April 2022
Vol. XLI, No 04

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ www.keystonemac.com

Keystone MacCentral April Program

April 19, 2022 07:00 PM

Please see your membership email for the links to this month's Zoom meeting or email us at KeystoneMacCentral@mac.com.

This month we plan to have presentations on

Finder
(that really important thing that allows us to work with our computers)
and

Digital Wills
(best to plan ahead)

We might even have more about SnapSeed.

We have virtual meetings via Zoom on the third Tuesday of each month.

Emails will be sent out prior to each meeting. Follow the directions/invitation each month on our email – that is, just click on the link to join our meeting.

Contents

By Josh Centers

Apple Releases iOS 15.4, iPadOS 15.4, macOS 12.3 Monterey, watchOS 8.5, tvOS 15.4, and HomePod Software 15.4

Just ahead of its new devices shipping this week, Apple has released iOS 15.4, iPadOS 15.4, macOS 12.3 Monterey, watchOS 8.5, tvOS 15.4, and HomePod Software 15.4.

The most significant addition to the Apple experience from these updates is Universal Control, which Apple is still labeling as a beta. Universal Control lets you use the same keyboard and pointing device to control multiple Macs and iPads, switching between devices seamlessly. At least that's the theory. We'll put it through its paces soon.

Many of the changes are shared among the different operating systems, so we've covered most of the ground for iOS 15.4 and then focused on the differences for the rest. Note that after you update to iOS 15.4 and iPadOS 15.4, you'll be greeted by a new "Hello" screen that writes out the word in numerous different languages, much like the Hello screensaver in Monterey.

When should you update? If you're interested in trying Universal Control or having Face ID on your iPhone work even when you're masked, we suggest waiting a couple of days to ensure there aren't unexpected gotchas. Those who don't find those features compelling can wait a week or two since Apple doesn't identify any of the security fixes as being actively exploited.

Either way, these are probably the final feature releases of Apple's 2021 operating systems. Apple will likely unveil the next major releases in June at WWDC and release them to the public in September, so until then, you can expect mostly security updates and the occasional bug fix.

iOS 15.4

The big win of iOS 15.4 for those using an iPhone 12 or later is that Face ID should now work when you're wearing a mask. The feature requires setting up Face ID again, and if you wear glasses, it asks you to train Face ID with and without your glasses. Those who wear multiple pairs of glasses can add those to the training set, too.

The update also provides new emojis and a new gender-neutral Siri voice, and it lets you initiate SharePlay directly from supported apps (see "How to Use FaceTime Screen Sharing and SharePlay," 8 November 2021). You can finally add notes to saved passwords, making Apple's built-in password manager more capable. European users can now use the Health app to download their EU Digital COVID Certificate and display it in Wallet.

iOS 15.4 provides a slew of smaller improvements as well:

- Podcasts lets you filter episodes by season, played status, and saved or downloaded episodes.
- You can manage iCloud custom domains from Settings (see "How to Set Up Custom Email Domains with iCloud Mail," 27 August 2021).
- News makes audio content more discoverable in the Today feed and Audio screen.
- It's now easier to add Live Text to Notes and Reminders.
- Safari translation now supports Italian and traditional Chinese.
- Emergency SOS is now activated by pressing and holding the side button by default. Triggering Emergency SOS with five presses of the side button remains an option.
- The Magnifier app now uses the ultra-wide camera on the iPhone 13 Pro and Pro Max for better closeups.
- Siri can now provide offline time and date information on the iPhone XS, iPhone XR, and the iPhone 11 or newer.

When you upgrade, you may also appreciate iOS 15.4's bug fixes:

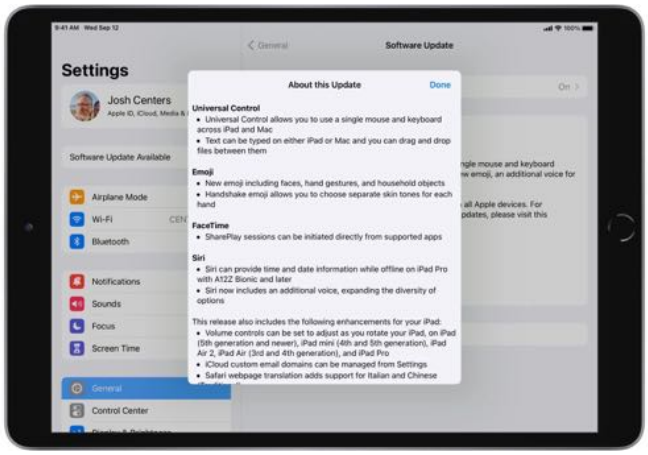
- The keyboard no longer puts periods between typed numbers.
- News widgets in the Today view now reliably open articles when tapped.
- Photos and videos now sync to iCloud Photos more reliably.
- Live Listen can now reliably be turned off in Control Center.

iOS 15.4 and iPadOS 15.4 include 36 security updates. The update is a 1.21 GB download on an iPhone 11 Pro.

iPadOS 15.4

Other than Universal Control, the high points of iPadOS 15.4 are similar to those of iOS 15.4. The differences are as follows:

- Siri can now provide offline date and time for any iPad Pro with an A12Z Bionic processor or later.
- You can set volume controls to change when you rotate your iPad on the fifth-generation iPad, fourth-generation iPad mini, iPad Air 2, and iPad Pro or later.
- Security recommendations in Settings can now be hidden.
- The Speak Screen Accessibility feature should no longer crash in the Books app.



The iPadOS 15.4 update is a 914.2 MB download on a 10.5-inch iPad Pro.

macOS 12.3 Monterey

Besides Universal Control and the changes in iOS 15.4, the big changes in macOS 12.3 Monterey are:

- Dynamic head tracking for spatial audio is available in Music if you're using an Apple silicon Mac and compatible AirPods—you can adjust the settings in Control Center.
- Shortcuts now supports adding, removing, and querying tags with Reminders.
- Battery capacity readings should be more accurate.

macOS 12.3 Monterey includes 45 security fixes, and the update is a 4.38 GB download.

watchOS 8.5

watchOS 8.5 has fewer notable changes than the other updates:

- You can now use your Apple Watch to authorize Apple TV purchases in tvOS 15.4.
- You can display your EU Digital COVID Certificate on an Apple Watch.
- Apple improved irregular atrial rhythm notifications.
- Apple Fitness+ includes audio hints for visually demonstrated moves during workouts.

watchOS 8.5 features 22 security fixes, and the update is a 542 MB download for an Apple Watch Series 4.

tvOS 15.4

As mentioned above, tvOS 15.4 lets you authorize purchases using an Apple Watch running watchOS 8.5. You can also keep a constant eye on a HomeKit camera in a Picture in Picture window while watching another program. Finally, tvOS 15.4 supports "captive portal" Wi-Fi networks that force you to click through a Web page before connecting, as you may see at hotels.

tvOS 15.4 includes 21 security fixes.

HomePod Software 15.4

If you've been hoping to take your HomePod on vacation, HomePod Software 15.4 includes support for those "captive portal" Wi-Fi networks. It also adds Siri voice recognition support for Dutch and French, perhaps suggesting where you might take that vacation.

By Glenn Fleishman

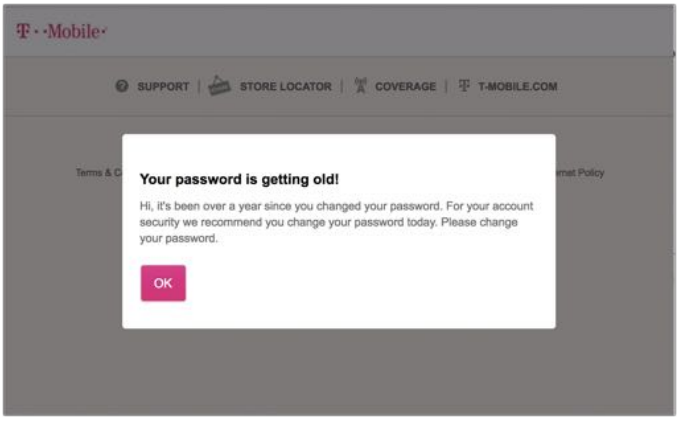
Never Change Your Password

I'm going to set off all your smoke alarms when I make this fiery statement: *Never change your password.* Before you call the fire department, consider these three crucial provisos. Never change your password…

1. **If it's sufficiently strong**
2. **If you created a unique one for each account**
3. **Unless there's a security breach where it's stored**

Passwords do not age. They do not sour, spoil, or go stale. Yet some organizations want to convince us that your passwords become increasingly

susceptible to attack over time. Just yesterday, I logged into my T-Mobile account and was told my password was old and should be changed. Fortunately, the carrier included a Skip button—which wasn't always the case.



