A Practical Guide to

NETWORKING AND SECURITY IN iOS 8

By Glenn Fleishman

$15

Welcome

Welcome to *A Practical Guide to Networking and Security in iOS 8*, version 1.0.0, published in February 2015 by Aperiodical LLC.

This book describes how to use your iPhone, iPod touch, or iPad with iOS 8 on Wi-Fi and cellular/mobile networks securely, making connections with ease while protecting your data. It also covers Bluetooth networking, tracking an iOS device, Personal Hotspot, two-step verification with Apple ID, using AirDrop and AirPlay, and solving connection problems.

Visit **our updates page** to check for new versions and re-download any of the ebook files. Use the password `nimbleskull`. **Sign up for our announcement email list**, and you'll be notified about free updates to this edition of the book, as well as receive a note and a discount coupon when we release future editions covering newer versions of Apple's operating system. We will not sell, rent, or share your information. Find us on the Web at **http://glennf.com/guides**.

This book was written by Glenn Fleishman, edited by Jeff Carlson, and copyedited and proofread by Scout Festa. The cover illustration is by Christa Mrgan. (This is an update of a book originally published by Take Control Publishing, and edited by Tonya Engst and Michael Cohen.)

If you have the ebook edition and want to share it with a friend, we ask that you do so as you would with a physical book: "lend" it for a quick look, but ask your friend to buy a copy for careful reading or reference. Aperiodical is a tiny independent publishing company — just Glenn! (A print edition of this book can be ordered at the above link.)

Introduction

Networking should be simple, and security should be automatic. And money should grow on trees. Despite how intuitive it is to pick up and use an iOS device, requiring little thought as to how it connects to a cellular or Wi-Fi network, it becomes quite complex as soon as you drill down to any details. This is especially true when connectivity fails,and you try to troubleshoot.

Security is an even denser area. Apple makes the default choices in iOS reasonably secure, but to ensure real protection for your data—while your bits are traveling through the æther or in the event that your device is stolen—you need to know how it all works.

The book is divided into two major sections, one on networking and one on security, though there is, of course, overlap.

TABLE OF CONTENTS

NETWORKING

SECURITY

NETWORKING

It’s true that an iOS device can be used without a live network connection, but its natural state is always hooked up. In the first part of the book, you’ll learn how to work with the three types of iOS wireless communication—Wi-Fi, cellular, and Bluetooth—for general connectivity, with personal hotspots, for audio/video streaming, and for file transfer.

Connect to a Wi-Fi Network

Wi-Fi works quite simply in iOS, but there's a lot of hidden detail. In this chapter, you'll learn how to interpret the Wi-Fi settings view, manipulate custom network settings, and troubleshoot common problems.

Join a Network

Open the Settings app and tap Wi-Fi to view nearby networks. Tap a network name to join it.

The first time you tap a network name to connect, your device joins the network immediately unless encryption is enabled on the network. In that case, you are prompted for a password; once you've entered the password and tapped the Join button, you join the network.

Note: For more on connecting with a password or other methods, see **Connect to a Secure Wi-Fi Network** in the Security section of the book.

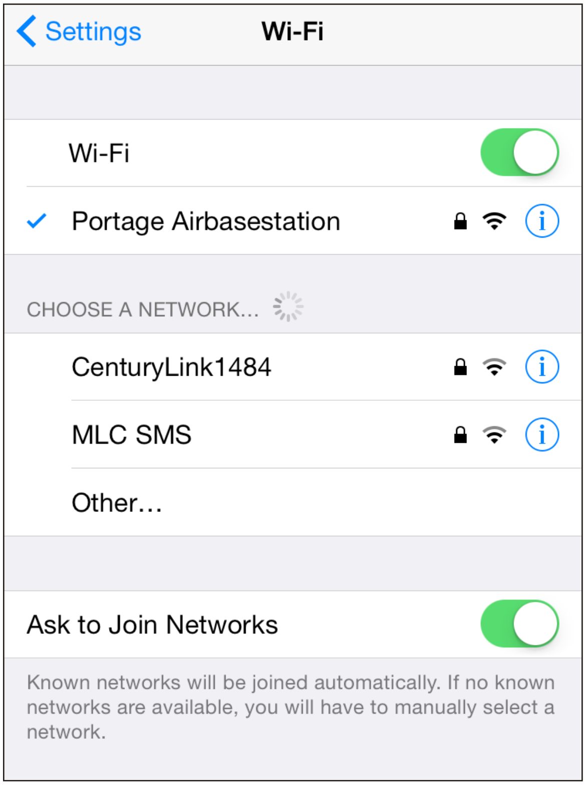
Tip: Are you tired of your device popping up a list of nearby Wi-Fi networks while you're trying to do something else? Turn off Ask to Join Networks, described a couple of pages ahead.

Once your iOS device joins a network, the network name and any associated login information is added to an internal network list. Unlike in Mac OS X and Windows, you can't examine this list and remove entries. The device uses this list to re-join a network when it is in range.

Tip: You can remove a stored network's entry only when you're connected to it. See **Forget This Network**.

Managing Wi-Fi Connections

iOS centralizes Wi-Fi management in the compact space of the Wi-Fi settings view (**Figure 1**). To reach it, open the Settings app and tap Wi-Fi.



Wi-Fi

✓ Portage Airbasestation

CHOOSE A NETWORK...

CenturyLink1484

MLC SMS

Other...

Ask to Join Networks

Known networks will be joined automatically. If no known networks are available, you will have to manually select a network.

Figure 1: *The Wi-Fi view has a list of available networks.*

The Wi-Fi view always has three elements, with an optional fourth:

- **Wi-Fi switch:** Tap this switch to disable and enable the Wi-Fi radio.
- **Choose a Network:** In this area, you may see a list of networks. Each entry in the list has three or four elements:

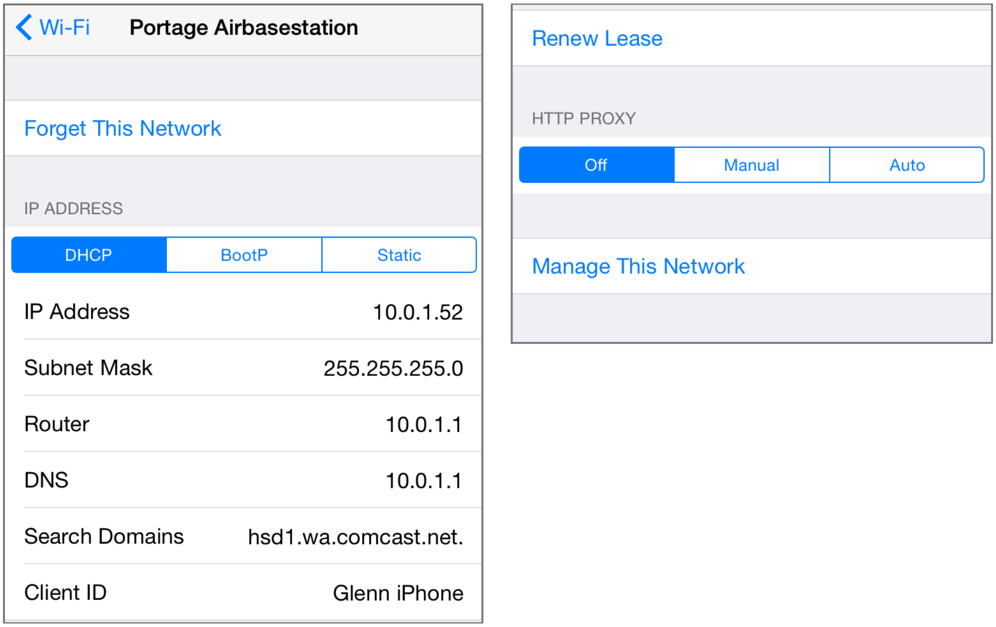
    - **Network name:** A network uses this name to *advertise* itself to Wi-Fi adapters that are looking to make a connection. The network name is also called the SSID (Service Set Identifier) in some of the geekier base station configuration tools.
    - **Lock icon:** A lock may appear, indicating that there's some form of protection on the network.
    - **Signal-strength indicator:** One, two, or all three radio waves in the indicator are black (starting at the bottom) to show the strength of the signal being received by the device.
    - **Information:** Tapping the info ⓘ button—carefully, because it's a small target—reveals technical details about the network, as well as an option to forget the network. For more about these details, see **Drill Down to Network Details**, a few pages ahead.
- **Set Up an AirPort Base Station:** This option appears only if your device detects a nearby unconfigured Apple-branded base station. (I talk more about that in ***Take Control of Your Apple Wi-Fi Network***, a guide to wireless networking with Apple base stations and hardware, published by Take Control Books.)
- **Ask to Join Networks:** With this switch, you can choose whether to be alerted about nearby networks to which the device hasn't previously connected.

  > **Tip:** If Ask to Join Networks is off, you won't be alerted about new networks nearby when a known network isn't available. However, the Choose a Network list always shows all named networks around you.

Drill Down to Network Details

For most network connections, you don't need to go beneath the surface. However, for an unusual connection, such as one requiring a fixed, or static, network address or a different domain name server than the network's default, go to Settings > Wi-Fi and then tap the info ⓘ button for the current network (a checkmark is by the listing) to set up the connection details.

The resulting view has the network name at its top and three or four configuration areas, depending on the network (**Figure 2**). Let's look at each in turn.



Wi-Fi Portage Airbasestation

Forget This Network

IP ADDRESS

DHCP | BootP | Static

IP Address	10.0.1.52
Subnet Mask	255.255.255.0
Router	10.0.1.1
DNS	10.0.1.1
Search Domains	hsd1.wa.comcast.net.
Client ID	Glenn iPhone

Renew Lease

HTTP PROXY

Off | Manual | Auto

Manage This Network

Figure 2: *You can view or set network connection values. (Top of view at left; bottom at right.)*

Forget This Network

Tap the Forget This Network button to remove the network from the list of previously joined Wi-Fi networks. This also disconnects the device from the network immediately and prevents it from connecting to that network automatically in the future. Forgetting a network can solve network problems, too, by letting iOS dump any corrupted or cached information before the next time you connect.

Auto-Join/Auto-Login

As described in **Auto-Join and Auto-Login the Next Time**, these options appear only for hotspot networks for which the device has retrieved certain settings that allow it to make an automatic Web-based login behind the scenes.

IP Address

The IP Address section covers TCP/IP values used for the Internet's addressing and routing system, divided vertically into sections. You start with three kinds of standard network connection methods, which you can see as the DHCP, BootP, and Static buttons near the top of Figure 2, above. Tap a button to display the related choices underneath. You should almost never need to change these values. DHCP (Dynamic Host Configuration Protocol) is the most common method of obtaining an address.

DHCP lets your mobile gear request a network address from a router on the network, and then use it to interact on the local network and beyond. When your device uses DHCP to get an address on the local network, you can't change the IP Address, Subnet Mask, or Router fields, as those values are provided by the DHCP server on the router.

DNS (Domain Name System) is used to convert human-readable domain names, like `www.glennf.com`, into machine-readable IP addresses, like `173.255.209.35`. The DNS field in the DHCP settings can be modified or added to. This can be useful if the network to which you're connected has poorly run or slow default DNS servers. Use a comma to separate multiple entries.

Use the Client ID Field for a Fixed Network Address

On a home or work network, you may want to assign a fixed address to your devices. Apple offers this option as DHCP Reservation in the AirPort Extreme, Time Capsule, and AirPort Express base stations.

In your device's DHCP settings, if you set Client ID to a unique value, like `Glenn's iPad 4`, you can set your base station to assign the same local network address to your device every time it connects over Wi-Fi to the network.

This is useful if you want to use a consistent IP address to connect to certain apps that provide network services, like Air Sharing HD and GoodReader, for remote access to file storage. For details on configuring DHCP Reservation, read my book ***Take Control of Your Apple Wi-Fi Network***, published by Take Control Books.

Tip: Unfortunately, you can't set DNS globally for iOS—you can set it only for individual network connections. It may not be worth the effort to set it for connections you use infrequently, but it's worthwhile for a network that you use often, such as your home Wi-Fi connection.

For certain network configurations that you will never have to enter for a public Wi-Fi network, you may need to tap the Static option and enter settings for IP address, subnet mask, router, and DNS. Those values would be provided by a system administrator or an ISP. Likewise, BootP is almost never used anymore, but remains for backward compatibility.

The Renew Lease button is specific to DHCP. A lease is the assignment of an address by DHCP to your device. A lease can have a duration (like 15 minutes or 15 days). Occasionally, when you seem to have a network address but can't connect, tapping Renew Lease will obtain a new address and resume connectivity.

HTTP Proxy

This option, located at the bottom of the detail view, is typically used only in companies and schools. It redirects Web requests that you make to the Internet at large to a local server that handles them indirectly. It also allows the use of a caching proxy, in which recent pages retrieved by anyone in an organization are fed to you from this server instead of from the remote Web site. This reduces bandwidth consumption.

Manage This Network

On a network that uses Apple's Wi-Fi hardware, this button will appear. Tap it, and it launches the AirPort Utility app if it's installed, or prompts you to download it if not. The app lets you view the network's configuration, make changes, and examine some details of operation.

Turn Wi-Fi Off

Whenever the Wi-Fi radio is active, even if you aren't connected to a network, it's scanning for networks, which can slowly drain the battery. If you're nowhere near a network you can access or if you want to conserve battery life, turn off Wi-Fi by tapping Settings > Wi-Fi and then setting the Wi-Fi switch to Off. (See Airplane Mode for more details.)

Capture the Page

iOS has a clever feature that lets it display a hotspot network login screen and, in some cases, remember the login and other details. However, you can get stuck reconnecting to the same network.

You'll find these types of networks in public places such as cafés, libraries, and airports. After you connect to the network, which appears as open and unprotected, you're required to launch a browser and view a hotspot connection page (also called a captive portal) before you can use the Internet.

Normally, to reach the captive portal, you must try to visit any Web site in a browser, and have your browser be redirected by the network to the login page. Instead, iOS (and Mac OS X since Lion) does a test that detects such redirections whenever you connect to a Wi-Fi network.

Immediately after your iOS device joins a Wi-Fi network, it tries to connect to Apple's Web site. If it doesn't get through, it assumes that it has reached a captive portal. Then, the next time anything happens on the device that requires Internet access (like Mail retrieving messages), iOS displays a special screen that shows the portal's Web page as if it were in the Safari browser.

The hotspot network's captive-portal page will typically ask that you do one of the following (rarely more than one):

- Read a set of terms and conditions for use and tap an Agree button; enter an email address and tap an Agree button; or check a box that says "I agree" and tap a Submit button.
- Require that you register an account to use the network at no cost. With an account, you can log in and use the network.
- Require that you either pay for a connection to the network using a credit card, or enter login information for an active account on the network or an active account of a roaming partner.

After you carry out any of those actions, iOS should close the special screen and Wi-Fi service should be available. These pages are still often absurdly not customized for mobile devices, and the type and buttons are tiny. You'll need to pinch to zoom in almost all of the time.

Connect to a Captive Portal If It's Not Detected

If the special screen doesn't appear, you can reach the captive portal by launching the Safari app. Most of the time, the previously visited page in Safari will try to load; if you have a blank page, enter any site address, like `example.com` or `apple.com`, and tap Go.

After you enter any required data, the login system should redirect you to the Web page you tried to visit in the first place.

Mobile Device Hotspot Access via Boingo

You have an alternate way to pay for hotspot access. Boingo Wireless resells access at a flat monthly rate to over 400,000 hotspots worldwide. Boingo's iOS and other apps automatically join free networks, too, bypassing the special screen and login procedure you often have to go through.

Boingo has two unlimited usage plans that each cost $9.95 a month (and half off on the first month), with only a monthly service commitment. The mobile plan lets you connect to any of its hotspots worldwide using up to two phones, tablets, cameras, or the like at a time. A North and South America plan allows two devices of any kind, including laptops, at a time.

Boingo also has regional and global plans, as well as an hourly and pay-as-you-go service. While Wi-Fi is typically free in America, elsewhere in the world Wi-Fi for a single night at a hotel or a few hours in a coffeeshop can cost more than the monthly plan.

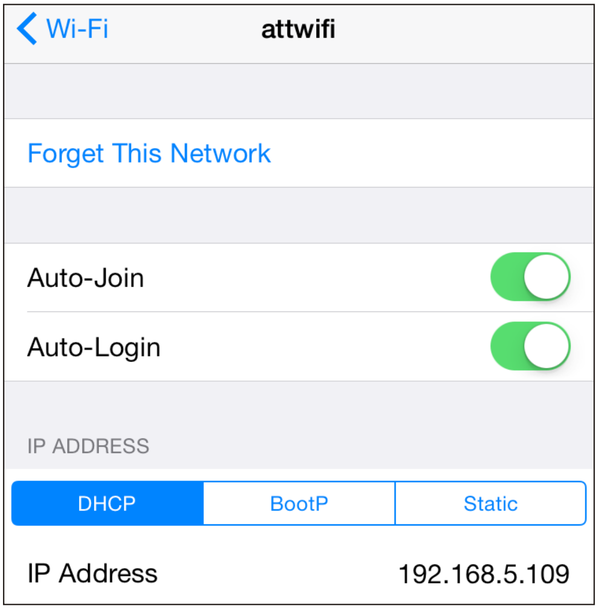
Apple doesn't let hotspot apps run in the background to manage logins. You must launch the Boingo app before you connect, and it handles getting you in.

Auto-Join and Auto-Login the Next Time

The next time you visit a hotspot network that you've previously accessed, iOS will automatically join the network and attempt to use the same credentials or button clicks that you used the previous time to gain access. This can lead to problems if that information is no longer valid or if the device doesn't present it correctly.

In my testing, iOS often shows the same screen for login again without automatically filling it, especially if there's an Agree button to tap in order to avoid you agreeing to terms that might have changed.

You can disable joining and logging in to the network again in this fashion by turning off Auto-Join or Auto-Login for the connection, an option that is available only when you are connected to the Wi-Fi network, even if you haven't logged in or proceeded past the connection Web page (**Figure 3**).



Auto-Join ●
Auto-Login ●

IP ADDRESS

[✓ DHCP] BootP Static

IP Address 192.168.5.109

Figure 3: *When you connect via a portal to a hotspot, the detail page provides additional options.*

To turn off Auto-Join or Auto-Login, follow these steps:

1. In the Settings app, tap Wi-Fi.
2. In the Choose a Network list, tap the info ⓘ button to the right of the network name.
3. In the configuration view that appears, switch off Auto-Join, Auto-Login, or both.

Time-Limited Hotspot Access

Some hotspots limit your use to a specific period of time. This might be implicit, using your unique network adaptor's ID—its MAC (Media Access Control) address—or another bit of tracking information based on when you first accepted a network's terms of services.

Some locations with hotspots give you a network code to enter at a portal page, which grants you access for a fixed amount of time. In those cases, you should turn Auto-Login off; otherwise, the next time you connect, it may attempt to enter a one-time use code that's expired, and it may be difficult to connect properly with a new code.

Wi-Fi Troubleshooting

While Wi-Fi generally works well, you may at times be unable to get a live network connection. Here is troubleshooting advice for common cases.

Can't See Wi-Fi Networks

If your device can't see a Wi-Fi network you think should be available:

- Swipe from the bottom to reveal the Control Center (or launch Settings) to be sure that Wi-Fi isn't turned off. This has happened to me more times than I'd like to admit.
- It's possible that you are out of range. Move the device closer to where you know (or think) a base station is located. Although every iOS device sports an excellent Wi-Fi radio, Wi-Fi reception can be blocked by thick obstructions, such as solid stone and brick walls, or by walls made of chicken wire covered by plaster.

Note: It's also possible that the base station, not your handheld, is in trouble. And I have seen the Wi-Fi radio in an iOS device fail intermittently or completely, requiring that the device be entirely replaced.

No Wi-Fi Signal Strength in the Indicator

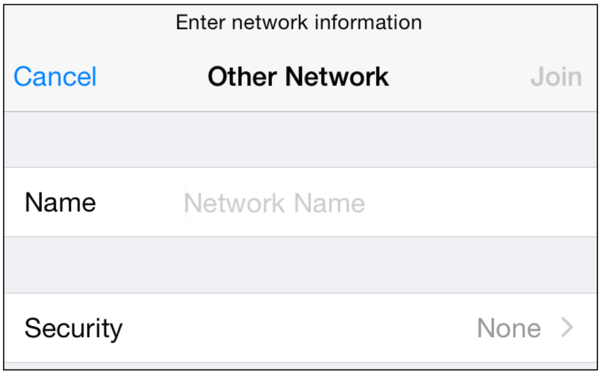
You've selected a network and, if necessary, entered a password, and tapped Join—but the signal-strength indicator in the upper left still shows gray radio waves instead of black. This means that an initial connection was made, but then you quickly moved too far away from the base station, or the base station was shut down or restarted with new information. If the connection process had failed while underway, you would have seen a notification alerting you.

Try connecting again. If that fails, restart your device: Press the Sleep/Wake button until you see a red slider for powering down. Slide it, wait until the spinning indicator disappears and the screen goes entirely black, and then hold down the button again for a few seconds. An Apple icon appears and the device starts up.

Too Many Wi-Fi Networks

There are times when so many Wi-Fi networks in the vicinity may make it hard to select the one you want to join. If you know the network's exact name, you can type it in:

1. Launch Settings.
2. Tap Wi-Fi.
3. Slide down until you can tap the Other button (**Figure 4**).



Enter network information

Other Network

Name: Network Name

Security: None

Figure 4: *The Other Network option lets you enter a network name and optional password from scratch.*

4. Enter the network name exactly and, if there's a password:
   a. Tap Security.
   b. Select the method (almost certainly WPA2).
   c. Tap Other Network to return to the previous screen.
   d. Enter the password in the Password field.
5. Tap Join.

Tip: If you don't know the kind of network security on the network you're trying to join and you have a Mac nearby, hold down the Option key and select the Wi-Fi menu, then hover over the network name. A small popup displays the security type.

Correct Password Not Accepted

As described in the chapter, Connect to a Secure Wi-Fi Network, a network that requires either a password or a username and password will reject your device if you enter it improperly.

But what if you're positive you're entering the password or username and password absolutely correctly?

- Check whether you were given the password with correct capitalization, which counts in Wi-Fi passwords as in others.
- Spaces can be part of WPA2 passphrases, but are often hard to indicate if someone has written down the password. Confirm you're not missing a space.

No Internet Service after Connecting

You connected to a Wi-Fi network but cannot access the Internet from any programs you try. Here's how you can figure out what's wrong.

Check a Web Page with Safari

The most common cause of this problem is that you've connected to a network, likely a hotspot network but possibly a guest network, that requires a password, button tap, or other action.

Launch Safari and try to reach any page, such as google.com:

- If you are redirected to a login page, follow the instructions. You may need to pay for access, or you may have connected to a network that requires a password; consult Capture the Page for more information.

> ***Remember to forget:*** *Because you've connected successfully to the Wi-Fi network, even though you haven't been granted access to the Internet, you need to remove the network from the list of those you've previously joined or you'll have this problem every time you're in range. Tap Settings > Wi-Fi, tap the info ⓘ button beside the network name, and then tap Forget This Network. Confirm.*

- If Safari throws up a connection error, try the next fix.

Check or Ask about the Base Station

If you're on a network where you can control the base station or ask someone who has access (a friend, barista, network administrator, or the like), you might ask them to confirm that there's no problem.

In some cases, a base station can continue to provide service to users who are already connected, but not properly allow new users to connect. Some have limits, as low as five or 10 connected devices, and that limit may only rarely be hit.

Check IP Address Settings

This may sound obscure, but it's an easy way to see if your device is obtaining a network address from the router you've connected to. To check on your assigned IP address, follow these steps:

1. In Settings, tap Wi-Fi.
2. Tap the info ⓘ button to the right of the currently connected network's name.

   The IP Address section should be set to DHCP for almost all networks; another value should be chosen only if you've been told otherwise. (See **Drill Down to Network Details**, earlier in this chapter.)

   If the IP address starts with `169`, then iOS wasn't able to obtain an address from the network. The `169` address range is self-assigned, meaning the device gave itself an address that can't be used on the network, and stopped checking.

Here are several ideas for fixing the IP address:

- Tap Renew Lease; this causes iOS to ask again for a network address. If successful, the IP address will change from a number starting with `169` to an address starting with another range, typically `192.168` or `10`.
- In the main Wi-Fi view, tap the Wi-Fi switch to Off, wait a moment, and tap it back to On. Tap the network name's info ⓘ button to see if the address is now assigned.
- If you're at an event or a hotspot venue, ask the network's operator, the front desk, or whomever. The router may have crashed. (You can look around and see if other people look frustrated, too.)
- Restart the device. Press the Sleep/Wake button until a red slider appears. Slide to power off. Wait until the spinning indicator disappears and the screen turns black. Hold the button down again for a few seconds. An Apple icon appears, and the device starts up.

Make a Mobile Hotspot

Every iPhone and every "Wi-Fi + Cellular" iPad has, in addition to a Wi-Fi radio, a built-in data modem that lets the device access high-speed mobile data networks. The logical question in the iPhone's early years was: why can't we use that same modem with our laptops (or other devices) when we're traveling instead of having to buy a separate cellular modem or router and pay a separate monthly service fee?

Fortunately, Apple followed the suit of other smartphone makers and added Personal Hotspot, which lets you use your phone or tablet as a conduit to the mobile Internet. While the name implies a Wi-Fi hotspot connection, which is one component of it, you may also use Bluetooth or USB with desktop computers and other devices to extend access. All three methods may even be used simultaneously.

Personal Hotspot's availability varies by carrier, although operators around the world offer it: **consult this list by Apple** to check on yours. In North America, all carriers in America and Canada allow its use except for two tiny ones in Canada.

In America, the four largest carriers all include mobile hotspot use in their current plans, and count bandwidth consumed just as they do any other data used by an iPhone or iPad.

> ***Which models?*** *In previous releases, some models that could install the latest iOS version couldn't use every Personal Hotspot feature. But every iPhone model and Wi-Fi + Cellular iPad model that can use iOS 8 can use every option.*

Note: In this chapter, I talk about a mobile hotspot or Personal Hotspot to refer to all the features, but I use the term tethering when the discussion is specifically about Bluetooth or USB.

Turn On Personal Hotspot

There are two ways to turn on the Personal Hotspot feature: directly on your iOS device or through another computer or iOS device.

Whenever you use these methods, the device that turns on the Personal Hotspot then automatically connects to it.

WARNING! *Devices that connect to a Personal Hotspot typically don't treat it any differently than a regular Wi-Fi or Ethernet network—which can mean it's easy to rack up huge amounts of usage. You will want to pause or disable sync services, like Dropbox, and online backup systems, like Backblaze or CrashPlan. You may also want to avoid using any streaming video services or digital media downloads while connected via a Personal Hotspot.*

Turn On in iOS 8

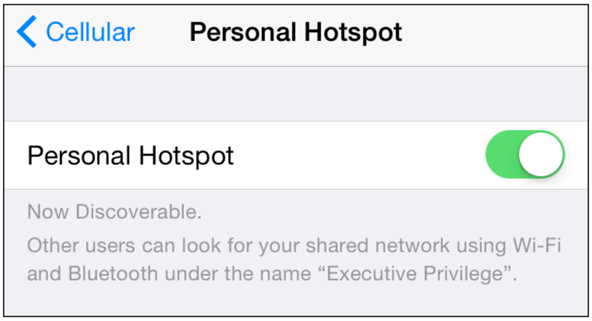
Enable it in Settings > Cellular Data (iPad) or Settings > Cellular (iPhone).

