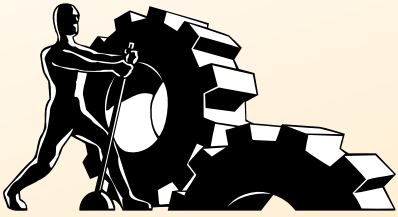


Check for Updates

Make sure you have the latest information!



TidBITS Publishing Inc.

Take Control of

vl.1

iPad Networking and Security

Glenn Fleishman

\$15

[Help](#)

[Catalog](#)

[Feedback](#)

[Order Print Copy](#)

Table of Contents

READ ME FIRST 4

Updates and More	4
Basics	5
What's New in Version 1.1	6

INTRODUCTION 8

QUICK START TO NETWORKING AND SECURITY 9

QUICK CONNECTION GUIDE 11

Connect with Wi-Fi at Home or Work.....	11
Connect to a Wi-Fi Hotspot	14
Connect with 3G	16

IN-DEPTH ON WI-FI 19

Managing Wi-Fi Connections	19
Wi-Fi Troubleshooting	25
Tweaking Your Home Network for Faster iPad Performance	27

CONNECT TO A SECURE WI-FI NETWORK 29

Connect with WPA/WPA2 Personal	30
Connect with WPA2 Enterprise	31
Outdated Methods	33

WORK WITH 3G 38

Why Use 3G	38
How to Use 3G.....	39
Choose to Use 3G or Wi-Fi.....	52
Cross-Border 3G iPad Use.....	54
Alternatives to Built-in 3G	56

SET UP BLUETOOTH 62

Bluetooth Basics.....	62
Pairing Any Device.....	63
Apple Wireless Keyboard	65
Audio Devices	67

AIRPLANE MODE 70	
What's Airplane Mode?	70
Turning Radios off Separately	71
REMOTE ACCESS AND CONTROL 72	
iTeleport (Formerly Jaadu VNC).....	73
LogMeIn Ignition	79
ACCESS DOCUMENTS 85	
What Kinds of Storage	85
Air Sharing HD	90
GoodReader	100
Connect to an iPad WebDAV Server	110
Dropbox.....	113
iDisk.....	116
TRANSFER DATA SECURELY 118	
Exposure.....	118
Secure Solutions	123
KEEP DATA SAFE 129	
Exposure.....	129
Mitigation.....	131
WHEN YOUR iPad GOES MISSING 139	
Safety Tips while Out and About.....	139
Find My iPad via MobileMe	140
Remote Tracking Software.....	147
ABOUT THIS BOOK 149	
About the Author.....	149
Author's Acknowledgments	149
About the Publisher	150
Production Credits	150
COPYRIGHT AND FINE PRINT 151	
FEATURED TITLES 152	
Increase Your iPad IQ	152
More Take Control Ebooks	152

Read Me First

Welcome to *Take Control of iPad Networking & Security*, version 1.1, published in June 2010 by TidBITS Publishing Inc. This book was written by Glenn Fleishman and edited by Tonya Engst.

This book covers how to use your iPad on a Wi-Fi or 3G network securely, making connections with ease while protecting your data and your device. It also covers other tasks that rely on a network, such as retrieving documents to read and remotely controlling computers from your iPad.

Copyright © 2010, Glenn Fleishman. All rights reserved.

If you have an ebook version of this title, please note that if you want to share it with a friend, we ask that you do so as you would a physical book: “lend” it for a quick look, but ask your friend to buy a new copy to read it more carefully or to keep it for reference.

Discounted [classroom and Mac user group copies](#) are also available.

UPDATES AND MORE

You can [access extras related to this ebook](#) on the Web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or purchase any subsequent edition at a discount.
- Download various formats, including PDF and—usually—EPUB and Mobipocket. (Learn about reading this ebook on handheld devices at <http://www.takecontrolbooks.com/device-advice>.)
- Read postings to the ebook's blog. These may include new information and tips, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.
- Get a discount when you order a print copy of the ebook.

BASICS

In reading this book, you may get stuck if you don't understand a few basic iPad-related facts or a few conventions that the Take Control series uses. Important things to know include:

- **iPad touchscreen:** I often mention tapping an item on the iPad screen, such as “tap the Join button.” Occasionally, you may need to double tap, or even touch. *Touching* means putting your finger on the touchscreen and keeping it there until something happens. You may also need to swipe or drag your finger across the touchscreen.
- **iPad Settings app:** I frequently tell you to adjust options in the iPad's Settings app. By default, this app appears on the first page of the Home screen. To view the Home screen, press the round Home button on the edge of the iPad. To open the Settings app, tap its icon.
- **iPad navigation:** To describe moving around in the iPad's interface, I sometimes use a shortcut. For example, if I wanted to tell you to open the Settings app, tap the Wi-Fi option at the left, and then—in the right hand Wi-Fi Networks pane—tap Other, I might instead tell you to “tap Settings > Wi-Fi > Other.”
- **Using an external, physical keyboard with an iPad:** Some directions assume you are using the iPad's onscreen keyboard. If you are using a physical keyboard, you may need to press the Return or Enter key to enter certain information, instead of tapping the Join or Search button that would otherwise appear on the onscreen keyboard.

More iPad information: For lots more general information about the iPad, consult the free [Take Control of iPad Basics](#).

- **Desktop vs. mobile:** In this ebook, a *desktop device* is either a laptop or a traditional computer that would sit on a desk, typically running Mac OS X or Windows. A *mobile device* means a portable or handheld computer-like device such as an iPad, Kindle, or Blackberry.

Mobile software or a *mobile operating system* refers to software running on a mobile device, such as the iPhone OS (which, despite

its name, is the iPad's current operating system) or the mobile version of Apple's *desktop* Safari Web browser, which is technically called *Mobile Safari*, even though Apple calls it "Safari" on the iPad's Home screen.

- **Menus:** To describe choosing a command from a menu in the menu bar on a desktop computer, I use an abbreviated description. For example, if I wanted to tell you to create a new playlist in iTunes, I could write "go to the File menu and choose New Playlist." Instead, I get to the point more quickly, by writing "choose File > New Playlist."
- **Radio types:** Both iPad models have Bluetooth and Wi-Fi radios. *Bluetooth* is a short-range wireless technology for linking audio headsets, wireless speakers, and keyboards and mice. *Wi-Fi* is a high-speed networking standard for moving data among computers and other devices on a local network.

A cellular data version of the iPad, which I call the *3G iPad*, has two more radios: a *cellular modem*, which allows data communications on mobile networks, and a *GPS receiver* for calculating position based on satellite signals, just like with a standalone GPS navigator.

WHAT'S NEW IN VERSION 1.1

This updated version includes three changes.

- **AT&T U.S. data plans:** Let's start with the big one. The same day we released version 1.0 of this book, AT&T revised its pricing for 3G iPad service in the United States. Before June 7, AT&T offered an option for unlimited service for \$29.99 per 30-day billing cycle, which could be canceled at any time, and which was automatically renewed at the end of each billing period until you canceled service. You could also resume service at any time.

The replacement plan—made at the same time as an overhaul of AT&T's iPhone cellular data plans—offers just 2 GB of 3G data for \$25 over a 30-day period. If you run out of data in a given billing period, you can buy another 2 GB and start the clock on 30 days again.

3G iPad users who signed up for unlimited service before June 7 and who do not cancel such service may continue to renew it indefinitely. See [Pick a Plan](#) (p. 41) for more details.

- **iPhone OS 4 is now named iOS 4:** The second change is that Apple renamed iPhone OS to iOS for the upcoming fourth release. iPhone OS works on the iPhone, iPad, and iPod touch, and a name change was overdue. The company will release iOS 4 for iPhone 3G and 3GS, and second- and third-generation iPod touch models, as well as preinstalled on the iPhone 4, in late June. The iPad version is slated for third quarter of 2010. For now, you can learn more in “Apple Previews Major New Features in iPhone OS 4,” at <http://db.tidbits.com/article/11176>.
- **Dropbox support in Air Sharing HD:** Finally, Air Sharing HD has been updated to include Dropbox support within the program. I made a few small changes in the manuscript to include this information; see [Air Sharing HD](#) (p. 90).

Introduction

An argument against the iPad before its introduction was that it was just “a big iPod touch.” In reality, it is not: the bigger screen makes it possible to use it in a different way altogether. But from the standpoint of networking and other communications, the iPad is like a giant iPod touch—with some iPhone features thrown in, too.

Like the iPod touch, the iPad cannot place phone calls via a cellular network, and it has Wi-Fi built in; like the iPhone, Apple offers an iPad model that sends and receives data over a 3G cellular network—but which can’t handle cell phone calls. This combination of options—and the likelihood that you probably don’t own both a Wi-Fi-only and a 3G iPad—has implications for the choices you make about how you connect and the security of those connections.

One of the most important ongoing decisions you’ll make about your iPad is how to obtain a network connection. If you have a 3G iPad, you may choose each month whether to enable cellular data connectivity or not. Those with Wi-Fi-only iPads may spend a fair amount of time finding, connecting to, and interacting with Wi-Fi networks all over. There’s plenty of advice in this title on both 3G and Wi-Fi connections and networks.

In this book, I guide you through how to make consistent and secure network connections, whether over Wi-Fi or 3G, and how to best protect your data and your iPad.

Calling: *Just to muddy the water even further, you can make phone calls from an iPad using voice over IP (VoIP) programs, like [Skype](#), that connect calls between Skype users or to and from the public switched telephone network over the Internet.*

Information related to 3G iPads is highlighted: I use a special blue box to call out information particular to the 3G iPad.

Quick Start to Networking and Security

This book explains how to use an iPad safely on a network, including how to connect and customize a connection, and how to secure data that's on your iPad or that's passing over a network. You can read the ebook in order or skip to topics of particular interest.

To make a connection right away with a minimum of fuss, skip to an option in the “Make a connection fast” list, just below. For Wi-Fi connections, note that [Connect to a Secure Wi-Fi Network](#) (p. 29) explains security and password options and [Wi-Fi Troubleshooting](#) (p. 25) has advice for fixing problematic connections.

Also, if you have a Wi-Fi–only iPad and are wondering how you can make a 3G connection, don't miss [Alternatives to Built-in 3G](#) (p. 56).

Make a connection fast:

- Get on a Wi-Fi network without fuss. See [Connect with Wi-Fi at Home or Work](#) (p. 11)
- [Connect to a Wi-Fi Hotspot](#) while you are out and about (p. 14).
- Set up your iPad's 3G service plan, and connect to a cellular data network. See [Connect with 3G](#) (p. 16).
- Add Bluetooth devices to your iPad. See [Set Up Bluetooth](#) (p. 62).

Ensure you're secure:

- Set up a secure Wi-Fi connection. See [Connect to a Secure Wi-Fi Network](#) (p. 29).
- Prevent others from sniffing your passwords and data over wireless networks. See [Transfer Data Securely](#) (p. 118).
- Don't let your iPad's data fall into the wrong hands. See [Keep Data Safe](#) (p. 129).
- Find out what to do [When Your iPad Goes Missing](#) (p. 139).

Learn to use cellular data services:

- Discover the ins and outs of cellular data plans. See [How to Use 3G](#) (p. 39).
- Keep cellular data costs under control outside your home country. See [Cross-Border 3G iPad Use](#) (p. 54).
- Find alternatives for cellular access without buying a 3G iPad. See [Alternatives to Built-in 3G](#) (p. 56).

Discover other networked uses of an iPad:

- Control a computer's screen and input from an iPad. See [Remote Access and Control](#) (p. 72).
- Grab and view documents, images, and videos over a network or the Internet with apps. See [Access Documents](#) (p. 85).

Go under the hood, gain more control, and solve problems:

- Read [Managing Wi-Fi Connections](#) (p. 19) to learn the ins and outs of joining and forgetting hotspot networks, configuring your iPad to connect in complex scenarios, and work through problems with [Wi-Fi Troubleshooting](#) (p. 25).
- Find tips for setting up a residential Wi-Fi network to work well with iPads in [Tweaking Your Home Network for Faster iPad Performance](#) (p. 27).
- Get advice on setting up a secure wireless network in [Connect to a Secure W-Fi Network](#) (p. 29).
- Learn how to turn off the iPad's Wi-Fi and cellular radios in [Airplane Mode](#) (p. 70).

Quick Connection Guide

You have an iPad in your hands and you want to get on a network. Read this section to make a connection right away. Other parts of the book provide more detailed information about settings, cover less-common connection options, and discuss security.

Your iPad has Wi-Fi built in; all models do. You may have bought an iPad that also features 3G hardware. This section looks first at making a Wi-Fi connection in various situations. It then turns its focus to how to [Connect with 3G](#) (p. 16).

CONNECT WITH WI-FI AT HOME OR WORK

In this topic, I cover three common ways to connect any iPad to a home or work Wi-Fi network. (For help with how to [Connect to a Wi-Fi Hotspot](#), perhaps at a café or airport, skip ahead a few pages.) There are three typical approaches for connecting an iPad to Wi-Fi at home or work:

- Simply tap the name of a network that requires neither a security key nor a password.
- Tap the name of a network that requires a security key or password, and then fill in the required details.
- Enter a network name for a *closed* network that doesn't appear in a list, with or without a key or password.

Let's look at each option in turn.

Connect by Name (No Password)


To connect your iPad to a Wi-Fi network that has a publicly available name and no security key, follow these steps:

1. Open the Settings app.
2. Tap Wi-Fi at the top of the Settings list.

3. Tap the network's name when it appears in the list at right. The iPad may take a few seconds to complete scanning and showing all networks in the list, during which time it shows a strobing icon.

Your network doesn't appear: You may be too far away from it or have a solid obstruction in the way; or, it's possible the Wi-Fi base station has crashed or been unplugged.

Lock icon next to the network name: The lock icon indicates a network that requires a password to join.

Your iPad should join the network, and an icon showing a Wi-Fi connection  should appear in the upper left corner of the screen.

No Wi-Fi connection icon appears: Consult [No Internet Service after Connecting](#) for help figuring out the connection problem.

Connect by Name (with a Password)

Many home and business networks use a password or encryption key to limit network access to those who have a valid reason to use the network. To join such a network, you must enter the password when prompted during a connection. If you don't have the password, you can't join the network.

Follow these steps:

1. Open the Settings app.
2. Tap Wi-Fi.
3. Tap the network's name when it appears in the list. The list may take a few seconds to complete scanning and showing all entries.


Your network doesn't appear: You may be too far away from it or have a solid obstruction in the way; or, it's possible the Wi-Fi base station has crashed or been unplugged.

No lock icon next to the network name: The lock icon indicates a password-protected network. If there's no lock, the network isn't secured, and you can skip Step 4.

4. The iPad prompts you to enter a network password. The iPad determines which kind of network security is being used; you should be able to enter the password without a prompt to select the security method.

User name and password prompt: *If you connect to a network, typically at a large corporation or university, you may be prompted for a network user name along with a password. That name should have been provided to you at the same time as the password. If not, ask your network's administrator.*

5. Tap Join on the right side of the keyboard.

Your iPad should join the network, and an icon showing a Wi-Fi connection  should appear in the upper left corner of the screen.

No Wi-Fi connection icon appears: Consult [No Internet Service after Connecting](#) for help in figuring out the connection problem.

Connect to a Closed Network

Some people and companies choose to set up *closed* networks, in which the network name isn't indiscriminately broadcast.


No extra security: *While closed networks appear to provide additional security, in reality, there's scant difference except in making a connection harder for those who are entitled to join.*

To join a closed network, follow these steps:

1. Open the Settings app.
2. Tap Wi-Fi > Other.
3. In the Other Network screen, Tap the Name field, and enter the network's name as you set it or it was provided to you.
4. If the network has any security option set:
 - a. Tap Security
 - b. Choose the security method from the list. If a password or a user name plus a password were provided to you, you should have received the security method's name as well. If you set the

security method for the network yourself, you must recall which method you used.

- c. Tap Other Network to return to the previous screen.
 - d. Assuming you chose a security method other than None, tap the Password field, and enter the password exactly as it was provided.
 - e. If you chose the WPA Enterprise or WPA2 Enterprise security method, tap Username and enter the user name you were provided for access.
5. Tap Join on the right side of the keyboard.

Your iPad should join the network, and an icon showing a Wi-Fi connection  should appear in the upper left corner of the screen.

No Wi-Fi connection icon appears: Consult [No Internet Service after Connecting](#) for help in figuring out the connection problem.

Tip: See [In-Depth on Wi-Fi](#) for other Wi-Fi network options, and [Connect to a Secure Wi-Fi Network](#) for a full explanation of how to use security options.

CONNECT TO A WI-FI HOTSPOT

Wi-Fi hotspots are often found in places like libraries, hotel lobbies, and hospitals. When you connect to a network in a Wi-Fi hotspot, it's much like connecting to any network that doesn't require a password. However, most Wi-Fi hotspots require you to take an additional step via a Web browser such as using an account (even a free account), accepting an agreement, or providing payment.