T-Mobile used to require you to change your password every 12 months, as shown. Now it offers a Skip button.

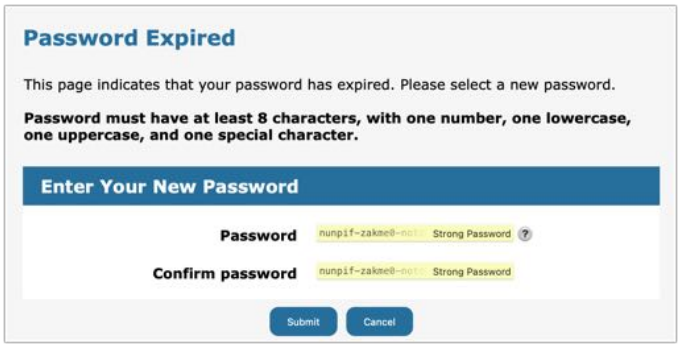
The reason to change a password should relate to an active problem: someone has stolen your password, it's so weak that someone will crack it any moment now, or you're notified of a password leak. Otherwise, there's no reason ever to bother.

Where did this idea of passwords having an expiration date originate, and why is it wrong? To find out, let's delve into what's behind each of those three provisos.

Proviso #1 Background: Very Old Passwords Were Too Weak

It was only in 1960 that computing systems began to require passwords. For 40 years, they remained weak and crackable, often with only modest effort. You often weren't even allowed to create a password longer than 8 characters. This was considered not just an acceptable level of security, but the only necessary level of security. For much of that time, you could even use a dictionary word or words or all letters—no punctuation, mixed case, or numerals required.

Once networks interconnected, even before the Internet existed, password theft became a problem. In the early days, you could just print out a file that contained the passwords in plain text. (The first admitted theft was in 1962!) As passwords became better protected within operating systems, weak, guessable passwords remained a liability. System administrators began issuing password guidance and enforcing it. That's where the now-familiar demands for complexity and regular rotation originated.



As recently as 2004, the National Institute of Standards and Technology produced a report that recommended complexity in password composition rules in part because password length was so short. The ability to crack a password becomes nearly exponentially more difficult the longer it is. Increasing complexity (the randomness of characters chosen) doesn't increase the cracking difficulty as easily as simply making a longer password.

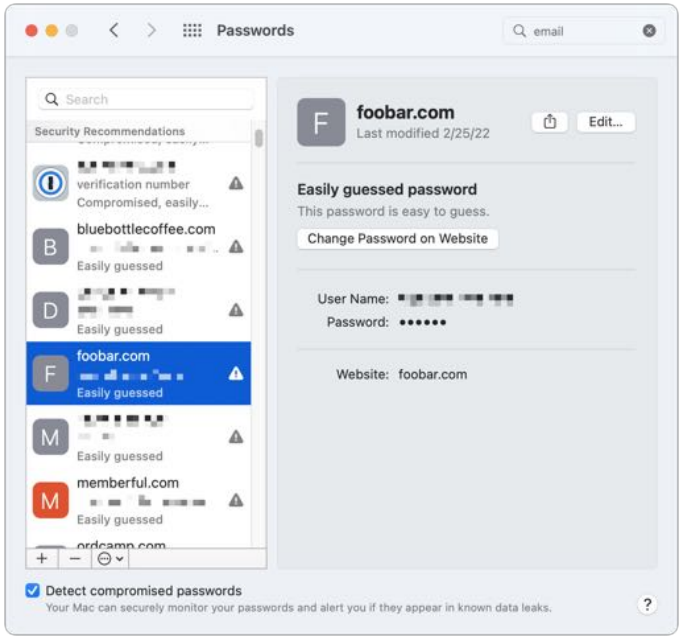
Some sites still allow 8-character passwords, but my anecdotal experience is that most want something longer, like 10 or even 12 characters. The shortest secure password resistant to modern cracking is a minimum of 12 characters if it's randomly generated from nearly all typeable symbols and at least 20 if it is composed of randomly selected words. Passwords that meet those limits have sufficient resistance to brute-force cracking that they should last well beyond your lifetime or cost a cracker far more than your specific password could be worth—perhaps tens of billions of dollars, by one estimate. Substantial breakthroughs in certain forms of computation would be required to render those passwords weak enough to break. (Astonishingly, Microsoft still recommends a minimum password length of 8 characters in its Windows 10 administrator

