November 2019
Vol. XXX, No 10

KEYSTONE MacCentral

printout

Keystone MacCentral Macintosh Users Group ❖ http://www.keystonemac.com

November Program

Dennis will also discuss the RAVPower FileHub. This device appears to be a very valuable tool for travelers. The FileHub

- is a travel router
- provides wireless storage backup for your phone or tablet
- supports reading usb hard drives up to 3tb and sd/sdhc/sdxc cards up to 256gb
- provides one key backup from sd card to usb hard drive

We will discuss other items of current interest.

Meet us at

Bethany Village Retirement Center

Education Room
5225 Wilson Lane, Mechanicsburg, PA 17055

Tuesday, November 19th 2019 6:30 p.m.

Attendance is free and open to all interested persons.

Contents

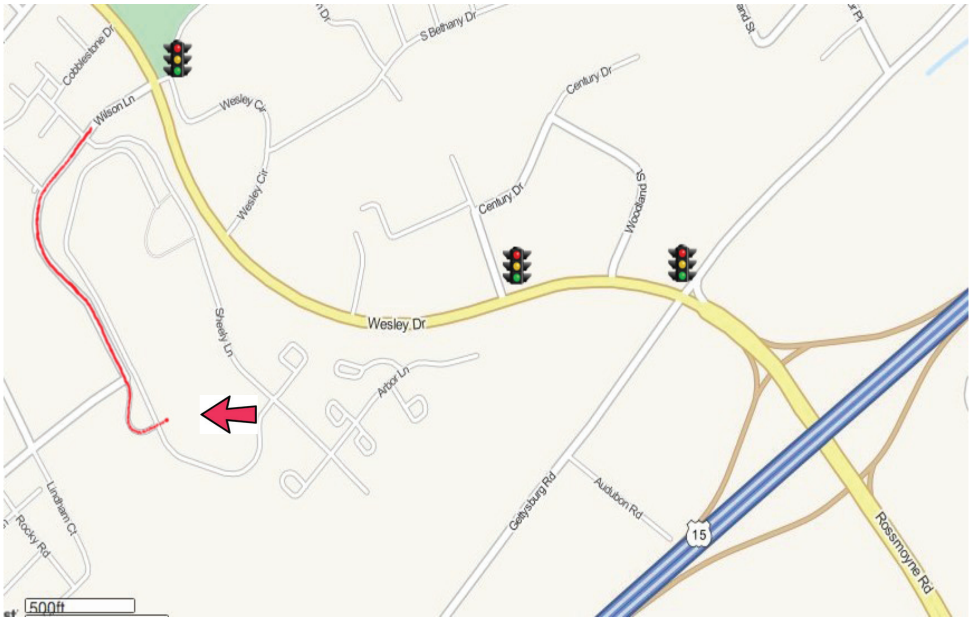
Keystone MacCentral is a not-for-profit group of Macintosh enthusiasts who generally meet the third Tuesday of every month to exchange information, participate in question-and-answer sessions, view product demonstrations, and obtain resource materials that will help them get the most out of their computer systems. Meetings are free and open to the public. The *Keystone MacCentral printout* is the official newsletter of Keystone MacCentral and an independent publication not affiliated or otherwise associated with or sponsored or sanctioned by any for-profit organization, including Apple Inc. Copyright © 2019, Keystone MacCentral, 310 Somerset Drive, Shiresmanstown, PA 17011.

Nonprofit user groups may reproduce articles form the Printout only if the copyright notice is included, the articles have not been edited, are clearly attributed to the original author and to the Keystone MacCentral Printout, and a copy of the publication is mailed to the editor of this newsletter.

The opinions, statements, positions, and views stated herein are those of the author(s) or publisher and are not intended to be the opinions, statements, positions, or views of Apple, Inc.

Throughout this publication, trademarked names are used. Rather than include a trademark symbol in every occurrence of a trademarked name, we are using the trademarked names only for editorial purposes and to the benefit of the trademark owner with no intent of trademark infringement.

Board of Directors



Keystone MacCentral Essentials

Meeting Place
Bethany Village West
Maplewood Assisted Living (Bld 21)
5225 Wilson Lane
Mechanicsburg, PA 17055

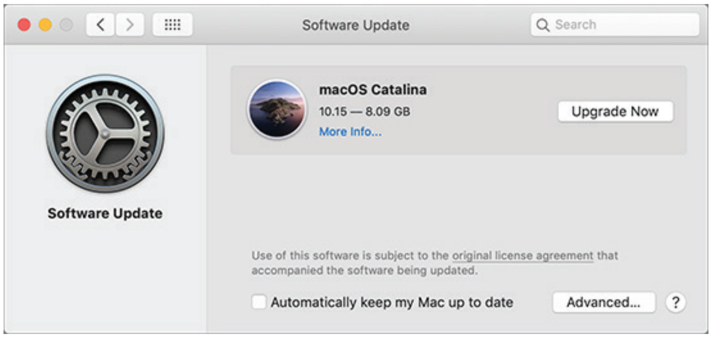
Web Site
http://www.keystonemac.com

Mailing Address
310 Somerset Drive
Shiresmanstown, PA 17011

By Adam Engst

macOS 10.15 Catalina Ships, Upgrade with Caution

Apple today released macOS 10.15 Catalina, leaving just iOS 13 for the HomePod and watchOS 6 for the Apple Watch Series 1 and Series 2 as vaporware. Catalina advertises itself as an 8.09 GB download in System Preferences > Software Update, but its App Store page claims that it's only 4.9 GB. For an overview of what's new, see "No Mac Is an Island with macOS Catalina" (3 June 2019).



Use of this software is subject to the original license agreement that accompanied the software being updated.

□ Automatically keep my Mac up to date

We're dying to know if, as Michael Cohen pointed out in our TidBITS Slack group, Apple intentionally waited to release Catalina on the 477th anniversary of the Portuguese explorer Juan Rodríguez Cabrillo claiming Santa Catalina Island for Spain on 7 October 1542. It certainly wasn't a discovery — the island had been inhabited by the native Pimugnans since 7000 BCE.

Regardless of whether or not the release date is a historical coincidence, you're now faced with the question of when to upgrade to Catalina. Note that I say "when" and not "if" because something, such as the purchase of a new Mac, the need for updated software, or compatibility with iOS, will force you to upgrade at some point. It's better to do so proactively than reactively. When that time comes, we strongly recommend that you follow the advice in Joe Kissell's *Take Control of Upgrading to Catalina.*

Nevertheless, for most people, we recommend delaying your upgrade for a while for a variety of reasons:

Catalina won't run 32-bit apps: No TidBITS readers should be surprised by this news at this point. If you rely on 32-bit apps, you'll need to upgrade them (which may be expensive), find alternatives (which may be pricey and comes with a learning curve), or run them in a virtual machine (see "Moving to Catalina: Keep Your 32-Bit Mac Apps Running with Parallels," 18 September 2019). If you still need to download Mojave, Apple has a support document explaining how to get it.