Follow the steps in [Connect by Name \(No Password\)](#), and then:

1. Open the Safari app.
2. If a Web page isn't already in the browser reloading, tap the URL field and enter anything, such as [google.com](#) or [example.com](#). Tap Go in the lower right corner.

A Web redirect page will appear if the hotspot requires that you proceed through an additional step. That page will have information that varies by the kind of site:

- For a free hotspot without accounts: The page explains the terms of service, and it requires that you check a box, enter initials into a field, or otherwise signify agreement.
- For a free hotspot requiring an account: A page explains that a free account is required to use the wireless connection. The page allows you to log in or set up an account.
- For a paid hotspot: You should see an explanation of the cost of service, how to pay, and how to login if you have an account. You might also have an account with a service that resells access to the network or allows roaming onto the network, such as Boingo Wireless, Verizon Wireless, AT&T, iPass, or any of several other firms. Pay or enter credentials to proceed. (See [iPad Hotspot Access via Boingo Mobile](#) to learn more about Boingo's offering.)

Whether you'd prefer not to pay a fee or can't get a hotspot to accept your credentials, you may want to use 3G: Read [Forget This Network](#) for how to forget a Wi-Fi network you've joined; [Disabling Wi-Fi or 3G](#) for forcing a 3G rather than a Wi-Fi connection; and [How to Use 3G](#) for details on paying for a 3G plan.

3. Follow the directions to finish establishing your connection.

When you've completed the appropriate procedure, you should be able to visit any Web page.

Hotspots May Not Send Your Outgoing Email

Some hotspots won't send your outgoing email if your iPad uses the standard unsecured email port 25. (You can think of a *port* as a kind of cubbyhole attached to an Internet address and assigned to a specific service, like outgoing email.) To work around this problem, either use webmail, which doesn't suffer from that limitation, or configure your Mail account to use an alternate port, or, preferably, a secured connection. Consult your email host or Internet service provider for details, and see [Transfer Data Securely](#) for more on securing email connections.

Your Data Carrier May Connect Your 3G iPad to Wi-Fi

If you have an iPad with a 3G radio and are currently paying for 3G service with AT&T, your iPad will automatically connect to any AT&T Wi-Fi network within range.

AT&T includes Wi-Fi access at its 21,000 hotspots as part of its paid iPad 3G service, which typically gives you a far faster upstream and often faster downstream Internet connection. (It also saves AT&T money by moving more traffic off its crowded cellular network.)

If you're signing up for 3G service outside the United States, the carrier you choose may include limited ("fair use") or unlimited Wi-Fi service, too.

CONNECT WITH 3G

If you have an iPad with 3G, you have the option at any time to enable or disable 3G mobile broadband access. Apple made it easy to enable 3G service without having a Wi-Fi or cellular network connection already active, as long as you are in an area covered by the carrier from which you purchased the iPad, or the one associated with the iPad's 3G micro-SIM card.

The micro-SIM connects you to a carrier: *A micro-SIM contains information that connects an iPad to a carrier's network, both for Internet access and for billing. If you purchase a 3G iPad from a carrier, you receive a micro-SIM from that carrier. If you buy a 3G iPad from a retailer or directly from Apple, you may have a choice of carrier at the point of purchase or you may be able to obtain a different micro-SIM later. Most 3G iPads are sold unlocked and can accept a micro-SIM from any carrier.*

Note: Different carriers have many variants, discussed in [Pick a Plan](#). For example, some offer account management from a Web site instead of via the iPad.

To turn on 3G networking in the United States with AT&T, follow these steps:

1. In the Settings app, tap Cellular Data.
2. Enter your name, phone number, and the email address at which you want to receive messages about the account. Then, think up a password, select a plan, and enter your credit-card information (**Figure 1**).

Cellular Data Account Cancel

at&t
Your world. Delivered.

User Information

first name	Required
last name	Required
telephone	(555) 123-4567

Login Information

email	Required
password	Required
verify password	Required

Recurring Domestic Plan Options

The selected plan will start immediately. Your credit card will automatically be billed every 30 days, on the date your current plan ends.

250 MB of data for 30 days for \$14.99
2 GB of data for 30 days for \$25.00 ✓

Figure 1: Enter account information, choose a plan, and type in your billing information. (Top part of scrolling screen shown.)

Plans last for 30 days and are automatically renewed unless canceled before the start of the next billing period:

- The \$14.99 plan includes 250 MB of combined downloaded and uploaded data.

- The \$25 plan includes 2 GB of data.

If you run out of data during a 30-day billing cycle, you can purchase an additional 250 MB or 2 GB of usage, which restarts the clock for another 30 days. Unused data in a given 30-day period doesn't roll over into the next month. See [Activate Service](#).

3. Tap Next.
4. A screen showing the terms of service appears. Tap Agree.
5. A summary screen shows your information and your total charges. Tap Submit to proceed.

International rates: You can buy high-priced international data service at this stage or add it later, too. Read [Cross-Border 3G iPad Use](#) for more details.

6. A final screen asks you to wait a few minutes for activation. Tap OK to exit the screen.

A notification appears on screen when the service is active. Tap OK to dismiss it (**Figure 2**).



Figure 2: The iPad alerts you when your 3G service has been activated on the network.

Tip: See [Work with 3G](#) to learn more about 3G connectivity, including how to [Cancel Service](#) if you want to halt an automatic 3G service plan renewal.

In-Depth on Wi-Fi


Wi-Fi works quite simply on the iPad, but there's a lot of hidden detail. In this section, you will learn how to interpret the Wi-Fi Networks screen, handle automatic hotspot connections, manipulate custom network settings, and troubleshoot common problems.

I also explain how to configure a home or small office Wi-Fi network to best take advantage of the iPad's Wi-Fi adapter, which is substantially more advanced than that found in the iPhone or iPod touch.

MANAGING WI-FI CONNECTIONS

The iPad centralizes all its Wi-Fi management into the compact space of the Wi-Fi Networks pane. To reach it, open the Settings app and tap Wi-Fi.

The Wi-Fi Networks pane has three elements:

- The Wi-Fi On/Off switch, which is used to disable and enable the Wi-Fi radio.
- The list of Wi-Fi networks beneath the Choose a Network label. Each entry in the Choose a Network list has three or four elements:
 - ◇ The network name, which is also called the SSID (Service Set Identifier) in some of the geekier base station configuration tools. This is the name that a network uses to *advertise* itself to Wi-Fi adapters that are looking to make a connection.
 - ◇ A lock icon (optional). A lock indicates that there's some form of protection on the network.
 - ◇ A signal strength indicator. The three bars in the indicator are lit up in succession to indicate the strength of the signal being received by the iPad.
 - ◇ A detail  button. Tapping this—carefully, because it's such a tiny target—reveals technical details about the network, as well as an option to forget the network. For more about these

technical details, see [Drilling down to Network Details](#), a few pages ahead.

- The Ask to Join Networks switch, which lets you choose whether to be alerted about networks in the vicinity to which you have not previously connected successfully.

Join a Network

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

User name prompt? *On many corporate and college networks, you are prompted for a user name (typically the first part of your email address or a network login used for file servers) and a password.*

Once you join a network successfully, the network and any associated login information is added to an internal list of networks. Unlike in Mac OS X and Windows, you can't examine this internal list and remove entries. The iPad uses this list to re-join a network whenever you are in range.

Tip: You can remove a stored network's entry only when you're connected to it. See [Forget This Network](#).

Tip: If you set Ask to Join Networks to Off, you won't be informed of any new network in the vicinity when a known network isn't available. However, the list always shows all networks around you.

Auto-Joining a Hotspot Network

The iPad has a clever feature first introduced on the iPhone and iPod touch that lets you choose to remember the login or other details when joining a hotspot network. Hotspot networks, found in cafés, libraries, airports, and beyond, have an open network to which you connect. Many such networks then require that you launch a browser and view a connection page to proceed. The iPad can intercept these connection pages and provide a simpler login or approval screen, but Apple has

never made it clear which hotspot networks are covered, or in what circumstances a hotspot login interception occurs.

For clarity, the details using a hotspot connection page are as follows:

1. In the Settings app, tap Wi-Fi and select the network from the Choose a Network list.
2. After the Wi-Fi signal indicator appears in the upper-left corner of the iPad, press Home and then tap the icon for the Safari app.
3. Most of the time, the previously visited page in Safari will try to load once again; if you have a blank page, enter any site address, like example.com or apple.com, and tap Go.
4. The hotspot network will intercept your Web page request and redirect it to a local login or information page. That page will typically ask that you:
 - 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 to 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 account on a roaming partner.

In each of these cases, Apple may intercept the page and present you with a simplified method of entering any necessary data or approving the connection.


5. After carrying out any of the actions in Step 4, the browser should automatically redirect you to the page you were trying to reach.

The next time you visit a hotspot network that you've previously accessed, the iPad will try to log in using the information you provided. This can lead to problems if that information is no longer valid or the iPad doesn't present it correctly. (The iPad is filling out a Web page and submitting it behind the scenes.)

You can disable joining the network again in this fashion by turning off an Auto-Join option. That option 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.

To turn off Auto-Join, follow these steps:


1. In the Settings app, tap Wi-Fi.
2. In the Choose a Network list, tap the detail  button to the right of the network name.
3. In the configuration screen that appears, switch Auto-Join Off.

iPad Hotspot Access via Boingo Mobile

You have an alternative for hotspot access, especially if you use or want to use a lot of for-fee locations. Boingo Wireless resells access at a flat monthly rate to over 120,000 hotspots worldwide. For mobile devices, the fee is \$7.95 per month with no contract commitment (<http://mobile.boingo.com/>). The service is paired with the free [Boingo Mobile Wi-Fi](#) app, which allows automated connections to the Boingo network. Because Apple doesn't allow programs to run in the background on the iPad, you must launch the app at a hotspot to connect before using the Internet.

Note: Once you've connected to a Wi-Fi hotspot, if you can't send email, look for advice in [Hotspots May Not Send Your Outgoing Email](#), a few pages earlier. See also [Protecting Particular Services](#) for advice on setting up secured email.

Drilling 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, to set up the connection details, go to Settings > Wi-Fi, and then tap the detail  button for the current network (a checkmark is by the listing). The resulting screen has the network name at its top and three or four configuration areas, depending on the network. Let's look at each in turn.

Forget This Network

Tap Forget This Network to remove the network from the list of previously joined Wi-Fi networks. This disconnects your iPad from the

network immediately, and it prevents the iPad from joining the network automatically in the future.

Forget to fix: *Forgetting a network may solve network problems. It seems that forgetting allows the iPad to store new information.*

Auto-Join

Auto-Join appears only for hotspot networks for which the iPad 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 at the top. Tap a button to display the related choices underneath. You should almost never need to change these values except for a particular home or work network configuration. DHCP is the most common.

The Dynamic Host Configuration Protocol lets your iPad request a network address from a router on the network, and then use it to interact on the local network and beyond. When your iPad 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.

The DNS field can be modified or added to; use a comma to separate multiple entries. *DNS* is used to convert human-readable domain names, like www.takecontrolbooks.com, into machine-readable IP addresses, like 216.168.61.41.

You would change the DNS field for two reasons:

- The network to which you're connecting has an internal DNS server, and the necessary network configuration information isn't assigned automatically when the iPad connects to the network. This is most likely to happen with a network run by a large organization.
- It takes a long time for the iPad to "look up" Internet addresses when connecting to the Internet through a particular network. A symptom of long lookups is a frequent, annoyingly long delay before

anything happens after you enter a URL in Safari's address field. If this happens, you can switch to a faster DNS server by using a service such as OpenDNS.

Unfortunately, you can't set DNS globally for the iPad—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.

Tip: OpenDNS (<http://www.opendns.com/>), which has free and low-cost options, can be a fast alternative to an ISP's DNS servers, and it offers some filtering and anti-phishing options.

For certain network configurations that you will never find a public Wi-Fi network, you may need to tap the Static option and enter settings for IP address, subnet mask, router, and DNS manually. Those values would be provided by a system administrator or an ISP. Likewise, BootP is almost never used any more, but a company or academic institution might tell you to use that setting.

The Renew Lease button is specific to DHCP. A *lease* is the assignment of an address by DHCP to your iPad, and leases 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 your connectivity.

HTTP Proxy

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

Disabling Wi-Fi or 3G

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 you want to conserve battery life, turn off Wi-Fi as follows:

1. In the Settings app, tap Wi-Fi.

2. Set the Wi-Fi switch to Off.

Leave Wi-Fi on and Disable 3G

With a 3G iPad, you may want to turn off 3G and leave Wi-Fi on because a 3G radio drains battery life faster than a Wi-Fi radio. You might also want to conserve bandwidth on a 3G plan or be traveling outside your home country. You can disable the 3G radio in two ways, both in the Settings app. Either tap Cellular Data and set the Cellular Data switch to Off (**Figure 3**), or, in the main Settings screen, set Airplane Mode to On. With Airplane Mode on, you can enable Wi-Fi by tapping Wi-Fi and setting the Wi-Fi switch to On. (With Airplane Mode on, you can't enable Cellular Data.) See [Airplane Mode](#) for details.



Figure 3: The Cellular Data switch lets you turn 3G service on or off separately from Wi-Fi networking. Data Roaming affects international use.

WI-FI TROUBLESHOOTING

While Wi-Fi generally works well, you may find circumstances in which you don't get the desired result: a live network connection. Here's some troubleshooting advice for common cases.

Can't See Wi-Fi Networks

If your iPad can't see a Wi-Fi network that you think should be available, it's possible that you are out of range. To solve the problem, move the iPad closer to where you know (or think) a base station is located. Although the iPad has 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.

Of course, it's also possible the base station is in trouble, not the iPad.

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, too, restart the iPad: Press the Sleep/Wake button until you see a red slider for powering down. Slide it, wait until the iPad shuts off, then press the button again.

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 [Connect to a Wi-Fi Hotspot](#), earlier, 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 your 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 detail  button to the right of the network name, and then tap *Forget This Network*. Confirm.

If you're not redirected and Safari throws up a connection error, try the next fix.

Check IP Address Settings

This may sound obscure, but it's an easy way to see if your iPad 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 detail  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 [Drilling down to Network Details](#), earlier in this section.)

If the IP address starts with 169, then your iPad wasn't able to obtain an address from the network. The 169 address range is *self-assigned*, meaning the iPad 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 cause the iPad 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 198 or 10.
- In the main Wi-Fi Networks settings pane, tap the Wi-Fi switch to Off, wait a moment, and tap it back to On. Tap the network name's detail  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 iPad. Press the Sleep/Wake button until a red slider appears. Slide to power off. Wait a moment. Press the button again.

TWEAKING YOUR HOME NETWORK FOR FASTER IPAD PERFORMANCE

The iPad is Apple's first mobile device with 802.11n built in and with support for two different frequency bands: 2.4 gigahertz (GHz) and 5 GHz. The two bands allow greater flexibility: the 2.4 GHz range works over longer distances, but suffers from interference from nearby networks, baby monitors, microwave ovens, and Bluetooth devices. The 5 GHz range is more effective over shorter distances, offering twice the speed or greater on the same device used in 2.4 GHz.

The 2.4 GHz band was the original Wi-Fi spectrum range, and older 802.11b and 802.11g devices (including original AirPort base stations and 2003–2006 AirPort Extreme base stations) can work only with that networking option. The 5 GHz band is used primarily by 802.11n,

but it is also used by an old, still-in-use standard called 802.11a, which is on very few devices.

Note: Oddly, certain early Intel-based Macs secretly included 802.11a. My wife, for instance, has an original series MacBook that connects in 5 GHz over 802.11a.

While you can't configure networks you use out in public to make the iPad work better, you can fix your home network, and you can either change or suggest changes to an office network, depending on who runs it.

Having the choice of these two bands makes it easier for the iPad to move data back and forth at high speeds, such as for streaming media or downloading files directly from the Internet. Your best bet for high performance is to have a 5 GHz network operating. The iPad, like Macs sold since October 2006, will preferentially pick the best network for its location. If an iPad is close to a wireless router, it will choose 5 GHz for speed; if it is farther away, and it can't get a clean 5 GHz connection, it drops to 2.4 GHz to keep the connection active.

Note: The original iPhone, iPhone 3G, and iPhone 3GS use 802.11g networking in 2.4 GHz; the iPhone 4 was upgraded to add 802.11n networking, but also only in the 2.4 GHz band.

You can create a Wi-Fi network that offers simultaneous use of both bands in one of two ways, either of which may require hardware you don't already own:

- Use a simultaneous dual-band router, such as the 2009 or later models of the AirPort Extreme Base Station or Time Capsule. Such routers have two separate radio systems, and can push out signals over 2.4 GHz and 5 GHz at the same time at full speed on each.
- Use two separate base stations, at least one each for 2.4 GHz and 5 GHz. Attach them with Ethernet to form one network. The 2007 and 2008 models of the AirPort Extreme and Time Capsule, and all 2008 and later AirPort Express base stations, offer 802.11n but work on only one band at a time.