guidance and doesn't allow policies to require one longer than 14.)

In an era of weak passwords, a high level of entropy—the amount of measurable randomness in the password text—coupled with regular replacement reduced the odds someone would have sufficient time and processing power to crack your password using what was often an easily purloined password file or database table. (I first had a password file stolen in 1994 due to a Unix exploit.)

If your password is sufficiently strong, as required by Proviso #1 above, there's no reason to change it. If, on the other hand, you're still rocking a password under 12 random characters, yes, you should change it to something much stronger. But you only have to do that once. There may never be a reason to replace it.

How can you tell if your password is weak? Apple will tell you, via iOS/iPadOS in Settings > Passwords, Safari in Safari > Preferences > Passwords, and macOS 12 Monterey in System Preferences > Passwords. 1Password, LastPass, and other password managers offer similar insights.

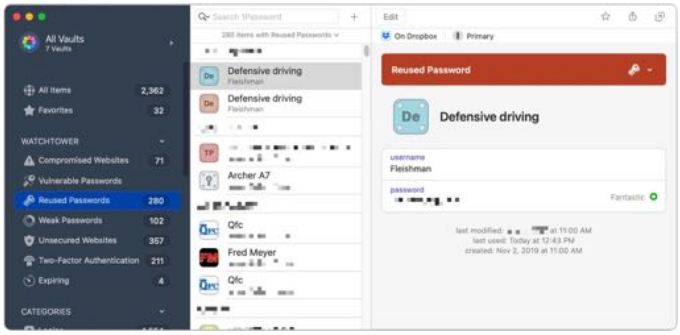


Proviso #2 Background: Passwords Were Often Reused

For many years, it was also acceptable to create one strong password and use it across all your important accounts. While that password may have been hard to type and difficult to memorize, regular use helped you surmount those problems. This was the ultimate instance of putting all your eggs in one basket. Security experts quite rightly saw this approach as a serious vulnerability. I suspect that some password change requirements came about because sysadmins understood that if your password was broken or leaked somewhere else, it could also allow access to their systems. That wasn't excessive caution—breaches happened regularly, including for accounts with deep system privileges. Forcing a replacement was a misguided way to try to stay ahead of crackers, the assumption being that older passwords were more likely to be discovered and cracked elsewhere.

Because we now have easy access to password managers—including Apple's built-in option in iOS, iPadOS, and macOS that can be synced across iCloud in a highly secure manner—there's absolutely no excuse to use the same password twice, per Proviso #2. Memorize your device passwords or, with 1Password and other password managers, your vault or storage password. Never use those passwords elsewhere. And you're golden.

If you're not sure whether or not you have used a password at multiple sites, check your password manager. Apple's Passwords shows Reused under Security Recommendations for any password with multiple entries. 1Password's Watchtower section, shown below, has a Reused Passwords category that lists the same. LastPass has a similar feature in its Security Dashboard.



Password managers must still deal with the vagaries of websites that require passwords to contain at least one number, a piece of punctuation from a permissible list, and an eye of newt. The last item might be a joke. (These policies are designed to ensure the most cracking-resistant password if a user chooses to enter one of only the minimum length.) But at least you can use the password manager to generate the best strong password under the circumstances.

You should still use a password manager to create passwords even when there are no complexity policies in play. Apple discontinued a feature in Keychain Access's Password Assistant to create "memorable" passwords that contained words. 1Password recommends a passphrase of four or five words, depending on your circumstances, to achieve the necessary robustness.