Some backup apps aren't yet compatible with Catalina: One of the big changes in Catalina is the way macOS runs from a read-only system volume that's separate from the writeable data volume that stores your apps and documents. This change, along with others, has caused issues for backup apps. Developers are taking it into account, but it would be stupid to upgrade to Catalina before your backup app supports it. Pay attention to the TidBITS Watchlist for important updates. For instance, Carbon Copy Cloner 5.1.10 and later are compatible with Catalina, as is Retrospect 16.5, but Shirt Pocket has yet to make a statement about SuperDuper's Catalina compatibility.

Catalina's notarization requirements may cause trouble: One of the ways Apple has increased security with Catalina is to require that apps distributed outside the Mac App Store be notarized by Apple to run. Those requirements don't apply to previously distributed software, so older apps already on your Mac should continue to run, but you may not be able to install an older, unnotarized app in Catalina.

Catalina forces apps to request more permissions than before: Again, in the interests of increasing security and privacy, Apple requires apps to request more permissions in Catalina than in previous versions of macOS. In Catalina, apps will have to ask for permission to access files in your Desktop and Documents folders, iCloud Drive, and external volumes. Plus, you'll be prompted before any app can capture keyboard activity or a screenshot or screen recording. That's good for security, but it's possible that older software won't know how to ask or won't work correctly if you deny its request.

There could be unanticipated backward-compatibility issues: This concern is purely speculative, but it has bitten Mac-using offices in the past. In essence, if you upgrade to Catalina, that may force you to upgrade an app you rely on. If the new version of that app saves its documents in a format that older versions can't read, that could cause problems for users whose Macs either shouldn't be upgraded right away or can't be upgraded at all.

Apple's OS releases so far this year have been riddled with bugs: Apple's software testing, coupled with reports from users of the public betas, has historically done a decent job of identifying and fixing the most common and annoying bugs in major operating system releases. This year, however, in less than two weeks, Apple has already released iOS 13.0, 13.1, 13.1.1, and 13.1.2; iPadOS 13.1, 13.1.1, and 13.1.2; and watchOS 6.0 and 6.0.1 (for only the Apple Watch Series 3 and later). We're always happy to see Apple fix bugs quickly, but we'd prefer to wait longer for releases that are less buggy.

We have no way of knowing whether Catalina will suffer from the kind of bugs that Apple has been scrambling to fix in iOS, iPadOS, and watchOS, but it's worth being cautious. We often recommend that those who aren't early adopters wait until the .1 or .2 releases; when those come out, we'll adjust our upgrade advice as appropriate. We're not alone in recommending caution — at Six Colors, Jason Snell has published his full review of Catalina, titling it "macOS Catalina review: New era ahead, proceed with caution."

Of course, if you love trying the latest and greatest and have a test Mac that you don't rely on to get your work done, feel free to upgrade to Catalina right away! That's what many of us are doing, and if we end up capsized by Pacific storms en route to Catalina, well, we knew what we were signing up for.

By Josh Centers

Here's What Sets iPadOS Apart from iOS

After some uncertainty on the release date, iPadOS is now out. While Apple markets iPadOS as being a completely different operating system than iOS, it's essentially iOS 13.1 with a few iPad-specific features. You can download iPadOS 13.1, which weighs in at 3.02 GB on a 10.5-inch iPad Pro, through Settings > General > Software Update or via iTunes. (Shortly after releasing iPadOS 13.1, Apple followed up with iPadOS 13.1.1 to fix bugs in the initial release —see "iOS 13.1.1 Fixes Bugs and Keyboard Security Issue," 27 September 2019.)

In addition to iOS 13 features like improved text editing, Sign in with Apple, enhanced Maps, and redesigned photo editing, iPadOS improves the multitasking system, beefs up Safari to support complex Web apps, adapts the Home screen for the larger iPad screens, improves markup features, and adds a new one-handed floating keyboard. For more on iOS 13 and iPadOS, see my freshly updated book, *Take Control of iOS 13 and iPadOS 13*.

Multitasking in iPadOS

Apple enhanced the multitasking system in iPadOS in small ways, so it's better, but not drastically different than how it worked in iOS 12. In fact, it remains entirely possible to use an iPad without even realizing it can do multitasking. (That's not necessarily a bad thing — while there are plenty of excellent use cases for Split View and Slide Over to see two apps or windows at once, a case can also be made for increasing your productivity by focusing on only one thing at a time.)

As in iOS 12, you usually initiate iPad multitasking from the Dock. While viewing an app, pull up the Dock by swiping up from below the bottom of the screen. Tap, hold, and then drag an app icon from the Dock onto the current app. A gray "window" appears around the app's icon. Drop it directly on the current app to open the app in a Slide Over window, or move it all the way to the left or right to open the app in Split View. (Technically, you can also start dragging an app icon from the Home screen — ignore the wiggling icons if they start — or Siri Suggestions with one hand, and then use your other hand to switch to the main app you want to use, but that requires a good bit of dexterity.)

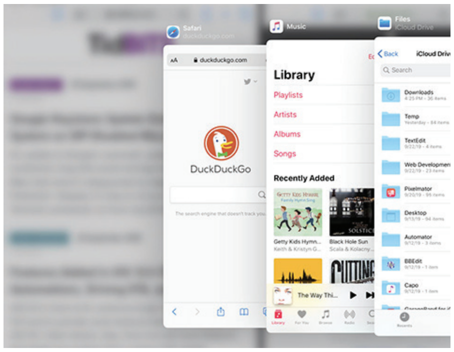
You'll notice a couple of minor niceties right away:

When you open Split View, the default split is now 50/50, as opposed to the odd 70/30 split in iOS 12. You can still adjust the split to 70/30 on either side.

You can now position Slide Over on either side of the screen to start (previously, Slide Over always started on the right side).

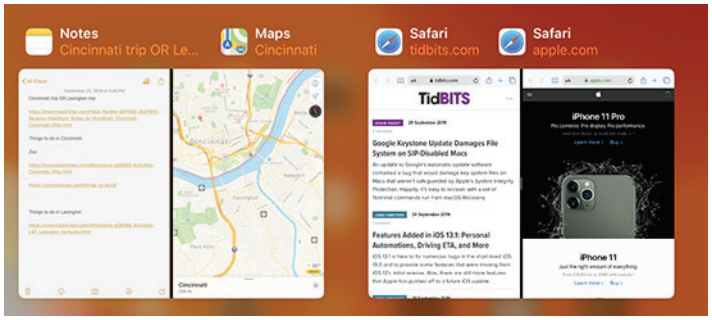
Slide Over works much like it always has: drag the short gray bar at the top of the window to move it to the left or right side of the screen. Swipe the gray bar (or just the left side of the Slide Over window) all the way to the right to hide it, and swipe left on the right-hand edge of the screen to bring Slide Over back.