For enormously more advice on setting up various Wi-Fi networks, see my book [*Take Control of Your 802.11n AirPort Network*](#).

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 networks requires a little bit of knowledge and planning to avoid roadblocks. This section looks at how to connect an iPad to a network, and any problems you may come across.

Wi-Fi security divides out into three main types:

- **Simple network security:** Since 2003, the best option for a home or small office network is Wi-Fi Protected Access, which comes in WPA and WPA2 flavors. This what's now mainly used, due to Apple and Microsoft improving their operating systems, and wireless router makers improving their devices. See [Connect with WPA/WPA Personal](#) (next page).
- **Corporate/academic security:** Many companies and colleges rely on WPA/WPA2 Enterprise, a stronger method of security that's fully supported on the iPad. Read [Connect with WPA2 Enterprise](#) (p. 31).
- **Outdated, unreliable "security":** This category is where I put Wireless Equivalent Privacy (WEP), a Wi-Fi security method that was broken in 2003, but still is in use. It's also where I put MAC address filtering, in which unique adapter numbers are used to control access. Consult [Wired Equivalent Privacy \(WEP\)](#) (p. 33) and [Mac Address Filtering](#) (p. 35) to learn more.

Of course, I'd prefer you always made a secure connection, but you may not have control over how a network is protected.

Separate security on 3G networks: 3G networks have their own security methods, which are partly based on the Subscriber Identity Module (SIM). The SIM identifies a phone or data device to a network and is used to make sure that an account is active.

Hotspots not hot on security! Public hotspots, whether free or fee, typically have no security at all; if they do, it's a shared password that provides no protection from other people on the network. When you connect to a hotspot, I recommend using only secured services or a virtual private network (VPN) connection. Read [Transfer Data Securely](#) for details on both topics.

CONNECT WITH WPA/WPA2 PERSONAL

The latest and best security method for connecting to a Wi-Fi network is Wi-Fi Protected Access. WPA comes in two “personal” flavors: the original WPA and a later revision called WPA2. Nearly all computer hardware with Wi-Fi sold starting in 2003 supports WPA2, including the iPad, iPhone, and iPod touch.

Impersonal: The complement to Personal is Enterprise, discussed next.

The *Personal* part refers to protecting the network with a password—sometimes called a *passphrase* since it can be comprised of 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 passphrase is set on a base station, and then provided by whomever set it up to anyone who needs permission to connect to the network. If you've set up the network yourself, you're the person who picks the passphrase.

Tip: If you're setting up a base station, pick a good passphrase. The best WPA/WPA2 passphrases should be 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.

WPA2 includes a stronger encryption type, but for ordinary purposes either WPA or WPA2 is fine. If you're working with sensitive material, in the healthcare or financial industry, or if you just want the best security you can get even if there's no risk from the “weaker” flavor,

make sure that your network is configured to use only WPA2's stronger key type, described in the sidebar just ahead.

Apple hides the complexity of key choice and other variables by presenting a simple Password field on the iPad when you select a network protected by any WPA Personal or WPA2 Personal combination. Type the password in, tap Join on the onscreen keyboard, and you're done.

The Keys behind WPA and WPA2

Briefly, the difference between WPA and WPA2 is that the former standard supports a revised basic encryption key type called TKIP (Temporal Key Integrity Protocol); WPA2 includes support for TKIP and a much more advanced key type called AES-CCMP (Advanced Encryption System...and you don't want to know what CCMP stands for).

Some routers ask you to select between TKIP and AES or both; others show WPA, WPA/WPA2, and WPA2, but mean TKIP only, TKIP or AES, or AES only.

Apple's 2007-and-later base stations default to offering a choice of WPA/WPA2 Personal, which allows a computer or device to connect by offering either a TKIP or AES version of the network's password, or WPA2 Personal, which requires an AES transaction.

CONNECT WITH WPA2 ENTERPRISE

There are stronger ways to secure a network, and if you use your iPad in corporate or academic settings, you will likely encounter *WPA2 Enterprise*. WPA2 Enterprise is an instance of 802.1X *port-based authentication*, which can be used with Ethernet and older Wi-Fi standards, too. All the flavors of 802.1X let you connect in a limited fashion to a network; this controlled connection only allows you to send your login details. Only when those details are confirmed does an 802.1X system give you access to the full network.

WPA Enterprise missing? *While WPA Enterprise is still in use, any organization that cares enough about its security to use this option will have upgraded to WPA2 unless they have specific older computers or devices for which backward compatibility is needed.*

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

Tip: Mac OS X Server (10.5 and later) includes full support for setting up WPA2 Enterprise even on the smallest network. The server can be elsewhere on the Internet, too; it doesn't have to be on the same network as the base station.

User Name and Password Login

In the simplest setup, to connect your iPad to a WPA2 Enterprise network, you must enter a user name and a password provided by the network administrator or IT department. 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 user name 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 on the iPad.

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.*

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 user name and login because the certificate can't be written down on a sticky note or extracted in some fashion. An IT worker would

create and provide you with a certificate used for WPA2 Enterprise and usually install it for you.

The iPad can receive a certificate via email, and install it when you tap it as an attachment. However, that might be too much of a security risk. Instead of using email, the IT department could use the iPhone Configuration Utility (<http://support.apple.com/kb/DL851>). This free tool is available for Mac OS X and Windows, and it allows an administrator to create connection and other profiles and install them directly on any iPhone OS or iOS device.

Note: To learn about configuring a network with the best security for your situation, consult my two related books, *Take Control of Wi-Fi Security* and *Take Control of Your 802.11n AirPort Network*.

OUTDATED METHODS

This topic explains how to connect with out-of-date or ineffective security methods that are still, unfortunately, in relatively wide use. If you're using them, please consider upgrading to WPA/WPA2 Personal.

Wired Equivalent Privacy (WEP)

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—WEP has been used as the basis for criminal prosecution in some places when a network's been broken into. The other reason you might see WEP is that Mac OS X's built-in software base station (accessible in the Sharing system preference pane as the Internet Sharing service) allows encrypted connections using only WEP. This is a shame, and Apple has been urged to add WPA to Internet Sharing for several years.

Why share? *You might wind up using a Mac as a Wi-Fi base station if that Mac connects to the Internet with a 3G modem.*

Note: WEP can be set with either a 40-bit key (older systems were limited to this) or a 128-bit key. The longer key doesn't provide any greater protection against key-breaking systems developed in the last couple of years.

A problem with WEP can be determining the password. WEP passwords come in three varieties, but the iPad (and all iPhone OS and iOS devices) allow entry only in *hexadecimal*, the base 16 numbering system. In hexadecimal, numbers from 0 to 15 are represented by digits for 0 to 9 and the letters A to F for 10 through 15. A "hex" WEP password must be either 10 or 26 hex numbers long, which correspond to the two forms of WEP encryption (40 bit and 128 bit). Type such a password into the Password field when joining a network. If the person supplying the password isn't clued in, you might instead be dealing with a password in one of two text formats, plain WEP ASCII and Apple's special text format, both of which I explain how to convert.

Standard WEP ASCII

An ASCII WEP password uses plain text characters only (typically only upper- and lowercase letters along with numerals), and it can be either 5 or 13 characters long. ASCII passwords can be converted directly into hexadecimal. For instance, the password **SOFas** (mixed upper and lowercase letters) is translated into five hex numbers as **534F466173**.

You can convert an ASCII password into hex by visiting this site: <http://www.wifizard.com/wi-fi/convert.htm>. If you are uncomfortable typing your Wi-Fi password into a Web site, you can also look up each ASCII hex value for each character at <http://www.asciitable.com/>.

Apple's Text to Hex

The Apple text-to-hex password style requires an Apple-specific conversion of regular text, which can be any length, into a hex key used internally by Mac OS X and Apple base stations. It requires a more elaborate method than the standard WEP ASCII password to obtain in hex format. You can extract an Apple WEP key created in this fashion using Airport utility.

Tip: On the Mac, Airport Utility is in the [Applications/Utilities/](#) folder. For Windows, download and install the free program from <http://www.apple.com/downloads/macosx/apple/windows/>.

To extract the hex key from any Apple base station, follow these steps or provide them to the person who has configured the base station:

1. Launch AirPort Utility.
2. Select your base station.
3. Choose Base Station > Equivalent Network Password.

A dialog appears from which you can write down or copy the contents (**Figure 4**).



Figure 4: The Network Equivalent Password dialog gives you the hex key value of a text network key.

MAC Address Filtering

The second outdated security method that's still in use is *MAC address filtering*. MAC in this case means *Medium Access Control*, a technical term for the hardware in a network adapter used to pack and unpack data. The MAC address is a unique number assigned by companies to every piece of equipment shipped. This unique address is used to label data packets as they move around a local network.

Note: While there are ways to change a MAC address from the value the company shipped, that's rarely necessary, and typically causes more problems than it could ever be worth.

MAC address filtering allows a router to restrict access only to devices for which a MAC address has been entered. Many routers, including all of Apple's gear, support this option. MAC address filtering is easy to overcome. If a network is password protected, then MAC address filtering isn't necessary. If a network has no password protection, a mildly interested cracker using free software can *sniff* data passing

over the network, extract an allowed MAC address, and change the MAC address on his or her Wi-Fi adapter to the allowed address.

However, some networks use filtering as yet another deterrent and as yet another “no trespassing” sign. To join such a network, you must find the iPad’s Wi-Fi MAC address and enter it into the network’s configuration. Tap Settings > General > About, and look for Wi-Fi Address (**Figure 5**). Write it down; you can’t copy and paste.

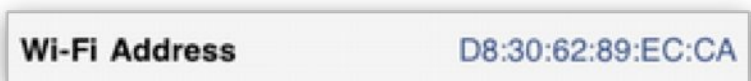


Figure 5: The Wi-Fi Address is the MAC address of the Wi-Fi adapter built into your iPad.

You can easily set up MAC address filtering on an Apple base station. Launch AirPort Utility, select the base station, and click Manual Setup. In the Access Control view, choose Timed Access. Enter as many MAC addresses as you like, and limit access by day of week and time of day (**Figure 6**).

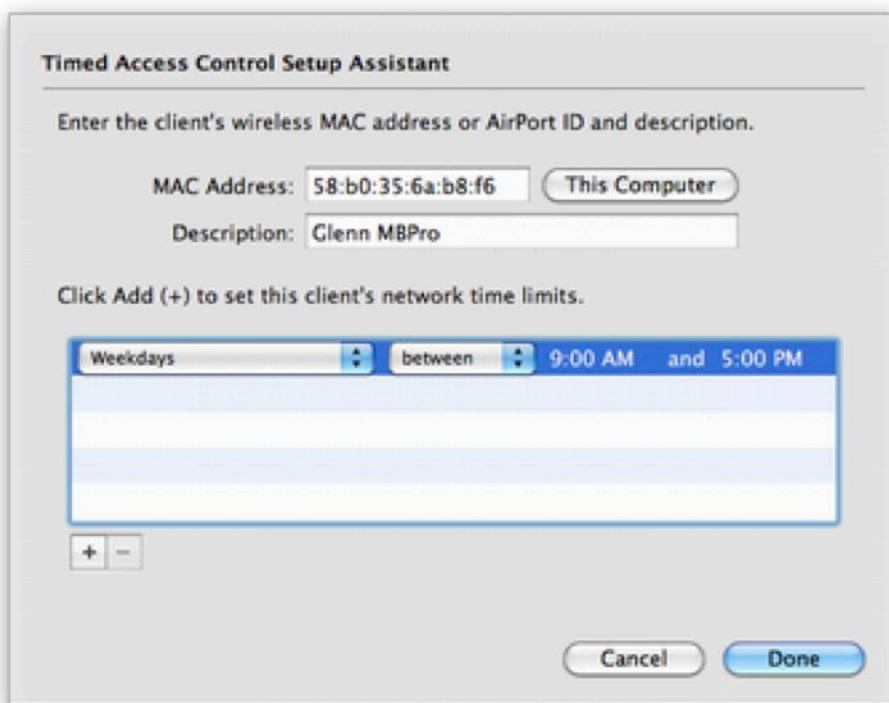


Figure 6: AirPort Utility lets you set which MAC addresses may access the network, and, optionally, when they are allowed.

Closed Networks Provide No Additional Security

You might notice that I don't mention *closed networks* here, networks that are set to not broadcast their names; I describe how to connect to them in [Connect to a Closed Network](#).

The reason is that a closed network doesn't prevent someone from finding out the network name as soon as any device that knows the name accesses the network. A closed network gives no proof of its existence until such a device connects, but it's far harder to connect to than a named network.

It's better to use robust encryption than to make the network difficult to find.

Work with 3G

The iPad with 3G is an odd beast. It can connect to 2G and 3G mobile broadband networks in order to access the Internet, but it doesn't have cellular voice calling built in. The 3G iPad can connect to the Internet with Wi-Fi instead of with a mobile broadband network, but you can sign up for a mobile plan if you need ubiquitous Internet access.

Because every 3G iPad has both Wi-Fi and 3G capabilities, you're often balancing the advantages of one versus the other. Let's look at the choices you can make and how to set them up.

At the end of this section, I discuss [Alternatives to Built-in 3G](#) (p. 56), to help you extend 3G service to any iPad, regardless of whether it has a 3G radio or an active 3G plan.

WHY USE 3G

If you bought a 3G iPad, you have already made the decision that ubiquitous Internet access is useful enough to warrant paying a higher price for the device. Or, perhaps, you wanted the GPS receiver that's in the 3G iPad and thought you might occasionally want mobile broadband access.

The primary reason to pay extra for a 3G iPad is flexibility. If you believe you'll use the iPad mainly within range of free Wi-Fi or Wi-Fi you've subscribed to, then you likely don't need the 3G iPad. But if you will travel with the iPad, and prefer to have access everywhere, whether in a park, hotel, conference center, airport, or restaurant, or as a passenger in a car, the 3G option makes sense. Using 3G, the iPad can transfer data at a raw rate up to 7.2 Mbps from the Internet, and up to 384 Kbps to the Internet.

Exactly how fast? For a description of data rates, see [Table 1](#), which explains indicators (p. 53).

Although you can purchase a subscription to nearly all travel-related Wi-Fi worldwide for \$7.95 per month from Boingo Wireless (<http://boingo.com/>), that may not cover every venue you visit, especially less conventional venues, such as hotel chains that don't deals with Boingo.

The additional flexibility with the 3G iPad is that you pay for cellular service only when you need it. If you travel extensively for a few months of the year, and are locked in a home-work-coffeeshop routine where there's free Wi-Fi the rest of the time, then you need only enable 3G service when you're on the road.

Warning! *Neither Apple nor your cellular service will remind you to cancel your service if you don't need it in a subsequent month. I recommend setting a recurring calendar reminder a week or more before the end of your current 30-day billing cycle to remind yourself to consider whether or not you need the service the following month. There's no penalty to cancel and sign up again.*

HOW TO USE 3G

The 3G iPad comes with Wi-Fi turned on, like an iPod touch, but 3G data service is inactive. In most countries where the 3G iPad is sold, you can sign up for 3G service at any time by choosing among multiple service plans from one or more carriers. Plans can range from 1 day to 31 days. The 30- and 31-day plans include an automatic renewal.

In the UK, for instance, three carriers offer iPad service. You can buy a 3G iPad from Apple, and then activate on one of the three networks, and later swap to another network. You must change out the micro-SIM card to change carriers, but you're not otherwise tied to a carrier, except in Japan.

You can cancel at any time without penalty, with the cancellation taking effect when you hit your data limit or at the end of the current billing period, whichever comes first. The one exception so far is SoftBank in Japan, which offers either a 1 GB plan for a 30-day period, or a 2-year contract for "unlimited" usage with cancellation fees.

A month may be 30 days: Depending on the carrier with which you sign up for 3G service, a “month” may be from the same day of the month in one month to one day before that day in the next (March 5th to April 4th, for instance). In other cases, a “month” is defined as 30 days. AT&T uses a 30-day billing cycle, and is fairly consistent about using that terminology.

AT&T also offers an option to change plans in the middle of a billing cycle; that option appears to be unique to AT&T among announced plans at this writing.

Most carriers have an automatic monthly renewal, and several allow additional units of bandwidth (to be used over 30 or 31 days) or time (a day or a week with a bandwidth limit) to be purchased if you run out of data.

Always Available

While you must sign up for a plan and pay for it before you can send and receive data over a cellular network, the 3G iPad is always searching for a live network signal if the 3G radio is active. The signal strength indicator and carrier name always appear in the upper left when a cell network is available whether or not you have an active plan (**Figure 7**). (You can turn off the 3G radio to save battery life when you’re not looking to sign up; see [Leave Wi-Fi on and Disable 3G](#).)



Figure 7: The 3G network connection is active and scanning for networks regardless of whether you have an active plan.

As long as your carrier’s name is shown and there’s a bar or more of service, you can sign up. Apple doesn’t require that your iPad be connected to a Wi-Fi network when you sign up for cellular data service. I believe that Apple’s lack of a Wi-Fi connection requirement is unique—and it’s certainly handy; you could be at an airport or hotel, find that the Wi-Fi service is expensive or unavailable, and activate 3G service on the spot.

