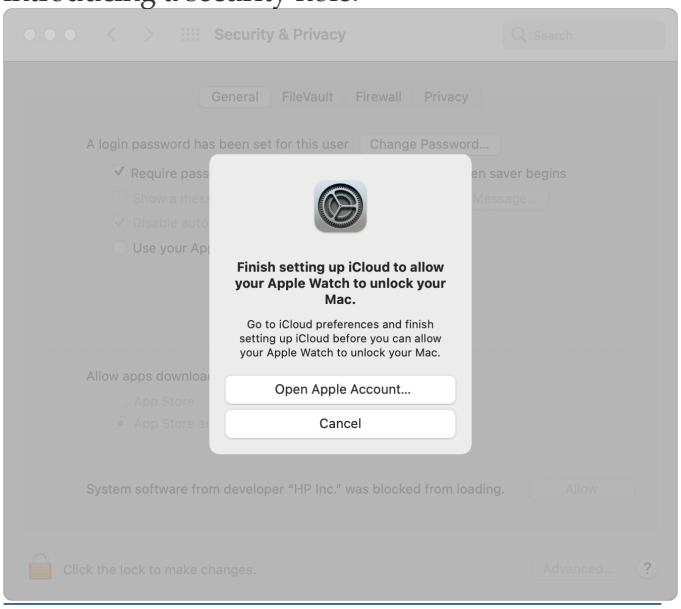


The fiddling required in the wake of the upgrade was driven mostly by the massive state changes inherent in upgrading macOS. Many parts of macOS and independent apps develop a sense that their environment is stable—they're correctly logged in, their underlying storage is the same as yesterday, they know what devices are connected, and so on. But things like switching to a new Mac, changing to a different boot drive, and upgrading macOS bring the foundational state of the Mac into question, causing macOS components and apps to distrust their authentication credentials, access permissions, document storage locations, and the like. For instance:

- Fantastical and LaunchBar both had to ask for permission to access my calendar and contacts, and Fantastical also needed permission to access reminders. Of course, I had granted those permissions long ago. Most other apps remembered their permissions.

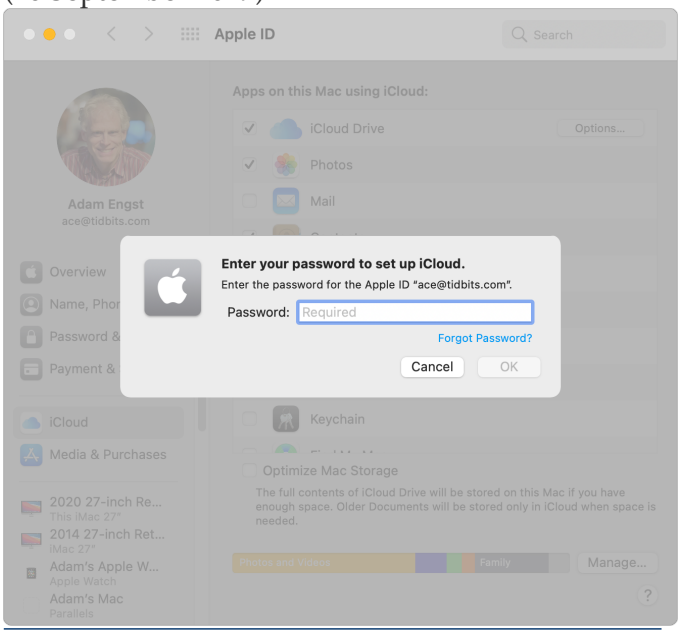


- The option for unlocking apps and my Mac with my Apple Watch—which I adore—was turned off and required me to finish setting up iCloud before I could enable it again. I've seen this option get disabled even by smaller macOS updates; I suspect Apple is playing it very safe to avoid introducing a security hole.