Proviso #3 Background: In the Security World, Life's a Breach

Once you have updated to robust, unique passwords across all your accounts, you never need to change those passwords again unless, per Proviso #3, you learn that a particular site or service has suffered a breach. The best way to learn this is by signing up for the free notification service at Have I Been Pwnd?, a site devoted to disseminating information about account and password breaches in a responsible fashion. You can also check your password manager, as most now license the Have I Been Pwned? database. Apple shows Compromised in its passwords list across operating systems, noting:

This password has appeared in a data leak, which puts this account at high risk of compromise.

Despite Apple's extreme language, you probably don't *need* to change your password even then—assuming, again, it's strong and unique—but it's better to be safe than sorry. Plus, you may have no choice: the site might force you to change it by resetting all passwords for all users.

An attacker can discover passwords in two primary ways: research and cracking. With research and manipulation, an attacker can extract secrets about you through social engineering (fooling a customer-service representative), phishing your password from you, or poring over credit reports and available online data.

You can guard against personal social engineering and phishing by never giving out your password in any circumstance other than when you initiate a visit to a Web site or open an app and can verify it's the site or app you intended. And you can protect your personal facts by replacing them with random words when creating answers to account security questions. Instead of my mother's maiden name, I generate a random word in my password manager and use that, storing it with a label so I can recall it when asked. The goal is to ensure that the answers to your security questions are also unique across all your accounts. (If you have to read the secret aloud to a customer service rep, it may sound strange, but that's the price of security.)

The other method attackers use is cracking passwords, trying to match a password by testing every possible value, starting with the shortest and most likely guesses. Those guesses might incorporate socially engineered and researched information about you in particular or a mass of users at a given website.

Crackers used to be able to run unlimited password guessing attempts at many website login pages. It took shockingly long for companies to build in throttles and timeouts to disable such attacks. Nowadays, only targeted knowledge that doesn't exceed a maximum number of failed attempts may work, and two-factor authentication stops that method cold. Crackers don't bother with such attacks anymore unless they find unthrottled login pages.

Instead, they focus their attention on cracking passwords stolen from servers. In those cases, you're forced to rely on the security and deployment expertise of the company that maintains your account information. Almost all the time, these passwords are encrypted and can be broken only by brute force. Sadly, that's not always the case: as recently as November 2021, a large-

scale breach at GoDaddy revealed SFTP passwords still stored as plain text.

Sites should never store passwords as plain text, but they also can't use simple encryption, where a static encryption key protects all password data. Instead, sites almost always store each password as the unique outcome of a cryptographic operation called a *hash*. The hash can't be guessed from the input, so two slightly different passwords produce vastly different hashes. Best practices for modern password storage also include adding random characters (called a *salt*) to a password before hashing to prevent an attacker from cracking a password used identically with multiple accounts at once. (If two people chose "adam-slurps-soup-soulfully" as their password, the hashing operation would produce the same hash. If you add "Az" and "8J" to the front of that password before hashing, the two resulting hashes would be completely and unpredictably different.)

The only way to figure out a password with no special knowledge of the user is to feed every possible combination through the same hashing algorithm and test against the stored value. Because these algorithms are computationally "expensive" (slow) to run, it can take a lot of time (and therefore money), even when throwing a lot of GPU or cloud processing power at it.

In cases where breached passwords were salted and used sufficiently powerful modern hashing algorithms, I'm unaware of any reports of accounts being compromised. Add good two-factor authentication to the account, and exploitation becomes nearly impossible.

All that said, when you're notified of a breach that may have revealed your login credentials, change the affected site's password anyway: it's only one, and you don't know how good the site's internal security design was.

What Should You Do?

Here's a simple checklist of improvements you can make to keep your passwords forever secret:

- If you aren't already, start using a password manager.
- Use the password manager to generate strong, unique passwords for every account.
- Review old accounts that contain personal, proprietary, or financial information and update their passwords using the password manager.
- Never share personal facts, like your pet's name, when required. Instead, replace a real fact with random text that you store in your password manager for later access.
- Enable two-factor authentication wherever available.