Tap Personal Hotspot to open the Personal Hotspot screen. Now you can switch the hotspot on and set a Wi-Fi password. The screen is also full of connection information (**Figure 5**).

After the first time you tap On, Personal Hotspot appears as an option on the Settings app's left pane (iPad) or main screen (iPhone) so you can access it quickly.

Turn On via Another Device

If you have multiple iOS devices running iOS 8 or the right vintage of Mac and are running Yosemite, you can take advantage of Instant Hotspot, a feature that lets you turn on Personal Hotspot from another device.



Personal Hotspot ●

Now Discoverable.

Other users can look for your shared network using Wi-Fi and Bluetooth under the name “Executive Privilege”.

Figure 5: *The Personal Hotspot view lets you turn access on or off as well as set a Wi-Fi password.*

Instant Hotspot is part of Continuity, a set of connections between your iOS devices and between iOS and Mac OS X. However, the devices must meet a list of conditions for Continuity to work:

- You have iOS 8.1 or OS X 10.10 Yosemite installed on the computer or device you’re using to activate the hotspot, and iOS 8.1 on the iOS device you’re using as a hotspot.
- Your Mac is a model released in mid-2012 (MacBook Air and MacBook Pro) or later (Mac Pro, Mac mini, and iMac).
- Your iOS device was released in the last 2 to 3 years. (See **complete list**.)
- Your iPhone and the other iOS device or Mac are signed in to the same iCloud account.
- Both devices have Bluetooth enabled and are on the same Wi-Fi network.

On a Mac, select the Wi-Fi menu, and choose the device in the menu under Personal Hotspot (**Figure 6**).

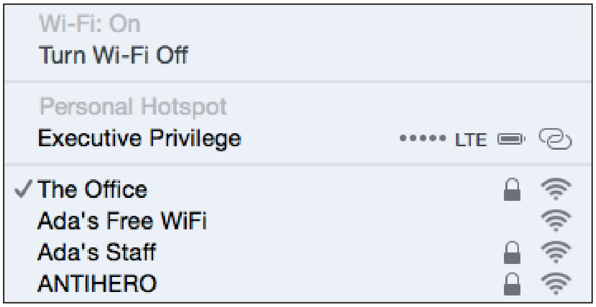
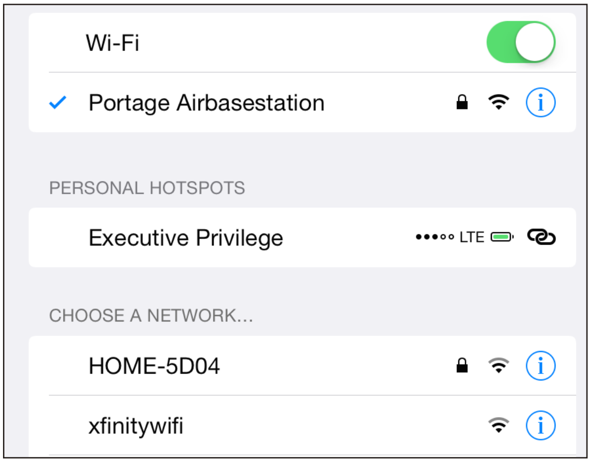


Figure 6: *Instant Hotspot puts an iOS device into your Wi-Fi menu in OS X.*

On another iOS device, launch Settings, tap Wi-Fi, and choose the device in the Personal Hotspots list (**Figure 7**).



Wi-Fi

✓ Portage Airbasestation

PERSONAL HOTSPOTS

Executive Privilege ●●●●○ LTE

CHOOSE A NETWORK...

HOME-5D04

xfinitywifi

Figure 7: *In iOS, pick a device from the Personal Hotspots list.*

Even if you're not planning to connect, you can see the battery life, signal strength, and connection strength of your iOS device as a compact set of graphics in the menu or list.

You Can't Always Use Cell Data while Talking

It can be a little confusing to tell whether an iPhone can continue to have an active cellular data connection while a voice call is underway. On some carrier networks, data is suspended; on others, it slows; and all that is changing right now, with the right iPhone models, too. Wi-Fi data always works during a voice call, but when you're using Personal Hotspot, you're always relying on the cellular network for data backhaul.

Because of both the different cell technology employed by AT&T, T-Mobile, and most other networks around the world (called GSM), and that used by Sprint and Verizon (known as CDMA), and the generation of hardware you have, the option to talk and use data at the same point depends on both your carrier and your phone model. (All iOS 8-compatible CDMA iPhones can also be activated on GSM networks, typically for roaming or switching carriers.)

Digital cell technology is divided up into second-, third-, and fourth-generation (2G, 3G, and 4G) standards, plus some interim ones like EDGE (2.5G) and 3G+ (often called 4G). 2G was the first to carry digital voice, and all forms of it allow either data (at dial-up modem speeds) or voice, but not both at once.

The 3G standard that GSM network operators picked could carry voice and pure data at once, but Sprint and Verizon opted for a flavor of network that would carry data only over 3G. Some non-Apple CDMA phones have two radios, to allow a 2G voice call and a 3G data connection at the same time.

LTE is a 4G standard, designed so voice and data would intermingle for all phones and carriers. However, phones and networks were upgraded before the voice part, Voice over LTE (VoLTE), was ready to go. Even today, the way that VoLTE was implemented by cell companies, the carriers can't connect VoLTE calls between their networks.

Data networking today when a call comes in

As a result, you see the following behavior on most iPhones and on most networks when there is an incoming call or you place a call:

- **Verizon, Sprint, and most CDMA networks:** Data use, including Personal Hotspot, is immediately suspended.
- **AT&T, T-Mobile, and GSM networks:** Data use continues, but is shunted to a 3G, 3G+, or pre-LTE 4G network.

If you don't answer a call or when you hang up, data use returns to the highest-speed available network.

Data networking with a VoLTE call

The list of requirements to make or receive a VoLTE call is daunting at the time of this writing:

- **Requires an iPhone 6 or 6 Plus.** Even though earlier iPhone models seemingly had the circuitry, these two models are the only ones supported at the time of this writing by the four American carriers, and likely worldwide by others.
- **Must be on the same network.** VoLTE doesn't yet work between carrier networks, only for calls that comprise parties on the same network.

- **Carrier must have deployed.** This sounds obvious, but it's hard to sort out. AT&T has deployed part of its VoLTE footprint and plans to finish in 2015. Verizon and T-Mobile have upgraded their LTE networks completely. Sprint plans to wait for a future carrier interoperable version of VoLTE.

If you meet these requirements—and the moon is half full and it's a Tuesday—receiving a call or placing one will happen over VoLTE, vand your Personal Hotspot or other data use will continue at full LTE speeds.

Yes, it's a mess.

> **Note:** Alongside VoLTE, carriers have been rolling out HD Voice, a higher-quality compression algorithm for voice calls. It sounds more like a Skype-to-Skype or FaceTime Audio call than a cellular call. Most VoLTE rollouts are happening alongside HD Voice, which also doesn't work across different carrier networks. Sprint is rolling out HD Voice alone.

Set a Wi-Fi Password

When you first turn on Personal Hotspot, iOS creates a strong WPA2 password. To connect a device over Wi-Fi to the hotspot, you must enter this password on that device.

The default password created by your phone is sometimes a sequence of recognizable words and numbers; other times, it may appear to be random. (At one point, the difference seemed to be by carrier, but now it's impossible to tell.)

You can't decide not to use a password at all, but you may choose to compose your own. You have to pick one that's eight characters or more, although you can make that `12345678` if you must. Tap to enter your own password.

For this kind of connection, where it's not a base station in a fixed location that someone might try to access, I suggest thinking of an eight- or nine-letter word and adding two punctuation marks to the end, like `memorable?%`.

Extra Security with Personal Hotspot

Using USB, Bluetooth, or Wi-Fi to connect to a hotspot device provides a strong layer of security around your connection, which is reassuring if you're at a location like a coffee shop, where the network may not be well secured. USB is a physical connection and can't be monitored. Bluetooth has its own strong automatic security. Apple's required use of WPA2 Personal for Wi-Fi ensures protection there, too. (See **Connect to a Small Network**.)

Although the backhaul to the mobile broadband network isn't impregnable, it does require either a dedicated effort to crack your particular communication or a wiretap at the carrier to intercept data. Personal Hotspot lets you secure the local link at a location where you would otherwise use Wi-Fi but where I would recommend using a VPN (virtual private network) to prevent interception by those around you.

Name Your Wi-Fi Network

The Wi-Fi network has the same name as your iOS device. This is typically your name, or that of whichever account you used to set up the iOS device (**Figure 8**). If you don't feel like broadcasting your account name whenever you turn on Personal Hotspot, you can change it.

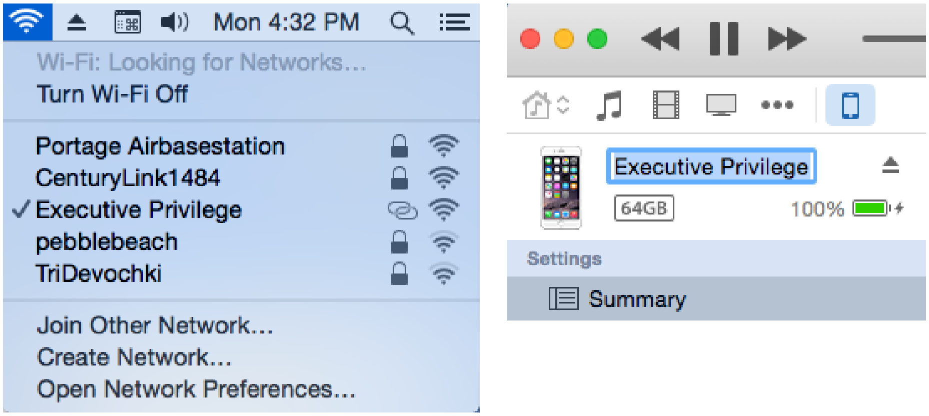


Figure 8: *The Wi-Fi network name (left) is identical to the name of your device, which you can see in iTunes (right) or in Settings.*

To change the name, visit Settings > General > About > Name and enter a new name. Or, with the device connected to iTunes via either USB or

Wi-Fi, click the device's icon in the top bar in iTunes, then click its name to select it, which highlights the name. Type a new name, and click again or press Return.

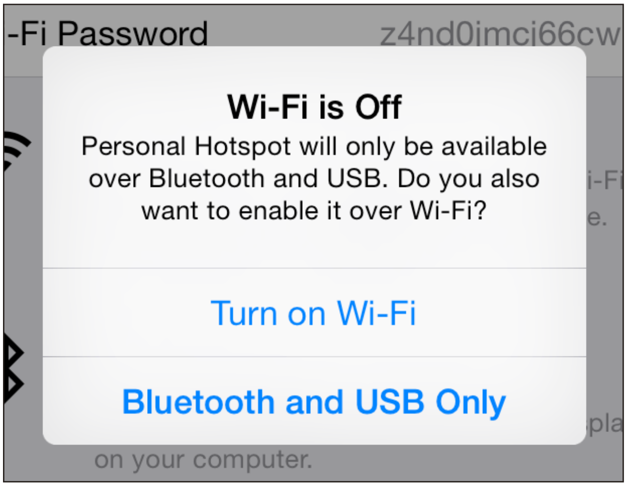
You need to turn Personal Hotspot off and back on for the new name to be broadcast.

Consider Turning Off Certain Radios

Now that you've turned on Personal Hotspot, you might not want it to be available through Bluetooth or Wi-Fi, because nearby devices of yours might accidentally connect to it. The only way to prevent a connection from a device with the right credentials is to turn off the Bluetooth or Wi-Fi radio.

WARNING! *Disabling radios turns off OS X Continuity features.*

To turn off Bluetooth, tap Settings > Bluetooth and slide the switch to Off. To disable Wi-Fi, tap Settings > Wi-Fi and slide the switch to Off. With either or both Bluetooth and Wi-Fi turned off, the Personal Hotspot feature pops up a warning when it's switched on (**Figure 9**).



-Fi Password z4nd0imci66cw

Wi-Fi is Off

Personal Hotspot will only be available over Bluetooth and USB. Do you also want to enable it over Wi-Fi?

Figure 9: *If any networking type used with Personal Hotspot is off, iOS prompts to turn it on.*

You can also change the Personal Hotspot Wi-Fi password to prevent devices that previously connected from gaining access again (see **Set a Wi-Fi Password**, slightly earlier).

Connect to Personal Hotspot

With Personal Hotspot on, you have three choices for how to connect:

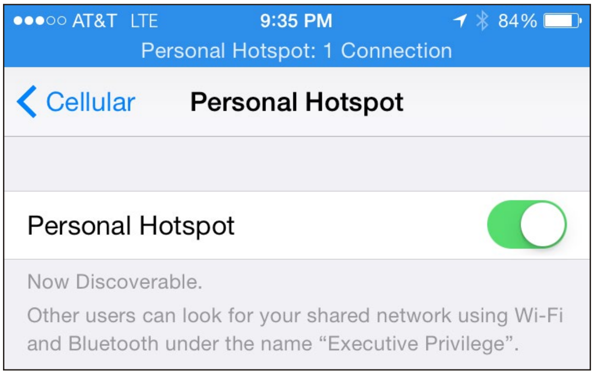
- Wi-Fi: Any Wi-Fi–equipped device can connect just as if the iOS device were a wireless router. Up to five devices can connect via Wi-Fi. (Verizon and Sprint used to limit this to three, but that appears to be lifted.)
- USB: Plugging your computer into your iPhone or iPad gives you a high-speed data connection that you know works as long as the cable isn't bad. The downside? Being literally tethered.
- Bluetooth: This method requires more steps to make a connection initially, but it gives you cable-free flexibility. Most Bluetooth-equipped devices can connect through this method, including iPhones, iPod touches, and iPads. No more than three devices may connect via Bluetooth at the same time.

Tip: Wi-Fi can use more battery power than Bluetooth, so you might opt for Bluetooth tethering. However, the data rate isn't stellar: Bluetooth 4.0, found on the iPhone 4S and later and on the 3rd-generation or later iPad, has a raw data rate of 3 Mbps for continuous connections, and an effective throughput of 2.1 Mbps. That's far below GSM 3G/4G rates and well below LTE rates.

There is a maximum of five total connections across all these methods. If you have five devices connected and try to connect another, the connection will be refused.

I explain how to make a connection shortly; for now, I want to mention that once you make a connection, a blue pulsing banner appears across the top of the iPhone or iPad's screen (**Figure 10**). The banner shows the number of devices connected, too.

If the phone or iPad is on standby, a smaller status banner appears on the Lock screen when you wake it (**Figure 11**).



Personal Hotspot: on

Now Discoverable.

Other users can look for your shared network using Wi-Fi and Bluetooth under the name “Executive Privilege”.

Figure 10: *A banner lets you know whenever your device is acting as a cellular modem for a computer via USB, Wi-Fi, or Bluetooth.*

Note: Windows computers, Android phones, and other devices can also connect via Wi-Fi; many devices can also connect via Bluetooth; and Windows at least can also tether via USB. The process is identical on those platforms to hooking into a Wi-Fi, Bluetooth, or USB shared network, and it neither needs special software nor displays any special indicators as in iOS and Mac OS X.

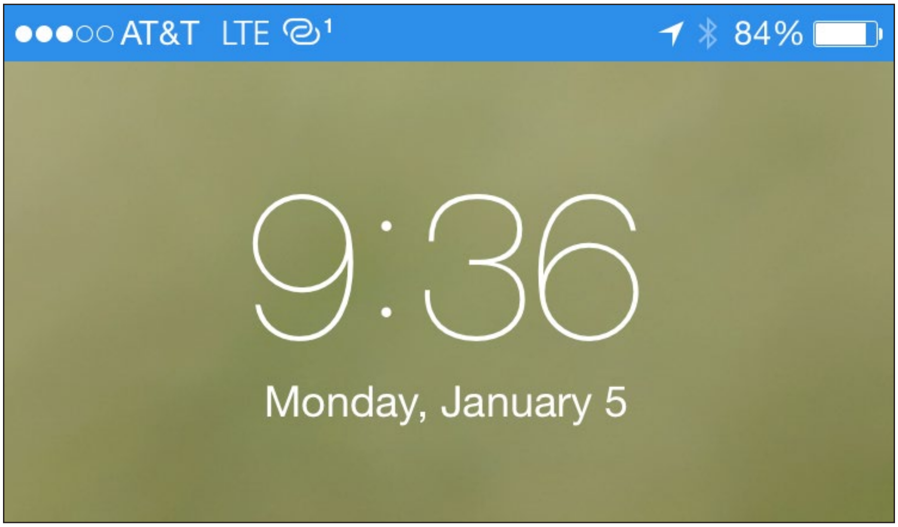


Figure 11: *The Lock screen also shows whether the hotspot is active, with a tiny superscript numeral revealing how many clients are connected.*

Access via Wi-Fi

Using Wi-Fi to connect to a Personal Hotspot is the easiest case because no special setup is required. You use whatever method you normally employ to connect to a Wi-Fi network from the device, and I provide directions for several common operating systems just ahead. The name of your iOS device is the name of the Personal Hotspot network.

Connect via Wi-Fi in Mac OS X

In Mac OS X, you can use the Wi-Fi 🛜 menu on the menu bar to select the Personal Hotspot network by name:

1. Click the Wi-Fi menu to see a list of available networks.
2. Choose the network's name.
   - For an iOS 8.1 or later Personal Hotspot and Yosemite, it appears as it does in Instant Hotspot: an item with the cellular connection type, battery level, and signal strength (**Figure 12**). (If Personal Hotspot is not active on the device, selecting the hotspot in the OS X menu turns it on.)

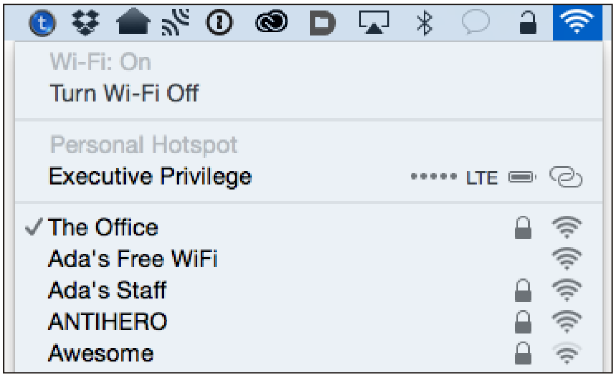


Figure 12: *Select the hotspot under Personal Hotspot.*

   - For an iOS 8.0 or earlier, or with earlier versions of OS X than Yosemite, Personal Hotspot shows up in the main list of networks with a linked-chain 🔗 icon just to the left of the signal strength icon (**Figure 13**).
3. Enter the password, and click Join (**Figure 14**).

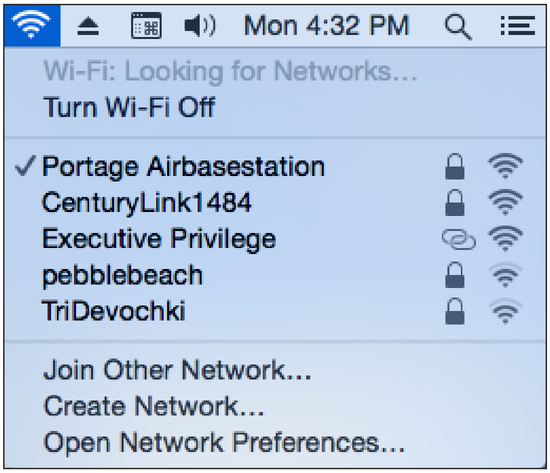
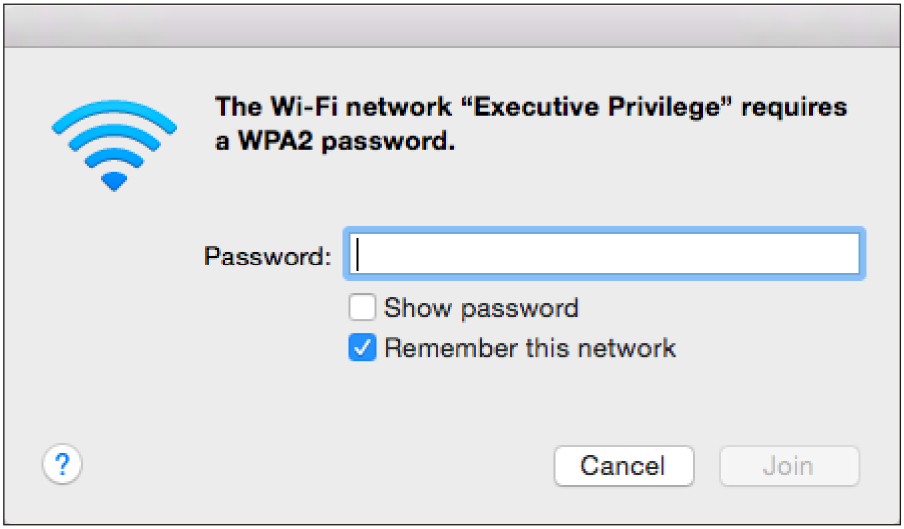


Figure 13: *In iOS 8.0 and earlier, the Personal Hotspot's network name appears in the Wi-Fi menu's networks list.*


The Wi-Fi network "Executive Privilege" requires a WPA2 password.

Password:

☐ Show password

☑ Remember this network

Figure 14: *Enter the network's password to connect.*

> ***Future connections:*** *If you leave Remember This Network checked, you won't be prompted in the future for the password. The flip side of that benefit is that it's difficult to prevent future automatic connections when the personal hotspot's Wi-Fi connection is active.*

You're now connected. Your Mac will stay connected as long as the Personal Hotspot feature is active. The next time you turn on the Personal Hotspot, your Mac will reconnect if you stored the password and if your Mac isn't already associated with a Wi-Fi network.

Disconnect from Personal Hotspot Wi-Fi

To stop using the Personal Hotspot, hold down the Option key and then select the Wi-Fi menu. Now select Disconnect From Network Name and your link is severed.

Don't auto-join in the future

If you want to prevent the Mac from connecting automatically in the future, follow these steps:

1. Launch System Preferences and select the Network pane.
2. Select Wi-Fi in the list at left.
3. Click the Advanced button.
4. From the Wi-Fi pane, select the Personal Hotspot network, then click the minus ⊟ button to delete it.
5. Click OK and then click Apply.

Connect via iOS

In iOS, you use the Settings app to connect to the Personal Hotspot network:

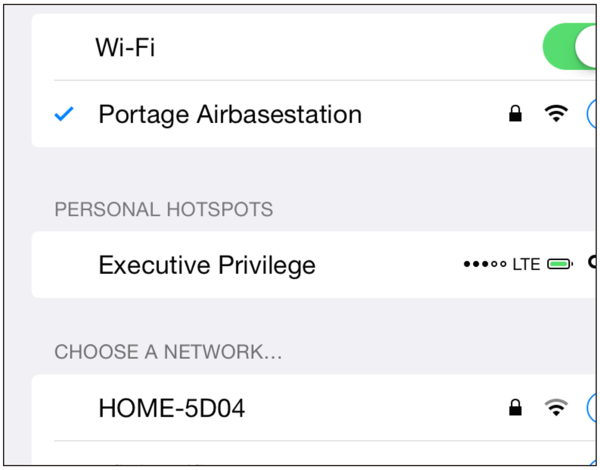
From and to an iOS 8.1 or later device

1. Select Settings > Wi-Fi.
2. Choose the network from the Personal Hotspots list (**Figure 15**).
3. Enter the password when prompted.

   You are now connected. The chain 🔗 icon appears at the left of the iOS status bar instead of the normal Wi-Fi icon.

To or from an iOS 8.0 or earlier device

1. Select Settings > Wi-Fi.



Wi-Fi

✓ Portage Airbasestation

PERSONAL HOTSPOTS

Executive Privilege ●●●●○ LTE

CHOOSE A NETWORK...

HOME-5D04

Figure 15: *Look for the chain 🔗 icon or in the Personal Hotspots section.*

2. Choose the network from the list. Personal Hotspot networks are shown with a special chain 🔗 icon in iOS 4.3 and later.
3. Enter the password when prompted.

   You are now connected. The chain 🔗 icon appears at the left of the iOS status bar instead of the normal Wi-Fi icon.

Automatic reconnection

As long as the password is stored for the iOS network and isn't changed, your iOS device will reconnect automatically whenever it's in range and the Personal Hotspot Wi-Fi connection is active. To stop using the mobile hotspot right away, choose another network from the list or turn off the Wi-Fi adapter.

If you want to prevent connecting automatically in the future, while the hotspot connection is active, tap the blue info ⓘ button next to the network name and then tap Forget This Network. This removes the network's stored setting and disconnects the device from the Personal Hotspot immediately.

Disable Wi-Fi sharing in iOS

To turn off the hotspot on the device that is sharing its connection, just tap Settings > Personal Hotspot and then turn off the Personal Hotspot switch. Or, you can tap Settings > Wi-Fi and turn off Wi-Fi entirely.

You can also block all existing connections from client devices by changing the Wi-Fi password on the Personal Hotspot screen. This will also prevent devices with a stored password from reconnecting automatically or manually until you provide the changed password.

Tether with USB in Mac OS X

With Personal Hotspot enabled, connect your hotspot device to your computer using a USB cable. The first time you enable Personal Hotspot and plug the device into a Mac via USB, Mac OS X alerts you that the interface is added and the Mac's Network system preference pane adds an adapter entry (**Figure 16**).

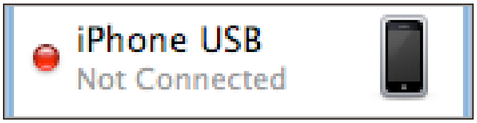


Figure 16: *An entry appears in the adapters list.*

Mac OS X automatically activates a tethered link and turns that red dot green.

> ***Not active?*** *If you're not seeing this, you may need to launch iTunes the first time you tether. iTunes doesn't seem to have anything to do with USB tethering except initial activation.*

To halt the active USB tethering connection, disconnect the USB cable. Alternatively, you can disable the iOS adapter profile. In the Network system preference pane in Mac OS X, select the iPhone USB or iPad USB adapter, and then from the gear ⚙ pop-up menu, choose Make Service Inactive. Click Apply in the lower-right corner.

Connect with Bluetooth

On your hotspot device, make sure Bluetooth is turned on: swipe up from the bottom to show the Control Center and check that the Bluetooth icon is active. If it's not, tap it. (You can also manage Bluetooth from the Settings app.)

Once you’re sure it’s enabled, you can make a Bluetooth connection from Mac OS X or iOS, as I describe next.