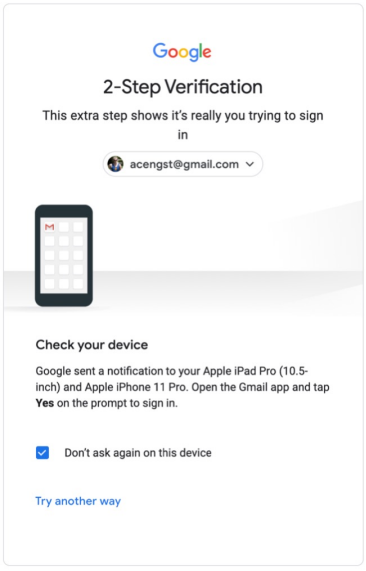


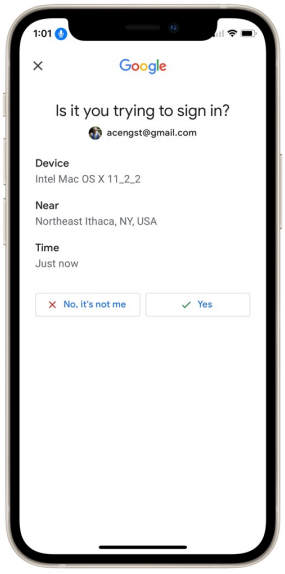
- When I opened System Preferences > Apple ID to set up iCloud, Big Sur prompted me for my Apple ID password, the iMac's password, and the password of my M1-based MacBook Air. All these authentication requests may seem excessive, but Glenn Fleishman explained why they make sense in "Why Apple Asks for Your Passcode or Password with a New Login (and Why It's Safe)"

(26 September 2019).

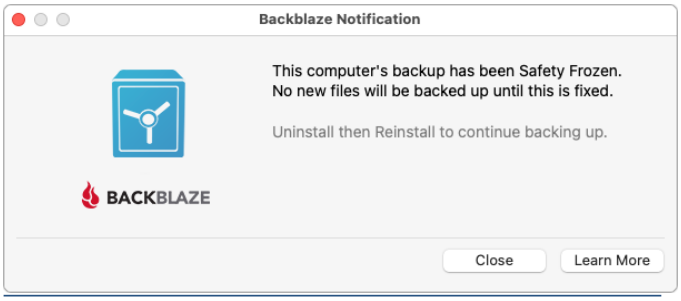


- I can't quite remember the context, but I had to sign in to Google again as well, likely due to using Google Calendar and the Backup & Sync app for integrating Google Drive into the Finder. I quite like how Google handles two-factor authentication by displaying a prompt in the Gmail app on my iPhone.





- Backblaze informed me that my backup was "safety frozen," so I had to uninstall and reinstall the Backblaze software before it would continue backing up. I was able to follow Backblaze's instructions for thawing my backup, though they were a little involved.



- Brave forgot all my logins, forcing me to log in again to any site that requires authentication. That's annoying, especially when it triggers a two-factor authentication code request that would otherwise be infrequent. I don't know if this is just a Brave (and likely Google Chrome) quirk or if other Web browsers would have been affected similarly. Upgrading to macOS 11.2.2 and again to 11.2.3 triggered the same problem, so it's not just major upgrades that cause this.

- As when setting up a new Mac (see "Moving to a New Mac: What's Left to Do After Migration?," 7 September 2020), I had to reselect my iMac in Settings > Messages > Text Message Forwarding to get SMS text messages to appear in Messages on my iMac.