What's new in Slide Over is you can now easily switch between multiple apps in it. Just open another app in Slide Over, and it will replace the current Slide Over app if one is open. Switching between Slide Over apps works as it does on Face ID-equipped iPhones: swipe up on the black bar at the bottom of Slide Over to reveal all open Slide Over apps and tap one to make it active. From the switcher, you can also swipe up on an app to close it. For faster app switching, swipe left or right on the black bar to cycle between Slide Over apps.

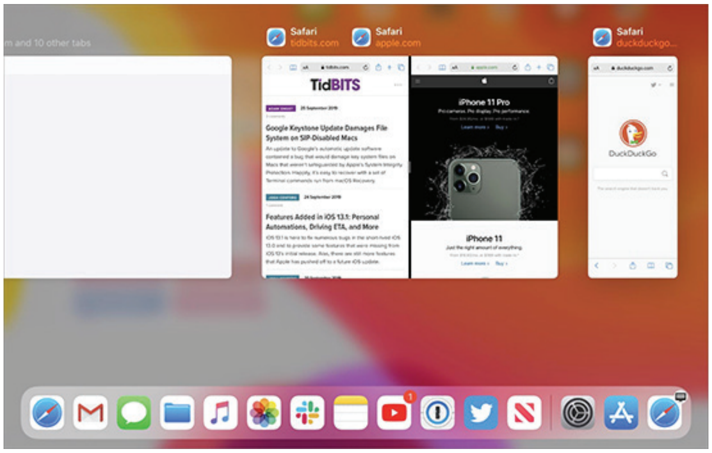


As before, you can put an app from in Slide Over into a Split View window by dragging down on the top bar and moving it to the right or left edge of the screen. Likewise, you can move an app in Split View into Slide Over by dragging down on the top bar and moving it away from the top of the screen. New in iPadOS, you can drag that top bar to the left or right to swap the positions of the Split View windows.

Apps can now have separate windows open in multiple spaces. For example, you could have a full-screen Safari window in one space, two Split View Safari windows in another space, and a third Split View space where Notes is in one window and Safari in the other. You can see all of these combinations in the App Switcher.



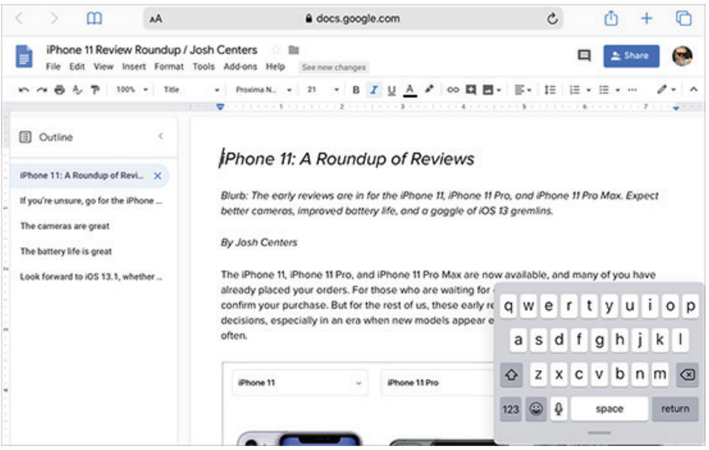
To see all of an app's open windows, bring up the Dock while viewing one of the app's windows, and then tap the app's Dock icon. Alternatively, tap and hold the app's icon anywhere and tap Show All Windows from the popover. While in this view, you might see a + button that lets you open additional windows for the app. If you close a window in this view (by swiping up on it), you might also see a Reopen Closed Windows button that lets you undo that action.



To split some apps into multiple spaces, you can take advantage of iPadOS's new drag-and-drop features. For example, if you're in Notes, you can tap and hold a note in the notes list, and then drag it to the right side of the screen to open it in a second Split View window. Safari can do this with tabs too, as I'll explain below.

"Desktop-Class" Safari

Apple boasts that the version of Safari in iPadOS is "desktop-class," suggesting that it supports many popular Web apps that tend to work poorly with mobile browsers. And it's true! Here's a screenshot of me editing a TidBITS article in the full Web version of Google Docs, which was impossible in iOS 12.


docs.google.com
iPhone 11 Review Roundup / Josh Centers
File Edit View Insert Format Tools Add-ons Help
See new changes
Share
Outline
iPhone 11: A Roundup of Revi...
If you're unsure, go for the iPhone ...
The cameras are great
The battery life is great
Look forward to iOS 13.1, whether ...
iPhone 11
iPhone 11 Pro

iPhone 11: A Roundup of Reviews

Blurb: The early reviews are in for the iPhone 11, iPhone 11 Pro, and iPhone 11 Pro Max. Expect better cameras, improved battery life, and a goggle of iOS 13 gremlins.

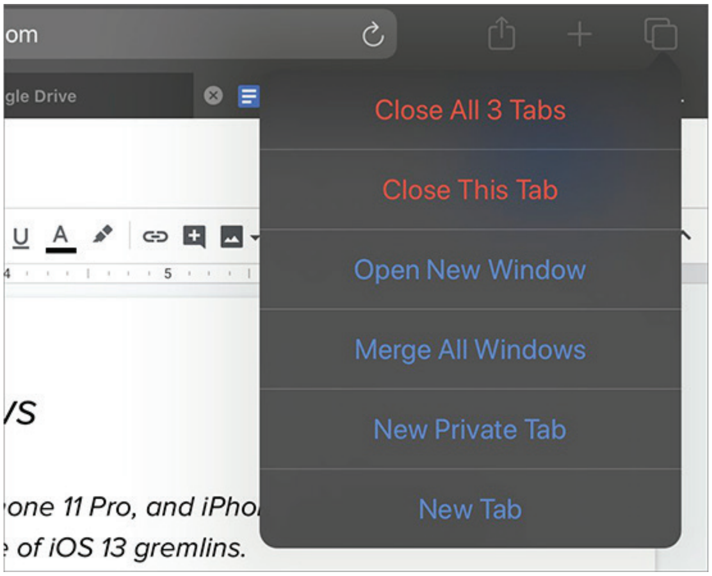
By Josh Centers

The iPhone 11, iPhone 11 Pro, and iPhone 11 Pro Max are now available, and many of you have already placed your orders. For those who are waiting for confirm your purchase. But for the rest of us, these early re decisions, especially in an era when new models appear e often.

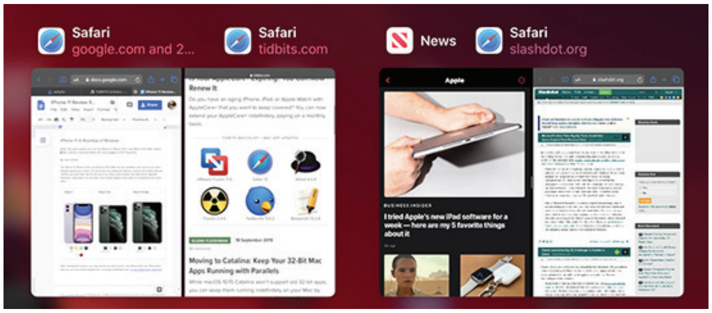
Note that if you have the Google Docs app installed, you'll need to remove it, because otherwise, iOS will open all Google Docs URLs in the app.