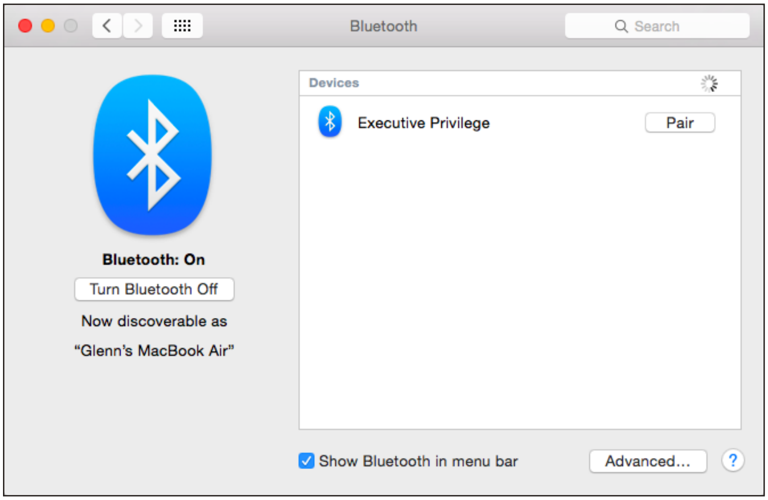
Bluetooth uses less power than Wi-Fi, almost nothing in standby mode, so a Bluetooth connection could allow both an iOS device and a paired piece of hardware to work longer without AC power.

Note: I cover Bluetooth in more detail in **Set Up Bluetooth** if you’d like to learn more.

Bluetooth tethering with Mac OS X

Follow these steps to set up a Bluetooth connection between your hotspot device and a Mac running Yosemite or later (instructions are substantially different in earlier versions of OS X):

1. Launch System Preferences, and select the Bluetooth pane.
2. Your iPhone or iPad should appear in the list of devices (**Figure 17**). Click Pair. (If it doesn’t appear, check that Bluetooth is enabled on the iOS device and that it’s within a few dozen feet of your computer.)



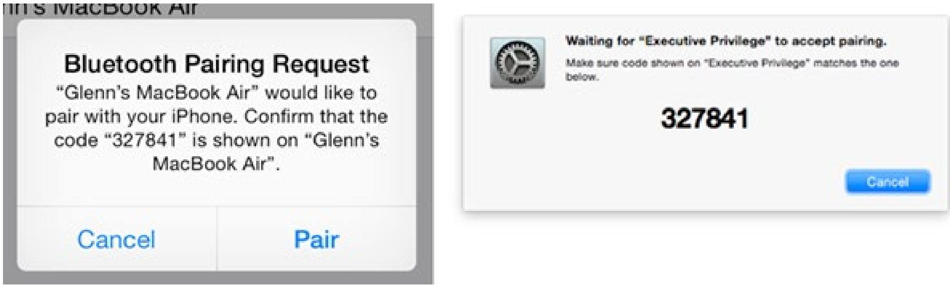
Bluetooth: On

Now discoverable as
“Glenn’s MacBook Air”

☑ Show Bluetooth in menu bar

Figure 17: *Initiate pairing from OS X.*

3. A pop-up dialog appears with a 6-digit code. On the iOS device, a similar confirmation dialog pops up (**Figure 18**).



ın's MacBook Air

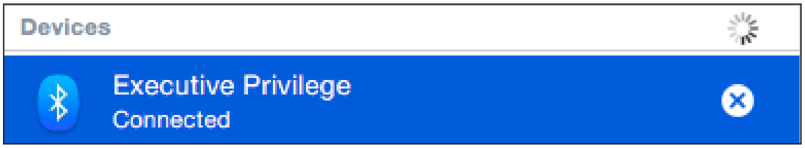
Bluetooth Pairing Request
"Glenn's MacBook Air" would like to pair with your iPhone. Confirm that the code "327841" is shown on "Glenn's MacBook Air".

Waiting for "Executive Privilege" to accept pairing.
Make sure code shown on "Executive Privilege" matches the one below.

327841

Figure 18: *The Mac and iOS device both display the same code.*

4. Confirm that the code is identical, which prevents a so-called man-in-the-middle attack with someone nearby trying to intercept the connection. (That's very unlikely, but it could happen.) The additional cue is the name of the device. Click Pair on the hotspot device. On the Mac, your iOS device should now appear in the list (**Figure 19**).
5. Now, in System Preferences, click Show All, then select Network.



Devices

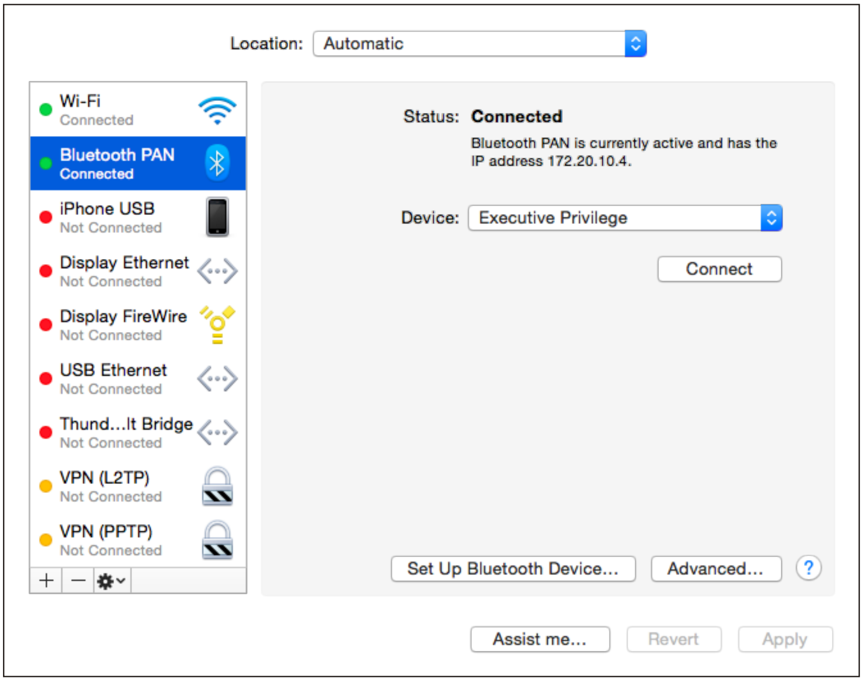
Executive Privilege
Connected

Figure 19: *The device is paired in OS X and connected.*

6. In the adapters list at left, you'll notice a new Bluetooth PAN entry; *PAN* stands for Personal Area Network, and it's the kind of network that Bluetooth creates. Your device should be selected in the Device pop-up menu (**Figure 20**). Click Connect.
7. On the Mac, you'll see the Status label set to Connected (**Figure 20**), and if the Bluetooth system menu ᛒ icon is showing, it will have dots bisecting it horizontally. On your hotspot device, the Internet tethering banner will appear.

   To disconnect Bluetooth tethering, you can do any of the following:

- In the Network preference pane, with Bluetooth PAN selected in the adapters list, click the Disconnect button.


Location: Automatic

Status: Connected

Bluetooth PAN is currently active and has the IP address 172.20.10.4.

Device: Executive Privilege

Figure 20: *The Network preference pane lets you manage the connection over USB.*

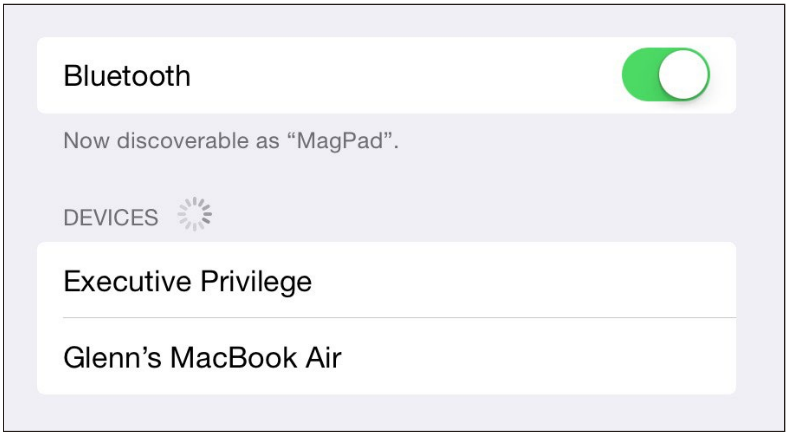
- On your hotspot device, in Settings > Personal Hotspot, tap the Personal Hotspot switch to Off.
- Turn off Bluetooth networking. In iOS, tap Settings > Bluetooth; on the Mac, look in the Bluetooth system preference pane or the Bluetooth ᛒ menu on the menu bar.

Bluetooth tethering with iOS

Although all iOS devices have Wi-Fi built in, Bluetooth consumes less battery power and may be a more appropriate choice. You can set up a Bluetooth connection between any iOS device running iOS 4.3 or later and a hotspot device quite simply:

1. View Settings > Bluetooth.
2. If Bluetooth is off, tap the switch to turn it on.
3. Tap the Personal Hotspot in the list of Devices (**Figure 21**).

   Both devices show confirmation dialogs (**Figure 22**).



Bluetooth

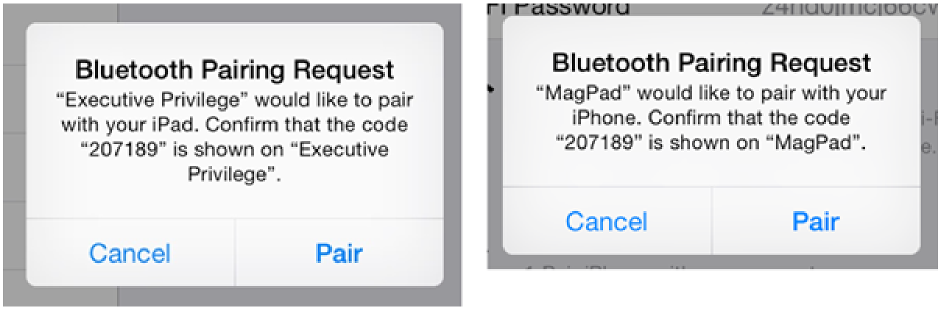
Now discoverable as “MagPad”.

DEVICES

Executive Privilege

Glenn’s MacBook Air

Figure 21: *The Personal Hotspot appears in the Devices list; here, it’s “Executive Privilege.”*



Bluetooth Pairing Request
“Executive Privilege” would like to pair with your iPad. Confirm that the code “207189” is shown on “Executive Privilege”.

Bluetooth Pairing Request
“MagPad” would like to pair with your iPhone. Confirm that the code “207189” is shown on “MagPad”.

Figure 22: *Tap Pair on both devices to proceed.*

4. If the codes match, tap Pair on both devices.

   The iOS device is now connected over Bluetooth, and a chain 🔗 icon appears at the left of the status bar instead of the normal Wi-Fi icon.

To disconnect from the Personal Hotspot, you can do either of the following:

- **On the connected device:** Slide Bluetooth’s switch to Off.
- **On the hotspot device:** Turn off the Personal Hotspot feature or turn off Bluetooth.

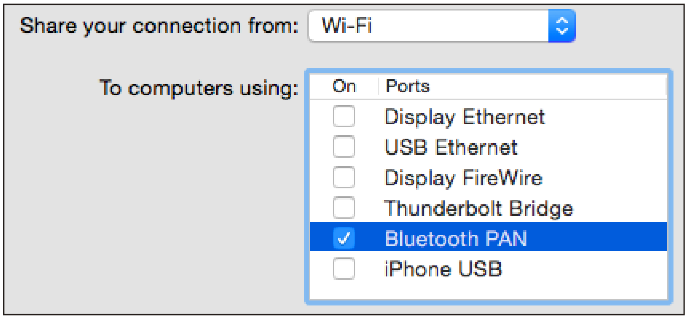
To reconnect, open Settings > Bluetooth and then tap the name of the Personal Hotspot in the Devices list.

You might want to discard a stored Bluetooth pairing from the Devices list if, for instance, you're using a friend's device or you don't want someone else using your iOS device with the paired connection. To remove the pairing, tap the info ⓘ button next to the device name and then tap Forget This Device.

Use Bluetooth Tethering from iOS to a Laptop

A side benefit of the capability to tether over Bluetooth is that you can also use your iOS devices to grab Internet access from a laptop. For instance, if you're in a hotel or other location in which you have to pay for each device you connect to a Wi-Fi network, you were previously out of luck in relaying an Internet connection from a laptop to an iPhone, iPod touch, or iPad. Now you can.

Under Mac OS X, use the Sharing system preference pane's Internet Sharing option to share the Wi-Fi connection via Bluetooth PAN. Choose Wi-Fi from the Share Your Connection From pop-up menu, and check the Bluetooth PAN box in the To Computers Using list (**Figure 23**). Then check the box next to Internet Sharing in the Service list at left.



Share your connection from: Wi-Fi

To computers using:

On	Ports
□	Display Ethernet
□	USB Ethernet
□	Display FireWire
□	Thunderbolt Bridge
☑	Bluetooth PAN
□	iPhone USB

Figure 23: *You can share your Wi-Fi connection via the Bluetooth PAN to iOS devices.*

If you don't see Bluetooth PAN in the To Computers Using list, open the Network preference pane. Click the plus + button at the bottom of the adapters list, and choose Bluetooth PAN from the Interface pop-up menu. Click Create, then click Apply. When you return to the Internet Sharing option in the Sharing preference pane, the Bluetooth PAN will be there.

Choose to Use Cellular Data or Wi-Fi

There are plenty of good reasons to pay attention to whether a cellular iOS device is accessing the Internet via a Wi-Fi network or mobile broadband. You may need greater bandwidth than the cellular network can provide, be budgeting data on a low-bandwidth plan, or be away from your home carrier territory and want to keep usage low.

Whatever the reason, you can determine which network you're on and set the type of network to which your device connects.

Which Network Are You On?

iOS has an indicator in the status bar (near the upper left) that shows which network connection is active (**Table 1**). The range of bandwidth is huge (such as 30 to 300 Mbps as the top rate), because iOS 8 runs on devices that span generations of cellular and Wi-Fi equipment. And each iOS device supports many rates for each standard while also offering backward-compatible support for older networks.

Select Which Service to Use

You can force a cellular device to use either cellular or Wi-Fi service instead of letting it automatically switch depending on whether or not a suitable Wi-Fi network is available. Because iOS doesn't offer network profiles as in Mac OS X, which would make it easy to switch, you must use the Settings app to enable or disable a service.

Table 1: *Deciphering Indicator Icons*

Indicator	Explanation	Bandwidth
No service	Can't connect to any network. You may also see five underscores.	None.
📶	Connected to a Wi-Fi network. The number of white waves, from one (shown as a dot) to three, indicates signal strength from weakest to strongest.	Rates as high as 30–300 Mbps, but limited by the broadband service to which a Wi-Fi router connects.
LTE	Connected via LTE.	From 5–100 Mbps downstream, 2–25 Mbps upstream.
4G	Connected via 4G (GSM only).	Downstream up to 6 Mbps and upstream up to 1.9 Mbps.
3G	Connected via 3G.	GSM: Down 1.7–4 Mbps; up 384 Kbps–1.9 Mbps. CDMA: Down, 600 Kbps–1.4 Mbps; up, 500–800 Kbps.
E	Connected via EDGE, a 2.5G standard (GSM only).	Roughly 200 Kbps downstream (all GSM iOS devices); 40–50 Kbps upstream
GPRS	Connected via 2G using either GPRS (GSM) or 1xRTT (CDMA).	Roughly 40–50 Kbps.
🔗	Connected via tethering; see **Make a Mobile Hotspot**.	

To enable or disable cellular service:

- To use a cellular connection solely and avoid Wi-Fi, perhaps to keep a continuous VPN connection or for security reasons, either:
  - Swipe up to show the Control Center and tap the Wi-Fi icon to disable it.
  - Tap Settings > Wi-Fi, and then set the Wi-Fi switch to Off.

  Avoid a flaky Wi-Fi network: *If a Wi-Fi network is acting flaky, you can avoid the problem by switching off Wi-Fi. Or, use the method noted in Forget This Network to forget the network.*

- To rely only on Wi-Fi, accepting that you may have times during which you have no Internet connectivity, tap Settings > Cellular Data (iPad) or Settings > Cellular (iPhone), and then set Cellular Data to Off. (In the case of an iPad, this disables all features related to using the mobile network; however, for an iPhone, voice calling, voicemail, and messaging remain available.)

  WARNING! *There’s one odd situation to look out for. When you’re using Personal Hotspot, you can connect from an iOS device to a Wi-Fi network while also sharing via Bluetooth or USB to a computer. However, while the iOS device connects to the Wi-Fi network, the shared Internet connection is still pulling from cellular data, even though your iPhone or iPad shows a Wi-Fi icon.*

Manage Cell Data Usage

When Apple introduced the iPhone, it also managed to get AT&T and then other carriers to offer unlimited data plans in the United States and in a few other countries. That didn't last, especially as networks became congested with heavy data use.

There are still millions of people grandfathered into old plans that allow unlimited data use, but most of us—and all new users and network switchers—are either on plans that have a fixed amount of data included in each billing period and then charge fees for overages, or on plans that allow "unlimited" usage, but after a certain amount of data is consumed, the connection is throttled from Mbps to Kbps for the remainder of the billing period.

I'm on a family plan with AT&T that allows 10 GB of use per month among all our cellular-enabled devices, and then charges $15 per additional gigabyte. After many months on this plan, we haven't exceeded our allocation.

This chapter offers a variety of advice on keeping your usage down.

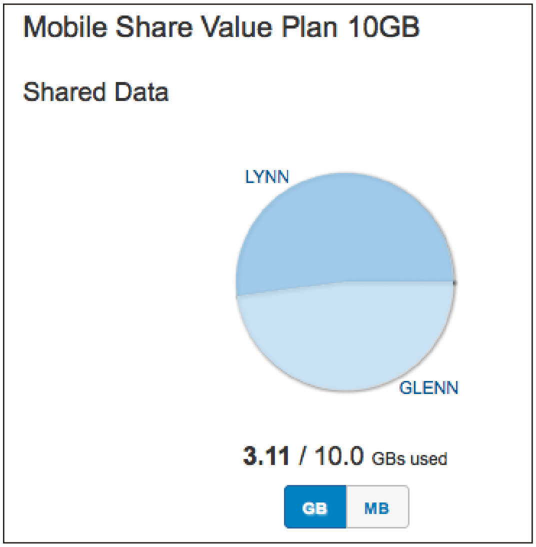
Keep Usage Restrained

You can have mobile access when you need it without breaking your limits, incurring overages, or paying for more chunks of data—if you ration usage. What you need is a strategy.

Tracking Cellular Usage on an iPhone

An iPhone shows your locally tracked consumption of cellular data via Settings > Cellular > Cellular Data Usage. This number has two problems:

- It’s not guaranteed to be accurate. Your carrier’s records are definitive (**Figure 24**). In practice, it’s pretty close.
- It isn’t aligned with your billing period. Rather, it’s a total of all data consumed since the last time you tapped Reset Statistics at the very bottom of the Cellular or Cellular Data view.



Mobile Share Value Plan 10GB

Shared Data

3.11 / 10.0 GBs used

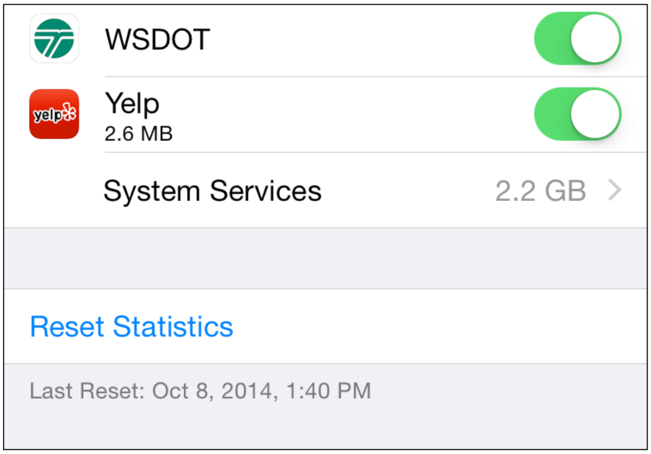
Figure 24: *AT&T’s online data statement is the only one you can rely on for billing.*

You can, of course, visit your carrier’s Web site and get usage information that’s typically accurate to within 24 hours, sometimes much less.

If you’d like this number to be more useful, set yourself a reminder in your calendar for the first of each month (or the start of your billing period if it’s another increment) to visit Settings > Cellular and tap Reset Statistics (**Figure 25**).

Check Usage in Settings

You can find out how much data you’ve used just via Personal Hotspot in the Cellular/Cellular Data view. Tap System Services at the bottom, and all the iOS uses, including Personal Hotspot, are displayed (**Figure 26**).



WSDOT

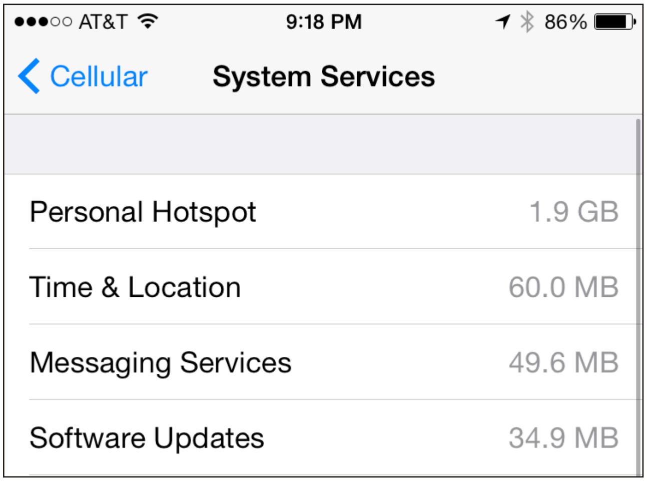
Yelp
2.6 MB

System Services 2.2 GB

Reset Statistics

Last Reset: Oct 8, 2014, 1:40 PM

Figure 25: *Tap Reset Statistics to zero out your current cellular data numbers.*



●●●○○ AT&T 9:18 PM 86%

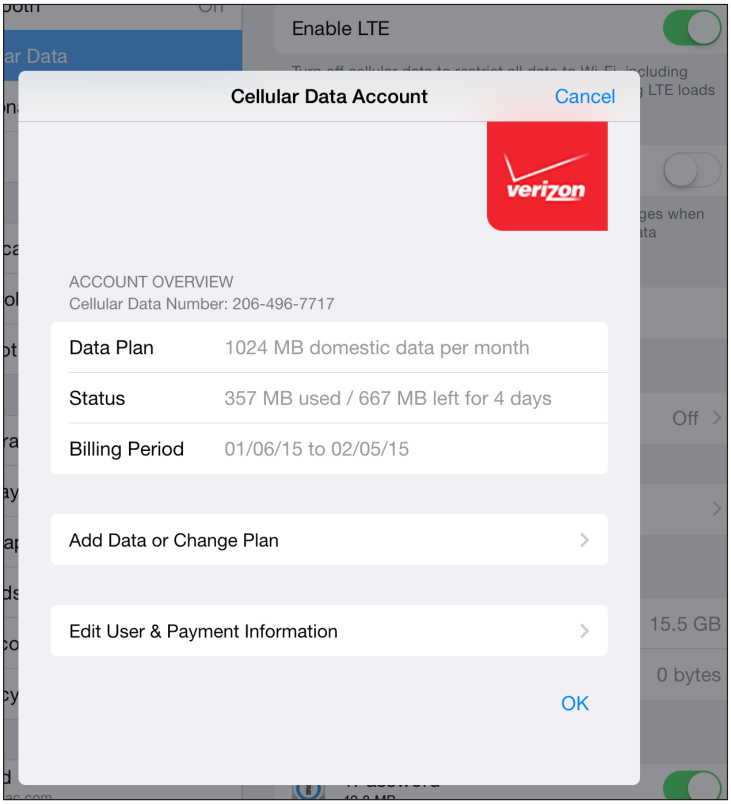
Cellular System Services

Personal Hotspot	1.9 GB
Time & Location	60.0 MB
Messaging Services	49.6 MB
Software Updates	34.9 MB

Figure 26: *You can discover Personal Hotspot's portion of overall cellular data consumed.*

Check Cellular Usage an an iPad

A Wi-Fi + Cellular iPad doesn't track cellular usage, because service is typically only sold in time and bandwidth units. The Settings > Cellular Data > View Account screen shows details from the carrier, including the billing period, how much data is included, and the data consumed so far in that period (**Figure 27**).



ACCOUNT OVERVIEW
Cellular Data Number: 206-496-7717

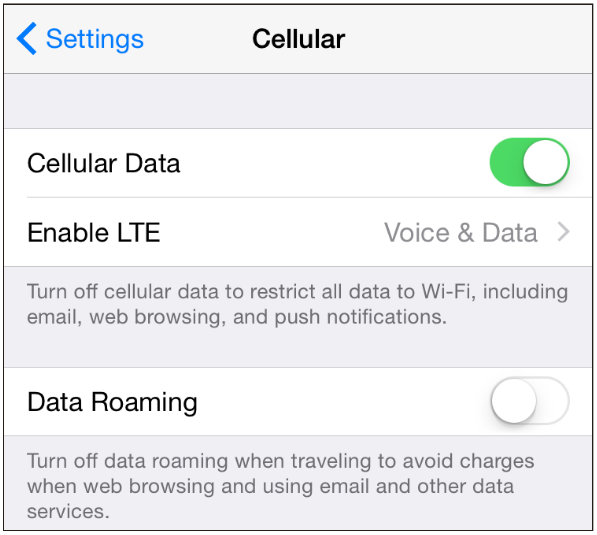
Data Plan	1024 MB domestic data per month
Status	357 MB used / 667 MB left for 4 days
Billing Period	01/06/15 to 02/05/15

Figure 27: *A Wi-Fi + Cellular iPad only shows information via Settings > Cellular Data > View Account, and only for the current billing plan period.*

Turn Cellular Data On Only When You Need It

There are times when you'd prefer not to have an active cellular connection or cellular data link on an iPhone or cellular iPad, notably when you're close to the maximum of your monthly service plan or traveling outside an area included in your data plan (out of the country or in certain remote areas, typically). You can change how the cellular radio interacts with a network in two ways:

- To turn off data only, in Settings > Cellular Data (iPad) or Settings > Cellular (iPhone), set the Cellular Data switch to Off (**Figure 28**). This disables the data link only. On an iPad, that's the entire link to a mobile broadband network; for an iPhone, you can still place and receive voice calls and send and receive SMS/MMS text messages.



Cellular Data

Enable LTE Voice & Data

Turn off cellular data to restrict all data to Wi-Fi, including email, web browsing, and push notifications.

Data Roaming

Turn off data roaming when traveling to avoid charges when web browsing and using email and other data services.

Figure 28: *The Cellular Data switch lets you turn all mobile broadband access on or off. Data Roaming affects use outside your home service area.*

- To shut off the entire cellular connection, set Airplane Mode to On in the upper left of the main Settings screen, or tap the Airplane Mode button in the Control Center. Airplane Mode turns off all radios, not just cellular. See Use **Airplane Mode** for details. It also dramatically extends your battery life in most cases.