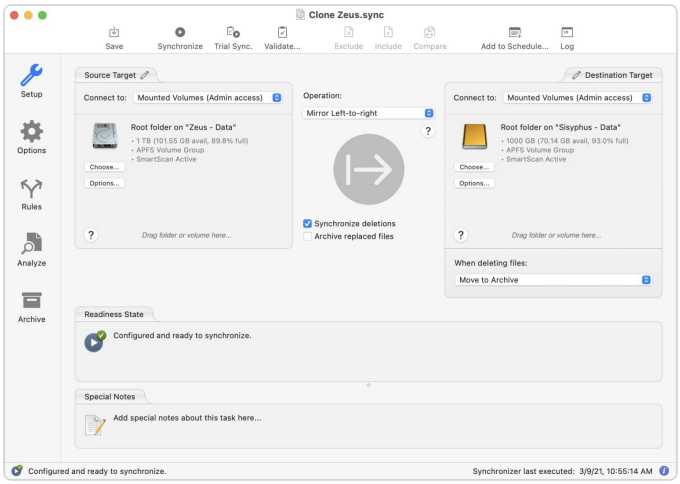
Other Post-Upgrade Adjustments

I had no problem getting back to work after upgrading to Big Sur because the vast majority of what I do is in third-party apps, which work as they always have. I don't regularly use Calendar, Contacts, Mail, or Safari, for instance, instead preferring Fantastical, Cardhop, Mimestream, and Brave, respectively. Nevertheless, there have been a few adjustments I've had to make, some good, some less so.

Switch from SuperDuper to ChronoSync

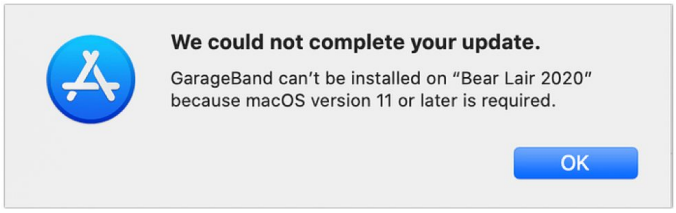
For many years, I've relied on SuperDuper to make a bootable duplicate. As I discussed at length in "The Role of Bootable Duplicates in a Modern Backup Strategy" (23 February 2021), making bootable duplicates is a trickier proposition in Big Sur. Although SuperDuper's workaround of using an older version to make a data-only duplicate worked fine, I decided to take the opportunity to try making a bootable duplicate using ChronoSync.

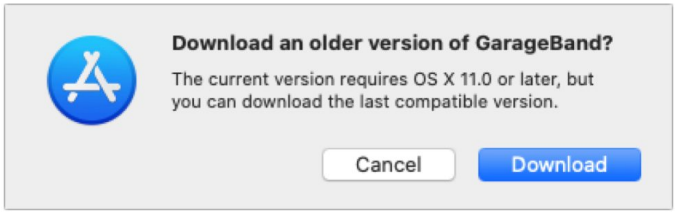
That entailed installing Big Sur on an empty drive and then pointing ChronoSync at it in accordance with Econ Technologies' instructions. Apart from a few days of accustoming myself to how ChronoSync manages scheduled backups and figuring out how to avoid a few seemingly irrelevant "date rollback" errors, it has worked fine. My general take is that ChronoSync is significantly more powerful than SuperDuper (and probably than Carbon Copy Cloner, with which I have little experience), and with that power comes added complexity.



Updating to GarageBand 10.4.2, Finally!

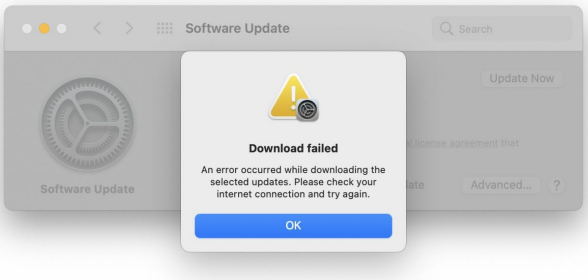
Upgrading to Big Sur had one immediate benefit. For unknown reasons much discussed in TidBITS Talk, Apple has made the update to GarageBand 10.4.2 require Big Sur while still showing it to everyone running Catalina. Every time you would check for updates in the App Store app, you'd get an error telling you that GarageBand could not be installed "because macOS version 11 or later is required." Bad Apple! In early February, Apple replaced the error with another dialog prompting the user to download "the last compatible version," ignoring the fact that it was already installed. So yeah, it's a minor thing, but upgrading to Big Sur let me stop seeing GarageBand in the update list (for other solutions, see "Hiding Apple's Big Sur Upgrade Badges," 19 November 2020).