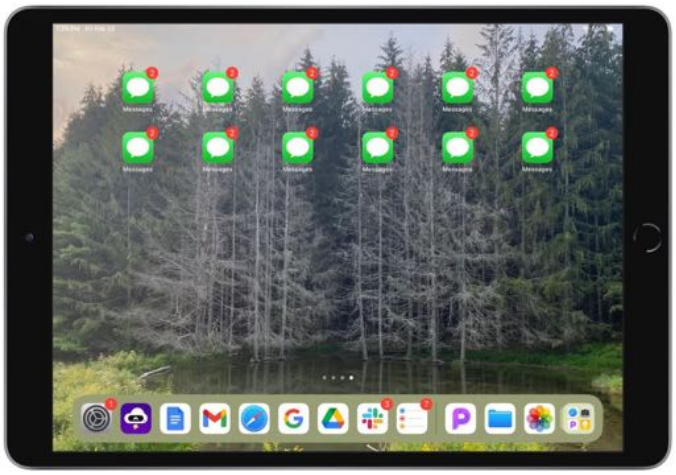
Finally, to return to the point of this article: Don't change a website's password purely because you're asked to. Only feel compelled to change it if it's weak, if it was used on other sites, or if a breach has occurred. And, if some site forces you to change your password, generate a new one that's strong and unique using your password manager.



By Adam Engst

How to Create App Aliases in iOS 15

Every so often, you make a discovery that throws the world as you know it into disarray. My latest foray into the Twilight Zone came when I found that it is now possible to create aliases to apps in iOS 15 and iPadOS 15. No longer are you limited to an app appearing just once on your Home screen—it can appear on multiple Home screen pages, in multiple folders, or even multiple times on the same Home screen page, pointless though that may be apart from making seemingly impossible screenshots!



Since each alias looks and works like every other one, this capability enables you to store an app in multiple folders—perhaps you want Messages to appear both in a folder for Apple apps and another that holds communications apps. Or, you could simulate a second iPhone "dock" by positioning the same four apps in the top or bottom row of each of your Home screen pages. It also may make Focus more useful by letting you specify custom Home screen pages containing aliases for different focuses (see "Apple's New Focus Feature May Be Overkill," 20 January 2022).

Through the Looking Glass

How do you create these app aliases? Before I explain, let me share another new feature of iOS 15 and iPadOS 15. When you swipe down from the middle of the Home screen page to invoke Search, you can work with any app that appears—either in the Siri Suggestions section or as a result of a search—just as though it were on the Home screen.

In short, you can now delete or move an app from Search. Touch and hold the app to reveal its contextual menu (including the Delete App option) or start dragging to move it to the Home screen. This feature would have been nice to have in pre-App Library days when searching was often the only way to find an app hidden among multiple Home screen pages. Note that deleting an app really deletes it from your device—you don't get an option to merely remove it from the Home screen.

While playing with the capability to drag apps out of Search to the Home screen, I inadvertently dropped an app into a folder, only to realize that the app already existed on another Home screen page. How could such a thing be possible? Before this, an app could appear only once on the Home screen.

I dug deeper and discovered that as long as I started the search from a Home screen page that did not already contain the app, I could drag the app directly to the Home screen. (When I started the search from a Home screen page containing the app, dragging it from the Search screen resulted in the existing app moving.) The world was turning upside down!

Next, I checked to see if this technique worked from the App Library as well. It did! Dragging an app from the App Library to a Home screen page created an alias. Again, there was a caveat. It worked unless the rightmost Home screen page already contained the app, which again caused the existing app to move.

Since dragging immediately to a Home screen page containing the app prevented an alias from being created, I tried dragging an app from one Home screen page to another that already contained the

app. Unlike the previous failures, this drag completed successfully, giving me two icons for the same app next to one another. The insane iPad screenshot at the top of the article is the best evidence yet that we're living in an alternative reality—I swear that I created it by repeatedly dragging the Messages icon from Siri Suggestions to another Home screen page and then over to this page.

How to Create App Aliases

Here are the step-by-step instructions for creating iOS app aliases from the Search screen. You can see the process live in Josh's video below (which has nothing to do with Spiderman besides the title card that he couldn't resist):

1. From a Home screen page that does not contain the app for which you want to create an alias, swipe down to invoke Search.
2. Find the desired app in either Siri Suggestions or by searching.
3. Touch and hold the app icon and start dragging. The Home screen will reappear in jiggle mode.
4. Drop the app in the desired location on any Home screen page.