  You can also control other cellular data parameters:

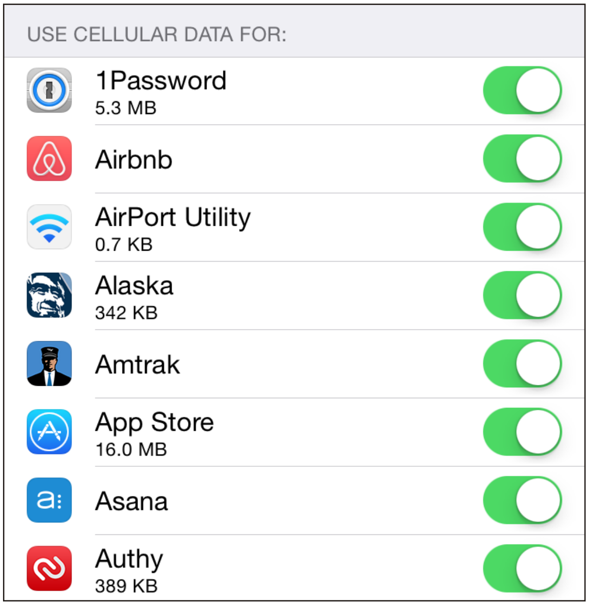
- Setting Enable LTE to Off will eliminate use of 4G LTE networks and rely on slower 2G and 3G networks. This is useful when LTE networks near you are spotty and you're having trouble staying connected as your device swaps back and forth between 2G/3G and 4G LTE. This can also reduce battery consumption in some cases.
- In some markets, the Enable LTE option may read Voice & Data, and let you pick 2G, 3G, or LTE as network options.
- Data Roaming can ensure that you don't consume cell bytes while you're outside the home area for your carrier. In some cases, you might have limits; in others, you might be charged. For instance, Sprint and Verizon allow roaming across their networks in areas they don't serve, but limit use to no more than 300 MB per month.

Limit Your Activities on the Cell Network

Unless you are connected with Wi-Fi, limit your Internet-related activities to those that don't use much data, such as checking email or viewing Web pages.

Various items in Settings let you limit whether cellular data can be used for an app or activity, including:

- Use the options in Cellular Data (iPad) or Cellular (iPhone) to prevent excessive use of certain services from consuming a lot of your data allocation. You can turn on and off specific apps, and see their data consumption (see **Figure 29**).



USE CELLULAR DATA FOR:

1Password
5.3 MB

Airbnb

AirPort Utility
0.7 KB

Alaska
342 KB

Amtrak

App Store
16.0 MB

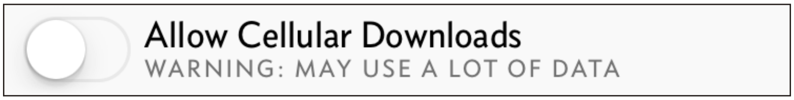
Asana

Authy
389 KB

Figure 29: *Opt out of cell data for certain iPhone apps.*

- In the Safari settings, you can disable syncing the reading list, which is relatively low bandwidth depending on how you use it.
- In iCloud > iCloud Drive, swipe to the bottom and you can disable syncing all items in the list over cellular.
- In iTunes & App Store, you can choose whether or not to use cellular data for automatic downloads (four different options for things you've purchased and updates), iTunes Match, and iTunes Radio.

- You can also enable or disable cellular use via settings within certain apps. For instance, the podcast app Overcast has a cellular data switch in its Downloads area to let you grab a specific episode or download any available episode via cellular whenever it's available (**Figure 30**).



Allow Cellular Downloads
WARNING: MAY USE A LOT OF DATA

Figure 30: *Overcast is blunt about what might happen.*

More generally, you should avoid using or disable the cellular use in Settings for:

- Audio-streaming apps, such as those used by radio stations and networks. Usage is generally small, but it can add up.
- Video-streaming apps like Hulu Plus, YouTube, Netflix, and Vimeo. It's easy to run through a gigabyte or more in an hour, depending on your device and connection.
- Photo-browsing apps like Flickr. Depending on the app, even swiping past a photo might download a megabyte or more.

Note: The Maps app used to consume lots of data because Apple loaded image data from Google to power its software, even after Google switched to offering *vector* data for plain maps. Vector data uses scale-independent points and arcs and straight lines between them to represent maps, using vastly less data. Apple's own Maps app and the revised Google Maps app both use vector data. In looking at heavy usage of Google Maps for a three-month period, my iPhone shows only 94 MB of data consumed over cellular.

Note: Your cellular iOS device will warn you if you start running out of data or start to near your current plan limit during a billing cycle.

Airplane Mode

Before you're flying so high with some guy in the sky, you need to disable radio communications on your mobile device. The Airplane Mode switch makes this simple.

Until recently, the FAA enforced a kind of commercial urban myth: that the cellular radios in cell phones as well as personal electronics could cause interference with the avionics (electronic flight systems) on commercial aircraft.

This was out of an abundance of caution even years after it was clearly proven that there was no such risk—and after it was shown that cell phones are routinely left on, or even used, in flight without any adverse effects.

The latest flight rules in the U.S. allow the use of handheld personal electronics below 10,000 feet, even though laptops and other large devices are supposed to be stowed so they don't become projectiles. (1,000-page books are still OK, bizarrely.)

Cellular radios remain banned, and one ostensibly isn't supposed to use Bluetooth at all, and should not turn on Wi-Fi unless in a plane equipped with Wi-Fi service.

What's Airplane Mode?

Airplane Mode in iOS, available to all iOS devices, is a simple way to set your device to a legally required quiet mode during flight. In the Settings app, tap the switch next to Airplane Mode. You see an airplane ✈ icon in the top status bar at the left when the mode is active.

Saves battery life, too: *If you don't need to use any of the radios for network access, peripherals, or location, Airplane Mode is an effective way to extend battery life, too.*

WARNING! *Airplane Mode effectively hobbles Find My iPhone. If you're concerned about losing your device and not being able to find it later, Airplane Mode disables all the necessary network access and GPS data to allow location tracking.*

When you turn on Airplane Mode in the Settings app, iOS turns off four separate radio systems on an iPhone or cellular iPad: cellular, GPS, Wi-Fi, and Bluetooth. On a Wi-Fi-only iPad or any iPod touch, Wi-Fi and Bluetooth are disabled.

Sleep doesn't disable radios or activity: *When you push the Sleep/Wake button on the top or side of your iOS device to put it to sleep, you might think the entire device is suspended. But this standby mode is pretty active. Certain background operations continue, and a cellular iPad and any iPhone can receive email and other updates via push over a cellular data connection. iOS also maintains Wi-Fi connections on a minimal continuous level. Sleep is more like lightly daydreaming for an iOS device.*

On flights on which Wi-Fi is available for Internet access—this option is available on many U.S. aircraft—you can separately tap Wi-Fi in the Settings app.

When you turn Airplane Mode back to Off after leaving a plane, all your previous settings for access are flipped back on.

Tip: Airplane Mode can also help avoid international charges, because when an iPhone has its radios off, it cannot receive calls. Also, you can neither inadvertently place a call nor use data. Unfortunately, because the mode turns off GPS with no separate way to re-enable positioning, you lose the ability to use navigation software that has built-in maps.

Turning Radios Off Separately

You can choose to separately turn off both radios in a Wi-Fi–only iPad or any iPod touch and three of the four radios in an iPhone or cellular iPad without engaging Airplane Mode:

- Wi-Fi: Swipe up to reveal the Control Center and tap the Wi-Fi icon; or, in Settings, tap Wi-Fi, and set Wi-Fi to Off.
- Bluetooth: Swipe up to reveal the Control Center and tap the Bluetooth icon; or, in Settings, tap Bluetooth, and set Bluetooth to Off.
- GPS: Tap Settings > Privacy > Location Services, and set Location Services to Off.

Is GPS really off? *GPS is a receive-only system; with Location Services off, ostensibly, the GPS receiver isn't powered up and attempting to find data, so it's "off" in that sense.*

WARNING! *Disabling Location Services prevents iOS from using GPS, Wi-Fi, and cell-tower based information to provide location data to apps and the operating system.*

There is no way to disable the cellular radio separate from Airplane Mode, however. You can opt to disable various cellular modes, as discussed in **Manage Cell Data Usage**.

Set Up Bluetooth

Bluetooth wireless networking lets you connect peripherals like battery-powered headphones, earpieces, headsets, and keyboards to an iOS device for listening to music and entering text.

Read this chapter to learn how to set up and manage Bluetooth devices.

> ***Tethering:*** *Bluetooth can provide Internet service to an iOS device from another piece of hardware, such as an iPhone with Personal Hotspot enabled, a laptop, or a cellular router with Bluetooth as an option. See the earlier chapter Make a Mobile Hotspot for details.*

Bluetooth Basics

The Bluetooth SIG, a trade group, certifies devices as Bluetooth compliant for particular profiles, which include things like text entry, stereo audio, file transfer, and modem access. Apple's iOS devices work with any device that meets the Bluetooth spec for several profiles, including audio, peer-to-peer transfer, and external keyboards.

> **Note:** Apple documents iOS device compatibility in a support note at **http://support.apple.com/kb/HT3647**.

When you connect with Bluetooth, the process is known as pairing. Some devices can be paired with several hosts (like computers or mobile devices); others can pair with only one host at a time, and must be re-paired to switch. Bluetooth devices are discoverable when they are set to allow a pairing connection.

Bluetooth is handled from the Bluetooth view (Settings > Bluetooth). This view lets you turn Bluetooth on and off and displays a list of Bluetooth peripherals under My Devices and Other Devices. The My Devices list shows any devices that have been previously attached to the device and the current status of such devices. The Other Devices list displays any discoverable devices within range.

Bluetooth 4.0 and Low Energy (LE)

Bluetooth 4 brought a low-power mode called Bluetooth LE (sometimes called Bluetooth Smart) to the mix. It lets devices with tiny batteries that are meant to be changed infrequently communicate in tiny, power-conserving bursts. You could have Smart devices in your home's alarm system, and an iOS app could let you tap to see if any windows are ajar, for instance.

Apple has used Bluetooth LE extensively in later releases of iOS and Mac OS X to enable signaling between devices for AirDrop (see **Exchange Files with AirDrop**) and some of the Continuity features, like Instant Hotspot (see **Turn On via Another Device**).

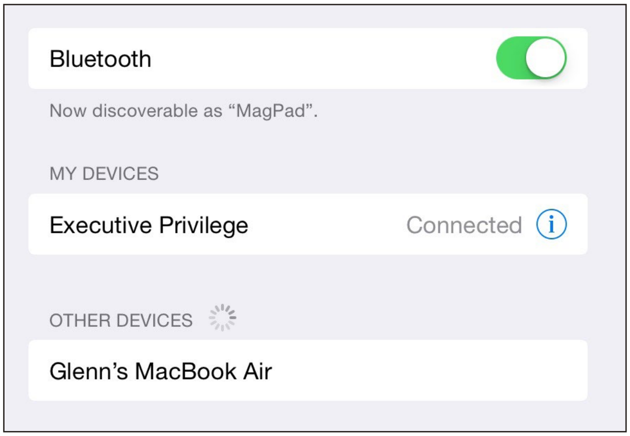
Bluetooth LE is also part of Apple's iBeacon, where a piece of hardware with location-specific information—such as a map in a mall, information about a historical site, or a coupon offered by a restaurant—can be sent over short distances to your phone or tablet.

Pairing Any Device

To start pairing, follow these general steps (the specifics for particular profiles are given later in this chapter):

1. Tap Settings > Bluetooth.
2. Activate Bluetooth discovery on the other device. Turning on discovery varies by device; check the manual. Typically, you hold down a button (sometimes a special pairing button) for several seconds.

   On your iOS device in the Bluetooth view, the other device appears, naturally enough, in the Other Devices list (**Figure 31**).
3. Tap the desired device. iOS attempts to connect.
4. Depending on the device, iOS will do one of the following:
   - Simply proceed: iOS pairs without requiring a code or confirmation. You'll see this with simple devices.



Bluetooth

Now discoverable as “MagPad”.

MY DEVICES

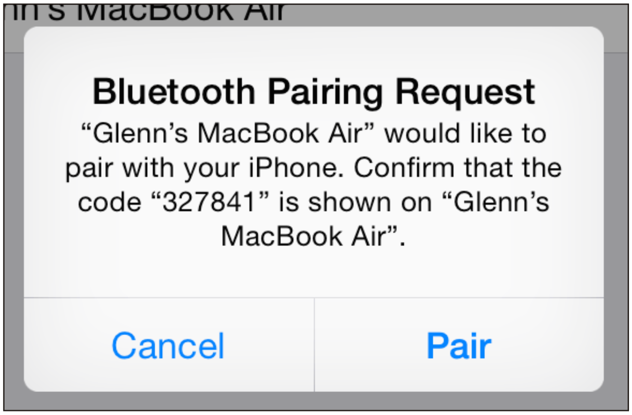
Executive Privilege Connected

OTHER DEVICES

Glenn’s MacBook Air

Figure 31: *An unpaired device (my MacBook Air) is discovered.*

- Show a Pair button: In some cases, you don’t need to type a pairing code, but you get a dialog like the one in **Figure 32** on each device. Compare the code, and tap Pair on each to confirm.



Bluetooth Pairing Request

“Glenn’s MacBook Air” would like to pair with your iPhone. Confirm that the code “327841” is shown on “Glenn’s MacBook Air”.

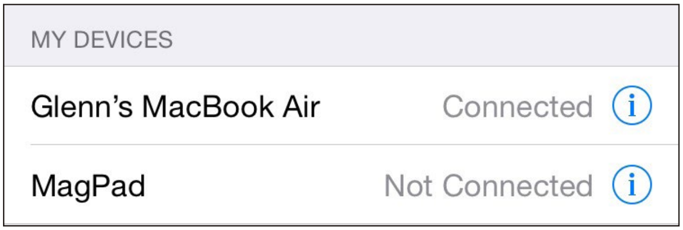
Figure 32: *iOS devices and Macs just ask you to confirm.*

Prevent accidental pairing and attacks: *You’re asked to confirm a code to ensure that it’s the right device and that nobody else is trying to control the two devices trying to pair. The cryptography behind this would prevent both devices from seeing the same code if someone had managed to interpose themselves into the pairing. Sometimes you’ll see a different code if someone else nearby happened to be trying to pair a Bluetooth device at the same time, however!*

- Show a field in which you enter a code: The code will either be provided by the other device or—in the case of a peripheral without a way to choose or display characters—noted in its manual. It's typically `0000`.
- Display a code that you enter on the other device: Your iOS device generates a PIN (called a "passkey" here) to be entered in the pairing device.

The paired device is now shown as Connected in the list.

iOS shows a Connected label for paired devices that are turned on and available, and Not Connected for those that aren't in range or are turned off (**Figure 33**).



MY DEVICES

Glenn's MacBook Air Connected ⓘ

MagPad Not Connected ⓘ

Figure 33: *The MacBook Air is paired and connected; the iPad is paired but not connected.*

Tip: To remove a pairing, select the peripheral in the Devices list, tap the info ⓘ button, and then tap Forget This Device.

Apple Wireless Keyboard May Need Handholding

Apple Wireless Keyboard, which ships with all new Macs, uses Bluetooth for connectivity, and can be paired with multiple computers and devices. But it can be tricky to connect the keyboard with the one you want if more than one paired device is in radio range.

To test this, I tried to pair a keyboard that was already associated with an iPad and an iPhone with a Mac. I found that I had to turn Bluetooth off on the iPad and on the iPhone (Settings > Bluetooth) and then turn the keyboard off before it could pair with the Mac. Pairing then worked fine. (You can't disconnect a Bluetooth device on an iPad or in iOS and leave it paired for future use; the only option is Forget This Device.)

After re-enabling Bluetooth on the iPhone, I turned the keyboard off and then back on to see which device it associated with. The Mac grabbed it first. From the Mac's system menu bar, I opened the Bluetooth menu and chose Disconnect from the keyboard's submenu.

Then, on the iPhone, in the Bluetooth settings, I tapped the keyboard's item in the My Devices list, and the iPhone associated with the keyboard. This is a little tedious, I know, but it's manageable if you want to use the keyboard with multiple devices.

WARNING! *If you walk away from a Bluetooth keyboard while it's still on, it can maintain a connection over a long distance. I was mystified as to why I couldn't get an onscreen keyboard to appear on my iPad when two rooms away from an Apple Wireless Keyboard until I recalled I hadn't turned it off.*

Hands-Free Profile

The Hands-Free Profile in Bluetooth lets you have audio conversations using the mic and headphones (or speakers) on a variety of devices, such as over-the-ear or in-ear headsets. You pair a device just as described in Pairing Any Device, earlier.

On an iPhone, you can answer incoming calls by tapping the answer button on the headset. When you place a call, the last chosen mic/headphone is used, but you can pick from the available options, even as the call is underway, by tapping the Audio button. In the example in **Figure 34**, I could choose among the headphones/headset combo I have from Sony, the iPhone's earpiece/mic, or the speakerphone option on the iPhone.

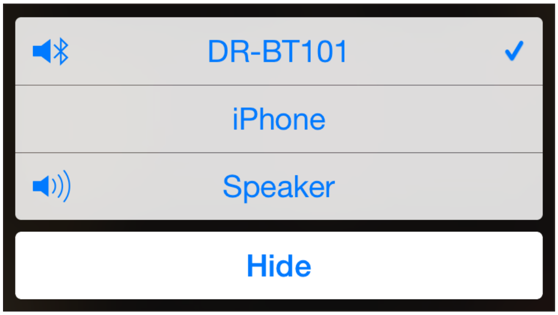


Figure 34: *When placing a call, you can choose a Bluetooth device.*

Picking an audio source also works to let you use a headset for other programs, such as Skype or FaceTime, that don't require a cellular network or an iPhone.

> ***Full support:*** *Apple has supported this profile in all iPhones, in the iPad since the iPad 2, in all iPad minis, and in the iPod touch starting in its 4th generation model.*

Audio Devices

iOS supports two of the three common audio playback profiles for Bluetooth: one for stereo audio playback, and another that allows remote control (pause, play, and stop).

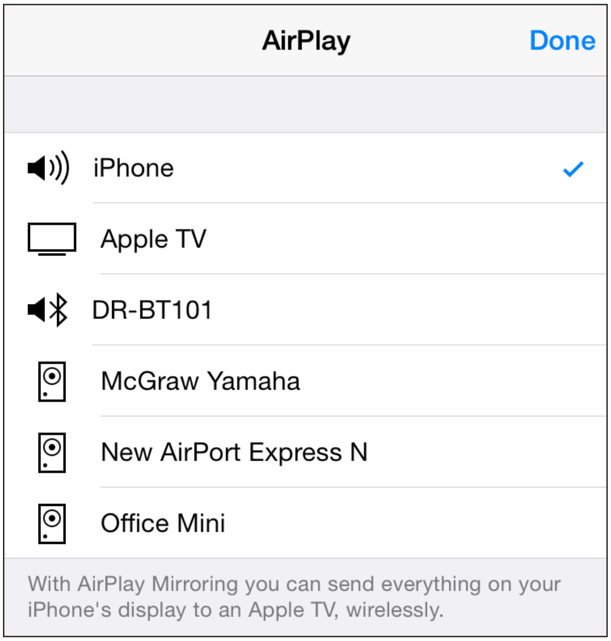
> **Note:** The technical names for these two profiles—useful if you're examining the spec of Bluetooth gear to buy—are the Advanced Audio Distribution Profile (A2DP) and the Audio/Video Remote Control Profile (AVRCP).

Once you've paired stereo headphones, you can use them just as you would headphones plugged into any iOS device. You can tap the start, stop, and other controls in an app playing back audio, or, if your Bluetooth headphones or headset has these controls, you can handle those options remotely.

Apps that allow audio playback should show a special AirPlay icon when multiple audio output options are available. You can also swipe up to reveal the Control Center and change all iOS audio output to another audio device. (See Stream Music and Video with AirPlay for more about that technology.)

Tap the icon to pick an audio destination, which includes the device itself (to use its built-in speakers), one or more active Bluetooth headphones, and any Apple TVs or AirPlay speakers connected to your network (**Figure 35**).

Only one output source may be selected from the list at a time. Tap a device to choose it. Audio continues to play throughout and seamlessly switches whenever you tap.



With AirPlay Mirroring you can send everything on your iPhone's display to an Apple TV, wirelessly.

Figure 35: *Tap the AirPlay button in the audio playback controls to choose among available audio output destinations.*

You can stop using Bluetooth headphones with one of three methods:

- Turn off the Bluetooth headphones using the power button.
- In Settings > Bluetooth, in the entry for the headphones, tap the info ⓘ button, tap Forget This Device, and then tap OK.
- Move the iOS device and the Bluetooth headphones out of range of each other. I like this option least, because Bluetooth can work over a long range. If you leave your headphones at home and take your mobile device with you, then this option makes sense.

In all cases, audio output reverts to the speakers automatically.

Exchange Files with AirDrop

AirDrop was introduced in Mac OS X 10.7 Lion to let you trade files, URLs, contact cards, and a few other kinds of things among Macs on the same Wi-Fi network. It was later added to iOS 7, but the iOS version only worked with other iOS devices!

Finally, with iOS 8 and Mac OS X 10.10 Yosemite, Apple upgraded to allow both intra- and inter-platform AirDrop support.

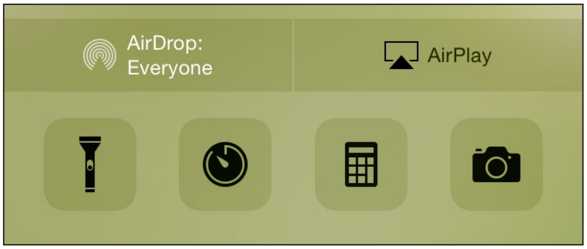
WARNING! *Apple's support for iOS/OS X AirDrop is a little asymmetric. Macs as far back as 2009 can use AirDrop with other Macs. However, to use AirDrop between Yosemite and iOS 8, a Mac has to meet the same requirements for the Handoff feature in Continuity. (See **Make a Mobile Hotspot** for details about Handoff.)*

Configure AirDrop

AirDrop is one of the simplest pieces of iOS technology. There's only one set of choices to make (**Figure 36**).

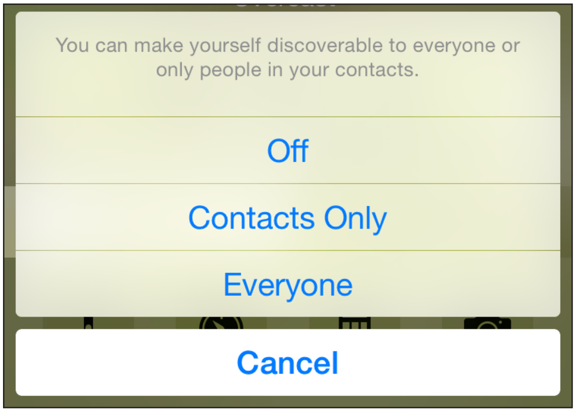
1. Swipe up to show the Control Center.
2. Tap the AirDrop area in the bottom left.
3. Tap one of the options (**Figure 37**):
   - Off disables AirDrop.
   - Contacts Only shows your device only to people whose email address is in your Contacts. This is the default option.

- Everyone lets anyone on the local network see that you're available to receive files.



AirDrop: Everyone

Figure 36: *The Control Center is where you set AirDrop access.*



You can make yourself discoverable to everyone or only people in your contacts.

Figure 37: *You can pick how AirDrop advertises itself on a network.*

Share with AirDrop

AirDrop is available in any Sharing sheet in iOS 8: you can send URLs, file, photos, contacts, and other items. When you tap the Share icon, AirDrop will appear at the top, whether or not you've turned off discovery in Control Center. You'll see a list of all users on the local network who make themselves discoverable to everyone, or who have you in their Contacts (**Figure 38**).

To share over AirDrop, tap the Share icon and then select the user. The recipient will either automatically receive or tap or click to accept or reject the file, as described below.

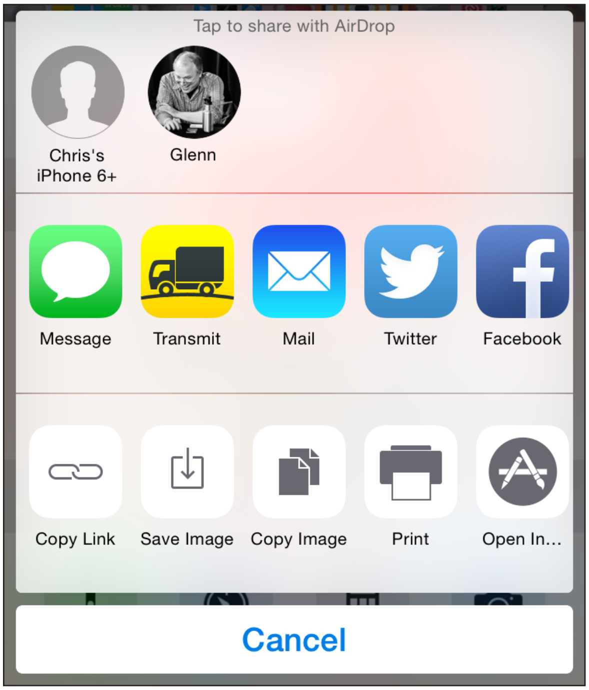


Figure 38: *The Share sheet shows all available AirDrop users.*

When a file or other item is accepted or received, the label Sent appears on the icon for the person to whom you transmitted the item (**Figure 39**).

Share from Yosemite

OS X has a slightly more elaborate way to share using AirDrop:

1. In the Finder, choose Go > AirDrop (Command-Shift-R) or click the AirDrop item in a Finder sidebar window. The AirDrop window shows all available recipients (**Figure 40**). (On Macs with Handoff support, it also has the same popup menu for configuring how your system is discoverable.)
2. Drag a file, folder, or set of items onto a recipient's icon.
3. The recipient is prompted to accept the files. If they agree, the files are transferred.

   In software that supports a Share sheet, click the sharing link and choose AirDrop, and you can pick a recipient for a URL, image, or other item (**Figure 41**).

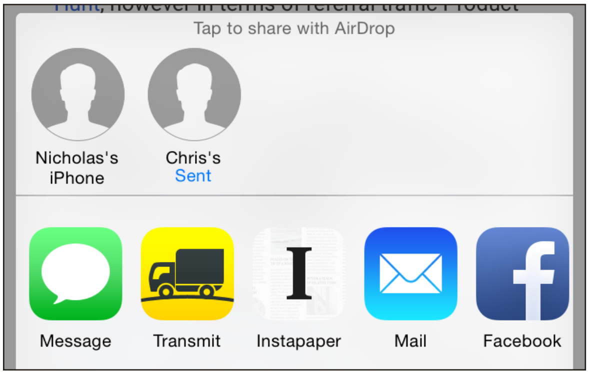
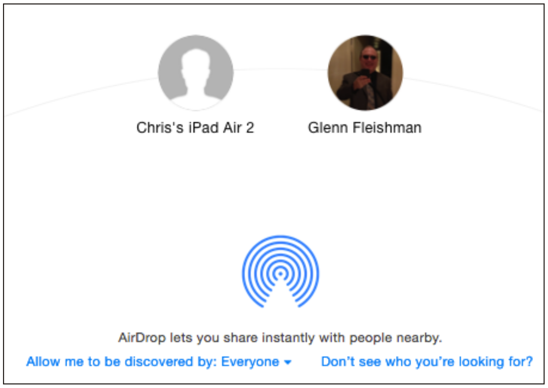


Figure 39: *The Sent label appears to confirm delivery.*


Chris's iPad Air 2
Glenn Fleishman

AirDrop lets you share instantly with people nearby.

Allow me to be discovered by: Everyone ▾
Don't see who you're looking for?