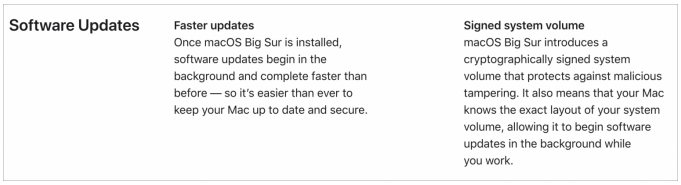
Big Sur Updating Issues

I don't know if this is related to Big Sur, Apple's update servers, or my Internet connection, but I've had trouble installing Big Sur updates. I must have tried to install macOS 11.2.3 at least 30 times between my 2020 iMac and M1-based MacBook Air, each attempt being met with a Download Failed dialog at varying points in the download process. Restarting the Macs, trying different user accounts, switching from Wi-Fi to Ethernet—nothing made any difference. (It seems unlikely to be our Internet connection, where we have 200+ Mbps downstream and don't notice any issues in videoconferencing.) While my iMac finally succeeded in updating, subsequent attempts on the MacBook Air continue to fail repeatedly.



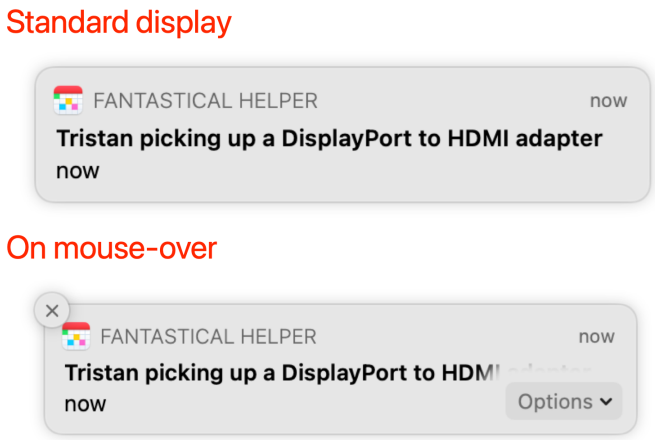
I haven't noticed such problems on the Macs running older versions of macOS, but they also haven't had as much to download—just occasional security and supplemental updates.

When Big Sur updates do download successfully, I'm unimpressed with how long they take to install. Apple promised that Big Sur would be faster at updating, but that's far from what I've experienced and what most people report. Just now, updating from 11.2.2 to 11.2.3 to fix a single WebKit security vulnerability on my iMac took nearly 30 minutes. During much of that time, my iMac showed a black screen with a progress dialog and a dubious estimate of time remaining.



Clearing Notification Alerts with the Keyboard

Finally, although folks in TidBITS Talk have assembled a long list of minor annoyances in Big Sur, mainly relating to its interface changes, the only one that has hampered my everyday usage is the hidden close button in notifications. For alert-style notifications, which remain on screen until they're dismissed, Apple replaced the Close button from Catalina with an X in the upper-left corner that appears only when you mouse over the notification. It suffers on both discoverability and accessibility grounds—you'd never guess it's there, and even once you know to look, it's a devilishly small target. If you have a trackpad on your Mac, you can swipe it away too, but I don't, so I went looking for a keyboard-driven approach.



As always, Peter Lewis's Keyboard Maestro proved to be the solution. On the Keyboard Maestro forum (nicely run in Discourse, like TidBITS Talk), Brad Bodine posted a macro that uses JavaScript to clear notifications. I attached it to the Clear key on my Das Keyboard's numeric keypad, and it works like a charm for dismissing notifications with the press of a key.

Gentlemacs, Start Your Engines!

To reiterate, I now think it's safe to upgrade from an earlier version of macOS to Big Sur, though I'd recommend scheduling it for a week or two after macOS 11.3 ships. Don't interpret that as me telling you that you should upgrade—if you wish to stick

with Mojave or Catalina for a bit longer, that's fine. (But if you're running High Sierra, it's best to update soon, given that you're not receiving security updates anymore.)

As always, though, remember that the longer you delay upgrading, the harder it's going to be and the more likely you are to run into problems. Upgrading is a *when* question, not an *if* question. As much as you might think you don't need any of the changes in new versions of macOS, no Mac is an island anymore. After enough time, a previously useful Mac will functionally degrade due to losing compatibility with updated apps, current Web browsers, security certificates, and online services.