This new desktop-class Safari isn't yet the equal of Safari on the Mac, but it's an impressive effort. If there are sites you couldn't get to work with mobile Safari before, give them a try in iPadOS and let us know how it works. If you stumble upon a problematic site, we recommend reporting it to Apple.

Back to those multitasking features. If you tap and hold the Tabs icon (two stacked squares) in Safari's toolbar and tap Open New Window, Safari opens a new window in Split View. You can also drag a tab from Safari's Tab bar to the side of the screen to open it in a Split View window. And for those with dextrous fingers, you can start dragging a tab from Safari, switch to another app in some other way, and drop the tab to create a new window in Split View or Slide Over, depending on whether you drop onto the app or to the left or right of it.



It's easy to end up with a plethora of Safari windows, spread across multiple spaces. You can consolidate them by tapping and holding the Tabs icon and choosing Merge All Windows.



Apple has added a Download Manager that looks and works much like the one in Safari on the Mac. It displays the progress of current downloads and lists recent downloads, letting you access them in the newly enhanced Files app. Tapping and holding on links for images, videos, or audio files reveals a Download Linked File option in the popover that lets you download such files.

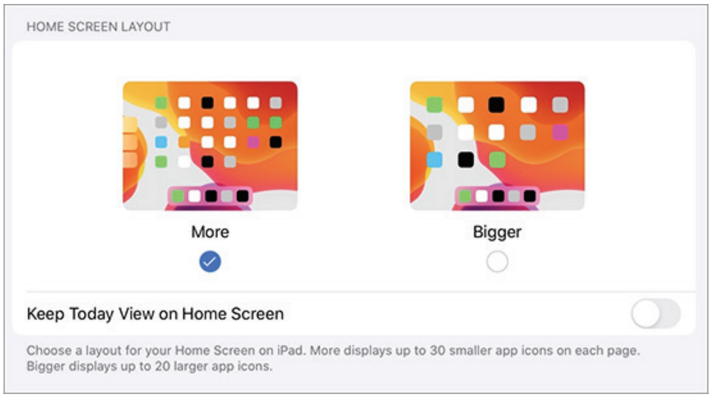
Apple also says that Safari in iPadOS supports many more keyboard shortcuts when used with a physical keyboard. We haven't compared with iOS 12, but to see which ones are on offer, press and hold the Command key.

The iPadOS Home Screen

Apple made two welcome improvements to the Home screen in iPadOS, increasing the density of the app icons and adding Today View widgets to the Home screen.

Greater App Icon Density

iPadOS now displays more app icons — up to 30 — on the Home screen by default, making it less like an oversized iPhone and more like the Mac's Desktop. If your eyes prefer larger icons — up to 20 of them — you can switch to the Bigger layout in Settings > Display & Brightness.



HOME SCREEN LAYOUT

More ●

Bigger ○

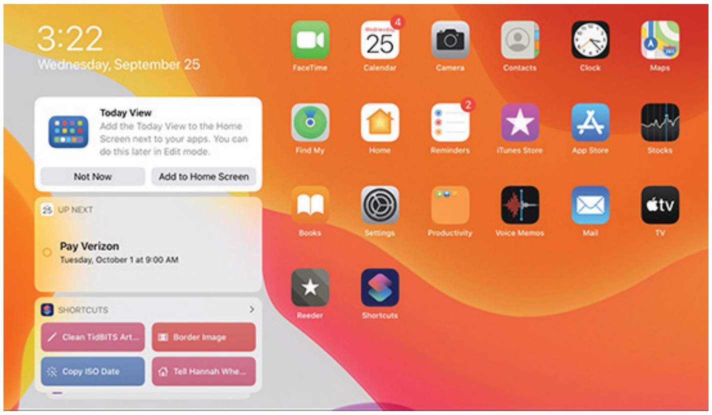
Keep Today View on Home Screen ○

Choose a layout for your Home Screen on iPad. More displays up to 30 smaller app icons on each page. Bigger displays up to 20 larger app icons.

Today View Widgets on the Home Screen

When you're on the first Home screen, you might notice that swiping from left to right to access your Today View widgets no longer takes you to a separate screen. Instead, the Home screen icons shift over to the right to make room for the widgets.

At first, you'll see another option there in the Today View widget: Add to Home Screen, which permanently fixes your Today View widgets to your Home screen. You can also adjust this setting later in Settings > Display & Brightness; it also appears if you scroll to the bottom of the Today View widgets and tap Edit to pick which widgets appear and in what order.



Today View

Add the Today View to the Home Screen next to your apps. You can do this later in Edit mode.

Not Now | Add to Home Screen

25 UP NEXT

Pay Verizon
Tuesday, October 1 at 9:00 AM

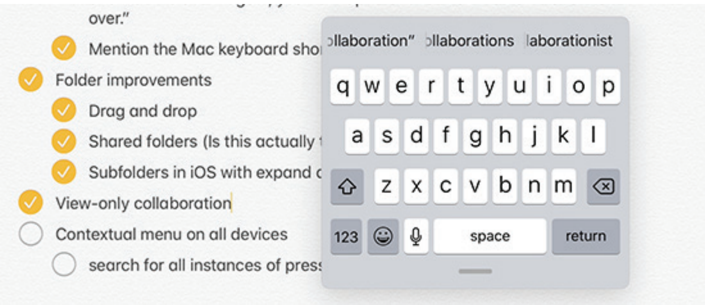
SHORTCUTS

Clean TidBITS Art... | Border Image | Copy ISO Date | Tell Hannah Whe...

The Floating Keyboard

The iPad's onscreen keyboard has always been awkward. Unless you can easily palm a basketball, the full-size keyboard is practically unusable while holding the iPad with both hands. To address that, Apple first made it so you can split the keyboard in two. That's better but still awkward.

In iPadOS, Apple is trying again with a new floating keyboard that you can use with one hand or thumb-type on with both hands like an iPhone. To access it, pinch in with two fingers on the full-size keyboard. Pinch out with two fingers to return to the large keyboard.



over."

- ✓ Mention the Mac keyboard sho
- ✓ Folder improvements
- ✓ Drag and drop
- ✓ Shared folders (Is this actually
- ✓ Subfolders in iOS with expand c
- ✓ View-only collaboration
- ○ Contextual menu on all devices
- ○ search for all instances of press

You can tap-type on the keyboard, but Apple's real intention here is for you to use slide-to-type, a feature Apple's marketing mavens call QuickPath. Similar features have been available for years from third-party iOS keyboards.