Figure 40: *A list of recipients is shown in the AirDrop window.*

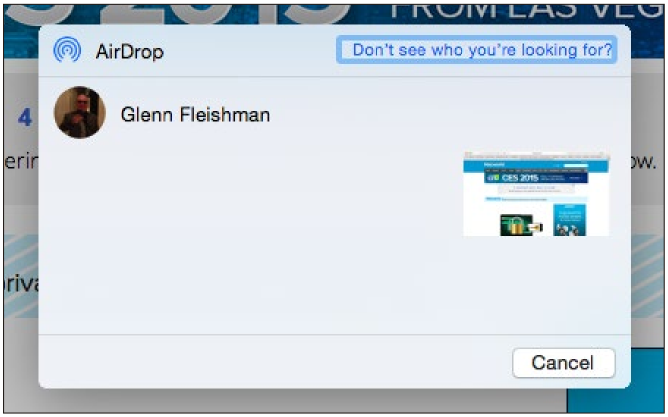
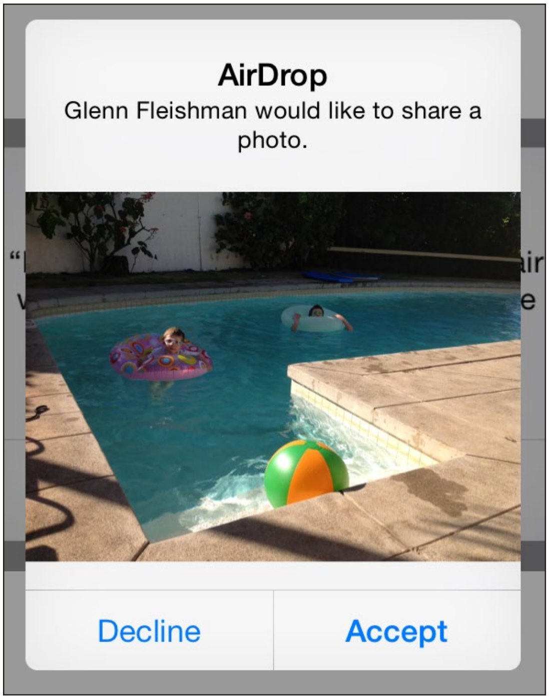


Figure 41: *You can AirDrop an item within an OS X app, too.*

Receive a File in iOS 8

In iOS, you are always prompted whether to accept the AirDrop transfer (**Figure 42**), whether or not the same iCloud account is logged in to on the sending device.



AirDrop

Glenn Fleishman would like to share a photo.

Figure 42: *You're prompted to accept incoming files in iOS.*

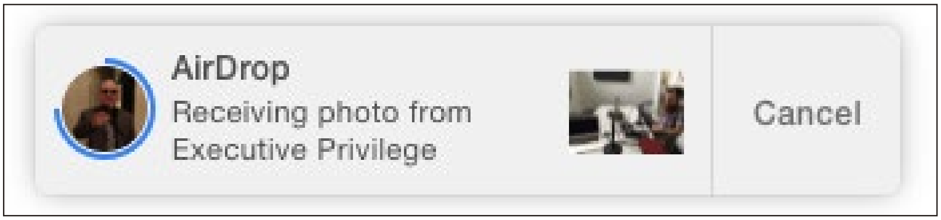
If you click Accept:

- Image files are added to your Photos collection, the Photos app is launched, and the image is opened.
- URLs are opened in Safari.
- Other files are opened by the appropriate app, or an Open In pop-up/pop-over menu appears from which you can select the appropriate app.

Receive a File in Yosemite

Yosemite varies receiving behavior depending on whether the sender is logged in to the same iCloud account or not.

- Same iCloud account: The file, URL, or other item is received automatically. If it's a URL, the Web page is opened. A small notification appears and a punctuated chime sounds (**Figure 43**).

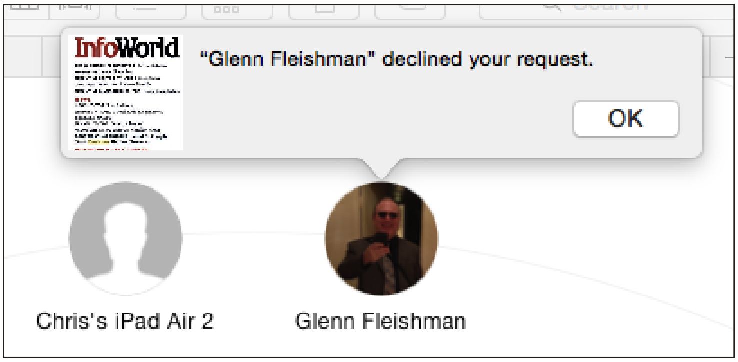


AirDrop

Receiving photo from Executive Privilege

Figure 43: *OS X automatically accepts files from iOS devices signed in to the same iCloud account. Progress is shown as a colored circle that fills the avatar's circumference.*

- Any other user: The recipient is asked to Save, Decline, or Save and Open a file (**Figure 44**).



"Glenn Fleishman" declined your request.

Figure 44: *In this case, shown on the sender's computer, the recipient declined the file.*

Stream Music and Video via AirPlay

Apple's AirPlay technology lets you stream audio and video from Apple equipment to a variety of other hardware, including stereo receivers, computers, the Apple TV, the AirPort Express base station, and more.

What's just as good is that Apple licenses the specification so that other companies can extend AirPlay to be more useful. In this chapter, you'll learn how to set up AirPlay, but also how to use it more broadly than with Apple's software and hardware.

Every iOS device that can install iOS 8 can use AirPlay.

Select AirPlay Devices

This chapter has to start a little backwards, because before you can use AirPlay, you need a destination. But it's easier to walk through how you can configure your iOS device to point to an AirPlay receiver, and then look at the many kinds of uses.

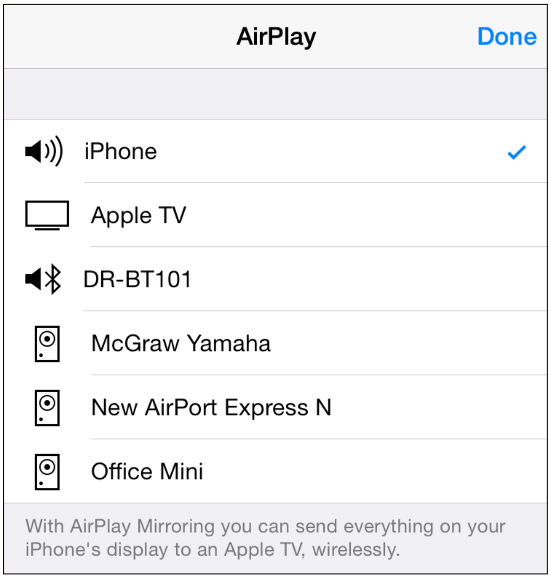
To select any AirPlay-compatible device on the same Wi-Fi network as your iOS device, follow these steps:

1. Swipe up to reveal the Control Center.
2. Tap the AirPlay area at lower right. (If no AirPlay destinations are available—or powered on—the AirPlay area doesn't appear.)
3. Select the device you want to use as a destination (**Figure 45**).

   ▸ Your device is shown at the top with a volume 🔊 icon.

- Bluetooth-capable audio devices are shown with an audio Bluetooth 🔈ᛒ icon.
- Other audio-capable devices are shown with a stereo speaker ▯ icon.
- Video-capable devices are shown with a TV ▭ icon.

4. Tap Done.



AirPlay **Done**

🔊 iPhone ✓

▭ Apple TV

🔈ᛒ DR-BT101

▯ McGraw Yamaha

▯ New AirPort Express N

▯ Office Mini

With AirPlay Mirroring you can send everything on your iPhone's display to an Apple TV, wirelessly.

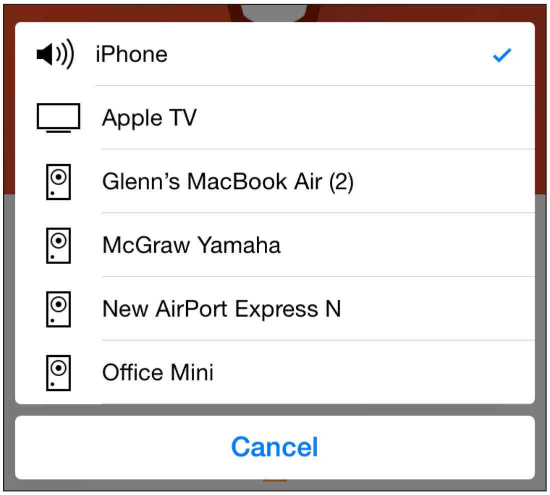
Figure 45: *Available AirPlay destinations are identified by type.*

Connecting with a Passcode or Password

An AirPlay device can be locked with either a four-digit passcode or a password.

- For code access, the device to which you're connecting will display the four digits, and those must be entered in the iOS device to connect.
- With a password, the destination device has a password set through whatever means (such as AirPort Utility with an AirPort Express), and then you enter that password in iOS.

Within individual apps, like the Overcast podcast player, you might have the option to select an AirPlay device as well. The same options appear, only in the form of a sheet with the option to select an item or tap Cancel (**Figure 46**).



iPhone ✓

Apple TV

Glenn’s MacBook Air (2)

McGraw Yamaha

New AirPort Express N

Office Mini

Figure 46: *The pop-up menu in an app shows Cancel rather than Done.*

Your iOS device retains media control, so you can use volume up/down buttons and onscreen controls such as pause and rewind.

With that out of the way, let’s look into uses of AirPlay.

Ways to Use AirPlay

The point of AirPlay is to shunt audio or video around your local network, and there are a number of ways this is useful. I walk through the most common or useful scenarios next:

- Send audio to an AirPort Express.
- Send audio or video to an Apple TV.
- Send audio to another computer or mobile using Airfoil, or receive it using Airfoil Touch.
- Mirror the display to a Mac using Reflector, a third-party app.

Tip: You can send AirPlay audio and video to any device that shows up in the list. For example, I have a Yamaha receiver with an AirPlay mode. On my local network, I select the Yamaha, which automatically turns on and selects its AirPlay mode for input. Unfortunately, you can’t turn it off via AirPlay; Yamaha offers a truly terrible iOS app that can be used, but I prefer to press the power button on the unit itself.

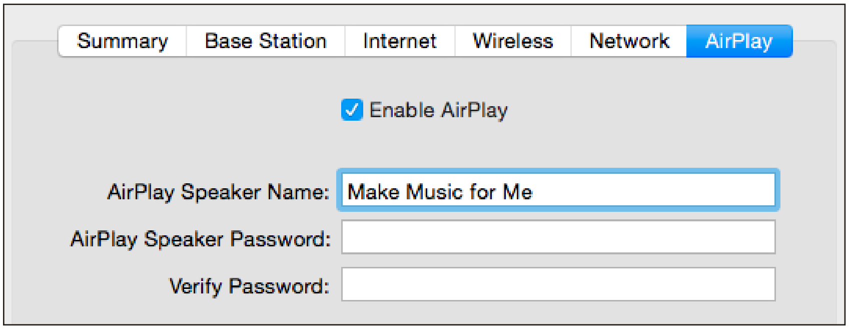
Configure AirPlay for an AirPort Express

Apple's own hardware lets you stream AirPlay. In fact, in its original form as AirTunes, it worked only with the AirPort Express. The AirPort Express oddly remains the only Wi-Fi base station with streaming audio support; the Apple TV offers both audio and video output.

An AirPort Express has a combined analog/digital audio port. You can use any standard 1/8-inch stereo plug, or a special digital fiber optic connection that has Toslink (an audio standard) on one end and a special compatible 1/8-inch plug on the other.

Setting up AirPlay is quite simple, and accomplished through AirPort Utility:

1. Launch AirPort Utility, either via iOS or in Applications/Utilities in OS X.
2. Select the AirPort Express base station. Enter the password if prompted.
3. Click the Edit button.
4. Navigate to AirPlay settings:
   - In OS X, click the AirPlay tab.
   - In iOS, tap the AirPlay item.
5. Turn on the Enable AirPlay checkbox (OS X) or switch (iOS).
6. Enter a name for the AirPort Express that will appear in AirPlay lists (**Figure 47**). You can optionally set a password, which must be entered twice identically. Click Done.
7. Click or tap Update in the Update Settings dialog that appears. The AirPort Express restarts with the new settings applied.



☑ Enable AirPlay

AirPlay Speaker Name: Make Music for Me

AirPlay Speaker Password:

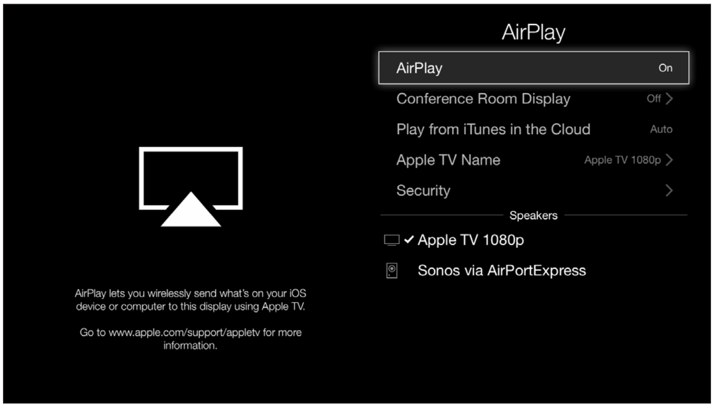
Verify Password:

Figure 47: *AirPort Utility in OS X allows AirPlay configuration for an AirPort Express.*

Configure an Apple TV for Audio and Video

Bring up your Apple TV's display on a TV set and use either its dedicated remote or the Remote app for iOS. Navigate to Settings and then select AirPlay (**Figure 48**). You can now:

- Select AirPlay to toggle it on or off.
- Select Apple TV Name to set the device's identifier in the AirPlay list used by other hardware and software on the network.
- Tap Security and set a password.



AirPlay

AirPlay On

Conference Room Display Off

Play from iTunes in the Cloud Auto

Apple TV Name Apple TV 1080p

Security

Speakers

✓ Apple TV 1080p

Sonos via AirPortExpress

AirPlay lets you wirelessly send what's on your iOS device or computer to this display using Apple TV.

Go to www.apple.com/support/appletv for more information.

Figure 48: *Apple TV lets you set AirPlay's name and whether security is active.*

Send Audio with Airfoil

Rogue Amoeba makes **Airfoil**, a remarkably straightforward software package for Mac OS X and Windows that lets you send audio from a computer to elsewhere. Airfoil lets you pick a piece of software as its input and one or more destinations to stream audio, and set the individual volume levels for each (**Figure 49**).

But Rogue Amoeba also offers complementary and complimentary (free) software that lets you use iOS more effectively.

First is **Airfoil Speakers**, available for Mac OS X and Windows. It turns a computer or Android mobile device into an AirPlay destination, so you can stream audio from an iOS device or a Mac. Systems running Airfoil Speakers appear in the AirPlay list in iOS.

Second is Airfoil Touch for iOS (free), which acts as a remote control for Airfoil for Mac or Windows, and lets you stream audio using a proprietary protocol from Airfoil to your iOS device.

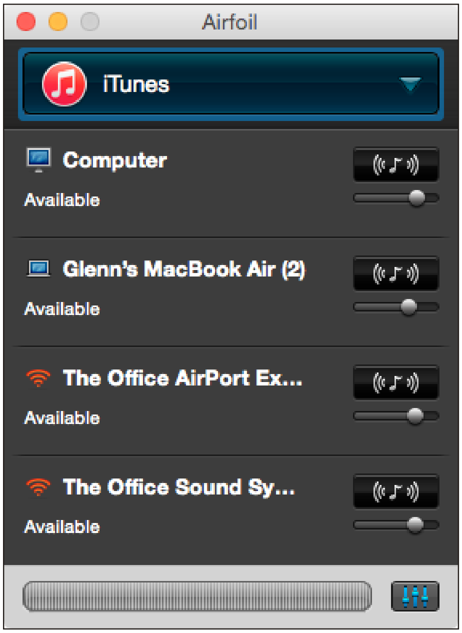


Figure 49: *Airfoil lets you stream audio from any app or the system to one or more AirPlay or proprietary Airfoil destinations.*

Note: Airfoil can stream to any AirPlay device, including Airfoil Speakers for Mac OS X and Windows. It can also stream to Airfoil Touch for iOS and Airfoil Speakers for Android and Linux, which use its proprietary standard and don't appear as AirPlay devices.

Mirror an iOS Screen

AirPlay is often used for audio or to push video playback to another device. But it can also be used to stream your active iOS display, whatever you're doing it with it, to a computer or other system.

Reflector from AirSquirrels ($14.99) acts as an AirPlay video target. Select it as a destination in your iOS AirPlay menu, and the iOS display—minus any indication of taps—appears in a window on your Mac. You can set passcode or password access.

Being able to stream your full iOS experience is useful for demonstrations and for recording movies of what you're doing to show other people later.

Tip: You can also record or show your iOS 8 screen in Yosemite using QuickTime Player without invoking AirPlay. With an iOS device connected to your computer via USB, launch QuickTime Player and then select File > New Screen Recording. From the wee tiny downward-facing arrow, select the iOS device. The window now shows an active preview of your mobile device, and you can then click the big red button to record. This feature also works inside **ScreenFlow** ($99), a screencast capture and edit program, to let you bring in iOS "video" directly.

SECURITY

Security encompasses many forms: How do you deal with a device being stolen? How do you protect its contents when it's out of your control? How do you prevent people from snooping on your network sessions? In this half of the book, you'll get answers that will make you feel better when using a device in all situations.

Connect to a Secure Wi-Fi Network

Most home networks are now secured, and nearly all businesses networks employ some way of keeping outsiders out. Connecting to these secured networks is often as easy as entering a password, but not always. This chapter helps you handle any difficult security situations that you might encounter.

Also, if you're setting up Wi-Fi security for a network, this chapter discusses what sort of security to set up and how users with iOS devices will connect to it.

Wi-Fi security divides into three main types: methods used for small networks, methods for large ones, and outdated methods that still exist but that you should avoid.

Note: Cellular networks have their own security methods, which are partly based on the Subscriber Identity Module (SIM) for GSM networks and on a unique set of identifiers for CDMA networks.

WARNING! *Public hotspots, whether free or fee, typically have no security; if they do, it's a shared password that provides no protection from other people on the network. When you connect, I recommend using only secured services or a virtual private network (VPN) connection. Read* ***Transfer Data Securely*** *for details.*

Connect to a Small Network

Nearly all home and small-office networks that have wireless security enabled require the entry of a short password or passphrase. Enter the password when prompted, tap Join, and, if entered correctly, you're done.

The password is stored for the next time you're near the same network, and it's automatically supplied by iOS 8. If you don't want to join the network automatically the next time you're nearby, or don't want to store the password on your device, launch Settings, tap Wi-Fi, tap the info ⓘ button next to the network, and tap Forget This Network. (This only works while you're connected to the network, however.)

If you have **iCloud Keychain** enabled, entering a Wi-Fi network password into any synchronized device means that you won't have to enter it again. Thus, you might connect to a network via iOS that you've already connected to in OS X and not be prompted, and vice versa. (iCloud Keychain requires iOS 7.0.3 or later or Mac OS X 10.9 Mavericks or later.)

What's Behind Simple Wireless Security

The latest and best security method for connecting to a Wi-Fi network in a home or office is Wi-Fi Protected Access 2 (WPA2). Nearly all computer hardware with Wi-Fi sold starting in 2003 supports WPA2, including the iPad, iPhone, and iPod touch.

> ***Et 2?*** *The original WPA (no number) was a backward-compatible, temporary solution that you may still see in use with older networks or when networks weren't upgraded. All Apple hardware sold since 2003 can use WPA2, and the same is true for that made by almost every other company.*

WPA2 comes in two forms: personal and enterprise. (I talk about enterprise just after this section.) The personal part refers to protecting the network with a password—sometimes called a passphrase since it can comprise multiple words. It can be up to 63 characters long and include punctuation, letters, and numbers. The passphrase is run through mathematical churns to produce something stronger.

A base station's administrator sets the passphrase and then provides it to anyone who needs to connect to the network. If you've set up the network yourself, you're the person who picks the passphrase.

Security on a Base Station

If you're setting up a base station, pick a good passphrase. The best WPA2 passphrases are at least 12 characters long; 20 is better. Choosing something memorable (like a song lyric) is fine so long as you insert a random character like `#` or `!` as well.

By the way, using a short password and obscuring it through substitution—plugging in an `@` for `a` or a `0` for an `o`—isn't effective. Crackers who try to break passwords try all common swaps as well as the real letters.

You should consider enabling only WPA2, even if there's a choice for mixed old-style WPA and new WPA2 encryption, unless some hardware that needs to use the network is too old for WPA2, such as a pre-2003 Apple iBook.

Connect to a Corporate or Academic Network

There are stronger ways to secure a network, and if you use an iOS device in corporate or academic settings, you will likely encounter WPA2 Enterprise. This flavor puts up a wall that lets you interact only in a limited fashion with the network to provide login details before your device is granted full access to the network and, typically, the Internet beyond.

Note: WPA2 Enterprise is an instance of "802.1X port-based authentication," which can be used with Ethernet and older Wi-Fi standards, too. It's a mouthful! But it's a mainstay of corporate network security.

WPA2 Enterprise networks are most frequently secured by a username and a password. However, a digital certificate (described below) can also be used for login. iOS supports these and other types of WPA2 Enterprise. Let's look at each option in more detail.

Username and password login

In the simplest setup, you must enter a username and a password provided by the network administrator or IT department to connect your device to a WPA2 Enterprise network. Often, these are the same credentials you use for file service, email, and other network resource access, such as your email mailbox name (the part to the left of the @) or full address (`user@domain.com`) for that network.

To connect to a WPA2 Enterprise network of this sort, select the network, enter your username and password, and tap Join. It's that easy. If you get an error, check your entries. If they are correct, then contact network support: you won't be able to troubleshoot this any further, because there are no settings to tweak in iOS.

WARNING! *Some networks may have policies that limit these sorts of logins to specific days and times, among other parameters. That's rare outside of high-security corporate networks, though.*

Certificate-based login

Some networks rely on digital certificates to handle logins. A digital certificate combines an encryption key with information that helps to validate the identity and integrity of that key. That is, the certificate lets a system make sure that the key hasn't been tampered with, and that it was created by the party that the certificate says created it. Digital certificates are used to provide a verified identity for server software, like a mail server, or for an individual.

In the case of WPA2 Enterprise, a certificate is used as an alternative to a username and login because the certificate can't be written down on a sticky note or extracted in some fashion.

Typically, an IT worker creates and provides you with a certificate and installs it for you. However, an iOS device can receive a certificate via email, and install it when you tap it as an attachment.

Outdated Methods

Wired Equivalent Privacy (WEP) was the first Wi-Fi security method, born in the same standard that unleashed Wi-Fi on the world (as 802.11b in 1999). But the standard had severe security compromises that were exploited by white hats (researchers who try to find flaws to fix them) and black hats (thieves, villains, and exploiters) alike.

As a result, since 2003, WEP hasn't been a reliable way to secure a network. It's useful as a flag that the network isn't meant for access by outsiders—breaking a WEP key to gain network access has been used as the basis of successful criminal prosecution in some places.

Apple has slowly phased out the ability to use WEP from iOS, in OS X, and in its base stations. It's unlikely you'd only be able to connect to a base station via WEP, although iOS devices can technically work with WEP.

Some base stations can be configured to accept a mixture of WEP and WPA (original flavor), but it's mostly disappeared.

Plain WPA (not WPA2) replaced WEP, allowing hardware made as long ago as 1999 to upgrade one step, and some base stations are configured to handle older WPA and newer WPA2 at the same time.

Viewing an Apple Base Station's Stored Passwords

If you've configured an Apple base station and can't recall or find the wireless password you set up, Apple's AirPort Utility software can reveal these in plain text so long as you have the administrative password that allows configuring the base station.

In iOS

1. Launch AirPort Utility. (It's a free app, if you don't already have it installed.)
2. Tap the base station in the graphical view.
3. If this is the first time you've used the app, or you opted on a previous use to not save the password and it's been a few minutes since the last

time you entered it, the Enter Password link appears. Tap it, enter the password, and then tap OK.

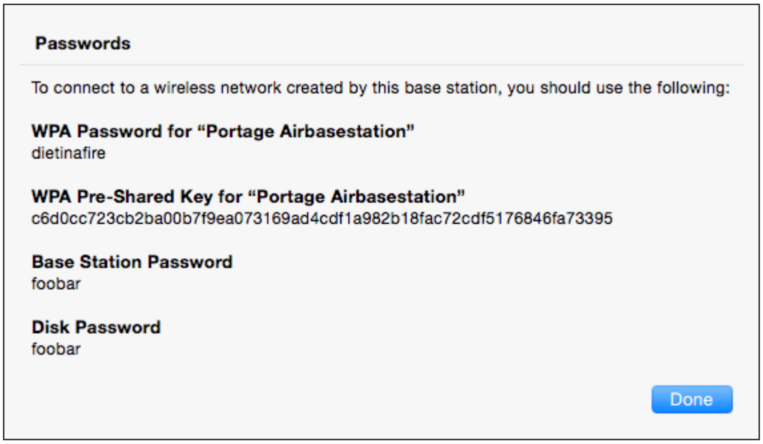
4. Tap the Edit button and then go to Advanced > Show Passwords. The Show Passwords view displays the network password at top and then the base station password (which you had to know to get this far).

> **Note:** If you tap the network password, the WPA Pre-Shared Key is revealed. Wait... the what?. It's the full underlying hexadecimal encryption key that your passphrase is converted into. I've never, ever had to enter this 64-character string into anything, but there's always a first time.

In Mac OS X

1. Launch AirPort Utility (found in Applications/Utilities).
2. Select your base station and click Edit.

   An edit dialog appears in the main window.
3. From the Base Station menu, choose Show Passwords.
4. From the dialog that appears, write down or copy the text for the WPA Password (**Figure 50**).



Passwords

To connect to a wireless network created by this base station, you should use the following:

WPA Password for "Portage Airbasestation"
dietinafire

WPA Pre-Shared Key for "Portage Airbasestation"
c6d0cc723cb2ba00b7f9ea073169ad4cdf1a982b18fac72cdf5176846fa73395

Base Station Password
foobar

Disk Password
foobar

Figure 50: *The Equivalent Network Passwords dialog gives you the hex key value of a text network key.*

Now that you have the password, you can enter it on your iOS device in order to join the Wi-Fi network. Email or text the password to your iOS devices so you can copy it and then paste it instead of retyping it.

Use Two-Step Verification

Apple's two-step verification for iCloud lets you secure your account with a password plus something extra that you have under your control. In this chapter, you learn how to set up two-step verification, how to secure your extra pieces against discovery or loss, and how to reset an account.

Dancing a Two Step

Apple lets you tie in an Apple ID for several purposes in iOS: for iCloud synchronization, iCloud Drive, iTunes purchases, iMessage, and more. However, without making an extra effort, an Apple ID is protected only by the password you set, and can be reset and potentially hijacked in a number of ways should someone gain access to your email or know your security questions for resetting a password.

The way around this is to use what Apple calls two-step verification, also known generically as two-factor authentication (2FA for short). A factor is a bit of proof that you are who you say you are. Requiring two factors of different sorts makes it more likely that you're the legitimate owner of an account or have authorized access for a service.