Lastly, I just want to note that I find major upgrades like Big Sur exciting. Sure, it looks different, and there will undoubtedly be new quirks to work around, but that's been true of every major operating system release from Apple since the debut of the Macintosh. The tech world changes continually, and since there's no escaping that fact, we may as well enjoy it.

By Adam Engst

The Role of Bootable Duplicates in a Modern Backup Strategy

Is it time to upgrade to macOS 11 Big Sur? I'll write more about that soon. However, there is one general concern that has caused us to hesitate to recommend upgrading. That's the complexity of creating a bootable duplicate of your startup volume, also known as a clone. To understand why this seemingly simple task—just read all the data from one drive and write it to another—is causing such consternation, we need to step back briefly. And once we've done that, we can reassess the role of a bootable duplicate in a modern backup strategy.

Why Bootable Duplicates Have Become Difficult to Make

In 10.15 Catalina, Apple introduced APFS volume groups, a way of bundling separate volumes together to create a bootable macOS. A System volume holds all the files macOS needs to operate, while the Data volume contains only your data. The two volumes appear as a single entity in the Finder and wherever you might select or navigate files. The System volume is also read-only, so malicious software cannot modify the operating system, whereas the Data volume that contains your files remains read-write so you can install apps and create and modify documents.

This architectural change forced backup apps that make bootable duplicates to jump through hoops, since they couldn't just read and write data anymore. Now a bootable duplicate had to have a System and a Data volume, and they had to be combined correctly into an APFS volume group. Eventually, all the leading apps figured out how to do this: see "Carbon Copy Cloner 5.1.10" (26 August 2019), "ChronoSync 4.9.5 and ChronoAgent 1.9.3" (11 October 2019), and "SuperDuper 3.3" (30 November 2019).

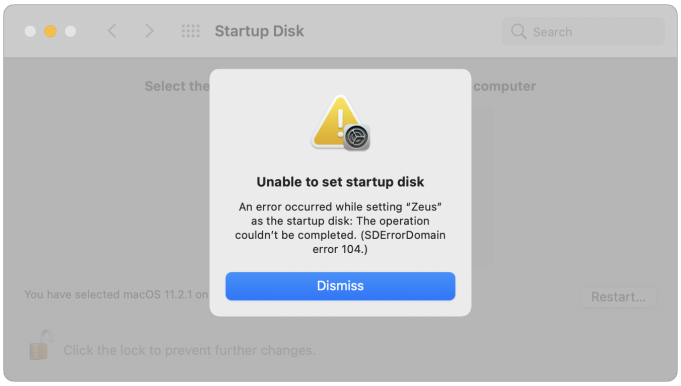
With Big Sur, however, Apple went a step further, adding strong cryptographic protections when storing system content on what is now called a *Signed System Volume*. (In fact, Big Sur doesn't even read files directly from this System volume to boot your Mac. It first takes the additional step of creating an immutable APFS snapshot—a reference to the volume at a particular point in time—and starts up from that snapshot. Thus, Big Sur is actually booting from a cryptographically signed,

immutable reference to a cryptographically signed read-only volume.)

This change increases security even more, but it also prevents all backup apps from creating bootable duplicates because they cannot sign the backed-up System volume. In theory, Apple's `asr` (Apple Software Restore) tool makes this possible, but it didn't work at all until just before Big Sur was released, still has problems, and even now cannot make a bootable duplicate of an M1-based Mac boot drive. On the plus side, Apple has said it plans to fix `asr`, but who knows when, or how completely, that will happen.

All three of the leading apps for making bootable duplicates have come up with workarounds. Carbon Copy Cloner *can make a one-time bootable duplicate of an Intel-based Mac (but you must boot from it to install macOS updates) and for M1-based Macs [italics added after publication]* recommends installing Big Sur onto a data-only backup after creating it. ChronoSync suggests installing Big Sur on an empty drive first and then using it for your data-only backup. The current version of SuperDuper has other issues with Big Sur, so SuperDuper's workaround involves downgrading to SuperDuper 3.2.5, using that to make a data-only backup, and then installing Big Sur on the backup drive if you need to boot from it. Unfortunately, once you do this, you can no longer copy to the backup until you delete the System volume, so it's best to stick with SuperDuper 3.2.5's data-only backups.