To use QuickPath, slide your finger from letter to letter without lifting it up in between letters. When you get to the end of a word, lift your finger. You can switch between tapping (best for unusual words or proper nouns that QuickPath might get wrong) and sliding on a word-by-word basis.

If you don't slide accurately, or if iOS guesses what you meant incorrectly, tap Delete to remove the entire word. If you'd rather delete a letter at a time, turn off Delete

Slide-to-Type by Word in Settings > General > Keyboard. QuickPath works in iOS 13 as well, so be sure to give it a try on your iPhone too.

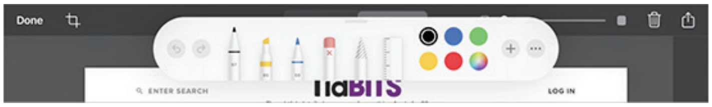
Improved Markup and Screenshots

Last, and probably least, iPadOS benefits from a few markup improvements:

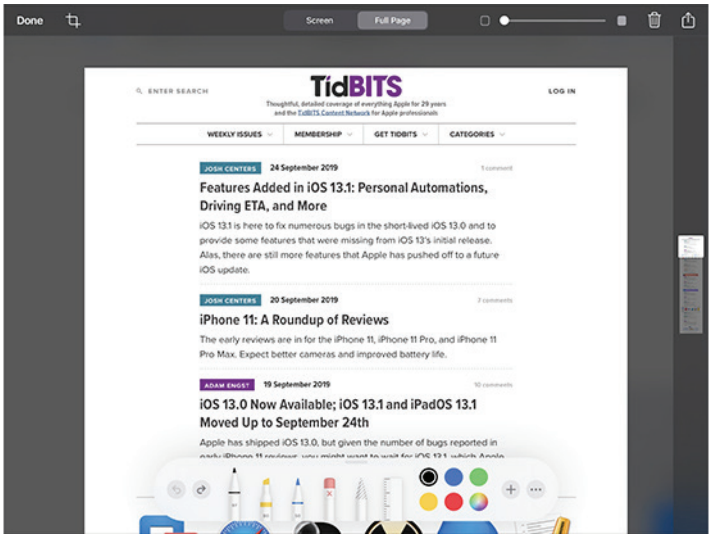
Apple Pencil latency is lower. Apple says it's as low as 9 milliseconds, which may not mean much to you, but it feels much more responsive.

You can take a screenshot by dragging the Apple Pencil from any bottom corner.

There is a new tools palette when marking up a screenshot or other document that you can move around to any side of the screen. It includes a new pixel eraser, which erases just part of a shape.



A related feature, which is also available on iOS 13, is the capability to take a screenshot of the entire contents of a scrollable page in some apps, notably Safari. To do this, first take a screenshot of a Web page in Safari. Then tap the preview thumbnail to edit it, and tap Full Page at the top of the screen. That captures the entire Web page. To scroll around the page, place two fingers on the screen and move them around, or use the scrollbar on the right. Saving it gives you a multi-page PDF in Files rather than a PNG in Photos.



Thoughtful, detailed coverage of everything Apple for 29 years and the TidBITS Content Network for Apple professionals

24 September 2019

Features Added in iOS 13.1: Personal Automations, Driving ETA, and More

iOS 13.1 is here to fix numerous bugs in the short-lived iOS 13.0 and to provide some features that were missing from iOS 13's initial release. Alas, there are still more features that Apple has pushed off to a future iOS update.

20 September 2019

iPhone 11: A Roundup of Reviews

The early reviews are in for the iPhone 11, iPhone 11 Pro, and iPhone 11 Pro Max. Expect better cameras and improved battery life.

19 September 2019

iOS 13.0 Now Available; iOS 13.1 and iPadOS 13.1 Moved Up to September 24th

Apple has shipped iOS 13.0, but given the number of bugs reported in

Sidecar in macOS Catalina and More

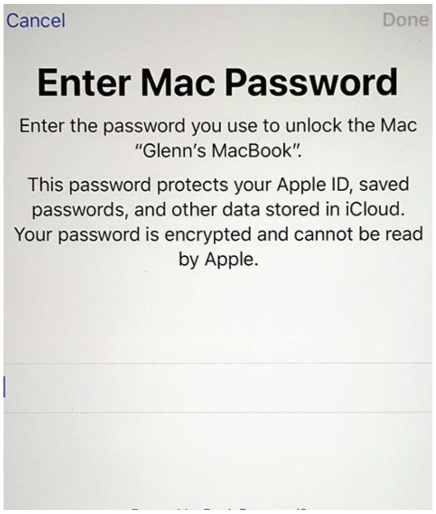
Given that macOS 10.15 Catalina isn't slated for release until sometime in October, there isn't much we can say right now about the Sidecar feature that lets you use an iPad as a secondary screen or as a graphics tablet.

By Glenn Fleishman

Why Apple Asks for Your Password with a New Login (and Why It's Safe)

If you've set up or restored an Apple device recently and have two-factor authentication enabled on your Apple ID, you may have seen a message during configuration that defies your understanding of how Apple maintains device privacy and account security.

The message reads something like, "Enter Mac Password. Enter the password you use to unlock the Mac 'name here'. This password protects your Apple ID, saved passwords, and other data stored in iCloud. Your password is encrypted and cannot be read by Apple." The prompt might instead ask for your iPhone or iPad passcode.



Enter Mac Password

Enter the password you use to unlock the Mac "Glenn's MacBook".

This password protects your Apple ID, saved passwords, and other data stored in iCloud. Your password is encrypted and cannot be read by Apple.

I had to take a photo of this unusual login screen, as it was during setup and screen capture wasn't available.

Doesn't this seem contradictory, confusing, and just plain wrong? Why would Apple ask for the password or passcode for one of your other devices? Could it be some sort of scam? What exactly is going on here?

I encountered this issue, as did Take Control publisher Joe Kissell, in preparing the iOS 13 and iPadOS 13 revision to my long-running networking and security book, *Connect and Secure Your iPhone and iPad.* (It has a new, shorter title in this release, and is already updated for iOS 13.1 — check it out if you're looking for more information about iOS networking, privacy, and security.)

While I had heard of this prompt happening once last year, I had never seen it myself. Now I've figured out what is going on by reviewing Apple's documentation and deducing the missing pieces. The short answer is that this prompt is actually Apple working to protect your security, and the explanation is accurate. But it's not sufficiently detailed — that would require screens of text — to explain what's going on. Here's the skinny.

iCloud Stores Two Kinds of Secured Data for You

All the data that's synced between your devices via iCloud is encrypted while in transit (generally using HTTPS) and at rest on Apple's servers. Some of it is available in decrypted form if you were to access it via iCloud.com. For that subset, Apple maintains the encryption keys that protect the data when it's at rest, and it could turn over that data if forced to by law enforcement.

Apple discloses which data is stored with encryption keys it possesses. In very rare circumstances, someone who compromised Apple's keys or server security could extract that iCloud.com-accessible information from a transmission or from iCloud. It's extremely unlikely, but it's not strictly impossible.