Or, from the App Library:

1. Ensure that the app for which you want to create an alias is not on the rightmost Home screen page.
2. Swipe left from that page to open the App Library.
3. Find the desired app, either by browsing through the App Library or searching within it.
4. Touch and hold the app icon and start dragging to enter jiggle mode. You can also touch and hold a blank spot in the App Library to enter jiggle mode first and then drag the app.
5. Drop the app in the desired location on any Home screen page.

Apple Updates

What's new in Shortcuts in iOS 15.4 and macOS 12.3
Mar 16, 2022

Overview

- Notifications can now be turned off for Automations (when Ask Before Running is turned off)
- Added support for tags in "Add New Reminder", "Find Reminders", and "Edit Reminder"
- "Get Current Web Page from Safari" now supports retrieving details like name, page contents, and selection on macOS
- "Set Playback Destination" now supports adding and removing playback destinations, so you can play to multiple devices at once
- "Translate Text" and "Detect Language" are now powered by Apple Translate
- "Take Photo" is now supported on macOS
- "Extract Text from Image" now supports all languages supported by Live Text
- "End If" and "End Repeat" can now be dragged in the Shortcuts editor
- "Find" and "Filter" actions have an improved design on macOS

- Double-clicking on an item in “Choose From List” now chooses the item and continues running on macOS
- On macOS, you can now add a shortcut to the Dock from the right-click menu in My Shortcuts
- Text entry dialogs can now be dismissed with the ⌘+return keyboard shortcut on macOS
- A “Provide Output” checkbox is now available in Shortcut Details, making it easier to use shortcuts with output
- The set of action icons in the Shortcuts editor have a refreshed appearance
- Automator Quick Actions can now be converted to shortcuts
- Fewer privacy prompts are presented, especially for shortcuts that you author yourself
- The Gallery now includes a Share button when viewing a shortcut on macOS

Editor

- Clicking the delete button on actions in the Shortcuts editor works more reliably on macOS
- Text entry works more reliably in the Shortcuts editor
- Items can now be reliably re-arranged in “Choose from Menu”
- Improved Shortcuts editor UI and reliability

Actions & Running

- “Run Shortcut” is now faster and more reliable
- “Combine Images” no longer produces empty images on macOS
- "Overlay Image” now uses coordinates anchored to the bottom-left instead of the top-left on macOS, to match iOS behavior
- ”Open URL” no longer fails when run from Apple Watch
- “Show in Calendar” now supports showing dates on macOS, in addition to calendar events
- “Edit Calendar Events” no longer fails to add attachments on macOS
- “Show Web Page” now includes Cancel and Done buttons on macOS
- “Send Message” can now send photo attachments when run from Siri
- “Open App” can now launch CarPlay-capable apps in CarPlay
- “Set Volume” now works on macOS when AirPods are connected
- “Send Email” now supports the “From” picker on macOS
- “Split Screen Apps” no longer fails to run if the apps are not already open
- “Eject Disk” no longer fails to eject an external disk drive on macOS
- “Delete Files” no longer fails to delete files in Dropbox
- “Get the state of My Home” now returns results more reliably
- Pinboard actions no longer show an unexpected keychain prompt when run on macOS
- The “Wind Down Begins” & “Bedtime Begins” automations now trigger more reliably
- The “Device Details” variable’s Screen Width and Screen Height options now return correct values
- Converting text to PDFs now works on macOS
- Fixed issues where calendar-related actions may fail unexpectedly
- Applications now properly re-gain focus when a shortcut dialog finishes on macOS

Scripting

- The list of shortcuts now loads faster in 3rd party apps on macOS, especially for users with many shortcuts
- The "Shortcuts Events" app, which provides scripting functionality for Shortcuts on macOS, no longer needs to be opened manually before it can be used from scripts
- When retrieving shortcuts via AppleScript, shortcuts are returned in the user’s order instead of in alphabetical order
- Other bug fixes and minor additions

Security Update 2022-003 (Catalina)
Mar 16, 2022 – 1.45 GB

macOS Catalina Security Update 2021-003 (19H1824) is recommended for all users and improves the security of macOS

Unitor Family Driver v3
Mar 11, 2022 - 319 KB

The Unitor driver is required for the following MIDI interfaces Unitor8, AMT8, and MT4