Things become even more confusing if you add an M1-based Mac into the mix. At the moment, Howard Oakley reports that you can make a bootable duplicate only onto a native Thunderbolt 3 drive—a USB drive doesn't work reliably for the purpose. That bootable drive also won't start up Intel-based Macs, even if you set up separate APFS containers. The reverse is true as well—an external drive that will boot an Intel-based Mac will not necessarily boot an M1-based Mac. So, even if you can make one, a bootable duplicate won't help you unless every Mac you want to use it with uses the same chip.



Do You Need a Bootable Duplicate?

Sometimes, when the world shifts in a way that renders past approaches unsatisfying, it's worth reexamining the base principles in play. Why have we recommended bootable duplicates as part of a backup strategy anyway? Three reasons:

- **Quick recovery:** The primary reason for having an up-to-date bootable duplicate is so you can get back to work as quickly as possible should your internal drive fail. Simply reboot your Mac with the Option key down at startup, select the bootable duplicate, and continue with your work. If your Mac were to die entirely, you could use the clone with another Mac you own or borrow, or a replacement that you can purchase and return within 14 days.
- **Secondary backup:** Any good backup strategy has multiple backup destinations, preferably created using different software. If you consider your primary backup to be Time Machine, for instance, having a bootable duplicate made with another app and stored on a separate drive protects against both potential programming errors in Time Machine and physical or logical corruption of its drive. It's best not to put all your eggs—or backups—in one basket.
- **Faster migration:** I have no data here, but if I needed to use Apple's Setup Assistant or Migration Assistant to migrate to a new drive or Mac, I'd prefer to use my bootable duplicate over my Time Machine backup. With Time Machine, the migration will have to figure out what the newest version of every file is, whereas the bootable duplicate is, by definition, an exact clone.

When you think about it, only the first of these reasons requires that the duplicate be bootable. A data-only backup using different software to a separate drive is sufficient for the second two.

The last time I needed to boot from my bootable duplicate was a disaster (see "Six Lessons Learned from Dealing with an iMac's Dead SSD," 27 April 2020). I had been backing up to a 5400 rpm hard drive connected to a 2014 27-inch iMac via USB 3.0, but using it as a boot drive was "painful beyond belief." Since then, I've switched to using a Samsung T5 external SSD for my bootable duplicate because its performance is so much better.

Performance isn't the only issue here. When my internal SSD died, I spent many hours troubleshooting the problem before discovering that my bootable duplicate wasn't going to help. I suspect that's common—you don't necessarily know that your internal drive is dead right away, so you're going to try to fix it before falling back on your bootable duplicate. Quick recovery? I could easily have reformatted my internal SSD and restored from a backup in the amount of time I spent troubleshooting. In fact, I started down that road too, only to discover that I couldn't even reformat, wasting even more time.

In the end, I got up and running with my everyday work using other devices: my 2012 MacBook Air, 10.5-inch iPad Pro, and iPhone 11 Pro. Most of what I do is in the cloud now, between email, Slack, Google Docs, and WordPress, so while I wasn't as productive on the other devices as I would have been on the faster, double-monitor iMac, I could get my work done. Since then, I've replaced the 2012 MacBook Air with an M1-based MacBook Air with more storage and vastly better performance, so I would have even fewer issues using it as my fallback Mac.

All this is to suggest that the bootable part of a bootable duplicate is no longer as essential for many people as it was when we first started recommending that a comprehensive backup strategy should include one. Since then, it has become far more common for people to have multiple devices on which they could accomplish their work, and much more of that work takes place in the cloud or on a remote server.