A two-factor system generally employs something you know, such as a memorized password, coupled with something you have or possess physically—such as a phone, a smartcard, or other hardware—or something you are, like a fingerprint or personal characteristic. Usually there's an emergency backup, too: a one-time-use code or set of codes that can be used in a pinch.

In Apple's implementation, when you enable two-step verification, you keep your existing password on your Apple ID, and add a phone number that can receive SMS (text) messages, and one or more trusted iOS devices. It also generates a 14-character Recovery Key that you must keep secret and secure.

> ***WARNING!*** *Once two-step verification is enabled you must have two of three elements to access your account: the password, a trusted or SMS device, and the Recovery Key. If you lose or lose access to two of those three things, your account is unrecoverable forever. You have to create a new Apple ID, and you lose access to purchases, unsynced items, backups, and the like.*

Turn On Two-Step Verification

To enable this two-factor setup on your account, you start at the My Apple ID site (**https://appleid.apple.com/**).

1. Click Manage Your Apple ID.
2. Enter your Apple ID and password.
3. Click Password and Security from the list at left.
4. In the Two-Step Verification section, click Get Started.

> ***Wait for up to three days:*** *At this stage, Apple may choose to have you wait up to three days, especially if a password or other element of your account was changed. They will send you an email telling you to wait, and then another email telling you that you can proceed. Return to Step 1 and continue through below.*

5. Answer the security questions presented to you. These will be questions you set up at some point in the past for your account.
6. Read through the three screens that explain how two-step verification works.
7. Click Get Started.

8. Set up an SMS device. Apple requires at least one SMS-receiving phone number per two-factor account, and that number may only be used once across all Apple IDs.

    a. Enter the SMS phone number.

    b. On the receiving device, you receive a text with a four-digit code.

    c. Enter the code on Apple's site.

9. Set up trusted devices, which are iOS devices associated with this account (and only this account).

    a. Select a device and click Verify.

    b. On the device, you receive a code. (You have to unlock the device to view the code, if it's locked.)

    c. Enter the code on Apple's site.

10. Click Continue.

11. Apple generates your Recovery Key. Print this out and keep it somewhere secure that you can find later. In fact, you may want to keep copies in multiple secure places.

    Note: I store mine in a password vault protected with a strong, unique password as an extra backup stage. No one with access to my computer can decrypt the vault without its password, which makes it both less risky (I have access everywhere) and more risky (someone could conceivably figure out my password).

    WARNING! *If you lose this Recovery Key you're sunk if someone attempts to hijack your account and Apple performs a security lock. When a security lock is in place, your password is deleted, and the account can only be unlocked and a new password set with the Recovery Key and a trusted device.*

    Because a Recovery Key is useless without a password, it's relatively safe to store and duplicate it as long as your password and your trusted devices are secure.

12. Re-enter the Recovery Key to confirm you have it.

13. Check the box that acknowledges you know what you're getting yourself into, and click Enable Two-Step Verification.

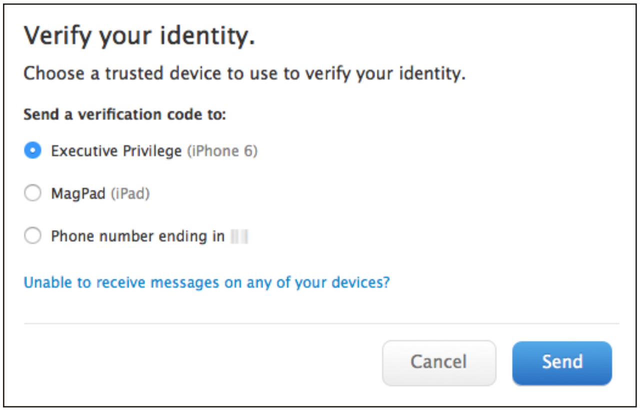
14. Click Done.

Log In with Two-Step Verification

Two-step verification presents itself in different ways in different places. In practice, it typically manifests itself as entering a password and then being asked which trusted device you want to receive the confirmation code.

Let's walk through logging in to the Apple ID site, as that uses all the pieces and allows direct recovery if you've lost one.

1. Go to the My Apple ID site (https://appleid.apple.com/).
2. Click Manage Your Apple ID.
3. Enter your Apple ID and password.
4. The site queries which trusted devices you want to use to receive your one-time-use login verification (**Figure 51**). Select it, then click Send.



Verify your identity.

Choose a trusted device to use to verify your identity.

Send a verification code to:

● Executive Privilege (iPhone 6)

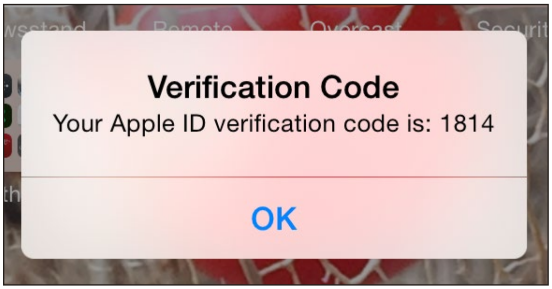
○ MagPad (iPad)

○ Phone number ending in [redacted]

Unable to receive messages on any of your devices?

Figure 51: *Pick a trusted device. The phone number's last two digits are obscured here.*

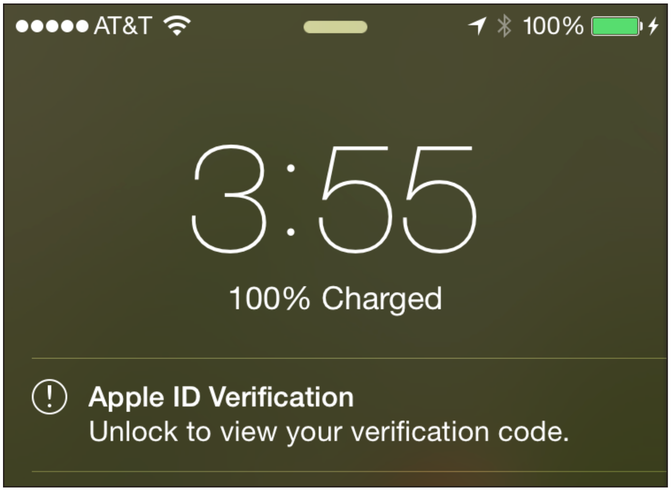
5. On your trusted device, you'll receive the four-digit code in one of two ways, depending on whether it's an iOS device (named in the Verify Your Identity list) with Find My iPhone active, or an SMS device (shown as Phone Number Ending In):
   - An alert message with the code (**Figure 52**). If your device is locked, the code isn't shown on a lock screen; you have to unlock the device to see the code (**Figure 53**).
   - An SMS message with the code.



Verification Code

Your Apple ID verification code is: 1814

Figure 52: *The code appears as a modal notification that is delivered via Find My iPhone.*



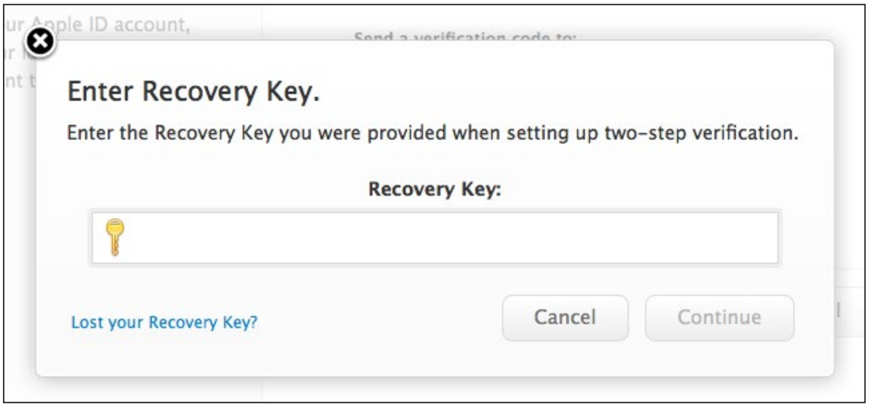
Apple ID Verification

Unlock to view your verification code.

Figure 53: *An iOS device has to be unlocked to display a verification code.*

Note: If you click Unable to Receive Messages on Any of Your Devices, you're prompted to enter your Recovery Key (**Figure 54**). Entering the key correctly then lets you link new trusted devices.

WARNING! *SMS Forwarding is a feature that appeared in iOS 8.1 and Yosemite as part of Continuity (https://support.apple.com/en-us/HT6337). This feature can allow security codes from Apple (and others) sent via SMS to be received on your Mac. If you have any concern about someone with access to your Mac when you're not around being able to both gain control of your password and send and receive that code, disable SMS forwarding.*



Enter Recovery Key.

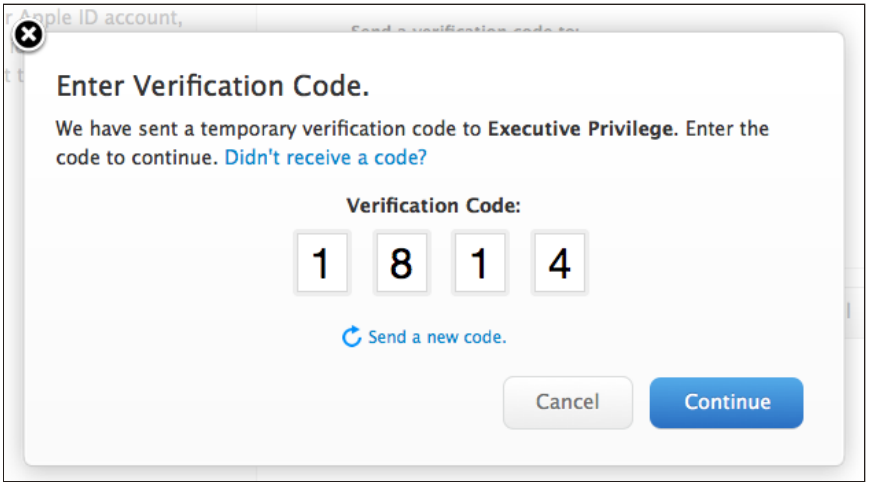
Enter the Recovery Key you were provided when setting up two-step verification.

Recovery Key:

Figure 54: *Entering the Recovery Key at this stage lets you link new trusted devices.*

WARNING! *An SMS code can be seen on the lock screen of an iOS device unless you've disabled notifications on the lock screen.*

6. Enter the code at the Web site and click Continue (**Figure 55**).



Enter Verification Code.

We have sent a temporary verification code to **Executive Privilege**. Enter the code to continue. Didn't receive a code?

Verification Code: 1 8 1 4

Figure 55: *Apple lets you enter the code. Clicking Send a New Code generates and transmits a new one.*

7. You're now logged in.

When you log in to iCloud (via the Web or other means), or purchase an item via iTunes, iBooks, or the App Store from a device that hasn't previously been used, you'll be prompted to validate your password-based login with a code sent to a trusted device.

Logins at Other Sites

Because calendaring (over CalDAV) and email can be used with non-Apple software, you can generate special app-specific passwords for discrete purposes via the Apple ID site.

After logging in to your Apple ID account:

1. Click Password & Security.
2. Click Generate an App-Specific Password.
3. In the dialog, enter the name of the service. Be specific so you can recall later what you assigned, like “BusyCal on home Mac mini.”
4. Click Generate.
5. Copy the password shown and paste it in or type it in to the program you want to use.

   If you ever want to revoke an app-specific password, return to Password & Security, click View Account History, and then click Revoke next to any password you want to abandon.

These app-specific passwords can’t be recovered. If you can’t recall one, just generate a new one and revoke the old one.

Recovering Account Factors

So you need two of three factors—how do you handle losing one? Here are the three scenarios for recovering a missing factor assuming you have two.

> ***WARNING!*** *As noted earlier, lose two of your three factors and you’re sunk forever. Apple secures your account information in such a way that it can’t recover it—for you, a government agent, or anyone.*

Lost Your Password

Visit the iForgot site (**https://iforgot.apple.com/**) and Apple will prompt you for your Apple ID, request your Recovery Key, and confirm via a trusted device. Then you can set a new password.

Lost One, but Not All, of Your Trusted Devices

You can manage your trusted devices through the Apple ID site, including removing devices after you've sold them or they're lost or stolen.

After logging in to your Apple ID account:

1. Click Password & Security.
2. Click Add or Remove Trusted devices.
3. In the list that appears, you can add SMS devices and trusted iOS devices (**Figure 56**). You can't remove an SMS device before validating a new number.

> ***Recover by moving number to a new phone:*** *Because SMS is attached to a phone number and not a piece of hardware, you should be able to get your carrier to activate the number for you on another phone if yours is lost or stolen. This is the only slight way out (and slight security hole) for coping with a missing trusted device.*

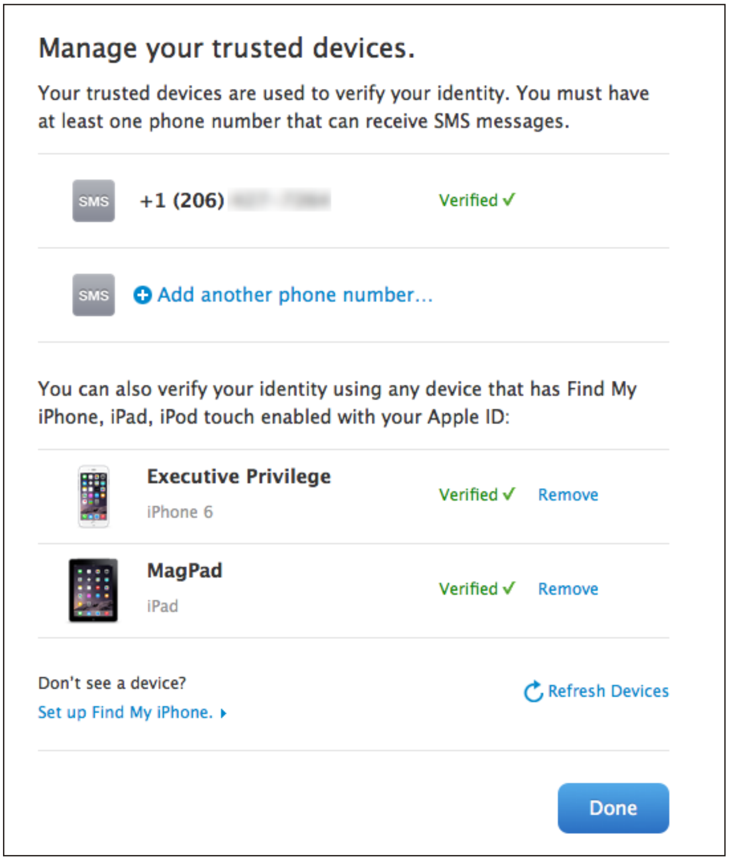
> ***WARNING!*** *I'd heavily suggest adding new devices before removing old ones to avoid being locked out of your account if something goes wrong before you've tested the new setup.*

Lost Your Recovery Key

The Recovery Key is easily reset through the Apple ID site.

After logging in to your Apple ID account:

1. Click Password & Security.
2. Click Replace Lost Key.



Manage your trusted devices.

Your trusted devices are used to verify your identity. You must have at least one phone number that can receive SMS messages.

SMS +1 (206) [redacted] Verified ✓

SMS Add another phone number…

You can also verify your identity using any device that has Find My iPhone, iPad, iPod touch enabled with your Apple ID:

Executive Privilege
iPhone 6
Verified ✓ Remove

MagPad
iPad
Verified ✓ Remove

Don't see a device?
Set up Find My iPhone. ▸

Refresh Devices

Done

Figure 56: *The Apple ID site maintains the list of trusted devices and lets you add and remove them.*

3. Click Next, and follow the remaining steps.

   Be sure, as with your original Recovery Key, to print it out and make sure you can find it should one of your other factors be lost or your account login be disabled for security purposes.

Transfer Data Securely

The data that travels to and from your iOS device isn't secure even when you're connected to a Wi-Fi network with a strong password. Any data you send that's not encrypted could be sniffed by anyone else on that network.

The same is true for any point between you and your data's destination or wherever you're running an active session, whether you're using a protected Wi-Fi network, an open one, or a cellular data connection: any party in between, for unencrypted services, can see exactly what you're doing.

But you can avoid this problem with secure services or a comprehensive solution called a virtual private network. I explain both in this chapter.

Why Encrypt?

When the previous edition of this book came out a few years ago, it was still necessary to explain the value of security and encryption. After dozens of corporate breaches, network attacks, and the disclosures of government snooping around the world (in democracies and dictatorships alike), the value is clear.

Encrypting our data in transit enables us to make decisions about how our data is being used and who sees it, preventing criminals, relatives, and government agencies from overstepping our rights.

Protect Particular Services

Nearly every kind of service you can think of offers an encrypted option, and, fortunately, most modern services employ some kind of encryption by default. Here's a laundry list of what you should consider:

- Always use SSL/TLS email connections. There’s no good reason not to employ SSL/TLS (Secure Sockets Layer/Transport Layer Security). If your mail host doesn’t provide secured email for your incoming email (POP or IMAP; almost always IMAP in iOS) and for your outgoing email (SMTP), find a new host. Without security, email programs may send passwords in the clear or with weak encryption, and likely send all data in the clear. iOS will always attempt to configure your mail settings securely.
- Secure access to Web sites. You can usually make a secure connection to a Web site.
  - Most Web sites, including social networks like Facebook and Twitter, have switched from using plain-text http connections to secured SSL/TLS or https connections. You log in securely (which is true on almost all sites), but then remain securely connected at all times.
  - If you’re not sure, look in the security settings for a Web site where it notes something like “Always use https” or “Always use secure connection” and check that box. (A login is almost always secure, so your account name and password is rarely at risk.)
  - For other Web sites, try to always use the secured flavor by typing in or bookmarking `https` instead of `http` as the start of the URL. Many sites offer SSL/TLS sessions as an option reachable just by entering the URL in this fashion.
- Transfer files securely. When making an FTP connection, use only a secured alternative to plain FTP, such as the SSH-based SFTP or one of several SSL/TLS-protected methods. FTP programs otherwise send passwords and data in the clear. **Transmit for iOS** is the app of choice for secure file transfer ($9.99).

  Tip: On a Mac, enable Remote Login and File Sharing in the Sharing preference pane to allow SFTP over a local network or via the remote Back to My Mac service.

  Note: Most services with iOS apps that transfer data, such as Dropbox, CrashPlan, Facebook, and Twitter, secure the connection using SSL/TLS or something better.

Umbrella Protection with a VPN

A virtual private network connection is a nifty way to prevent any sniffing of your local network hookup. A VPN encrypts all the data coming and going from a device, such as an iPad or iPhone, creating an encrypted tunnel that extends between the device and a VPN server somewhere else on the Internet, traversing with protection any local network and hubs as well as every node on the Internet between the two points.

For corporations, VPNs can extend the aegis of corporate security to remote devices. For individuals, that's less the case. With a company, the VPN server is within the corporate network and any data leaving that server is protected by company firewalls and intrusion prevention.

But if you're using a VPN just to protect your local link (the connection between your device and the hotspot), data remains encrypted only until it hits the VPN server, usually located in a data center. From that data center to its destination, data is unprotected (unless wrapped in an encrypted method, like SSL/TLS on the Web, describe earlier), but that's typically just fine. The main locus of risk is the local link.

And because major Internet sites—like Google, Apple, and the rest—have distributed sets of computers and even private links to big data centers, the hop from the VPN server to the destination network may be within the same building or close by.

Before you can set up a device, however, you need to find a VPN service.

Find a VPN Service and Install an App

Several firms offer "VPN for hire," letting you pay for a fixed period of time or a recurring subscription. The connection you make, as noted above, runs from your iOS device through the local Wi-Fi or cellular network, then goes through any intervening local area network routers and higher-level backbone routers, and finally winds up at one of the company's VPN servers located in a data center.

There are many such services to choose among, some of which offer apps and some of which require manual or partly manual configuration. I've had experience with two that I can recommend because:

- I've had personal experience with them, and tested them. (You can read a Macworld column of mine about how we trust companies.)
- They offer an app, which is the simplest way to configure and connect in iOS. (They both offer Mac OS X apps, too.)
- They let you subscribe using a single subscription that works across all your iOS devices or across iOS and Mac OS X hardware you own.
- Their software is elegant and works well.
- They offer a "transporter" option that lets you terminate in another country, which allows viewing media or accessing resources that otherwise require being physically present in that country.

> **Note:** I used to recommend VPN-for-hire services that typically required manual configuration. Now, I'd prefer to recommend app-based services, as they require less fuss without any greater cost.

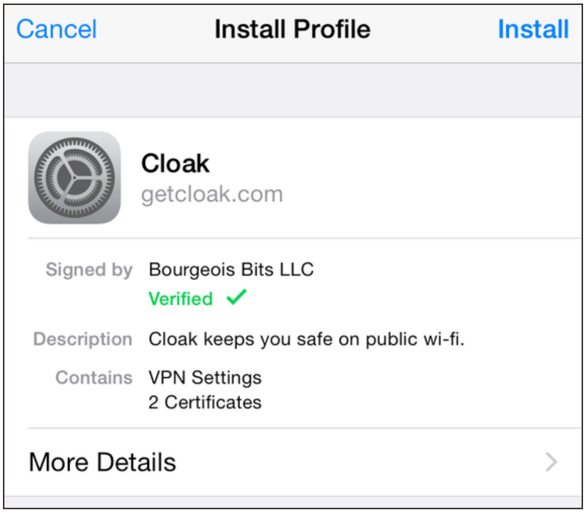
The two services are Cloak (**https://www.getcloak.com**) and TunnelBear (**https://www.tunnelbear.com**). Both support iOS 7 and 8 and Mac OS X 10.9 and 10.10. TunnelBear also supports OS X as far back as 10.6.8, as well as having Windows and Android clients.

The two services try to remove as much complexity as possible, which means eliminating manual configuration both in iOS and OS X. (OS X is simpler, because Apple doesn't restrict access to the network innards required to set things up.)

Set up a VPN app

To get set up in iOS, you download a service's free app. Neither service has a trial in iOS directly, so visit their Web sites to sign up for an account that can be used in the app. TunnelBear offers a 500 MB-per-month free usage tier, while Cloak has a 30-day free trial.

After installing the app, you have to accept an iOS profile that encapsulates all the VPN configuration details (**Figure 57**). This is nice because you don’t need to deal with the fiddly bits described in the manual setup section below. And if the profile needs to be updated because the service’s details change, they can push a fresh one through their update, rather than asking you to reconfigure by hand.



Cloak
getcloak.com

Signed by Bourgeois Bits LLC
Verified ✓

Description Cloak keeps you safe on public wi-fi.

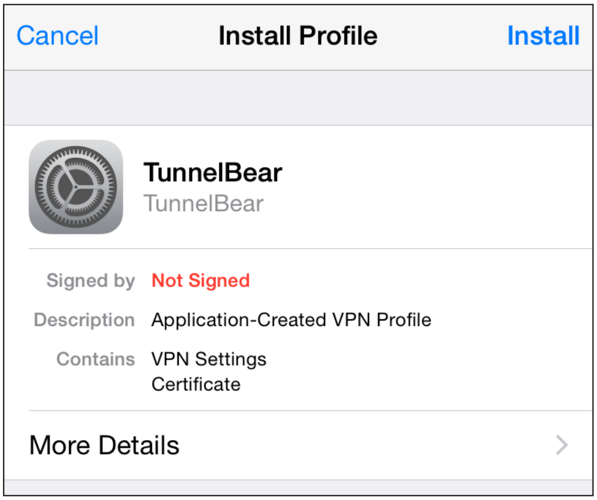
Contains VPN Settings
2 Certificates

Figure 57: *The VPN apps prompt you to install a profile, which includes all the configuration details for their services.*

To install a profile:

1. Launch the app, which will detect that no profile is available and request to install it (**Figure 58**). (In Cloak, there’s a round-trip via Safari to its Web site to generate an appropriately tailored profile.)
2. Enter your passcode when prompted.
3. Read the Warning screen that explains what the profile will be able to do, and then Tap Install.
4. Tap the red Install button.
5. Tap Done, and you’re returned to the app.

> **Tip:** If you ever have trouble connecting with the app, try deleting the profile from Settings > General > Profiles and then launching the app, which will walk you through the steps above again.



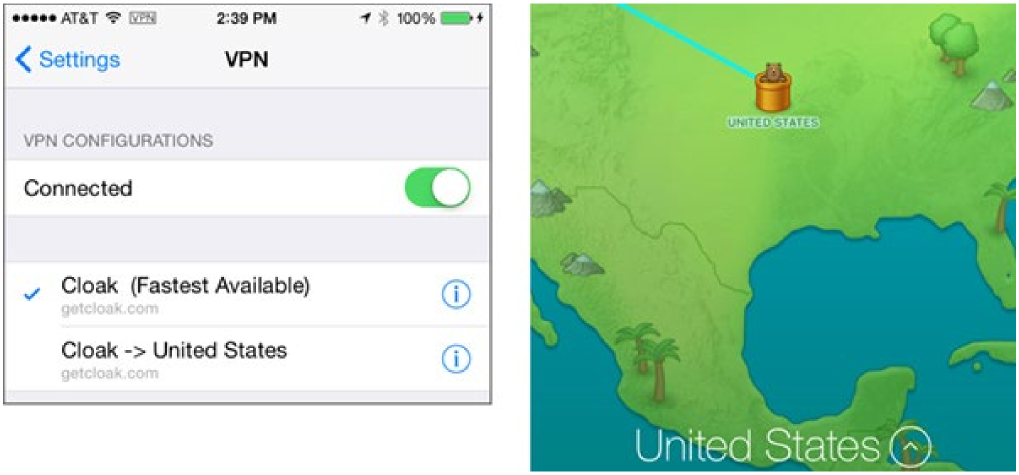
TunnelBear
TunnelBear

Signed by Not Signed
Description Application-Created VPN Profile
Contains VPN Settings
Certificate

Figure 58: *TunnelBear needs your permission to dig a den in your device.*

After installing a profile, you can use the Settings > VPN view to start or end a connection. A VPN label will appear in the status whenever the connection is active. You can find more information about these options in the next section, Make a VPN Connection.

TunnelBear also has an option to disable the connection in the app, which features bears (**Figure 59**).



VPN CONFIGURATIONS
Connected
✓ Cloak (Fastest Available)
getcloak.com
Cloak -> United States
getcloak.com

Figure 59: *Cloak uses the Settings > VPN section for connections (left). TunnelBear can be managed there, or via its app. Rowr.*

Both services can also initiate a VPN connection "on demand," too, when you reach out to the Internet (and both can disable it during idle times). Opt in via either app's configuration options.

Cloak also lets you pick trusted Wi-Fi networks to bypass enabling a VPN, and opt to automatically connect on all others.

> **Note:** Whenever you make changes to Cloak's settings, it will note in the app that "settings are out of sync." Tap that message, then tap Sync Settings Now. Cloak connects via Safari to produce a newly updated profile, which you're prompted to install.

Country-hopping with a VPN

There's one more trick up the sleeve of VPNs: they can let you seem to be accessing a service from a country other than the one that you currently occupy. This is useful to evade certain per-country licensing limitations on free and subscription online streaming and other services (**Figure 60**). For instance, BBC iPlayer only works in the United Kingdom.