Pick a Plan

AT&T announced its 3G iPad connection plans for U.S. customers first, and we've had some time to digest the original service offerings along with a set of changes that came just a few weeks later. In May 2010, carriers in Australia, Europe, and Japan announced pricing plans, and many more are on the way.

Let's look at what's available.

United States

The two contract options from AT&T are:

- 250 MB of combined upstream and downstream usage for a 30-day period, costing \$14.99 per period.
- 2 GB of usage for \$25 for a 30-day period.

Formerly unlimited: *Until June 7, 2010, AT&T offered a truly unlimited 3G plan for the iPad for \$29.99 per month. If you signed up for such a plan before that date and don't cancel it, you can continue using unlimited data. The unlimited plan is no longer available for new subscribers.*

If you exhaust the data in the plan level you've chosen before 30 days is up, you can sign up for a new 250 MB or 2 GB plan, pay the fee for that level, and start a new 30-day billing cycle.

Australia, Europe, and Japan

Outside the United States, plans are more baroque, with all kinds of varied options, terms, exclusions, and pricing. The most important factor is that, like AT&T, all carriers limit usage after a preset point. Once you use the included bandwidth, the carrier either freezes your data usage or—in the case of an “unlimited” plan—throttles it to 64 Kbps for the remainder of the day (for daily limit plans) or of the 30- or 31-day billing cycle.

The plans break down into five categories:

- **Daily or weekly on-demand plans:** A few mobile operators are offering daily and weekly rates. Orange in Spain and O2 in the UK charge €2 and £2 per day, respectively, for up to 500 MB in usage. Orange has a £7.50 per week plan that covers usage up to 1 GB during that period.

- **Low-bandwidth auto-renew monthly plans:** Carriers are generally offering a low-bandwidth plan of 200 MB to 500 MB for rates close to AT&T's in the United States, although several charge more. For instance, Vodafone in Germany offers 200 MB for use within a month for €19.95 (about US\$25).
- **High-bandwidth auto-renew monthly plans:** Most carriers offer high-capacity plans that includes from 1 GB to 10 GB, and cost about \$30 to \$45 (in U.S. dollars) per month. Vodafone in Australia offers the only unlimited monthly plan in the world following AT&T cancellation of its unlimited option; it costs Au\$49.95 (US\$42).
- **Longer duration plans with fixed data:** Vodafone in Australia appears to be the only carrier offering this interesting option, which provides a data allotment that expires long beyond a month. Its two plans are Au\$100 for 6 GB to be used within 180 days, and Au\$150 for 12 GB used within 365 days. That's tremendously flexible.
- **Service contract plans:** SoftBank in Japan is the only carrier so far to announce a discounted data contract that requires a 2-year commitment with cancellation penalty.

A few carriers include Wi-Fi hotspots in their service plans. Orange's UK Wi-Fi is limited to a separate pool of 750 MB per month distinct from its far higher 3G limits, as the company relies on a partner network; in continental Europe, though, Orange's French service includes what's described as "unlimited Wi-Fi" without any footnotes.

European carriers typically list restrictions for what you can do with 3G. Many bar the use of VoIP, peer-to-peer file sharing (which I don't know of a way to do with an iPad), and odd things like instant messaging and newsgroups. Read the fine print.

Tip: Usually, an iPad is sold *unlocked*, meaning it can use a micro-SIM from any carrier in any country. Apple is selling the 3G iPad without activation in some nations, and even if you buy an iPad from a carrier, you can opt to switch to another carrier's plan by swapping in a micro-SIM from the new carrier.

But not in Japan! *If you buy a 3G iPad in Japan, whether from Apple or from data carrier SoftBank, your iPad will be locked to SoftBank while it is in Japan. However, you can take the iPad to another country and use a different micro-SIM in it. It's unclear whether or not you can use an unlocked 3G iPad in Japan with a micro-SIM from a Japanese carrier other than Softbank.*

Consider Your Likely Usage

Unless you sign up for Vodafone's Australia unlimited plan, or some other truly unlimited plan that has yet to be announced, you need to match your likely Internet usage to your plan, while considering your budget, of course. You should look at what you think your typical activities will involve. If you plan to use email, surf the Web, and use apps that consume relatively little bandwidth when you're not connected via Wi-Fi, a lower-use plan may suffice. The flexibility of upgrading in the middle of a billing cycle to another chunk of data (most countries), or switching to unlimited (Vodafone in Australia) removes a lot of sting.

On my iPhone, I average about 100 MB per month, which surprised me since I thought I was a heavy user; but it turns out that most of that use is over Wi-Fi at my home or office. And I certainly wasn't streaming video to the iPhone. A single hour of streaming Netflix video over 3G could chew up 250 MB of usage. That's an expensive hour.

Note: Video services have to throttle streaming rates over 3G to reduce network usage. Netflix's 250 MB per hour rate is, apparently, the throttled rate! It pulls down even more data over Wi-Fi, if the bandwidth is available.

Further, comparison between apps carrying out identical tasks on an iPhone and 3G iPad shows two to six times the data consumed. The reason? The iPad's bigger screen allows larger photos and more information. A full-screen image on the iPad has more than five times the pixels of a full-screen iPhone or iPod touch image.

As you decide which plan makes the most sense for you, skip ahead a few pages to [Keeping Usage Restrained](#), to see how well that advice might apply to your situation.

Activate Service

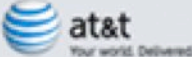
When you power up a 3G iPad in an area covered by your carrier, the device shows a signal-strength indicator and the carrier name in the upper left. As long as you have a bar of access and your carrier's name is shown, you can pay for and activate cellular data access.

Warning! *The specifics of the following steps will almost certainly be different outside the United States.*

Follow these steps to activate service:

1. In Settings, tap Cellular Data.
2. Tap the View Account button to open the Cellular Data Account screen (**Figure 8**).

Cellular Data Account Cancel

 **at&t**
Your world. Delivered.

User Information

first name	Required
last name	Required
telephone	(555) 123-4567

Login Information

email	Required
password	Required
verify password	Required

Recurring Domestic Plan Options

The selected plan will start immediately. Your credit card will automatically be billed every 30 days, on the date your current plan ends.

250 MB of data for 30 days for \$14.99
2 GB of data for 30 days for \$25.00 ✓

Figure 8: The long setup screen lets you enter all the information needed to activate 3G service. Just a portion is shown here.

No Cellular Data Account screen? *If this screen doesn't appear when you tap View Account, press the Home button and launch Settings again.*

3. You have to set up a new account with AT&T. The sign up screen covers two pages, which you have to scroll to see all the details in. The page is divided into four sets of options:

- **User Information:** Enter your name (first and last) and the phone number you want associated with this service plan.

Not part of other AT&T accounts: *AT&T doesn't offer the iPad service plan as an add-on to an existing AT&T account, so you can enter any phone number you use.*

- **Login Information:** You have to create an account here that uses your email address (where you'll receive any notifications from AT&T) and a password you create.

Password recovery: *If you forget your password, you can recover it via email.*

- **Recurring Domestic Plan Options:** Here's where you pick the 250 MB limited plan or the 2 GB plan. Apple kindly sets the 2 GB plan to be selected by default.
- **Payment & Billing Information:** Hand over the goods here using either a Visa, MasterCard, Discover, or American Express card, and the associated billing address.

Because some people have a credit-card bill sent to a P.O. box, or to an address that may be outside AT&T's coverage area, there's a separate Service Address area: tap Use a Different Service Address to reveal it below the credit-card address area. You can provide a street address representing your home or work. (This option was added after launch after complaints.)

Pay in advance by plastic: *You can't pay without a credit-card number, and payment is in advance of the use of services. A prepaid option to load value on a micro-SIM may appear later from AT&T or other carriers.*

4. Tap Next to proceed.
5. The carrier agreement from AT&T appears. Tap Agree to proceed.
6. The summary screen has a brief reprise of your information and what you're agreeing to (**Figure 9**); tap Back if anything's wrong. It also lets you add an international data plan, which I discuss later in this section, in [International Plans](#). Tap Submit to proceed.

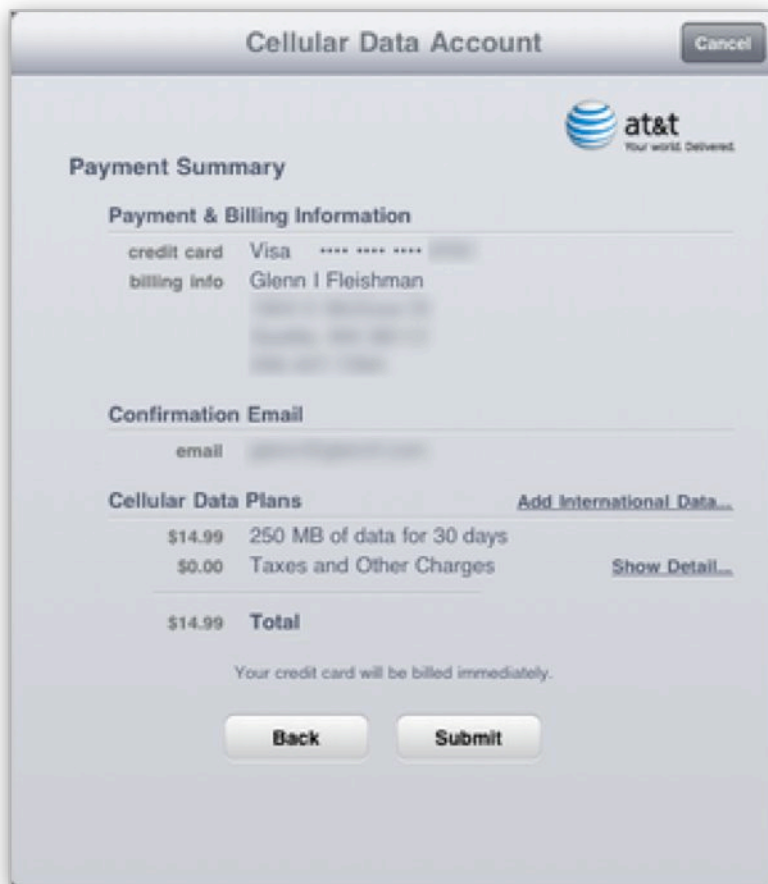


Figure 9: The summary screen lets you review what you've chosen and your billing information. You can tap Back to change details.

7. The final screen tells you that it might be a few minutes before 3G service is activated. Tap OK to dismiss.

After a few minutes, more or less, a notification comes up in the push style (it appears regardless of whether you have push notifications set on or off) and confirms your account is active (**Figure 11**).



Figure 10: Confirmation appears that your cellular service has been turned on.

If you receive no notification: Log back in to your account by tapping *View Account* to see if the account is actually active. If it shows up as negative there, call AT&T's customer support.

AT&T automatically connects 3G iPads to Wi-Fi: If you're currently paying AT&T for a 3G data plan, your iPad will automatically connect to any AT&T Wi-Fi network within range, even if there's 3G service available. AT&T includes Wi-Fi access at its over 21,000 hotspots as part of its paid iPad 3G service.

Switch Plans or Extend Service

AT&T offers a few options that you can choose to take effect at the end of the current 30-day period or when you run out of data on either the 250 MB or 2 GB plan within the 30-day period, whichever comes first:

- If you are already on a capped plan, you can add an extra 250 MB or 2 GB of data (depending on your plan), which resets your billing period to a new 30-day period that begins when you start using the extra data. However, if you don't use any of the extra data in the current 30-day period, then billing continues normally.
- Switch to a different plan. The change takes effect at the end of your current 30-day cycle or when you run out of data in the current cycle, whichever comes first. If you have an unlimited plan, you can switch to a capped plan.
- If you had an active unlimited service plan in effect on June 7, 2010, and you have auto-renew set, it will continue to renew indefinitely. However, if you cancel unlimited service and don't sign back up for

unlimited service before the end of a 30-day period, you will never have the option for this plan again.

Here's how to extend or change your service:

1. Launch Settings and tap Cellular Data.
2. Tap View Account.
3. Enter your password and tap Next.
4. Tap Add Data or Change Plan.

The screen that appears lets you know how many days are left in the current plan (if any), and it explains when the next plan starts and you're billed. It also shows your options for adding data or changing your plan (**Figure 11**).



Figure 11: With a plan active, you see your options for adding data or changing plans. Your options depend on your current plan, so you may see slightly different wording or not see the third option.

In this figure, you can see that I am currently signed up for AT&T's now-discontinued unlimited plan. Because the plan is active, I can opt to renew. Otherwise, I can switch to either of the two capped bandwidth options. After I switch (or fail to renew), however, there's no going back to unlimited, and that option disappears.

5. Tap a plan option.
6. Tap Agree to submit to AT&T's usage terms.
7. A summary screen shows the charges. Tap Submit. Your card is charged immediately, even if the next cycle is weeks away.
8. The final screen displays a confirmation message; tap OK to close it.

Final Screen Confusion

The message on the final screen doesn't match precisely with what you previously selected, but it makes sense.

When I upgraded from a 250 MB plan to the no-longer-available unlimited plan, the final screen said, "You have successfully re-established an auto-renew plan on your account. Your renewal date is [end of my current billing cycle]." At first glance, you might say, "whu-uh-uh?" But it's consistent: AT&T is saying that your change is in effect as expected at the end of the current billing cycle. It could be more clear!

If you sign up for the 250 MB plan and use less than 500 MB in any 35-day period, you come out nearly ahead of the 2 GB plan. As long as you don't wind up paying more than about \$30 over 35 days, then you might string along 250 MB units to keep costs lower.

Cancel Service

When you cancel service, you can either cancel immediately or at the end of your service plan; the end is at the completion of a 30-day billing cycle or earlier if you run out of data sooner. Thus, cancel can mean either "cancel immediately" or "stop automatically renewing my plan."

To cancel your service, follow these steps:

1. Launch Settings and tap Cellular Data.
2. Tap View Account.
3. Enter your password and tap Next.
4. Tap Add Data or Change Plan.
5. Tap Cancel Plan, which actually disables automatic renewal.
6. You have two options, which control whether your credit-card and address information remain stored for the short term:
 - **Cancel Plan and Delete Account Now:** This deletes your account, which immediately prevents your iPad from using the 3G network. You must create a new account to sign up for service again.

Warning! *If you cancel and delete your account "now" any unused portion of the plan is lost; there are no pro rata refunds.*

- **Cancel Plan and Delete Account Later:** With this option, your account is maintained for 60 days following the end of services, which lets you resume service using the same account information, including the billing information.

There's *no penalty* for canceling whenever you want, and then re-starting service even moments after the cancellation ends. This is part of what makes AT&T's iPad 3G service so flexible.

Keeping Usage Restrained

The difference on AT&T's plans between 250 MB and 2 GB is about \$120 per year, if you keep a plan active every month; the difference in Australia between Vodafone's 250 MB and unlimited plan is Au\$40 per month! And the difference can be the same or more between a low-usage and high-usage plan on other carriers—and you still face caps on usage even if you choose a 1 GB to 10 GB plan.

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

Turn Cellular Data on Only When You Need It

In the Settings app, tap Cellular Data, and then set the Cellular Data switch to Off. Reverse that to On when you need it. For more details, see [Choose to Use 3G or Wi-Fi](#), ahead a few pages.

Limit Your Activities When Using the Cell Network

Unless you are using Wi-Fi, limit your activities to checking email and Web pages. Don't use video or audio streaming programs (YouTube, Netflix, and others), or programs that load large amounts of image data, such as the Maps app, or navigation programs that load maps live over the Internet as you move about. Don't update apps via the App Store, either.

Warning! *Loading part of two views in Maps consumed 1.4 MB in my testing.*

Disable Push and Fetch

In Settings, tap Mail, Contacts, Calendars > Fetch New Data. Set Push to Off and Fetch to Manually. This disables server-to-iPad (push) and iPad-from-server (fetch) automatic retrieval of messages, event

updates, and contact changes. You can run through megabytes of data a day by leaving these on.

Warning! *Disabling Push and Fetch prevents Find My iPad from working. See [Find My iPad via MobileMe](#).*

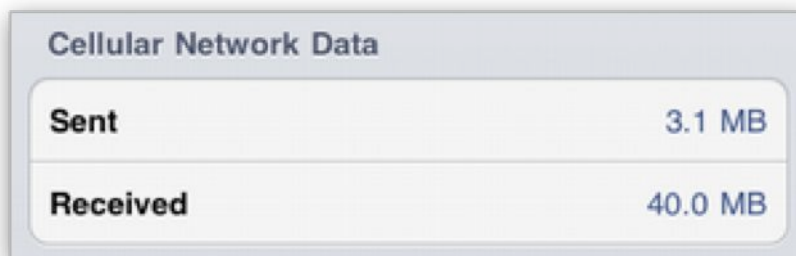
Find Free Wi-Fi

There's an increasingly large amount of free Wi-Fi around North America, and in some countries in Europe. In the United States, all 12,000 McDonald's outlets with Wi-Fi charge nothing, and a number of airports (including Seattle-Tacoma and Denver) have free service. Starting on July 1, 2010, Starbucks will offer free Wi-Fi service in all its company-owned stores in the United States, which number about 7,000. Libraries often offer free Wi-Fi.