The Parts of a Modern Backup Strategy

Allow me to update what I consider to be the pieces you can assemble into a comprehensive backup strategy that acknowledges the reality of today's tech world. In order of importance:

- **Versioned backup:** Everyone should have a versioned backup made with Time Machine. Versioned backups are essential for being able to recover from corruption or inadvertent user error by restoring an earlier version of a file or the contents of a folder before deletion. Other backup apps, like ChronoSync and Retrospect, can make versioned backups too, but Time Machine backups are particularly useful because of how Apple integrates them into macOS migrations. I won't pretend that Time Machine is perfect, but it's part of macOS, has insider access to technical and security changes in macOS, and generally works acceptably.
- **Internet or offsite backup:** Local backups are worthless if all your equipment is stolen or damaged by fire or water. Historically, the recommendation was to rotate backup drives offsite, but in the modern world, an Internet backup service like Backblaze is much easier.
- **Backup Mac or another device:** Particularly given how hard it is for anyone but Apple to repair Macs, if you can't afford days of downtime, think about both what device you could use for your work if your Mac were to fail and how you'd get your data to it. It might be a laptop you mostly use when traveling, your previous desktop Mac, or even an iPad. Just make sure to take your backup device out for a test run before you need it.
- **Cloud-based access to key data:** This isn't a requirement—lots of people either can't or don't wish to store data in the cloud—but for many, it can be a way to access essential data from any device or location. For instance, $9.99 per month gets you 2 TB of iCloud Drive storage, and

Apple's Desktop & Documents Folders syncing feature could make it particularly easy to get back to work on another Mac. A similar amount of money would provide 2 TB storage on Dropbox, Google One, or Microsoft OneDrive.

- **Nightly duplicate, data-only or bootable:** Even if a duplicate can't easily be made bootable, it's still a worthwhile part of your backup strategy. It adds diversity by relying on different software in the event your Time Machine falls prey to bugs, by putting a backup on another drive, and by eliminating the need for special software beyond the Finder to restore data. And, of course, if you have to fall back to another Mac, a duplicate may be necessary so you can get back to work on your files.

Ensuring that you have an answer for all five options above would provide the most protection and the fastest recovery. But for many people, all five would be overkill.

I'd say that every Mac user should be making Time Machine backups, and some combination of Internet backup or cloud-based storage of data is a good idea. If your house were to burn down, wouldn't it be nice if you didn't lose your entire photo collection? iCloud Photos isn't a full backup like Backblaze is, but either would ensure the survival of your irreplaceable photos and videos.

People whose livelihoods depend on their ability to meet tight deadlines might feel the need to have a relatively powerful backup Mac available at a moment's notice, but for many people, an older Mac or less powerful laptop might be sufficient. For those who don't rely on their Macs for work, an iPhone or iPad might meet all your communications needs until you can repair or replace a dead Mac. Also, remember that you can buy a new Mac from Apple and return it within 14 days, something that Apple Store employees reportedly recommend as a way to get up and running while waiting for a repair.

Similarly, those who keep a lot of data in the cloud or simply don't value their data all that highly might be willing to risk having Time Machine be their only backup.

That said, I'll stick with my nightly duplicates because they're just too useful for troubleshooting and recovery. But I can't say that bootable duplicates are the necessity they once were.

What do you think? How often have you relied on a bootable duplicate to return to work quickly after an internal drive failure? Have you been stressing about bootable duplicates in Big Sur? How would you respond to your Mac failing entirely?

Apple Updates

macOS Catalina 10.15.7 Supplemental Update 2
Feb 8, 2021 – 1.35 GB

System Requirements
– macOS 10.15

macOS Catalina 10.15.7 supplemental update addresses an issue that may prevent the battery from charging in some 2016 and 2017 MacBook Pro models.

Security Update 2021-002 (Mojave)
Feb 8, 2021 – 1.63 GB

System Requirements
– macOS 10.14

Security Update 2021-002 is recommended for all users and improves the security of macOS.

Security Update 2021-001 (Mojave)
Feb 5, 2021 – 1.75 GB

System Requirements
– macOS Mojave

Security Update 2021-001 is recommended for all users and improves the security of macOS.

Graphics Hold Area

Apple Updates

?

? ? ?