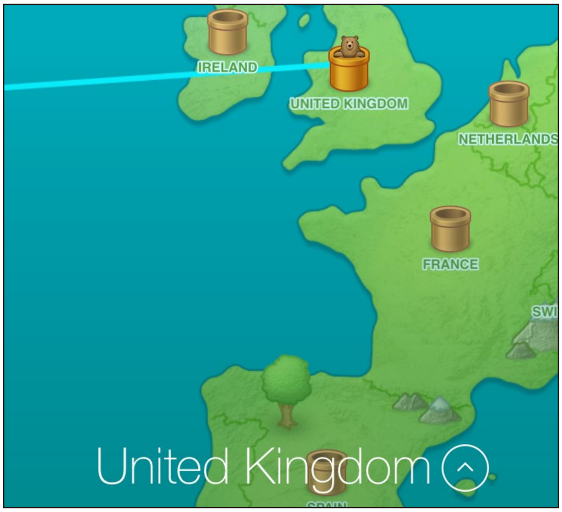


Figure 60: *The bear says, "what ho, guv'ner."*

Simply select a destination country in TunnelBear or Cloak, and when you connect, your VPN connects to a server at a data center in one of those lands. This can substantially slow down your throughput, because traffic has a longer topographical path from you to another country to the service in question and back. It can also bypass content-distribution networks (CDNs), which push media to you with the fewest possible Internet hops.

The ethics of such workarounds can be problematic. In the case of the BBC, the “Beeb” is paid for by both government funds and a television license, which every home with a TV set is required by law to pay. Using a VPN to “watch” remotely is taking a service that you’re not paying for. Many BBC programs are carried by foreign services, such as BBC America, that pay licensing or other fees, and many of its programs can also be purchased on DVD or as digital downloads. (For me, I sometimes watch Doctor Who via VPN, but I always purchase a season pass in the U.S. version of iTunes later so that the fees are paid appropriately.)

Netflix and other services that you can pay for, but are limited to the U.S. or a few countries, are another matter. They rely on licensing agreements that restrict access. However, Netflix alone reportedly has many millions of customers outside its service area who use a U.S. registered credit card and VPN access.

Eventually, all national licensing barriers will have to fall because of such absurdities, but consult your internal ethical compass.

Pricing options for VPN apps

Every VPN service is paying not just for servers and the overhead of staff and the like, but for the bandwidth you consume as well: every gigabyte you send through a VPN is one gigabyte inbound (which is often cheap or free) and one gigabyte outbound (about 5 to 10 cents per GB). Some users will consume 50 GB a month; others a trickle.

As a result, plans may seem expensive, but they’re typically priced very reasonably relative to both the value and the hard costs the company has to pay to keep its software and security up to date.

The deciding factor between these two services might be your particular number of devices, data usage, and interest in—or fear of—bears.

Cloak

Cloak sells time-limited passes as iOS in-app purchases, and passes and recurring subscriptions from its Web site. Every account may be used with an unlimited number of devices by a single person across iOS and Mac OS X.

The fees range from $3.99 for a week to $99.99 per year for non-recurring passes, all with unlimited data. A monthly subscription costs $2.99 with 5 GB of data included; unlimited monthly and yearly plans are $9.99 and $99.99, respectively.

TunnelBear

TunnelBear has a slightly different approach. In iOS, you can purchase non-recurring passes that work only in iOS, not across platforms, for from $2.99 (one month) to $29.99 (one year) with unlimited data.

Via the Web site, you can sign up for a free plan that includes 500 MB per month, or for unlimited data across up to three devices for $4.99 per month (recurring) or $49.99 per year (either recurring or for a single year).

Configure a VPN Manually

There are several kinds of VPN protocols, and iOS 8 supports the most popular: L2TP/IPsec (listed as L2TP), PPTP, and Cisco IPsec (listed as IPsec). The first two are generic, widely used standards. The last is a Cisco VPN flavor proprietary to its systems. (Apple, like many companies, spells IPsec with a capital S, even though that's the wrong capitalization.)

Note: Two VPN types that use SSL/TLS, one by Cisco and one by Juniper, are also available (**https://support.apple.com/en-us/HT201533**). However, to use either of these types, you must have your devices managed by an IT administrator who uses software from Apple called Apple Configurator.

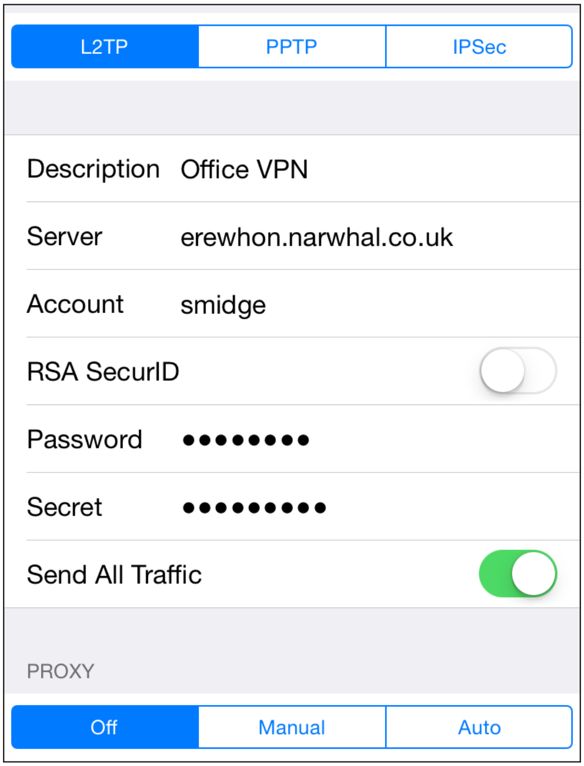
Almost any server operating system that offers VPN software at all can support one of these protocols, including Mac OS X Server and Microsoft Windows Server.

Set up a VPN profile

Start by making sure you have all the server settings provided by your VPN host or network administrator at hand, since you'll need to enter several pieces of data.

To set up a VPN profile, follow these steps:

1. Launch the Settings app, and tap General > VPN. (If you've configured a VPN before, it may show up in the top level of Settings.)
2. Tap Add VPN Configuration. The Add Configuration view appears (**Figure 61**).



[✓ L2TP] PPTP IPSec

Description Office VPN

Server erewhon.narwhal.co.uk

Account smidge

RSA SecurID ○

Password ●●●●●●●●●

Secret ●●●●●●●●●●

Send All Traffic ●

PROXY

[✓ Off] Manual Auto

Figure 61: *Enter the details provided by a for-hire service or a network administrator.*

3. In the Add Configuration view, fill in the settings:
    - Pick L2TP, PPTP, or IPsec, as appropriate. The choice here affects which options appear below the header.
    - The description appears in the VPN view after you create the configuration; enter something short and expository.
    - Server, Account, and Password tells iOS which Internet host to connect to using which credentials.
    - RSA SecurID (L2TP and PPTP) should always be off unless your employer provided you with a physical key fob.
    - Secret (L2TP and IPsec) is a shared bit of text that's used as an extra level of security.
    - Use Certificate (IPsec only) is enabled when you have a stored certificate to validate your identity.
    - Group Name (IPsec only) is set if a network administrator provides a group.
    - Encryption Level (PPTP only) is typically left set to Auto.
    - Send All Traffic (L2TP and PPTP) is typically left on. If it is off, you can filter which traffic is not encrypted and which is.
    - A Proxy option can be ignored unless you've been told otherwise.
4. Tap Save.

    You now have a configuration profile that you can use.

Make a VPN Connection

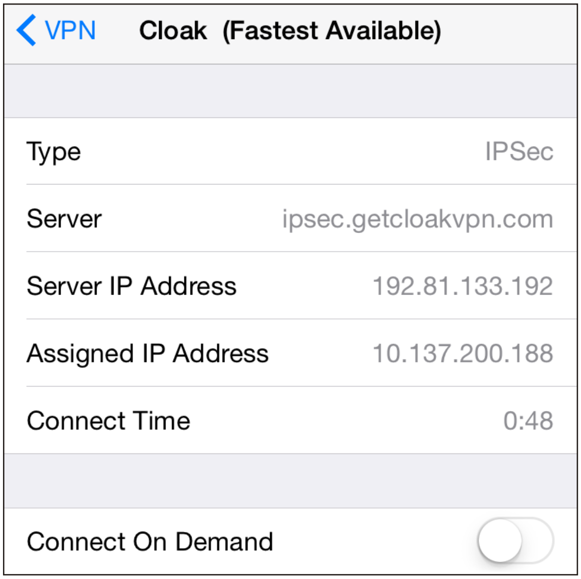
In the Settings app, in the VPN (top level) or General > VPN view, set VPN to On, and iOS will connect using the profile; if there's more than one VPN profile, the one that's used will have a checkmark next to it. (In some cases, you may see VPN Configurations and Personal VPN as separate lists, each of which will have a separate switch for enabling and disabling.) Corporate-style VPN apps will also let you enable the connection in the app.

You can tell that a VPN connection is active in two ways:

- A VPN indicator appears in the status bar.
- A Status entry appears in the Settings app's main view that reads Connected.

> ***WARNING!*** *VPNs are typically disrupted when you move between networks. If this happens to you, flip the VPN switch to Off and back to On to reset the connection.*

To check the status of your VPN connection, tap the info ⓘ button to the right of the currently active VPN configuration profile in Settings > VPN (**Figure 62**). The Server IP Address field provides a clue to the facility at which your VPN terminates. You can also switch on or off Connect On Demand in this view.



Cloak (Fastest Available)

Type	IPSec
Server	ipsec.getcloakvpn.com
Server IP Address	192.81.133.192
Assigned IP Address	10.137.200.188
Connect Time	0:48
Connect On Demand	○

Figure 62: *Connection details reveal a little more information about where the VPN terminates.*

You can cancel a VPN connection in process (before the connection is completed) by tapping the Cancel VPN Connection button that appears in the VPN view. To disable a VPN connection, set VPN to Off at the top of the main view in Settings, or in General > VPN; or use the app, when that's an option.

Protect Your Device

Now that you know how to keep your data from being intercepted in transit, how can you prevent your stored data—on an iOS device—from being rifled if your device is out of your control?

Apple has two robust ways to secure a device: with a passcode and, for newer hardware, with a fingerprint-recognition system called Touch ID.

All devices that support iOS 8 include robust hardware encryption. When a device is on and locked, its data is inaccessible until a passcode is entered or Touch ID accepted, which unlocks the encryption keys needed to read stored information.

WARNING: *If you lose the passcode and Touch ID isn't available (such as after a reboot), your data is lost forever.*

Set a Passcode

Your best single protection against anyone unauthorized having access to data is enabling the passcode lock. This allows you to set a four-digit code required to wake and gain access to the device.

To set the passcode lock, follow these steps:

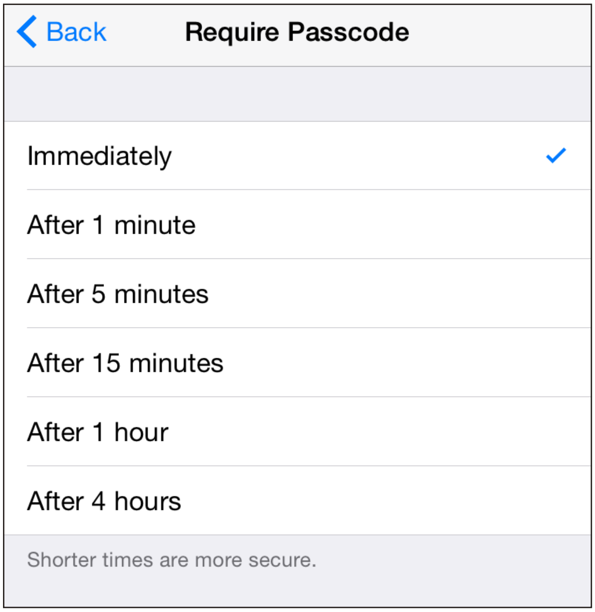
1. In Settings, tap General > Passcode. On Touch ID-equipped devices, the option reads Touch ID & Passcode.
2. Tap Turn Passcode On.
3. Enter a four-digit passcode, and re-enter it when prompted.

You can also enable the passcode lock remotely if you have an active iCloud account and Find My iPhone enabled on the device. See **When Your Device Goes Missing**, ahead.

> **Tip:** Is four digits not good enough for you? Turn off Simple Passcode. Then you can enter anything you can tap on the full iOS keyboard. If you use Touch ID, you may need to enter your passcode so seldom that you could create a long entry, which reduces the potential that someone could, through brute force, recover your passcode.

The Passcode Lock screen offers a few additional security options (**Figure 63**). You can set the time after which you must enter a passcode at intervals from Immediately to After 4 Hours:

- Immediately means you're asked for the passcode any time the device wakes up. You can put your handheld to sleep manually, of course, by pressing the Sleep/Wake switch, but you can also set it to sleep automatically, with the Settings > General > Auto-Lock.
- Longer intervals let the device be unlocked without a passcode for up to the time duration you've chosen from the list.



Require Passcode

Immediately ✓

After 1 minute

After 5 minutes

After 15 minutes

After 1 hour

After 4 hours

Shorter times are more secure.

Figure 63: *Choose the duration between when you're asked again for your passcode.*

You can also set which services are available when your device is locked in this view, which is a good way to prevent leakage of information, such as appointments, being able to present barcodes for scanning at stores or an airport, or using Messages to reply.

As a nuclear option, you can set your device to self-destruct—destroy its data, at least—if there are more than ten failed attempts to enter the passcode correctly by switching Erase Data to On. What do you lose? Only items created since the last backup and sync; see **Erase Device**.

Use Touch ID

Apple's Touch ID lets you turn to your fingertips to secure your device. Touch ID lets you train several later models of iPhone and iPad to recognize up to five fingerprints. It can be used not only to unlock your phone, but to use Apple Pay (on supported devices) and make iTunes/App store purchases as well.

Note: Your results may vary. With the iPhone 5s—the first device to offer Touch ID—iOS seemed to "forget" one of my thumbs after a while, but the other was fine. After an iOS 7 update, it got better. With an iPhone 6, I rarely have any trouble with recognition.

Tip: Touch ID in iOS 8 can be used to authenticate third-party software. 1Password and Authy are two apps I use that allow Touch ID for unlocking.

You select which of the Touch ID associations you want in Settings > Touch ID & Passcode, and then tap Add a Fingerprint. iOS guides you through enrolling a fingerprint. When it's finished, it names the entry Finger plus a number. As this isn't descriptive, tap that entry, then name it with something you remember. In that way, if iOS "forgets" your fingerprint, you can delete the appropriate entry and retrain it.

Touch ID allows fingers from different people, which is convenient, as you and others could all use Touch ID to unlock the same phone or tablet, or you could enroll a partner's fingerprint as an emergency fallback if they need to access your device.

Even with Touch ID enabled for all tasks, you will still be prompted to enter the passcode in a number of circumstances:

- After your iOS device has been powered up or restarted.
- If you haven't unlocked your device in more than 48 hours.
- Once five unsuccessful attempts have been made to unlock your phone or tablet via Touch ID.
- If you've put the device into Lost Mode via Find My iPhone.

Note: Matthew Green, a well-known security researcher, **tweeted this cautionary tale** in November 2014: "I woke this morning to find my 7 y/o levering my finger onto the TouchID sensor of my phone. Maybe time to go back to passwords."

When using Touch ID, it's important to remember that while it increases the relative security of your data while improving the speed and simplicity of use, you also open yourself up to your device being unlocked via coercion. If someone—a government agent, criminal, abusive spouse, or other party—can force your finger onto the sensor, they can gain access to at least some of your information.

When Your Device Goes Missing

Your mobile device is a desirable item for thieves. It's compact, it has a high retained value, and there's a huge market for used models.

Without freaking you out about theft, I want to tell you how you can protect your data when your device has disappeared, make it impossible for a thief to use your device, and find your device if it's stolen or lost.

Find My iPhone (and Other Devices)

Find My iPhone, introduced by Apple in 2009, has a name that belies its utility: it works with every kind of iOS device and, starting with Mac OS X 10.7 Lion, with Macs, too (as Find My Mac in the iCloud preference pane).

You can find the last reported position of any iPod touch, iPhone, iPad, or Mac by enabling the feature, which requires an iCloud account. You can also play a sound on the device, lock the device with a new four-digit passcode while displaying a message, or delete all its data!

Finding a device's current location and taking a remote action can be accomplished via the iCloud Web site or the free **Find My iPhone** app.

> ***One name for clarity:*** *For simplicity's sake in the text ahead, I'm calling the service Find My iPhone.*

With Family Sharing turned on, anyone in the family group can see where an iOS device is, unless the owner has disabled letting that person or anyone see his or her current location. With that user's password, all Find My iPhone features are available through other Family Sharing members' accounts.

Note: There are third-party tools available in iOS that track an iOS device, too, using the background location tracking feature added a few iOS versions ago. Most involve a subscription fee. The advantage to these apps is that some can be set to take photos of whoever has your device. However, none offers the fully baked-in locking, tracking, erasure, and other options of Find My iPhone.

How It Works

The feature relies on a device sending Apple's servers a regular update of location information derived from Wi-Fi, cellular, and GPS signals and data. All iOS devices and most Macs (provided they're running 10.7 Lion or later) use the built in Wi-Fi; iPhones and Wi-Fi + Cellular iPads add cellular radios and GPS.

With Find My iPhone active, a device with GPS and cellular regularly sends updates derived from its GPS receiver and from ranging information it has about nearby cell phone towers that allow it to trilaterate.

Note: You may be more familiar with the term *triangulation*, which relies on using known fixed positions and measuring angles. *Trilateration* uses the intersection of geometric areas, such as the radius of signal strength from cell towers.

All iOS (and OS X) devices also scan for nearby Wi-Fi networks and send a snapshot of that information to an online system run by Apple whenever the device has an Internet connection. This system approximates a position based on network details that it knows about from previous scans sent by other devices, including the name and some less-apparent unique hardware identifiers. The position is inferred based on the relative signal strength of the Wi-Fi base stations detected.

That lookup requires an active connection, which is fine for a cellular device with an active data plan that can use mobile broadband. But a Wi-Fi-only device must be connected to a Wi-Fi network to retrieve and send Wi-Fi–based position information, as well as to respond to queries from Apple's servers.

Note: Apple **caches some information** about location on the phone for up to 7 days to avoid frequent network access to look up information, or to use Wi-Fi positioning in an area you've been recently even if you don't have current Internet access.

Enable Find My iPhone

Find My iPhone requires an active Apple ID associated with iCloud. You likely set this up already when upgrading or setting up your iOS device or Mac.

To enable Find My iPhone on an iOS device, if you haven't logged in with an Apple ID account yet, go to Settings > iCloud and do so. Once you're logged in, that view shows the Find My iPhone switch, which you can set to On or Off.

WARNING: *Since iOS 7, Apple requires that you enter your iCloud password to disable Find My iPhone. This prevents a thief or other unauthorized party who has access to your unlocked phone from using it while also removing it from being tracked.*

Note: To enable Find My Mac, enable the Find My Mac checkbox in the iCloud system preference pane. If your Mac has Wi-Fi turned off with an active Internet connection (such as cabled Ethernet), it can still be contacted to perform actions, but it can't display a location.

View Your Device's Location

To view your device's location, you can choose between two similar tools: the Find My iPhone Web app on the iCloud site or the Find My iPhone app on an iOS device. Because the two options have nearly identical interfaces and features, you should use whichever one is easier for you to access.

Find My iPhone on the Web

To find your devices via a Web browser, follow these steps:

1. Go to https://icloud.com/find.
2. Log in with the correct Apple ID.

> ***Apple is smart about unattended machines:*** *iCloud.com allows you to stay logged in, but prevents unauthorized access to Find My iPhone by asking for a password even when you're already logged in to another part of the site. The Find My iPhone login times out after 15 minutes.*

In the Find My iPhone Web app, click the All Devices button at the upper center to reveal all your equipment (**Figure 64**). All Devices is the default selection, revealed in the map at whatever magnification level is required to show all the devices at once.

In the All Devices list, the dot beside each device name indicates the status: gray ● means trying to connect or offline, and green ● means online. It may take Find My iPhone up to 3 minutes to fix a precise location for a device.

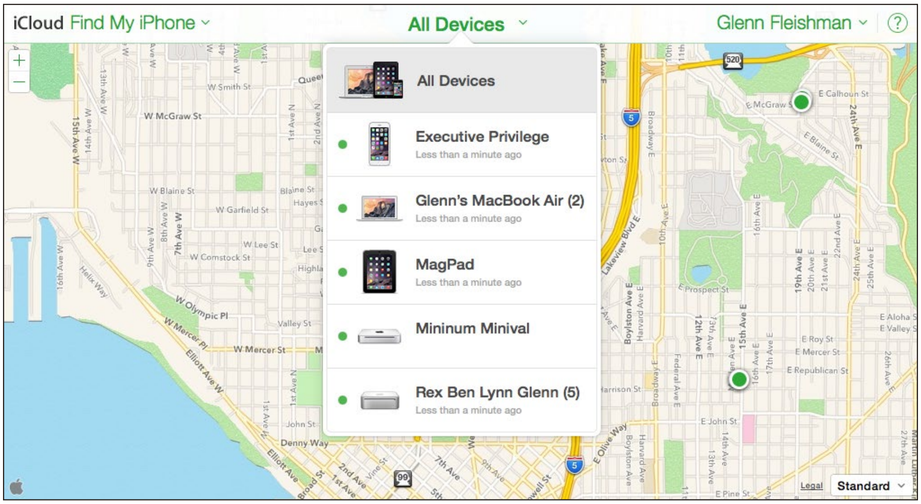


Figure 64: *The Find My iPhone Web app shows devices in a drop-down list at center and their locations on a map.*

3. Select a device in the list to see just its location.

Find My iPhone shows the location of the device on the map as a green dot. For GPS-enabled devices that have obtained a strong location fix, only the dot is shown. When the GPS information isn't good or it's a device without a GPS, the green dot is surrounded by a green outline, the radius of which indicates the amount of confidence in the location (**Figure 65**). With hardware relying on a GPS signal, the outline may appear briefly while a better fix is being obtained.

With All Devices chosen, click the All Devices label or click anywhere on the map to hide the drop-down, and then click any green dot on the map. A popover menu appears with options for actions, described a few paragraphs ahead, and the last time a fix was made on the location.

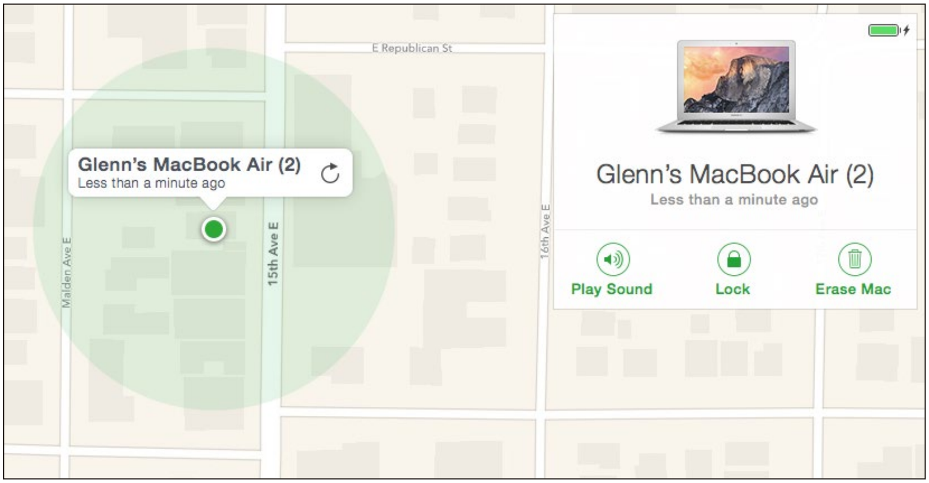


Figure 65: *The shaded green circle shows the degree of confidence. In this case, my MacBook Air might be half a block away (though the green dot is, in fact, accurate).*

If the device was previously found but can't be found now, you may get a message that says, "Your device is no longer locatable." The last-known location of the device should be displayed for 24 hours, along with the time showing the last moment it was known to be located there. Clicking the green dot on the map representing the device brings up a popover with a Refresh button you can click to force another attempt to locate it.

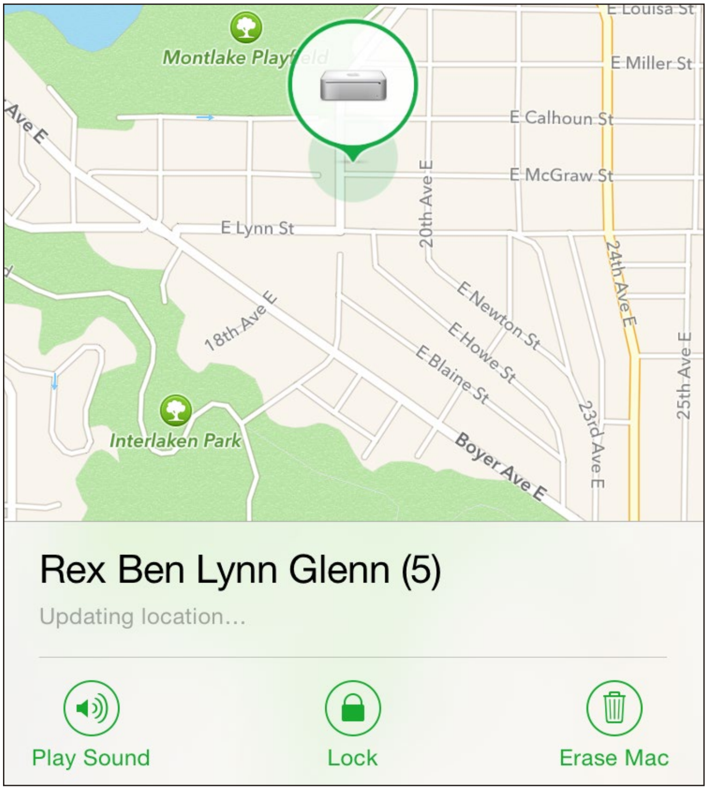
Battery life: *The Web app, but oddly not the iOS app, shows the remaining battery life on devices that are battery powered.*

Find My iPhone app

You don’t have to use a Web site to run Find My iPhone. Instead, you can download the free Find My iPhone app to an iOS device, launch it, and then enter your account and password. The app works similarly to the Find My iPhone Web app, although its interface is a little different in layout when a device is selected.

The default view shows all devices in a list at the bottom and their locations in a map shrunk to fit them all at the top. Tap any device in the list, and it’s selected and zoomed in on in the map. Tap the All button at the upper left to return to the full device list.

Tap the device in its green circle or tap the Actions button at the bottom to show the options for remote action (**Figure 66**).



Rex Ben Lynn Glenn (5)

Updating location…

Figure 66: *The Find My iPhone app lets you tap a device on the map and then perform remote actions.*

You can tap the automobile icon at lower left, and the Maps app is launched with the device's location preloaded as a destination.

Password not stored: *The app doesn't save your password, and it caches it for only a short time. If you borrow someone's iOS device to run Find My iPhone, you don't have to worry about that person finding your iOS devices in the future. And, to reverse the situation, if a thief steals your iPad, the thief can't use the app to locate more of your devices—or figure out where you are!*

Take Remote Action

You can now take action on your remote device, with three options that vary in utility based on whether your device has fallen behind a couch cushion, or has been misplaced or stolen (**Figure 67**). Whatever action you take, iCloud sends an email message to your Apple ID address, notifying you.