See my *TidBITS* article, "Find Free and Inexpensive Wi-Fi," for more advice: <http://db.tidbits.com/article/10872>.)

Check Data Usage Regularly

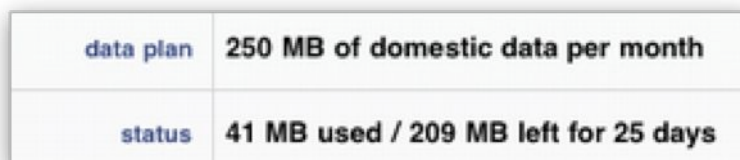
In Settings, you can tap General > Usage to see the current up and down transfer numbers (**Figure 12**); add them together for the total.



Cellular Network Data	
Sent	3.1 MB
Received	40.0 MB

Figure 12: These numbers capture how much data the iPad has registered that you've used.

To check your carrier's count of usage, log in at Settings > Cellular Data > View Account. These numbers (**Figure 13**) tend to lag 30 to 60 minutes behind actual usage.



data plan	250 MB of domestic data per month
status	41 MB used / 209 MB left for 25 days

Figure 13: Your carrier may show a different number, which lags an iPad's own internal count.

You Were Warned

Your iPad warns you as you start running out of data in your plan. These warnings are intended to come at 20 percent left (50 MB), 10 percent (25 MB) left, and none left. However, if you're burning through data quickly, a message may appear after one of those intended marks has been reached (**Figure 14**).

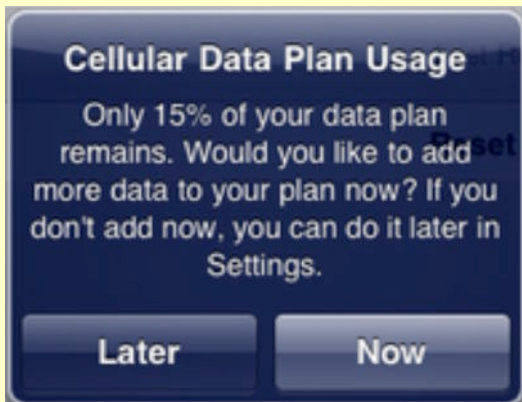


Figure 14: A warning tells you when you're nearly out of data.






CHOOSE TO USE 3G OR WI-FI

There are good reasons to pay attention to whether your iPad is accessing the Internet via a Wi-Fi network or mobile broadband. You may need greater bandwidth than the available cellular network can provide, you could be budgeting data on a low-bandwidth plan, or you might be outside your home carrier territory and want to keep usage low. Whatever the reason, Apple provides several tools and controls to help you know what network you're on, and you can set the type of network to which the iPad connects.

Which Network Are You On?

The iPad has an indicator in the status bar (near the upper left) that shows which network connection is active. See **Table 1** for an explanation of these indicators.

Table 1: Deciphering Indicator Icons

Icon	Explanation	Bandwidth
	The iPad can't connect to any network.	N/A
	The iPad is connected to a Wi-Fi network. The number of white waves, from one (shown as a small dot) to three, indicates relative signal strength from weakest to strongest.	A maximum of 30 to 40 Mbps, but it's limited by the broadband connection
	Connected via 3G (either 3.6 Mbps or 7.2 Mbps).	Downstream rates up to 1.7 Mbps on "3.6" network, 4 Mbps on "7.2" network*; upstream, only up to 384 Kbps
	Connected via EDGE, a 2.5G standard.	Roughly 200 Kbps
	Connected via GPRS, a 2G standard.	Roughly 40 Kbps
* AT&T hasn't yet enabled all the pieces needed to offer 7.2 Mbps speeds in most of the United States. Many carriers in other countries operate networks at 7.2, 14, and 21 Mbps, with backward compatibility for 7.2 Mbps. The iPad works at a maximum of 7.2 Mbps.		

Select Which Service to Use

You can force an iPad 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 the iPad doesn't offer network profiles as in Mac OS X, which would make it easy to switch configurations, you must use the Settings app to enable or disable a service.

To enable or disable 3G service:

- To use a 3G cellular connection solely and avoid Wi-Fi, perhaps to keep a continuous VPN connection or for security reasons, in the Settings app, tap Wi-Fi, then set the Wi-Fi switch to Off.

Avoid a flaky Wi-Fi network: *If a Wi-Fi network is acting flaky, you can switch to use 3G only to avoid the problem or use the method noted in [Forget This Network](#) to forget the network.*

- To rely only on Wi-Fi, accepting that you will have times in which you have no Internet connectivity, tap the Cellular Data item in Settings, then set Cellular Data to Off.

Keep usage low on a low-usage plan: *The option to switch off cellular data is marvelous when you've chosen a service plan with a relatively modest amount of data usage because it lets you parcel out when you use cellular networks. See [Keeping Usage Restrained](#), a few pages earlier.*

CROSS-BORDER 3G IPAD USE

The 3G iPad has a distinct advantage over any iPhone when you roam outside of your home country or service area. You can't accidentally run up huge international roaming fees.

Away from home: *"International" is often used erroneously to refer to "not in the United States." Here, I'm talking about using a mobile data service while you are outside the "home" country for your iPad.*

The iPad's sibling, the iPhone, is currently sold in the United States only on a *postpaid* service basis. Postpaid plans paradoxically require that you pay for basic service each month before you receive that service, but pay after the fact (the *post* part) for overages, such as extra voice minutes or, in some countries, extra data usage.

Prepaid plans let you use service only up to the level for which you have already paid. Beyond that, your service no longer works and you aren't charged. That's how most iPad plans work around the world, including AT&T's two service options.

The 3G iPad adds another level of safety on top of prepaid service: international roaming isn't automatically turned on. Horror stories of bills of thousands of dollars came not long after the iPhone appeared, when people took an active iPhone outside the United States and used its data connection. AT&T happily charged customers without warning them that such charges would be forthcoming.

Apple updated the iPhone OS to provide the Data Roaming switch which, when set to Off (the default when you first get an iPad), disables roaming outside the area covered by your carrier's service plan. But for

the 3G iPad, the Data Roaming switch makes a difference only when you've prepaid for an international plan and don't want to consume data from that plan accidentally.

Let's look at two options to roam outside your home country.

International Plans

For its U.S.-based customers, AT&T offers four 30-day usage packages with different amounts of data for use with a host of partner mobile networks around the world. You can access these plans by logging in at Settings > Cellular Data > View Account.

Warning! *Plans must be activated before leaving the United States.*

The rates are insanely high—at least, insane for anywhere but the cellular industry. Despite in-country rates in many places similar to AT&T's, AT&T's plans are \$24.99 for 20 MB, \$59.99 for 50 MB, \$119.99 for 100 MB, or \$199.99 for 200 MB—nearly 17 times more per megabyte than the 250 MB plan AT&T offers domestically. Data must be used within 30 days of activation, and you can set activation for a future date starting at midnight eastern time. There's no refund or rollover for unused data.

Plans for service in Europe, Japan, and elsewhere for when you're outside your home country haven't yet been provided as this book goes into production.

Get an Alternative SIM

It's possible that some carriers will offer prepaid micro-SIM cards with preset amounts of data at rates vastly below AT&T's roaming rates.

The first announced competitive offering is from MAXroam, a voice and data roaming firm that has deals with hundreds of cellular and wireline telephone operators (<http://www.maxroam.com/>). MAXroam will sell you a micro-SIM for roaming in Europe with a 3G iPad for €75 that includes 50 MB of usage with no expiration. More units of 10 MB are €25 and 50 MB are €75. This pricing isn't good, however, except for the lack of expiration date. AT&T's international roaming service costs about 40 percent less, but data must be used with 30 days.

You can also look into whether a friend or colleague in a country you're visiting would rent or loan you a micro-SIM.

ALTERNATIVES TO BUILT-IN 3G

While having 3G built into an iPad can be convenient, there are other options for 3G access. These options are helpful if you're not near a free or sufficiently affordable Wi-Fi hotspot.

Mostly United States: *The alternatives below aren't only available in the United States, but the details are specific to each country, and thus the advice is only generally applicable outside the United States.*

These options require that you sign up with a carrier other than AT&T and carry at least one more piece of equipment. Each option lets you connect multiple devices—including any iPad—over Wi-Fi to a laptop, mobile phone, or portable cellular router. The advantage of these options is that you can provide 3G access to multiple devices while paying a single fee. See **Table 2** for a quick comparison of options.

Table 2: 3G iPad Cellular Alternatives		
Method	How It Works	Tradeoffs
Broadband Modem in a Laptop	Buy 3G laptop service from a carrier, plug a modem into a laptop, and share the service with an iPad and other devices.	Most require 2-year contract; must carry laptop around; prepaid usage capped at 5 GB/month.
Cellular Router	Buy the router from a carrier, share with nearby devices.	Compact, but most require 2-year contract; prepaid usage capped at 5 GB/month.
Phone as Portable Hotspot	The phone acts like a cell router.	Verizon is the only U.S. provider to offer, via a couple of Palm Pro models; cost is very low, usage uncapped.
Phone Tethering	Via USB or Bluetooth, use your phone as a broadband modem.	The iPad can't connect via a tethered device.
Alternative Domestic Carrier	Use a micro-SIM from another carrier.	Competition has yet to emerge.

Broadband Modem in a Laptop

I list this first because it's straightforward, but I have a hard time imagining firing up a laptop in order to drive an iPad. I suspect that you'll carry such devices separately for different purposes; or use one in a workgroup in which different people have devices and a laptop with a broadband modem acts as the hub. This would also work for a family traveling together.

All four U.S. carriers and many outside the United States offer direct Mac OS X support for a variety of ExpressCard and USB broadband modems.

You can use a 3G modem as a conduit to the Internet for devices with Wi-Fi by sharing the connection from a laptop. You plug the 3G modem into the laptop, and connect it to the cellular network using the modem's driver software. Then you share the laptop's 3G connection to the Internet over Wi-Fi. If your laptop is a Macintosh, open the Sharing system preference pane and set up the Internet Sharing service. If your laptop is running Windows XP, Vista, or 7, set up Internet Connection Sharing.

Tip: Nova Media's launch2net Premium automates turning a Mac into a 3G gateway; the software includes drivers for most popular USB modems (<http://www.novamedia.de/en/mac-launch2net-premium.html>, \$49).

In the United States, despite the fact that T-Mobile is the smallest of the four national carriers, it's the one I recommend for speed, cost, and flexibility with national coverage. Another national alternative is Virgin Mobile (a division of Sprint), which has a fixed-rate prepaid 3G offering for more limited use. Finally, in parts of the country, Sprint's Clearwire division is cheaper and better than any alternative.

T-Mobile

AT&T, Sprint Nextel, and Verizon Wireless offer 5 GB per month 3G service for \$60 per month and require a 2-year contract, while charging 5 or 10 cents per MB for usage beyond 5 GB. T-Mobile has alternatives to all of that.

T-Mobile charges \$50 per month if you purchase a \$100 to \$130 modem in advance, and then offers a month-to-month plan that you

can cancel without penalty. The company recently switched to a 5 GB and throttle plan, in which after 5 GB of usage, the firm reserves the right to lower your throughput to a few hundred Kbps for the remainder of the 30-day billing cycle, but it doesn't charge you overage fees.

T-Mobile also has the fastest 3G network. The firm has HSPA 7.2 (roughly 7.2 Mbps raw, and 1 to 4 Mbps real) service across most urban areas, and is in the process of updating to HSPA+ (21 Mbps raw, and perhaps 3 to 6 Mbps real).

Virgin Mobile

If you want broadband on demand, Virgin Mobile has a plan that's similar to AT&T's for the iPad (<http://www.virginmobileusa.com/mobile-broadband>). The Broadband2Go offering requires that you purchase a \$99.99 USB modem, which comes with drivers for Mac OS X and Windows.

After that, you can buy one of four data plans whenever you need. The plans start at \$10 for 100 MB over 10 days; 30-day plans cost \$20 for 300 MB, \$40 for 1 GB, and \$60 for 5 GB. When you run out of days or data, you can purchase another plan, or just go on your merry way.

There's neither a contract nor a cancellation fee; it's a pay-when-you-want-it offer, like the iPad.

Clear from Sprint/Clearwire

The Clearwire division of Sprint Nextel offers a so-called fourth-generation (4G) networking service in a number of U.S. cities, with coverage expected to pass 120 million people by the end of 2010. The 4G WiMax flavor that Clearwire has deployed (under the brand name Clear, <http://www.clear.com/>) offers 3 to 6 Mbps downstream with peaks as high as 10 Mbps; upstream rates are as fast as 1 Mbps. The service can be used as a fixed home broadband offer with no caps using a home gateway, as well as via a USB modem in a laptop. (It also works with a portable [Cellular Router](#).)

If you're in an area that Clear covers—like my home region in the Puget Sound in Washington state—this may be the cheapest and fastest way to go. You need to purchase a USB modem. Clearwire offers 4G only (\$49.99 or \$69.99) or a combined 3G/4G modem that can work over 3G networks outside 4G territory (a whopping \$224.99!).

You pair the modem with a service plan. Depending on your area and other factors, you may see different offers. At this writing, I'm offered service over 4G at \$40 per month with no caps. For \$55 per month and the 3G/4G modem, service is unlimited in 4G areas, and capped at 5 GB in 3G areas with a 5 cent per MB overage fee.

Cellular Router

Three carriers offer *cellular routers*, which are portable, battery-powered 3G and 4G modems with a built-in Wi-Fi radio. These routers are quite small and hold a charge for 3 or 4 hours, although they can also be plugged into a car via an inverter or to AC power and used while charging. The MiFi fits in a shirt pocket. Up to five or eight devices can connect over Wi-Fi at once, depending on the device.

Each device requires a 2-year contract to obtain the pricing shown below; some are available only under a 2-year contract with early cancellation penalties. See **Table 3** for details.

Table 3: Cellular Router Options				
Carrier	Router	Devices	Initial Cost	Per Month
Clearwire	Clear Spot (4G)	8	\$189.98/ \$209.98*	\$40
Clearwire§	Clear Spot (3G/4G)	8	\$364.98*	\$55†
Sprint§	MiFi	5	\$0	\$59.99†
Sprint§	Overdrive 3G/4G	5	\$99.99	\$59.99†
Verizon		5	\$49.99	\$59.99†
<p>* The Spot is \$139.99, but it requires one of the two 4G-only USB modems (\$49.99 or \$69.99) or the 3G/4G combo modem (\$224.99).</p> <p>† 3G usage in a 30-day period over 5 GB combined is 5¢ per MB.</p> <p>§ Sprint covers much of the United States with 3G, but also roams onto Verizon's network in some areas. Sprint allows only 300 MB per month of such roaming.</p>				

Phone as Portable Hotspot

Rather than carry a separate device (no matter how small) along with your iPad and mobile phone, wouldn't it be nice if the phone could act as the router? We're starting to see more of that. With the right software, a phone can activate its 3G and Wi-Fi radios at the same time, and, like a laptop using Internet sharing, route cellular data to and from devices connected over Wi-Fi. (This option is distinct from [Phone Tethering](#), which relies on USB or Bluetooth.)

The only such commercially available, carrier-supported phones in the United States at the moment are offered by Verizon: the Palm Pixi Pro and Palm Pre Pro. These two, with a downloadable free, separate application, can be activated to share a 3G data connection. For competitive reasons, Verizon recently eliminated a separate fee for use of the phone as a hotspot. Now, with a minimum \$39.99 voice plan and \$29.99 mobile broadband plan (a truly unlimited plan), you're set to go. (AT&T has plans at this writing to offer Palm Pre phones, but hadn't announced hotspot pricing, or if it will even be available.)

Two other options recently became available:

- Version 2.2 ("Froyo") of the Google-backed Android operating system for smartphones was released in May 2010. The new version has tethering and mobile hotspot features, but the pricing and any limitations have yet to be announced. Verizon and T-Mobile heavily promote Android phones.
- Sprint introduced the HTC Evo 4G in June 2010, a hybrid 3G/4G phone that works on Sprint's 3G and on Clearwire's 4G network. It features a hotspot offering, which requires a separate \$29.99 per month fee on top of any data plan to use on a 3G network and is subject to the same 5 GB limits and overage fees that apply to other Sprint plans. When the phone was launched, it enabled the mobile hotspot feature only when a 4G network was present; Sprint said it will turn on 3G mobile hotspot use and add the fee in July 2010.

Phone Tethering

Tethering turns a cell phone into a mobile broadband modem that can pass data to and from a laptop or other device via USB or Bluetooth. If your mobile phone can work in a tethered fashion, it could provide cellular Internet connectivity to a laptop, which could then provide access via Wi-Fi to an iPad. That's an elaborate option, given that it requires three devices.