This data could also be at risk in a successful phishing attack. Phishing requires only that an attacker fools someone into thinking they are entering their credentials into a legitimate site that is, instead, a man-in-the-middle. There are many kinds of phishing attacks, one severe type of which involves obtaining fraudulently issued HTTPS certificates that can have all the trappings of a legitimate and secure site.

The attacker could then simply use your login name and password to initiate an attempt to log in to iCloud, even triggering Apple to send you an extra login token used for two-factor authentication, which, if you entered it on the phishing site, could be used by the attacker at iCloud.

Apple users have been phished, of course, although as far as I know, Apple has never suffered from a fraudulent certificate attack. Some visitors to Google sites were phished in this way on multiple occasions several years ago. Since then, certificate-issuing and -tracking procedures and the way browsers check for legitimately issued documents have substantially reduced but not eliminated that particular risk.

Because of phishing risks, Apple has chosen to protect some data that it views as highly secure or very private with end-to-end encryption that prevents Apple from knowing anything about the contents of the synced data. Apple doesn't possess any of the keys required to decrypt this data passing through its servers. Instead, those keys reside only on individual iPhones, iPads, and Macs.

There's a full list of end-to-end encrypted services at Apple's iCloud security overview page, but they include iCloud Keychain, Screen Time information, Health data, Wi-Fi passwords, the People album in Photos, and the new Find Me service's crowdsourced location information. There are also likely other bits of data that facilitate device-to-device interactions.

As a result, you cannot view these categories of data at iCloud.com, only using your devices. In essence, iCloud acts as a sync service with zero knowledge about what it's transmitting. If Apple were asked to disclose this information by a government, it could only produce unreadable encrypted data, by design. (This approach is distinct from the way Apple stores even more sensitive data — credit-card numbers, passcodes, and fingerprint or face parameters — in the Secure Enclave of iPhones, iPads, and Macs with T2 chips. That data never even leaves the Secure Enclave, and much of it is stored in the chip already irreversibly transformed through one-way encryption.)

Apple's iCloud syncing system relies on public-key cryptography, which uses linked pairs of keys: one public and one private. The public key can be shared freely and used by anyone who wants to encrypt material meant for the owner of the private key, who can then decrypt that data. For iCloud Keychain and similar sensitive data, Apple has your devices generate and maintain a set of public and private keys that enable interaction with the information synced across iCloud. The devices never reveal their private keys and have the public keys of all the other devices connected to an iCloud account.

The data protected in this way is stored as individual packages — for example, a URL, account name, and password as a single unit — and identified with random metadata that's meaningless except to establish a unique ID for each data package. Devices in the user's sync set, including newly enrolled hardware, sync by exchanging metadata information. Let's say your iPhone is missing a Web site login you just created on your Mac. The Mac encrypts the login entry with the public key of the iPhone, which receives it via iCloud sync, and then decrypts it with its private key. This approach is both typical and sensible.

The hard part isn't syncing data privately. Rather, it comes when you want to add a new device to this set. To understand how that works, we need to understand the role of your iCloud password.

An Extra Element to Protect against Interception

Apple's iOS 12 security white paper explains this system in some depth, noting that your iCloud Apple ID account password by itself can be used to enroll a new device. That isn't as worrying as it might sound, because Apple doesn't know your password. Instead, it stores only an encrypted form of the password. Whenever you enter your password, it's run through a one-way encryption algorithm that performs a vast number of mathematical operations — the process is called "hashing" — that makes it effectively impossible to determine the original password. (This is also used for a lot of data stored in a Secure Enclave, like your passcode.)

You could enable an iCloud Security Code as an "out-of-band" element — something that is never transmitted by the same means as other data. Out-of-band elements are a common way to block data hijacking by requiring a secret that has never been put online. In this case, it's something you create or Apple creates for you on one device and that you enter on another.

(Never heard of an iCloud Security Code? You're not alone! It's barely mentioned on Apple's site, and Apple's white paper doesn't discuss the code deeply. I recall using one years ago, and TidBITS publisher Adam Engst had never heard the term before editing this article.)

But there's a flaw in both the iCloud password and the iCloud Security Code approaches, and I wonder if that's why Apple is now asking for passwords or passcodes from other devices in your sync set. The iCloud Security Code is yet another piece of information to remember and deal with and thus runs counter to Apple's commitment to simplicity. It was also created when iCloud Keychain was the only set of data Apple secured end-to-end and synced via iCloud, and before both two-step verification and the later two-factor authentication for Apple ID. It may not be robust enough to match Apple's current security and authentication requirements.

As for the iCloud password, it suffers from a different set of concerns. While Apple doesn't know your iCloud password, whenever you log in at iCloud.com, your encrypted password is sent to Apple, which holds it just long enough to perform the hash and test it against its stored value. However, it's not inconceivable — though, again, it's unlikely — that the password could be captured during that transmission, phished, or stolen in some other way. Apple obviously thinks about it in this way: Since it's conceivable that the password could be intercepted, Apple has to defend against interception as though it happens every day.

Some companies have tried to move away from the need to transfer even a hashed password. AgileBits, for instance, built 1Password.com around newer browser-based encryption algorithms — no unencrypted passwords or data are stored by AgileBits or ever sent to the browser. Instead, the browser itself performs all the necessary encryption and sends the encrypted data to AgileBits. After login, the 1Password.com servers only send encrypted packages to the user's browser, which holds encryption keys locally and only for the duration of the session.

Apple hasn't transitioned to this method with iCloud.com, and so it makes sense that instead of relying on an iCloud password, which could be stolen or phished, it has instead moved to this device-passcode/password system. Apple hasn't yet documented this new approach, which is why I'm not being more precise about how it all works. None of the text on the screen users see appears on Apple's support or marketing sites, and there's no mention of the process in the white paper noted above or elsewhere. But I've heard about the process previously from readers, Take Control publisher Joe Kissell recently saw it on setting up a new device, and I finally saw it after upgrading to iOS 13 on my iPhone.

Here's how the new system works, as far as I can determine:

You log into your Apple ID on the device you're setting up and confirm a second-factor login. (Password-only Apple ID accounts, which Apple strongly discourages and which we recommend against, don't seem to get these dialogs.)

On at least one of the devices in the iCloud sync set, Apple adds an encrypted version of that device's passcode or password to the set of shared information. The only information attached to that payload that Apple can read is the type of device and the name of the device.

Apple syncs this information to iCloud, and the setup process on the new device then pulls it down, prompting you to enter the passcode or password.

Once you enter the correct passcode or password, the new device dumps the passcode/password data from the set, instead generating and relying on a new pair of encryption keys, just like the other devices. The new device becomes part of the trusted set of devices that can sync your end-to-end encrypted iCloud data.

It's possible that Apple retains the encrypted passcode and password of the shared key for every device that's in the set. However, that would seem to be an ongoing risk, as it would conceivably allow someone who obtains that secret to gain further access.