Tap one of the options and see the section below that corresponds to Play Sound, Lost Mode, and Erase Device. (For Macs and iOS 5 devices, the earliest ones supported, Lost Mode is replaced with Lock.)

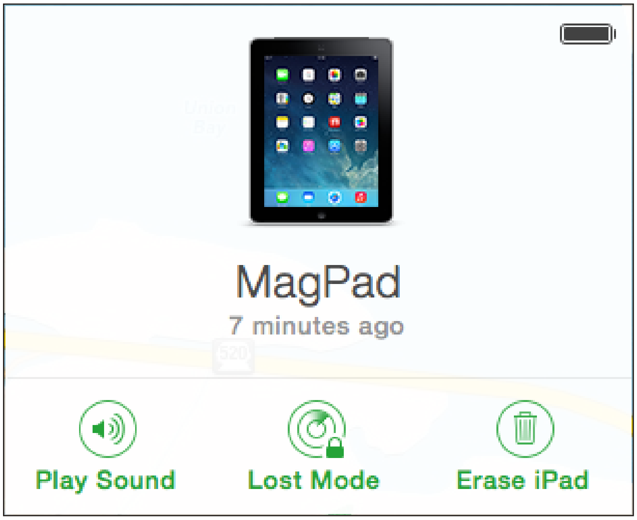


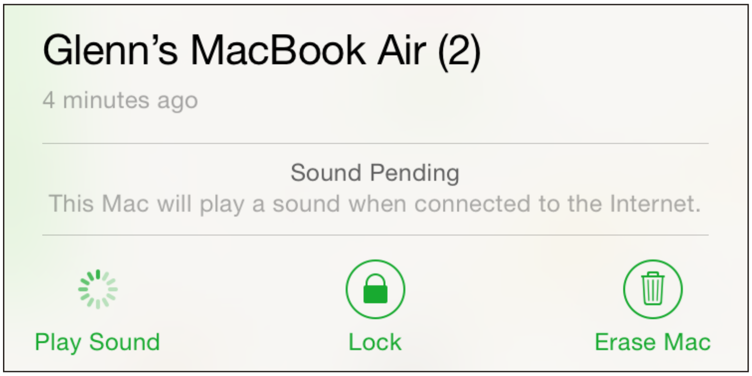
Figure 67: *The three remote actions: Play Sound, Lost Mode, and Erase Device. Note the battery life shown in the upper-right corner in the Web app version.*

WARNING! *If you know your device was stolen, consider taking location information to the police—call an officer if you have a report already opened—before trying to entice the thief to give it up. Although electronics are stolen all the time, reports from all over indicate that law enforcement responds favorably to being given a map and other data. That can, in turn, lead police to find a cache of other stolen hardware.*

Works Even If Offline by When It Comes Online

You can pick any of the below options even if the device is shown as offline, and iCloud will trigger it if the device comes online with Find My iPhone still active (**Figure 68**). You don't need to keep the Web app or iOS app open; if the trigger happens, you'll receive an email message.

Thieves tend to wipe stolen hardware as soon as practical. An iPhone or iPad with an active cellular plan could receive a Find My iPhone action over the cellular data network when it came back online; any device, if it connected first to Wi-Fi, could receive remote actions.



Glenn's MacBook Air (2)

4 minutes ago

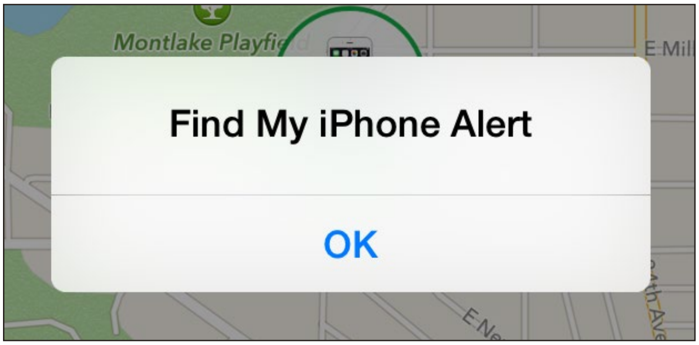
Sound Pending

This Mac will play a sound when connected to the Internet.

Figure 68: *Even an offline device can have an action applied when (or if) it comes back online.*

Play Sound

When you can't find a device but think it may be nearby, the Play Sound option should help you locate it. Tap or click Play Sound, and a loud pinging noise will play for 2 minutes on the device, which also displays the message "Find My iPhone Alert" (**Figure 69**).

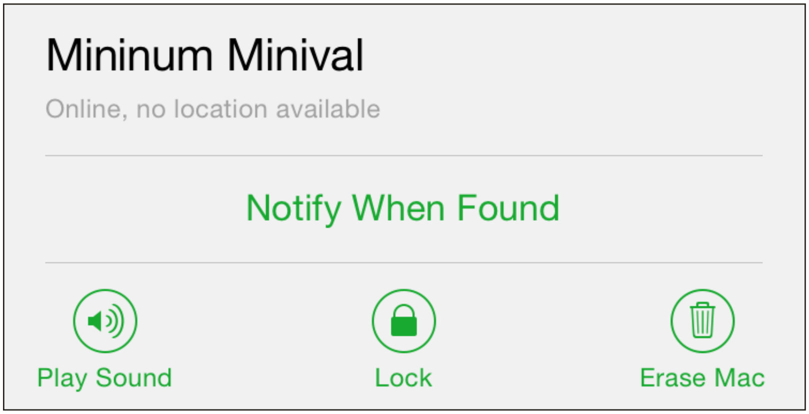


Find My iPhone Alert

Figure 69: *iOS shows this message when Play Sound is triggered.*

Notify when back online: *If a device isn't trackable after a moment in the Find My iPhone Web app or iOS app, you can select it from the Devices list and then select the Notify When Found box without having to trigger any other actions (**Figure 70**).*

Whether the device is offline or online, the next time it connects through Find My iPhone to Apple's servers, you'll receive an email message, see a banner when you sign in to the Find My iPhone Web app, and get a pop-up alert on iOS devices with Find My iPhone active.



Mininum Minival

Online, no location available

Figure 70: *Devices without a location can trigger alerts when they acquire a location.*

The sound will override any mute settings on the device. The sound can be stopped on the found iOS device by tapping OK if it's unlocked. If the passcode lock is active, enter it to stop the dratted noise.

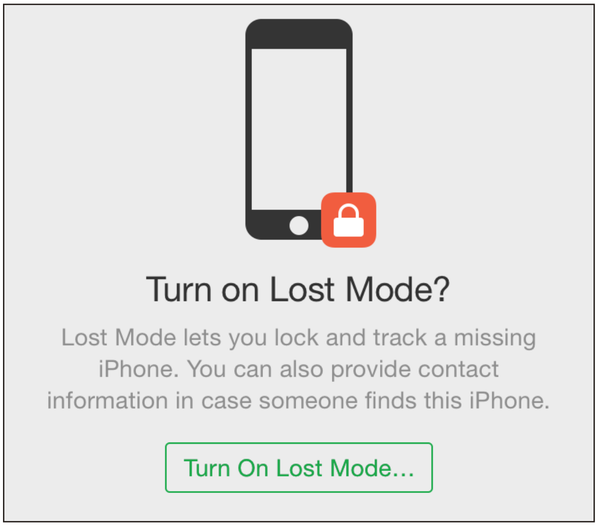
Lost Mode

This option is designed to help you recover a lost device. You can offer a reward and provide your phone number. It also puts the finder on notice that you know approximately where it is. ("I'm a block away, coming to pick it up. There's a reward.") Were your hardware stolen, this is a way to tell a thief that you have her location and other data, and advise her to give it up.

> **Note:** Lost Mode immediately disables Apple's side of Apple Pay for devices that are both capable of it and have the feature enabled. Thus, if your device is lost and someone has the passcode and attempts to unlock the phone when it's not connected to a network to pay for something, Apple will not pass the transaction on for approval.

This Lost Mode option has four steps:

1. After tapping or clicking Lost Mode, you have to confirm by tapping Turn On Lost Mode (**Figure 71**).

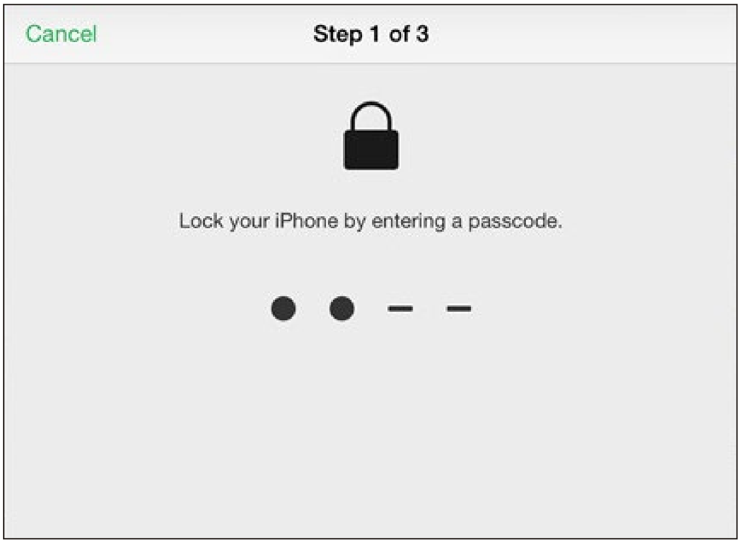


Turn on Lost Mode?

Lost Mode lets you lock and track a missing iPhone. You can also provide contact information in case someone finds this iPhone.

Figure 71: *Lost Mode doesn't involve a mysterious island.*

2. If a device doesn't have a passcode set, you are prompted to enter and verify a passcode (**Figure 72**).

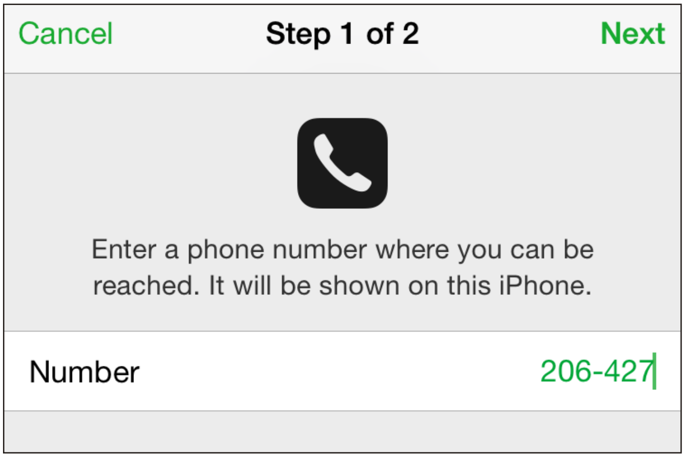


Lock your iPhone by entering a passcode.

● ● – –

Figure 72: *If a device doesn't already have a passcode in place, you are prompted to enter one and then verify it in the next step.*

3. Optionally, set a phone number for a call back (**Figure 73**). On an iPhone, the phone may be used to call *only* that number. On other devices, the call-back number is displayed but can't be used.

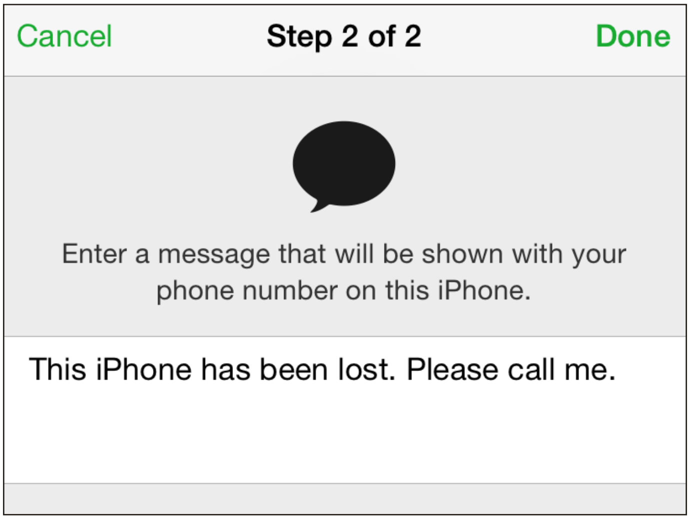


Enter a phone number where you can be reached. It will be shown on this iPhone.

Number 206-427

Figure 73: *You can opt to enter a call-back number.*

4. Optionally, enter a message to appear on the device (**Figure 74**). In this step, the dialog shows that a passcode has already been set and will be used to lock the device.



Enter a message that will be shown with your phone number on this iPhone.

This iPhone has been lost. Please call me.

Figure 74: *Choose to add a message.*

After you activate Lost Mode, the action is passed to the device, and an email message is sent to the email address for the Apple ID account you're using for Find My iPhone, confirming what you've done.

Once the action is sent, one of the following behaviors occurs:

- If the device is connected to a wireless network and asleep, the next time it's woken, a passcode must be entered to gain access.
- If the device is online and in use, iOS drops the user into the Lock screen where the passcode-entry dialog or keypad is shown.
- If the device is offline, the next time it accesses any network with an Internet connection, the passcode lock is put into place.

Lost Mode also enables tracking the next time the device is online, which appears in a map as a dotted red line (**Figure 75**). This lets you see wherever a device has gone—so long as it remains online. Even neater, if Location Services has been turned off, Lost Mode re-enables it so that you can track your device.

Erase Device

The last resort in some cases (or first in others) is a remote wipe, in which all the user data on the iOS device is erased.

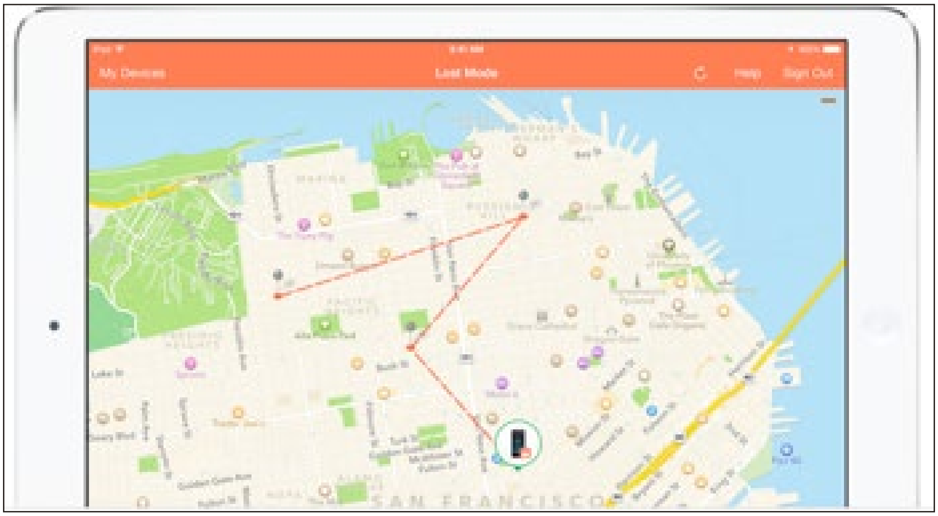


Figure 75: *While Lost Mode is enabled, the path a device takes as long as it has connectivity is recorded and shown as well. (Figure via Apple.)*

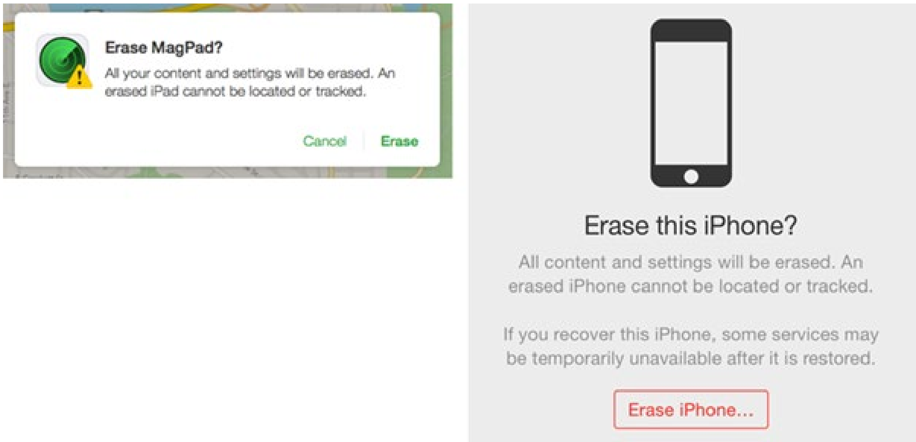
Since iOS 7, an erased device that has Find My iPhone enabled before erasure and remains associated with an Apple ID cannot be unlocked without the account password. The Erase Device option lets you provide a phone number and message so that a person who found (or stole) your device can get in touch. The iOS device is essentially useless to them without the password.

WARNING! *After erasing a device, Find My iPhone can no longer provide location information.*

Note: You can remove a device from your Find My iPhone list after erasing it by following Apple's instructions at **http://support.apple.com/kb/PH2702**.

It's a multi-step process to prevent accidental erasure:

1. In the Web app or the iOS app, tap Erase (Web) or Erase *Device* (iOS).
2. You're warned that everything is about to be erased. Tap or click Erase, but there are more steps ahead (**Figure 76**).



Erase MagPad?

All your content and settings will be erased. An erased iPad cannot be located or tracked.

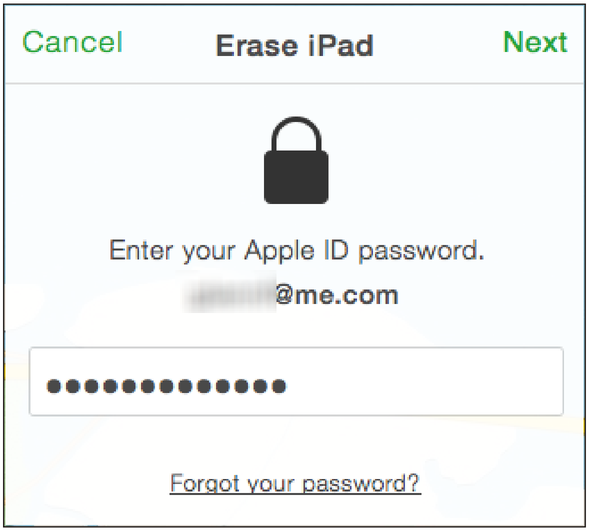
Erase this iPhone?

All content and settings will be erased. An erased iPhone cannot be located or tracked.

If you recover this iPhone, some services may be temporarily unavailable after it is restored.

Figure 76: *This step seems like you're about to erase your device immediately, but there are more steps ahead (left: iOS; right, Web).*

3. Enter your Apple ID password. For Family Sharing, if this is another member's device, enter his or her Apple ID password (**Figure 77**).



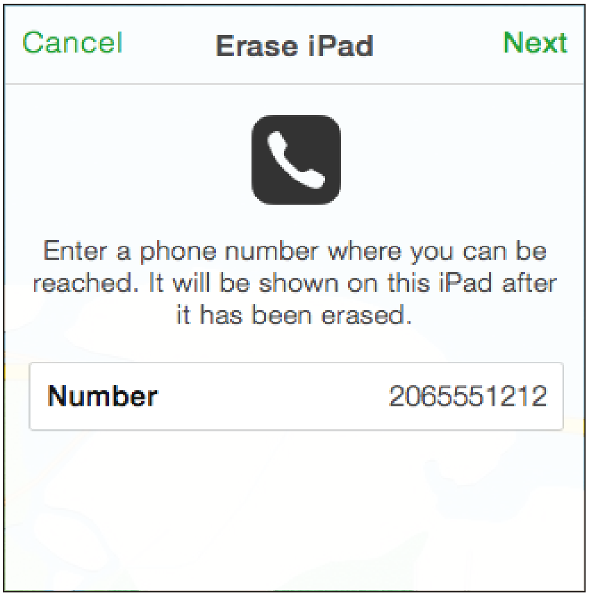
Enter your Apple ID password.

[redacted]@me.com

●●●●●●●●●●●●●

Figure 77: *Enter the appropriate Apple ID password.*

4. Enter a phone number at which you can be reached after it's erased, and tap Next (**Figure 78**).

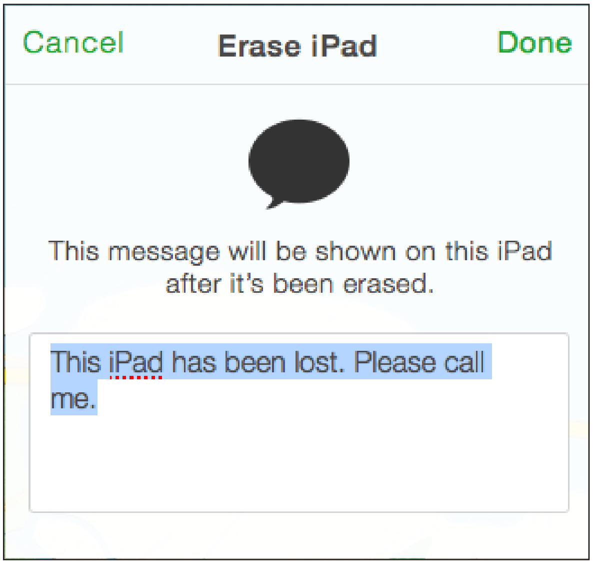


Enter a phone number where you can be reached. It will be shown on this iPad after it has been erased.

Number 2065551212

Figure 78: *If you want to provide a number, enter it at this step.*

5. Enter a message you want to appear along with the phone number (**Figure 79**). You'll notice there's a Done button. Tap that, and the remote device is erased—there's no going back!



This message will be shown on this iPad after it's been erased.

This iPad has been lost. Please call me.

Figure 79: *This message will appear after erasure as well.*

If the device is online, the Erase action immediately wipes all your data off it. If it's offline, the erase begins as soon as it next comes online through any networking method.

Note: Because Find My iPhone works with older versions of iOS, you might see slightly different options if you have iOS 5 or iOS 6 installed on an older piece of hardware.

The erasure happens quickly. Apple includes hardware encryption on all iOS devices that can run iOS 6 or later: all iPads, the iPhone starting with the 3GS, and the iPod touch starting with the 4th-generation model (2010). To "erase" all the device's stored data, the encryption key is thrown away and a few other settings rewritten, and everything is now completely unrecoverable.

Note: Macs with FileVault 2 (starting in 10.7.2 Lion) can similarly have their boot drives rendered unreadable: an encryption key is deleted, making the drive's encrypted contents irretrievable. (The drive can still be erased and a new system installed, however.)

However, wiping your device isn't as bad for your data as it sounds. All iOS devices are set by default to back up the unique data that's stored on them, like settings, passwords, and documents created by or associated with apps. These backups can be either local to iTunes on a particular computer or remote to iCloud.

Tip: You can also make both kinds of backups by manually switching between the options in iTunes when an iOS device is connected: do a backup with one, switch, and back up with the other.

Any media and apps kept on an iOS device are not stored in the backup. Instead, they are stored in some combination of a copy of iTunes (for your own music, videos, ebooks, and purchased movies) and iCloud (all apps or any media that you've bought from Apple, and your own music uploaded or matched using iTunes Match).

If you erase your device, and then either recover it or obtain a new device, you can restore from your most recent backup. If you were syncing any items to your device through iTunes, you can then sync them back to the device. Or, for items stored in iCloud, the restore process downloads them again.

If you were syncing any data wirelessly through iCloud or an Exchange account, such as calendar or contact information, you likely won't have lost any of that data up to the moment the device was lost or disconnected from a cellular or Wi-Fi network. You will lose any changes made on the device between the last sync (push, fetch, or manual) for each account and the remote wipe.

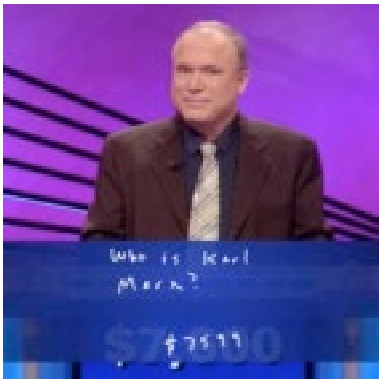
WARNING! *Erase can be used by a ne'er-do-well who obtains your Apple ID and password. That happened to writer Mat Honan in August 2012. His password was obtained by a malicious party who fooled Apple's customer service into bypassing protections on security questions and answers, and then the villain erased the data on Honan's iPhone, iPad, and MacBook.*

A Remote Wipe Makes a Mac Hard to Fence

When you send an Erase action to a Mac, you're prompted to set a recovery code and message. Wiping a Mac deletes the data on the main partition that you use to boot your system, but it keeps intact the Recovery HD, a small partition that Apple employs to help with common installation and other problems.

A thief who has a machine that you wiped using Find My iPhone won't be able to easily install a new system—he would require the passcode you set. If he tries to sell the system, whenever it boots, it will display the message you set—ostensibly advising that the machine is lost or stolen and how to contact you.

About the Author



Glenn Fleishman was trained as a typesetter, received a degree in art, and works as a journalist and programmer. Glenn is a regular contributor to the *Economist*, where he has filed hundreds of online stories, including a four-year stint as one of the lead writers of its Babbage blog, and dozens of print features.

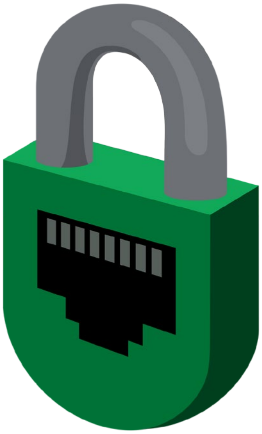
He also appears regularly in Boing Boing, TidBITS, *Fast Company*, *MIT Technology Review*, Macworld, and Six Colors. Glenn writes about security, privacy, nanosatellites, copyright, Bitcoin, crowdfunding, and much more. His blog is **http://glog.glennf.com**, and he overshares on Twitter at **@glennf**.

In October 2012, he appeared on the Jeopardy! quiz show and managed to win—twice! Alex Trebek seems like a very nice fellow, but you never get to really know him.

Acknowledgments

I dedicate this book to my wife, Lynn, and sons, Ben and Rex. They keep me sane and happy, and keep me from spending my entire day thinking about and using digital devices.

Thanks to editor Jeff Carlson, who made sense of this thorough overhaul of the book for iOS 8. Thanks to Scout Festa for her eagle eye in proofreading. And many thanks to longtime collaborators Adam and Tonya Engst, along with Michael E. Cohen, who saw this book through earlier editions.



Copyright and Fine Print

ISBN: 978-0-9914399-4-2 (ebook)
ISBN: 978-0-9914399-5-9 (print edition)
Aperiodical LLC, 1904 E. McGraw St., Seattle, WA 98112-2629 USA

http://glennf.com/guides

Ebook edition: This electronic book doesn't use copy protection because copy protection makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. You have our permission to make a single print copy of this ebook for personal use. Please reference this page if a print service refuses to print the ebook for copyright reasons.

All editions: Although the author and Aperiodical LLC have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither Aperiodical LLC nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

Many of the designations used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement of the trademark. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are the trademarks or that are the registered trademarks of Apple Inc.; to view a complete list of the trademarks and of the registered trademarks of Apple Inc., you can visit

http://www.apple.com/legal/trademark/appletmlist.html