AT&T will start offering iPhone tethering with the release of iOS 4, but has said an iPad can't use an iPhone for Internet access.

(You can't do the reverse—tether an iPad to a computer such that the iPad *gives* the computer Internet access. Neither iPad model has this option. Apple is a tease, though: the Bluetooth profile required is active on an iPad, but it doesn't work!)

Alternative Domestic Carrier

Yet another alternative is a competitive carrier in the country in which you live that uses the same cellular networking technology and that offers a micro-SIM card for data use. This should be a viable option in most countries except the United States.

In the United States, two technical differences prevent effect competition for iPad data plans, and it's not a lack of micro-SIM cards. First, AT&T and T-Mobile are the only two national U.S. networks that use GSM, the dominant worldwide mobile standard, and the only cell flavor supported by the 3G iPad. This excludes Verizon Wireless and Sprint Nextel, which use a different standard. Second, even though AT&T and T-Mobile both use GSM, each uses a slightly different set of licensed frequencies for 3G. Any device (a phone or portable digital appliance) made for T-Mobile's network, unless it's also designed for AT&T and international use, can communicate only at 2G (EDGE) speeds over AT&T's network.

Worldwide *quad-band phones* and similar devices like the 3G iPad support the four most common frequency bands used around the globe. But because those bands don't match up with T-Mobile, such devices can work on T-Mobile's network only at 2G (EDGE) speeds.

You could still sign up with T-Mobile (when it has micro-SIMs available, which it ultimately will for other devices), but it seems like a bad tradeoff in the price you'd pay for the speed you get.

Set Up Bluetooth

Bluetooth wireless networking lets you connect peripherals like battery-powered headphones, keyboards, earpieces, and headsets to an iPad for listening to music, entering text, and handling voice over IP (VoIP) phone calls.

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

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. The iPad seems to work correctly with any device that meets the Bluetooth spec for three profiles supported in the iPad: one for keyboard input and two others for stereo audio. Bluetooth hosts, like the iPad, aren't required to support all profiles. Apple documents iPhone OS 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 forget which hosts they were associated with previously, and must be re-paired to switch. Bluetooth devices are *discoverable* when they are set to allow a pairing connection.

On the iPad, Bluetooth is generally handled from the Bluetooth pane, reached in Settings by tapping General > Bluetooth. This pane lets you turn Bluetooth on and off and displays a list of (under Devices) of Bluetooth peripherals. The list shows any devices that have been previously attached to the iPad and the current status of such device. The list also displays any discoverable devices in the vicinity.

PAIRING ANY DEVICE

To pair any device, follow these general steps; the specifics for particular profiles follow.

1. Launch Settings, tap General > Bluetooth.
2. Activate Bluetooth discovery on the device with which you want to pair your iPad. This varies by device; check the manual. Typically, you hold down a button (sometimes a special pairing button) for several seconds.
3. The device appears in the Devices list on the iPad (**Figure 15**).

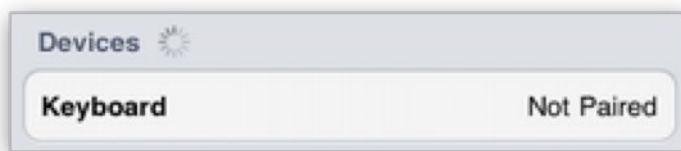


Figure 15: An unpaired device discovered.

4. Tap the device in the list with which you want to pair.
5. The iPad attempts to connect. Depending on the device, the iPad will offer one of three prompts:
 - A field in which you enter a code: The code will be provided either 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.
 - A code that you enter on the other device: The iPad generates a PIN to be entered in the pairing device (**Figure 16**).




Figure 16: Enter this code on the other device to complete the pairing process.

- Pairing is automatic without a code: For some devices, you can initiate a pairing request, which doesn't require a code to confirm. When the other device (like an iPad or computer) receives the request, it need only present a user with a dialog as shown in **Figure 17**. In this case, the headset DR-BT101 wants to pair with an iPad, and tapping Pair completes the process.



Figure 17: Some devices merely ask for confirmation to pair, rather than a code.

The paired device is now shown as Connected in the list. In the future, the device appears as available when it's turned on and within range.

Tip: You can remove a pairing by selecting the peripheral in the Devices list, tapping the detail  button, and then tapping Forget This Device.

The iPad shows Connected for paired devices that are turned on and available, and Not Connected for those that aren't in range or turned off (**Figure 18**).

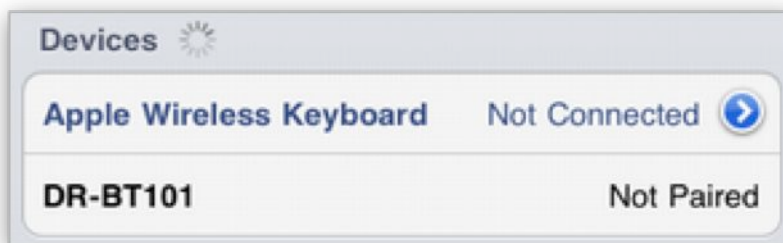


Figure 18: The keyboard is paired but not connected; the DR-BT101 (a set of headphones) is not yet paired.

APPLE WIRELESS KEYBOARD

The iPad was the first of its family of devices to support external keyboards, which includes both an Apple-branded keyboard/dock combination and any Bluetooth keyboard.

The \$69 Apple Wireless Keyboard is one of many Bluetooth keyboards that you can use with an iPad. It's stylish, compact, and easy to hook up (<http://www.apple.com/keyboard/>). To pair the Apple Wireless Keyboard with your iPad, use the general steps given just previously. In Step 2, press the power button on the keyboard's right upper side (**Figure 19**) until a green light starts to flash (**Figure 20**).



Figure 19: The power button is located on the right upper side of the Apple Wireless Keyboard.

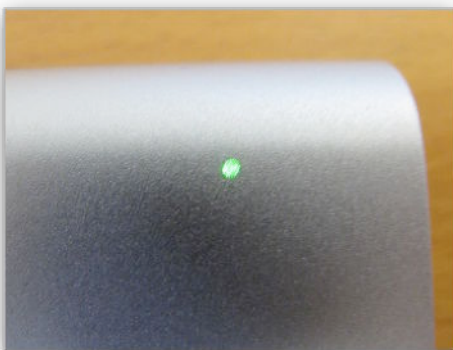


Figure 20: The green light that flashes while the keyboard is ready to be paired is tiny; the LED is invisible when the light is off.

Previously Paired Keyboard May Need Handholding

The Apple Wireless Keyboard can be paired with multiple computers and devices, but it can be tricky to make sure that the keyboard connects 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 with a Mac Pro. I found that I had to turn Bluetooth off (Settings > General > Bluetooth) and then turn the keyboard off (described on the next page) before it could pair with the Mac Pro. Pairing then worked fine. (You can't disconnect a Bluetooth device on an iPad and leave it paired for future use; only Forget This Device exists.)

After re-enabling Bluetooth on the iPad, I turned the keyboard off and then back on to see which device it associated with. The Mac Pro grabbed it first. From the Mac Pro's system menu bar, I opened the Bluetooth menu and chose Disconnect from the keyboard's submenu (**Figure 21**).

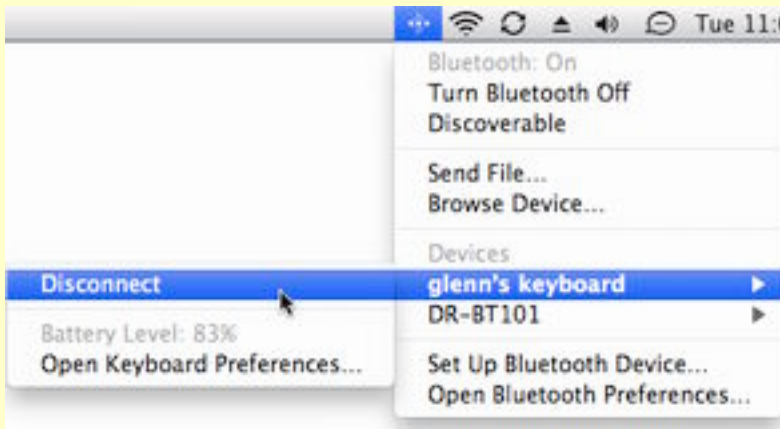


Figure 21: You can disconnect a keyboard on a computer to then connect to it on an iPad or other device.

Then, on the iPad, in the Bluetooth Settings pane, I tapped the keyboard's item in the Devices list, and the iPad 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.

Once paired, you can use the keyboard just as if it were directly connected to the iPad. Many of the special keys work, although you must touch the screen often to activate fields for entry or select certain kinds of buttons.

You'll also encounter situations where the iPad presents a dialog of fields to fill out, but provides no OK or Close button to tap. In cases like this, press Return on your keyboard to exit the dialog. Further, you may read directions telling you to tap a button on the virtual keyboard, such as Go or Join, that you can't access because the virtual keyboard is not showing. In such cases, press Return on your keyboard instead.

Tip: To make the onscreen keyboard appear while a Bluetooth keyboard is connected, press the Eject button on the Bluetooth keyboard. This toggles displays of the touch keyboard, but the Bluetooth keyboard can still be used.


To turn the keyboard off, hold down the power button for several seconds. The green indicator light stays steady while the power button is held down, and then goes out when you release. Press the button once to turn the keyboard back on.

AUDIO DEVICES

The iPad supports two of the three common audio profiles for Bluetooth: one for stereo audio playback, and another that allows remote control (pause, play, and stop). Unfortunately, a third profile for hands-free communication, such as with a Bluetooth headset, isn't supported in iPhone OS 3.2 on the iPad.

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

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

iPad apps that allow audio playback should display a special Bluetooth destination  icon. Tap it to select between one (or more!) active Bluetooth headsets through a pop-up menu (**Figure 22**). Tap a source to choose it, or it tap Cancel to exit the menu. Audio continues to play throughout and seamlessly switches when you tap.

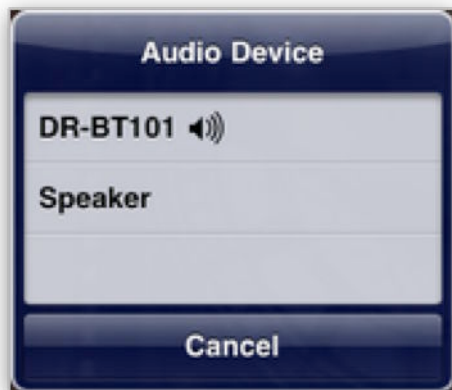


Figure 22: The Audio Device pop-up menu lets you choose among available Bluetooth and other output methods.

When you have multiple audio output choices available, apps should display the current device in use. iTunes shows the selected output in its upper-left corner; Netflix, using a standard audio control bar, shows the device below the play/pause button (**Figure 23**).



Figure 23: Top: The iPod app shows the audio output choice at the upper left, just below the status bar. Bottom: a standard set of audio controls shows the choice below the play/pause button.

You can stop using a Bluetooth headset at any time by using one of these three methods:

- Turn off the Bluetooth headset using its power button.
- In Settings > General > Bluetooth, in the entry for the headset, tap the detail ⓘ button, tap Forget This Device, and then tap OK.
- Move the iPad or Bluetooth headset out of range of the other. I like this option least, because Bluetooth can work over quite a long range. If you leave a headset at home and take the iPad with you, then this option makes sense.

In all cases, audio output reverts to speakers or headphones automatically.

Airplane Mode

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

Contrary to urban myth, cellular phones don't cause planes to crash. That's good, because researchers empowered by a joint government-airport study group that sets standards for airworthiness found that at least one mobile phone is left on during nearly all flights. (They also found no cause for alarm; you can read the whole report at <http://spectrum.ieee.org/aerospace/aviation/unsafe-at-any-airspeed/o>.)

The reason that the FAA and worldwide flight authorities demand that most kinds of electronics that produce or receive radio signals be turned off during a flight, as well as all electronic devices while flying below 10,000 feet, is because of a slight potential for risk that hasn't entirely been teased out from the reality of risk.

All electronic devices produce some emissions, and it's thought from years and years of testing that certain *avionics*—aircraft electronics—may be susceptible to some radio signals that are otherwise benign. Under 10,000 feet, a particular reading being knocked for a loop could be extremely dangerous. Hence the desire to reduce such risks.

WHAT'S AIRPLANE MODE?

The Airplane Mode in iPhone OS, found in all iPhones and in the 3G iPad, is a simple way to set your iPad to a legally required quiet mode during flight. (See [Turning Radios off Separately](#), next page, for advice for non-3G iPads.)

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

Warning! *Airplane Mode disables Find My iPad. If you're concerned about losing your iPad and being able to find it later, note that 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, the iPad turns off four separate radio systems: cellular, GPS, Wi-Fi, and Bluetooth. Put the iPad to sleep, and you're in compliance.

On flights on which Wi-Fi is available for Internet access—this option is now available on nearly 1,000 aircraft, mostly bigger jets on major routes—you can separately tap Wi-Fi in the Settings app and turn that radio back on when you're above 10,000 feet and have been notified that it's ok. You can also re-enable Bluetooth, which airlines typically do not specifically prohibit: tap General > Bluetooth; set the Bluetooth switch to On.

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

TURNING RADIOS OFF SEPARATELY

You can turn off both radios in a Wi-Fi iPad, and all four radios in a 3G iPad, via the Settings app without engaging AirPort Mode:

- **Wi-Fi:** Tap Wi-Fi, and set Wi-Fi to Off.
- **Bluetooth:** Tap General, then tap Bluetooth. Set Bluetooth to Off.
- **Cellular:** Tap Cellular Data, and set Cellular Data to Off.
- **GPS:** Tap General, then 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 the iPad from using GPS, Wi-Fi, and cell-tower based information to provide location data to apps and the operating system.*

Remote Access and Control

If you told me in 2006 that I would regularly use a handheld communicator to control a remote computer, I would've assumed that you were talking about an expensive tablet PC (few of which ever sold), or I'd tell you that maybe in 2010 or so there would be the right combination of software, hardware, and network robustness to make that work. I was off by a few years.

Since Apple began allowing third-party developers to write software for the iPhone and iPod touch in 2008, there has been strong demand for apps that let you view or control a computer's screen from an iPhone, iPad, or iPod touch, but not vice-versa. In this section, I look at two remote access iPad apps:

- In [iTeleport \(Formerly Jaadu VNC\)](#) (next page), I look at how this app provides remote access and control with the Virtual Network Computer (VNC) protocol that's a standard across many platforms and built into Mac OS X.
- In [LogMeIn Ignition](#) (p. 79), I discuss how this app employs LogMeIn's proprietary system for remote access and control.

Both apps offer similar feature sets and performance, and each app does a reasonable job, especially if the iPad is connected to an external Bluetooth keyboard or keyboard dock. I've left my laptop behind on multiple trips since starting to use these programs, not only with my newer iPad, but also with my iPhone. If you are trying to decide which one to purchase, I suggest you read this entire section to get a feel for which one is right for you.

Mocha VNC?

The other major remote-access program for iPhone OS is [Mocha VNC](#), a universal app by MochaSoft. It has similar functionality to iTeleport but costs \$5.99 instead of iTeleport's \$24.99 or LogMeIn Ignition's \$29.99. Even though they cost more, I prefer both iTeleport and Ignition because they allow access to computers without publicly reachable Internet addresses, and they work easily with, or include by default, strong encryption.

Input Replacement Apps

These remote screen control programs are distinct from the input replacement apps, such as [Air Mouse Pro](#) (RPA Tech, \$1.99) and [TouchPad Elite](#) (iTeleport, \$0.99), which control mouse input and let you type, but which don't show you the remote computer's display. Input-replacement apps work only over a local network and are intended for use with a computer that has a monitor, but for which it's difficult to use a mouse and keyboard. The apps in this section are full screen-sharing apps that work over local networks and over the Internet.

iTELEPORT (FORMERLY JAADU VNC)

[iTeleport](#) is a robust \$24.99 universal app for remote screen viewing that can connect to either Mac OS X's built-in VNC server or free server software provided by its developer. iTeleport also connects to any device running a Virtual Network Computer (VNC) server.

To use iTeleport, you first set up the computer(s) that you want to reach, and then connect to them via the iPad app.

Note: The company that originally made iTeleport was called Jugaari, and its software was named Jaadu VNC. Now both the company and the software are named iTeleport. You may still see the old names on the Web site or in iTunes.

Enable Remote Access

You have three choices for making a Macintosh available for remote access via the iTeleport app:

- Use the built-in VNC compatibility mode in Mac OS X 10.5 Leopard or 10.6 Snow Leopard. This is required if you want the iPad to access multiple monitors on a remotely controlled Mac, but it may not work if the iPad and the Mac are not on the same local network or when using an iPad over 3G. In the Sharing system preference pane, select Screen Sharing, and check the box next to it.
- Use Mac OS X's built-in VNC mode, plus a free utility from iTeleport that lets you make your Mac available for remote screen sharing over the Internet to a copy of iTeleport on an iPad by using

a Google account to connect the computer and your iPad. Instructions are at iTeleport's site under the "quick method," linked below.