What this process appears to show is that Apple never sees, handles, or stores your device passcode or password in unencrypted form, and it never passes the passcode or password over anything but secure transport. It requires only your Apple ID account name and password, sent over HTTPS, as the first stage of logging into iCloud, but not for the later stages.

Overall, this new approach seems rational and secure. Apple would do well to give users more confidence in what's happening by providing an explanatory support document, and I hope Apple will give in-depth details when it updates the iOS security white paper for iOS 13.

By Glenn Fleishman

How to Connect to Wi-Fi Networks Faster in iOS 13

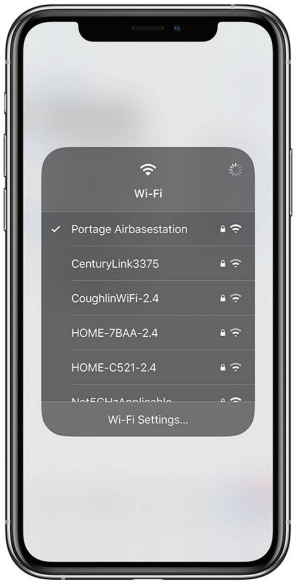
Alongside all the marquee features, Apple always sneaks in something extra when it updates its operating systems. In iOS 13 and iPadOS 13, the company added yet another way to connect to a nearby Wi-Fi network, and this new method is a little faster to use than the previous best one.

This new connection option brings the total to four! You may have trouble remembering all of them or have found some awkward to invoke. A fourth method isn't big news, but if you regularly need to connect to new Wi-Fi networks, you might find it more convenient.

I ran across this new Wi-Fi connection method while overhauling my book, *Connect and Secure Your iPhone and iPad,* for all the many changes in iOS 13 and the split into iPadOS 13, and then updating it again for 13.1. The book now includes these Wi-Fi connection tips, along with a hundred other new and improved elements, like explaining Apple's latest anti-tracking technology in Safari and using the revamped Find My service. If you need help with networking and security on your iPhone or iPad, please pick up a copy from Take Control. (And feel free to ask me any questions it didn't answer!)

Let's look at each of the four ways of connecting to a Wi-Fi network, starting with the newest method.

Use Control Center



Wi-Fi

✓ Portage Airbasestation

CenturyLink3375

CoughlinWiFi-2.4

HOME-7BAA-2.4

HOME-C521-2.4

Wi-Fi Settings...

You can now view the list of available Wi-Fi networks and join one via Control Center.

In iOS 13, Apple expanded the capabilities of Control Center to provide a new way to access the list of available Wi-Fi networks. Here's how to reach the new interface:

Swipe to reveal Control Center. (On an iPad or an iPhone X or later, swipe down from the top right of the screen; on older iPhones and the iPod touch, swipe up from the bottom of the screen.)

Tap and hold the network card (the shaded rectangle containing the network buttons) to expand it.

Tap and hold the Wi-Fi button to bring up a list of networks.

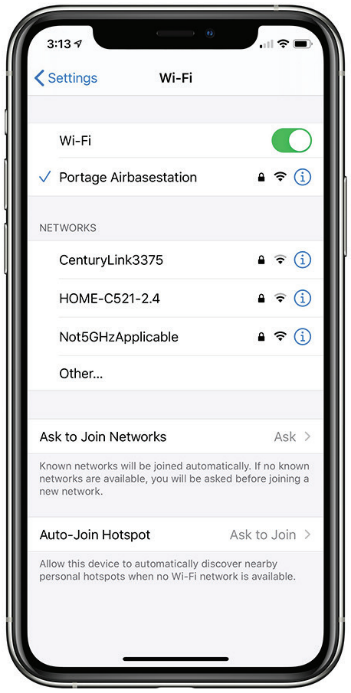
Tap the network you want to join.

Enter a password if prompted.

You can also tap Wi-Fi Settings at the bottom to open Settings > Wi-Fi.

This new option isn't earth-shaking, but it's definitely easier to get to, especially since you can start from the Lock screen without even unlocking your device.

Use the Settings App



3:13

Settings Wi-Fi

Wi-Fi

✓ Portage Airbasestation

NETWORKS

CenturyLink3375

HOME-C521-2.4

Not5GHzApplicable

Other...

Ask to Join Networks: Ask

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

Auto-Join Hotspot: Ask to Join

Allow this device to automatically discover nearby personal hotspots when no Wi-Fi network is available.

Select a Wi-Fi network from the list in Wi-Fi settings.

Since the earliest days of iOS, you've been able to connect to a Wi-Fi network through the Settings app:

Open Settings > Wi-Fi.

Tap a network name under Networks.

Enter a password if prompted.

If the network you want to connect to doesn't appear because it's "closed" or "hidden" — an outdated security-through-obscurity method that some people still use — tap Other and enter the network name and password.

To make this process more automatic, you can set Ask to Join Networks to either Ask or Notify. With either choice, your device will still preferentially connect to a known, stored network. If no known networks are available, however, you'll be prompted to join another network if Ask is selected. (Apple doesn't explain the criteria for which one appears.) A list of all networks appears if you have Notify selected.

If you have one or more devices with Personal Hotspot enabled, you'll get a Personal Hotspots list of networks as well. Plus, iOS 13 may also show a list of Popular Networks. It apparently determines them by passively scanning to see which networks around you other people are already connected to. This approach seems a little invasive, but it is using publicly broadcast information. I haven't yet been able to make the Popular Networks list appear; it's an Apple bullet point for the latest operating systems, but the company provides no clear explanation of it.

Apple also added Auto-Join Hotspot, which is a "failover" method. If iOS 13 can't find a known Wi-Fi network, it will use Personal Hotspot to connect to an iPhone or cellular iPad logged into the same iCloud account. It can even enable Personal Hotspot on the other device if it's off. (macOS 10.15 Catalina offers a similar option.)

One final tip. Family Sharing can now integrate with Personal Hotspot. If you're part of a Family Sharing group, tap Settings > Personal Hotspot > Family Sharing. When you enable Family Sharing for Personal Hotspot on that screen, you can then set each member of your family to either have automatic access or be required to ask you for access. This feature could be welcome when traveling as a family.

Join via a Contact

Since iOS 12, you can join a Wi-Fi network if someone near you has you in their contacts and has the password for a network you want to join. This is a handy feature if you're, say, visiting a friend's house and want to connect to their Wi-Fi. The key is that your friend's contact item for you has to contain the email address you use with iCloud. Here's how to use a friend's password:

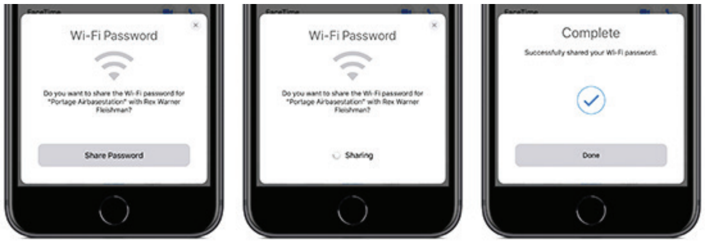
Make sure your device is near their iPhone, iPad, or Mac — the feature relies on Bluetooth and proximity.