- Use a combination of two free software packages from iTeleport: Vine-Jaadu Server and iTeleport Connect for Mac. This can work well for remote access, but the iPad can access only the Mac screen on which the menu bar is located. It doesn't require a Google account, and the Vine-Jaadu Server software offers more configuration options and security options. The explanation at iTeleport's site is under the "recommend method."

Under Windows, the easiest course of action is to install iTeleport's free remote access software.

Whichever method you choose, you'll need to set a server password. Later, when you connect, you'll enter the password.

Tip: For more about setting up the quick and recommended methods on the VNC server side of the equation, see iTeleport's setup instructions at <http://www.iteleportmobile.com/ipad/support/mac> or consult my book *Take Control of Sharing Files in Snow Leopard*.

Set Up iTeleport on an iPad

To get started with iTeleport, visit the iTunes Store or App Store to purchase the software and make sure it's installed on your iPad.

Follow these steps the first time you connect:

1. Launch iTeleport.
2. In the default Discovered view (**Figure 24**), tap the server on the local network under the Discovered Servers label. Servers labeled in blue are using iTeleport Connect.

(Servers are listed above the Discovered Servers label if the software has previously connected to them.)

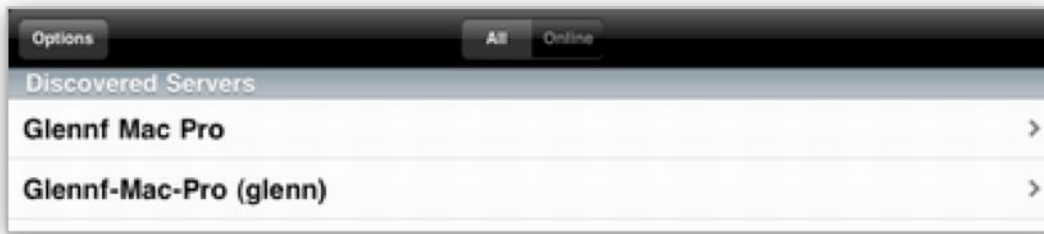


Figure 24: Local servers are shown in a list.

The New Server screen appears (**Figure 25**).



Figure 25: You can record server settings and use them to reconnect later by tapping Save Server.

3. Optionally change the server's name instead of using the Bonjour name, choose security options, and save the configuration without connecting.
4. Enter the VNC server's password, and to enable encryption if the server's configured for it:

Warning! I highly recommend using encryption. Otherwise, your sessions are entirely unprotected and can be monitored over open Wi-Fi hotspots. See [Transfer Data Safely](#).

- a. Tap Security.
- b. In the Password field, enter the VNC server's password.

c. I recommend setting Save Password to On.

If you do not have encryption set up on your server, you can skip to the next step. Otherwise:

d. Tap Encryption.

e. In the next screen, tap the Encryption switch to On.

f. Enter the user name and password for the machine to which you want to connect (**Figure 26**). In Mac OS X, that's a regular user account. (If you limit Remote Access in the Sharing preference pane to specific users, the user entered here must be in that list.)



Figure 26: Enter encryption details.

To save this profile without connecting: Tap Security at the top left, and then New Server. Tap Save Server. You can skip the rest of these steps.

5. Tap Connect.

6. If you're using encryption, the first time you make a connection the software prompts you to verify the *SSH fingerprint*, a kind of unique identifier, of the computer you're connecting to (**Figure 27**). Tap Accept.

No worries, in general: If your machine is under your control, there's no reason to worry about this; just tap Accept. This approval is stored for future connections.

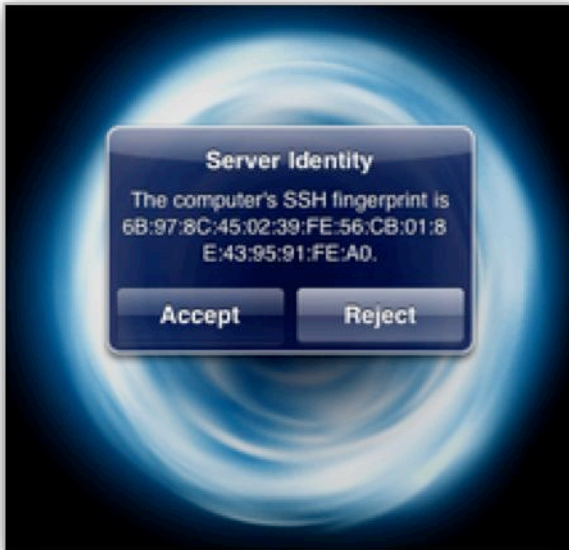


Figure 27: The Server Identity message is an extra check that the remote computer is the one you believe it is.

After a short pause, the remote screen should appear with a fascinating visual display. In the example in **Figure 28**, the server that's being viewed is Snow Leopard with built-in VNC compatibility.

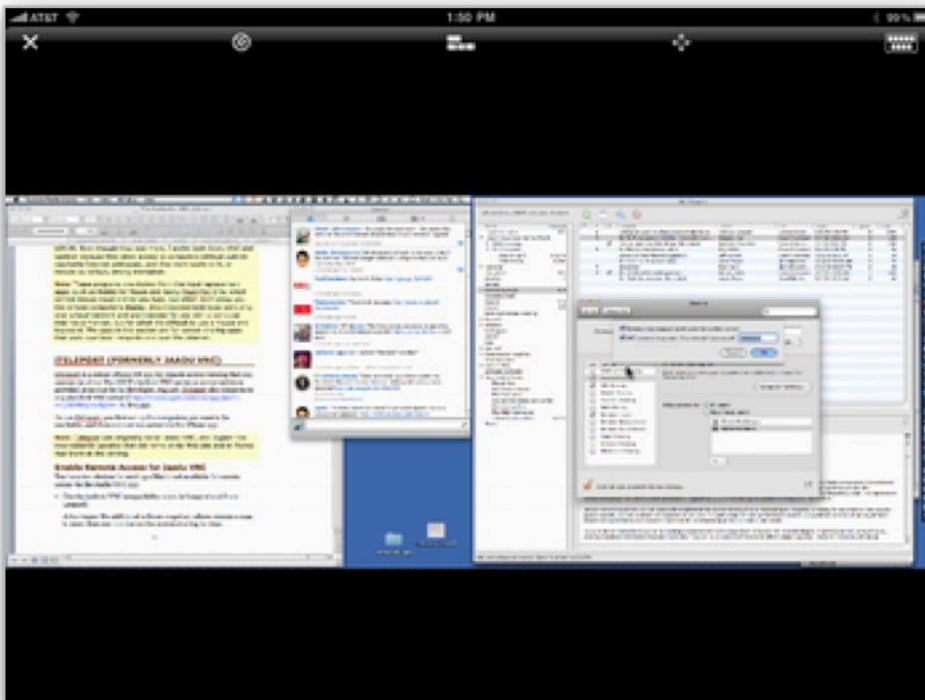


Figure 28: Two screens are scaled down significantly to squeeze into the iPad display in landscape orientation.

Make a Manual Connection

You can also enter an IP address or domain name in iTeleport. The steps are similar, but you start with tapping Manual at the main screen's bottom. You then tap + in the upper right, and fill out the details for the computer to which you're connecting.

Control a Computer

All the above merely gets you started using iTeleport to remotely control a computer. Once connected, you can do something! Your finger is your navigation tool. The virtual screen moves under your finger, and the mouse pointer follows your finger (**Figure 29**). Tap, and it's like single-clicking. Use pinch and expand gestures to zoom in and out on the remote screen.

iTeleport is rotation aware, so you can tilt the iPad to switch from landscape to portrait at will. Screen refresh is relatively fast even over 3G connections.

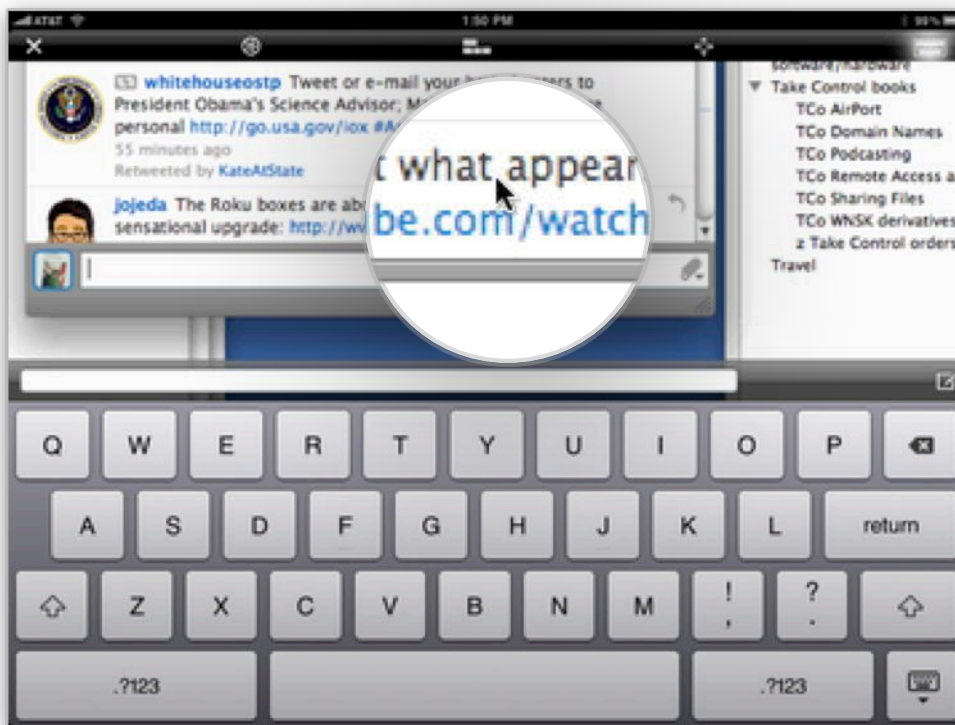


Figure 29: Move your finger to move the mouse and the virtual screen slides beneath. Tap the keyboard icon to bring up a keyboard for typing. (Circular area is enlarged to show detail.)

A row of buttons along the top of the screen provides access to a few special options and keyboard features. From left to right, these are:

- **Disconnect:** Tap Disconnect to end the session and return to the connection screen at which you started.
- **Settings:** You can set options such as locking orientation, so that switching the iPad from landscape to portrait doesn't rotate the iPad's display of the remote screen.
- **Modifier keys:** Tapping this button brings up onscreen Shift, Control, Command, and Option buttons for one or more combinations with keyboard letters.
- **Extended keyboard keys:** iTeleport neatly hides five screens of elements such as arrow keys, function keys, and media-control keys (such as play/pause) that you access by swiping through the screens. Arrow keys are intermingled with Escape, Back, Tab, and Space bar.
- **Keyboard:** This display lets you type directly on screen. iTeleport includes its own area to show what you're typing so that you can see what you entered even if it's not visible on the remote screen (**Figure 29**), above this list.

LOGMEIN IGNITION

LogMeIn makes remote-control programs that come in many versions for Windows, including “help desk” flavors designed for tech-support staff to offer remote assistance through remote screen control (<https://secure.logmein.com/>). LogMeIn has a free option for general use for Mac and Windows: LogMeIn Free. This service works spectacularly at providing remote access through all sorts of network weirdness, including cases where Back to My Mac doesn't work well. A Web-based account lets you manage which computers belong to you for remote administration.

Note: A Pro version of LogMeIn carries a monthly fee, but adds file transfer, guest access, and a number of other features.

The service became even more useful when the company released [LogMeIn Ignition](#) for iPhone and iPod touch, which is now available as a universal app for \$29.99. Ignition uses your LogMeIn account to connect to any LogMeIn client machines on any supported platform. It's a powerful tool, and it works fine over 3G and Wi-Fi. In many ways, it's similar to iTeleport. However, instead of using the standard VNC specification and a variety of software packages to gain remote access to otherwise inaccessible computers, LogMeIn uses its own protocols and software. This makes it simpler to configure and use.

No extra step for encryption: You need take no additional steps to enable security with LogMeIn, which always uses strong encryption for Web and mobile connections.

Here's how to make your first LogMeIn connection:

1. Set up an account at LogMeIn, and install LogMeIn software on one or more computers. I won't reproduce the instructions here because LogMeIn's process is so straightforward. After you have at least one computer configured with LogMeIn, your account at the Web site will look something like **Figure 30**, showing a list of computers and the accessible status of each.

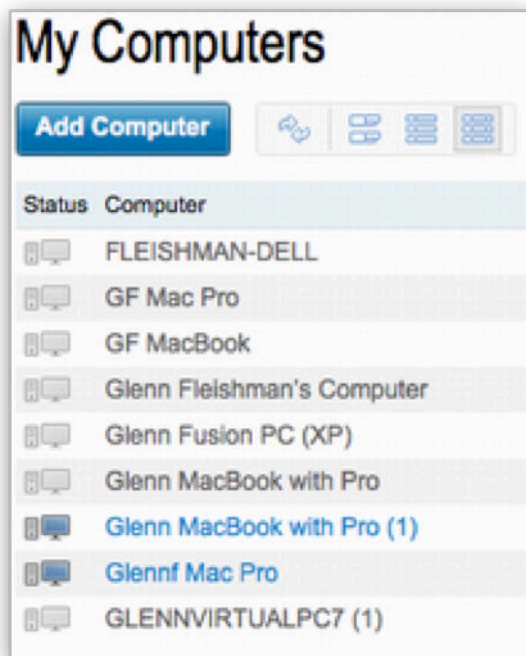


Figure 30: After logging into LogMeIn's site on a computer, you see a list of your devices and their respective status. Clicking a server starts the steps of remote viewing in a desktop browser.

2. Launch Ignition on your iPad to start a remote session.

The app displays a login screen (**Figure 31**).



Figure 31: The main login screen lets you store your password for future sessions.

3. Enter your login credentials. They are the same as those you used to set up your LogMeIn account.
4. If you like, tap the switch to have LogMeIn remember your password. This is useful if you've chosen a strong password that you don't want to re-enter regularly.

Warning! *I suggest storing your password only if you also use the iPad's passcode lock (configured in Settings > General > Passcode Lock). See [Keep Data Safe](#).*

5. In the Computers list that appears after a successful login (**Figure 32**), tap the computer that you want to start a session with. (This is the same list you would see at a Web login.)

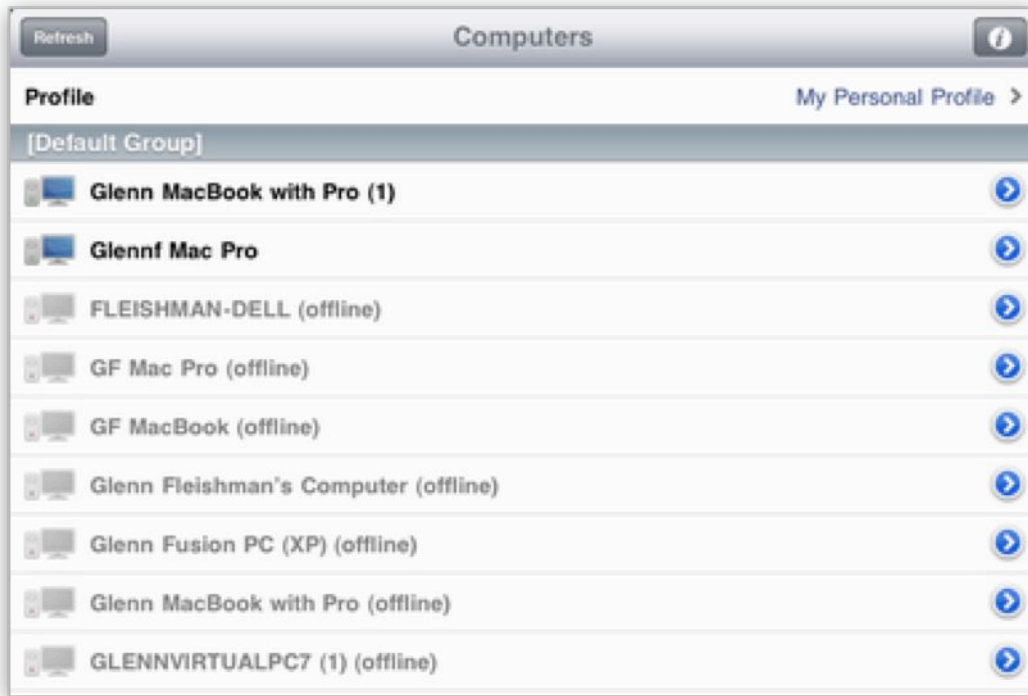


Figure 32: My various computers associated with LogMeIn.

6. Enter the same user name and password as you would to log in to an account on the machine itself. Enter this information, and optionally store the password (but see the **Warning!**, earlier in these steps). (**Figure 33**).

Figure 33: Enter your computer's user name and password and tap Log In, and Ignition starts up a connection.