Tap the network you want to join.

On your friend's device, a Wi-Fi Password pop-up appears that explains what network you want to join and your name. They need to tap Share Password.

The password is sent securely and silently to your device, which joins the network without any prompts.

Your friend taps Done to dismiss the dialog.



Do you want to share the Wi-Fi password for "Portage Airbasestation" with Rex Warner Fleishman?

Do you want to share the Wi-Fi password for "Portage Airbasestation" with Rex Warner Fleishman?

Successfully shared your Wi-Fi password.

You can join a network if someone who has you in their contacts has the network's password and is nearby.

Join via a QR Code

Back in iOS 11, Apple added a nifty visual way to share network details with a minimum of fuss via a QR code that you scan in the Camera app. This hotspot-sharing format, which was developed in the Android world, encodes the network name and its password.

While Wi-Fi–enabling QR codes aren't found in the wild all that commonly, I have seen them in coffee shops and gathering places, probably placed there by a QR Code aficionado like me. Some conferences also use them to help attendees connect to the conference network. You can also find them on some Wi-Fi routers, letting you make the first connection without finding the default network password.

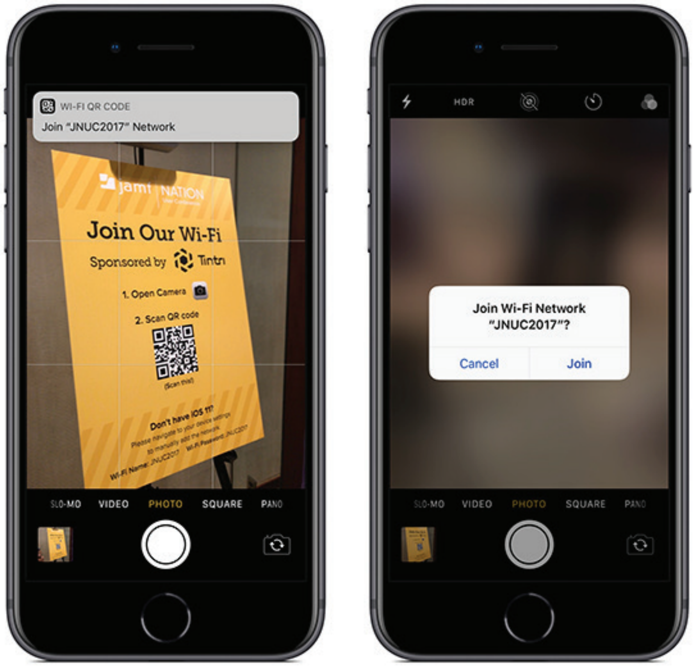
You can join a network via a QR code simply by pointing your iPhone or iPad camera at it. (Settings > Camera > Scan QR Code has to be turned on, which it is by default.) You can also use a Control Center control improved in iOS 13 and iPadOS 13 that looks just for QR codes. (Go to Settings > Control Center > Customize Controls and add QR Code Reader.)

To scan a Wi-Fi network QR code with the Camera app:

Point your camera at the code so it's entirely within the screen.

iOS recognizes the code and displays a Wi-Fi QR Code notification saying Join "Network Name" Network. Tap that notification.

Tap Join Network.



WI-FI QR CODE
Join "JNUC2017" Network

Join Wi-Fi Network "JNUC2017"?

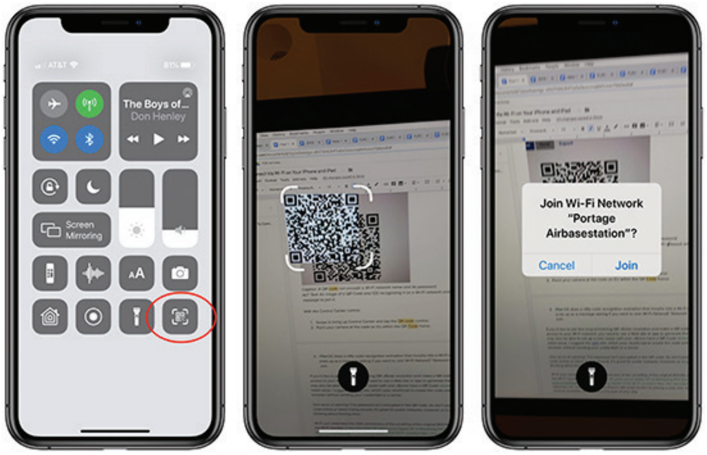
A QR code can encode a Wi-Fi network name and its password.

To scan a Wi-Fi network QR code from Control Center:

Swipe to bring up Control Center and tap the QR Code button.

Point your camera at the code so it's within the QR Code frame.

iOS does a nifty code recognition animation that morphs into a Wi-Fi symbol and ends up as a message asking if you want to Join Wi-Fi Network "Network Name"? Tap Join.



Join Wi-Fi Network "Portage Airbasestation"?

If you'd like to join the long-simmering QR Code revolution and make a QR code that gives access to your Wi-Fi network, you need to use a Web site or app to generate the code. I suggest the QiFi site, which uses JavaScript to create the code entirely in your browser without sending your credentials to a server. And if you get really into QR codes and want to build some automation to create them, check out Charles Edge's article on the topic.

One word of warning — the Wi-Fi password isn't encrypted in the QR code! So don't post such a QR code online or leave it lying around. It's great for public hotspots, however, or in your home. I'm thinking about framing mine.

Wi-Fi just celebrated the 20th anniversary of the unveiling of the original 802.11b standard and the Wi-Fi moniker. It has also been 20 years since Apple VP of Marketing Phil Schiller took one giant leap for wireless networking by jumping onto an inflatable mat while streaming a video on Apple's first Wi-Fi–enabled Mac, the clamshell iBook. Wi-Fi networks are now ubiquitous, but there's still some friction to joining a new one. Having more choices available can smooth a tiny part of your day.

Share Keystone MacCentral with other MACaholics

Name ____

Address ____

City _____________________________ State ___ Zip ________

Home Phone ________________ Day Phone ________________

E-mail Address ____________________________________

Date ____________ Is this ○ Renewal or ○ New?

How did you hear about us? __________________________

Dues for one person are ○ $20/yr. Family or Corporate dues are ○ $30/yr.

To join Keystone MacCentral, mail this form with your membership dues (payable to Keystone MacCentral) to:

Keystone MacCentral
Membership Chair
310 Somerset Drive
Shiresmanstown, PA 17011

Keystone MacCentral meetings are held at 6:30 p.m. on the 3rd Tuesday of the month at Bethany Village Retirement Center, 5225 Wilson Lane, Mechanicsburg, PA 17055