Tip: If you store the password, LogMeIn connects directly without prompting the next time.

7. Tap Log In.

The connection process can take from seconds to tens of seconds depending on your network connection.

Once you are connected, the remote screen appears. A row of buttons at the bottom of the screen in either orientation lets you control session behavior (**Figure 34**).



Figure 34: Controls from left to right are:

- **Keyboard:** Brings up a keyboard for typing and to gain access to modifier keys (**Figure 36**, next page).
- **Platform-specific key combinations** (pyramid of three keys): This button brings up Command-Tab and Command-` (back tick) buttons when connecting to a Mac.
- **Mouse button:** Lets you change a tap from a left click to a right click. It can be hard to see, but there's a little upper-left divot out of the toolbar's mouse icon for left click; tap it, and the divot moves to the right side for right- or Control-click actions.
- **Magnifying glass:** Toggles between 100-percent view and a fit-in-window view.
- **Settings:** Visit the settings screen to change configuration midstream.
- **Disconnect:** Ends the session with a prompt to confirm.

As with iTeleport, you use your finger to drag the virtual screen around with the pointer appearing where you drag. You can pinch and expand to zoom in or out.

Multiple Remote Screens

A single screen appears by default for a remote system with multiple displays, but you can bring up another screen by shaking your iPad, or change a preference to show multiple screens at once (**Figure 35**).

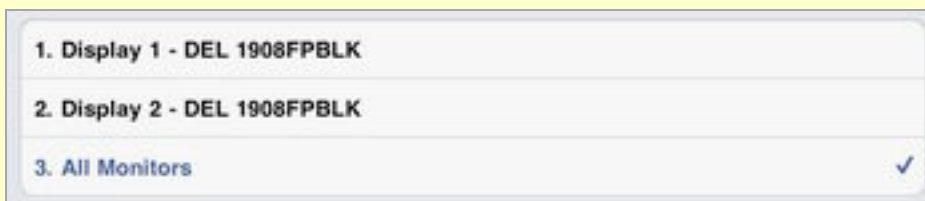


Figure 35: You can pick which of multiple monitors to display, or all of them.

When typing, as in **Figure 36**, you can type modifier-key keystrokes by tapping Ctrl, Alt, and Cmd at the top of the screen in any combination, and then pressing keyboard keys. The overlapping windows icon at the top brings up a set of additional keys you can swipe through, including function and arrow keys.

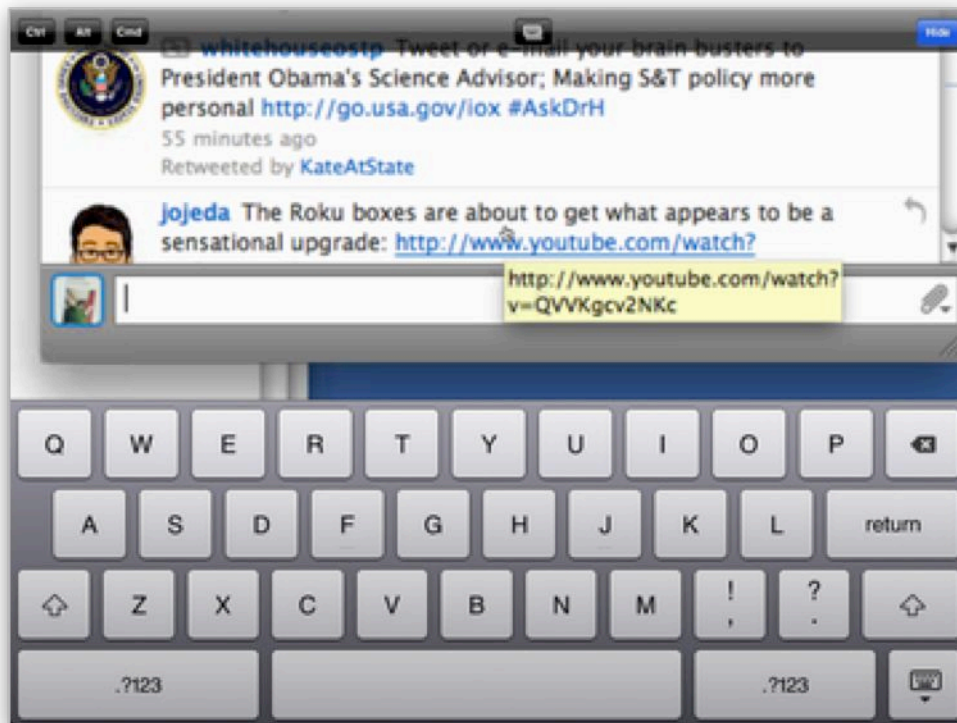



Figure 36: The keyboard lets you type directly as if you were in front of the computer you're controlling.

The folks behind LogMeIn take security quite seriously, which is why they offer an additional option for protecting your data. Tap the info  button on the main Computer screen, and you can erase any stored account logins—either for LogMeIn or for your remotely controlled computers.

Access Documents

No iPad is an island; each is part of the main—the main set of files you maintain all over the place. Many of us have multiple computers and storage locations. As a result, we use the iPad not so much as a file repository, but as a view into our file storage.

Several third-party apps and one Apple app make it possible to access and sometimes aggregate access to files stored all over.

In this section, I look at four programs that you might consider for handling these various kinds of storage: Air Sharing HD, GoodReader for iPad, Dropbox, and iDisk. Air Sharing HD and GoodReader can store documents across many sources and servers, and let you view (or play) certain stored files; Dropbox and iDisk are portals into one kind of storage with more limited viewing options.

WHAT KINDS OF STORAGE

Apps for the iPad give you access to four kinds of storage, with some apps handling more than one kind:

- **Over-the-air downloads:** In an app, you can view remote files and choose a file to download and optionally store in the app's local storage. The file is transferred via Wi-Fi or 3G from an email server, a file server, or other services. All four programs covered in this section can retrieve documents wirelessly.
- **Networked:** Air Sharing HD and GoodReader can act as WebDAV file servers while launched and allow other computers on the local network to use Bonjour or an IP address to access their file stores, and to transfer files to and from the iPad. (WebDAV is a popular method of accessing files from other servers; see [What's WebDAV?](#), two pages ahead.)
- **iTunes file transfer:** With an iPad connected to a computer running iTunes, an app may expose its internal document storage list. You can manage files in that list, including dragging documents

into it. Air Sharing HD and GoodReader support iTunes file transfer. See [Manage and Copy Files via iTunes](#), next page.

- **Attachments:** Email attachments can live in limbo on an iPad. In the Mail program, an attachment over a relatively small size is downloaded only when you request it. A downloaded attachment is then stored temporarily in Mail, but you can also choose an external program—Air Sharing HD and GoodReader are options—to open it, thus transferring the attachment to the iPad and storing it there. To learn more, read [Open Email Attachments in Another App](#), a few pages ahead.

***No soap, Safari:** So far, Safari doesn't allow links to document files to be opened in another program, but GoodReader has a neat workaround through a built-in browser that can download directly into the app. See [Download Files from Web Pages](#).*

Supported Formats

Each of these apps can read many different document, image, and movie file formats, because Apple has provided this support in the iPhone OS and makes it available to any app that wants to use it.

Apple currently supports these file types:

- **Movies:** H.264 and MPEG-4 (as .m4v, .mp4, and .mov), Motion JPEG (.avi); see <http://www.apple.com/ipad/specs/> for specifics on frames, resolution, and audio encoding.
- **Images:** JPEG, TIFF, and GIF.
- **Documents:** Apple iWork '08 and '09 (Keynote, Numbers, and Pages); Microsoft Excel, PowerPoint, and Word (including 2008 formats like .docx); Acrobat PDF; Rich Text Format (RTF); and the VCF contact information format.

What's WebDAV?

In the coverage of Air Sharing HD and GoodReader ahead, you'll read about using WebDAV to retrieve files into the apps, as well as how to share files from the apps over a local network to computers or other iPads—or even iPhones and iPod touches—on that network. But what is WebDAV?

The name is long: Web-based Distributed Authoring and Versioning. WebDAV was intended to let an ordinary Web server act as a file server, allowing access over a network to retrieve, modify, delete, and add files.

WebDAV and FTP are the most widely used methods to retrieve files remotely. Apple's built-in file-sharing flavor, Apple Filing Protocol (AFP) can work over the Internet, but is rarely used for that kind of remote access. Apple uses WebDAV for iDisk and supports it through Mac OS X.

Manage and Copy Files via iTunes

Moving files in and out via iTunes requires much less effort than the other options:

1. Connect your iPad to a computer to or from which you want to copy files, and launch iTunes.

Warning! *If this isn't the primary computer to which the iPad normally syncs, pay attention to any dialogs that might pop up asking you about syncing. To be extra safe, turn off automatic syncing in the iTunes preferences, in the Devices pane, before making the connection.*

2. In the sidebar, select the iPad in the Devices list.
3. Select the Apps tab.
4. Scroll down below the layout editor to the File Sharing section.
5. Select the appropriate app in the Apps list. The folders and files available in the data store are shown in the *App Name Documents* list to the right (**Figure 37**).

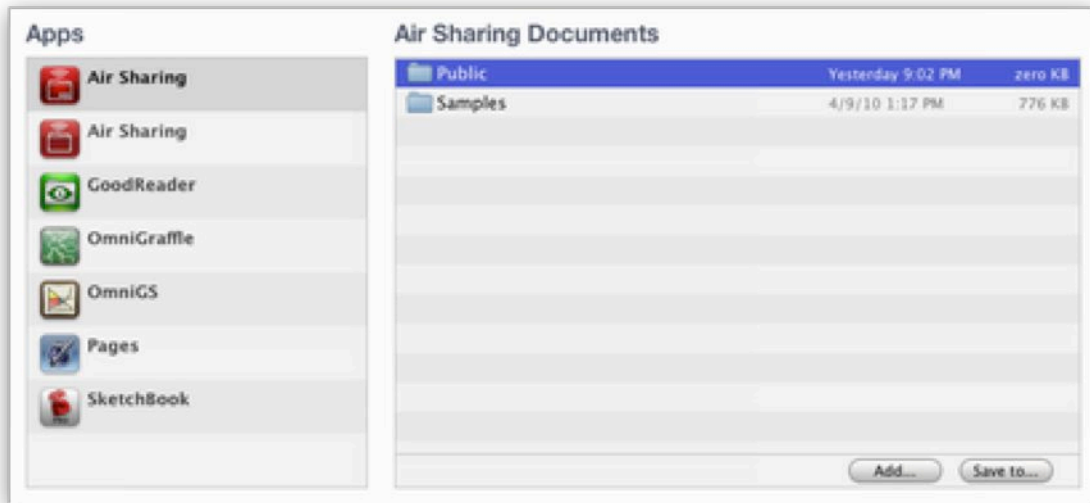


Figure 37: iTunes controls how you move files in and out of the data store for the app.

Now, you can carry out a variety of actions:

- Click Add to choose files to the data store, or drag files from the Desktop into the window. You can't create folders or put the items in a folder.
- Select a file or folder, wait a second, click it again, and you can rename the item.
- Select a file or folder, and click Save To in order to copy the item from the iPad to the computer; you can also drag files or folders (including multiple selections) to the Desktop. You can't copy items from inside a folder selectively.

Warning! A bug in the version of Air Sharing HD that I tested didn't refresh the display of files in the My Documents directory after making changes in iTunes. You must go back to the Servers list and then return to My Documents to access the changed data store.

Warning! You don't sync from iTunes to copy files; the files copy immediately when you add them to an app's file store. However, if you aren't using the copy of iTunes that your iPad normally syncs with and accidentally click Sync, you'll be prompted to copy purchases or erase and sync anew. If that happens, click Cancel.

Open Email Attachments in Another App

iPhone OS recognizes that certain programs are designed to view or edit particular document types. In the Mail app, you can use this feature to transfer attachments to GoodReader and Air Sharing HD among other apps.

The steps to use this feature are simple:

1. In the Mail app, select a message with an attached document.
2. Touch the attachment icon to reveal a popover (**Figure 38**) showing three options:



Figure 38: Mail offers multiple ways to view attached documents.

- Quick Look, which previews within the Mail app.
- Open in “*app name*”, which copies the file to that app.
- Open In, which brings up another popover that lets you select among multiple options for viewing the file (**Figure 39**).

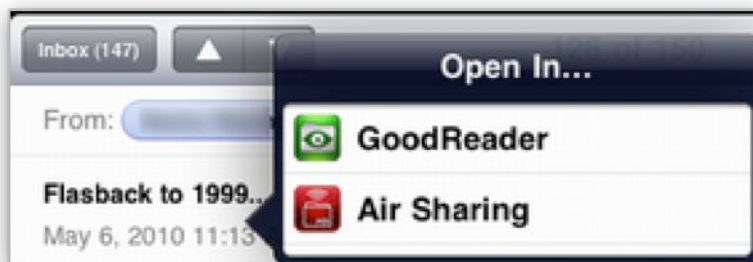



Figure 39: The Open In pop-over menu offers the full range of programs that support opening this kind of attachment.

3. The file opens in the selected program for viewing.

Tip: To transfer an attached photo from an open message in Mail to the Photos app, tap the Reply  icon and then tap Save Images or Save X Images.

AIR SHARING HD

Air Sharing HD, the \$9.99 iPad version of Air Sharing Pro from Avatron Software (<http://avatron.com/>), offers several broad categories of features:

- **Access Remote Files:** Air Sharing HD can access many types of remote servers, including iDisk and Dropbox accounts, as well as FTP, FTPS, and WebDAV servers—a Mac can be easily set up as a WebDAV server—and mail servers. You’d use the mail server option to view email attachments.
- **Save Files Locally:** Air Sharing HD can copy or move files from remote servers (or a few other apps, such as the Mail app) to its local file store on the iPad, making it easy for you to view or listen to those items at any time, even if you don’t have network access.
- **View or Play Files:** Once you have access to a file, whether it’s stored remotely or locally, you can “open” it and then view it or play it, depending on its file type.

Air Sharing HD can also print: *If you can open a document in Air Sharing HD, you can print it on a local printer. Other apps can also facilitate printing from an iPad;* [Take Control of Working with Your iPad](#) *has more details.*

- **Set Up Air Sharing HD as a Server:** If a file is stored *in* Air Sharing HD, you can set up Air Sharing HD as a *local* WebDAV server and then access that file from other local computers, including not only Macintoshes and Windows computers, but also—via the iPhone version of Air Sharing, for instance—other Apple devices like iPhones and iPod touches. And, if that wasn’t enough, you can also access Air Sharing HD’s file store through iTunes.

Once you’ve set up Air Sharing HD as a server or connected it to iTunes, you move files not only from it, but also *to* it. This more

or less takes you full circle back to the first bullet item in this list, giving you another way get remote files into Air Sharing HD, except this time you are actively working on a device that is not the iPad.

Air Sharing HD Adds Other Formats

Beyond Apple's [Supported Formats](#) (p. 86), Air Sharing can handle items in these formats:

- Web Archive (.webarchive), the offline storage format for Web pages (including images) created by Safari.
- RTFD, TextEdit documents with optionally embedded images.
- Source code in the form of text files with syntax-based color coding.

When you first launch Air Sharing HD, it shows two folders, both located in its “My Documents” local file store: Public and Samples (**Figure 40**). Public is for files that you want to share over a local network, while Samples has a few items that show how Air Sharing handles navigation and document display.

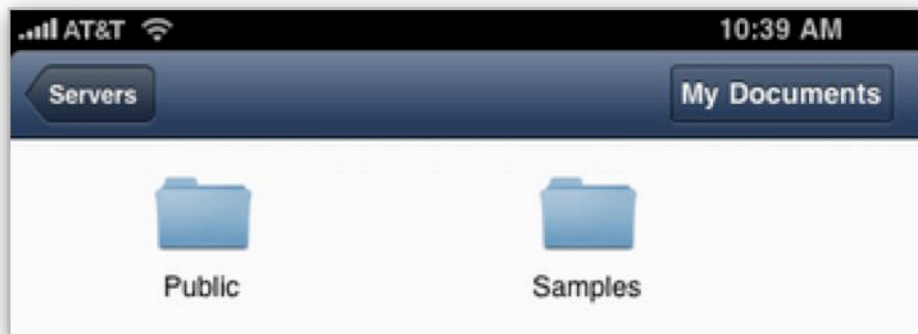


Figure 40: The default setup in Air Sharing HD shows two folders in the app's data store.

Access Remote Files

To see a list of servers accessible to your copy of Air Sharing, tap Servers in the upper left. To add a source, tap the plus **+** button (**Figure 41**). Choose the server type to which you want to connect, and then enter the required credentials for access.

Warning! Most remote access to servers isn't secured, and I don't recommend accessing servers from Air Sharing HD on public networks. The exceptions are mail servers for which you have Use SSL enabled, SSH (SFTP) and FTPS, Dropbox (all transfers), and WebDAV servers that have URLs that start with <https>. See [Transfer Data Securely](#).

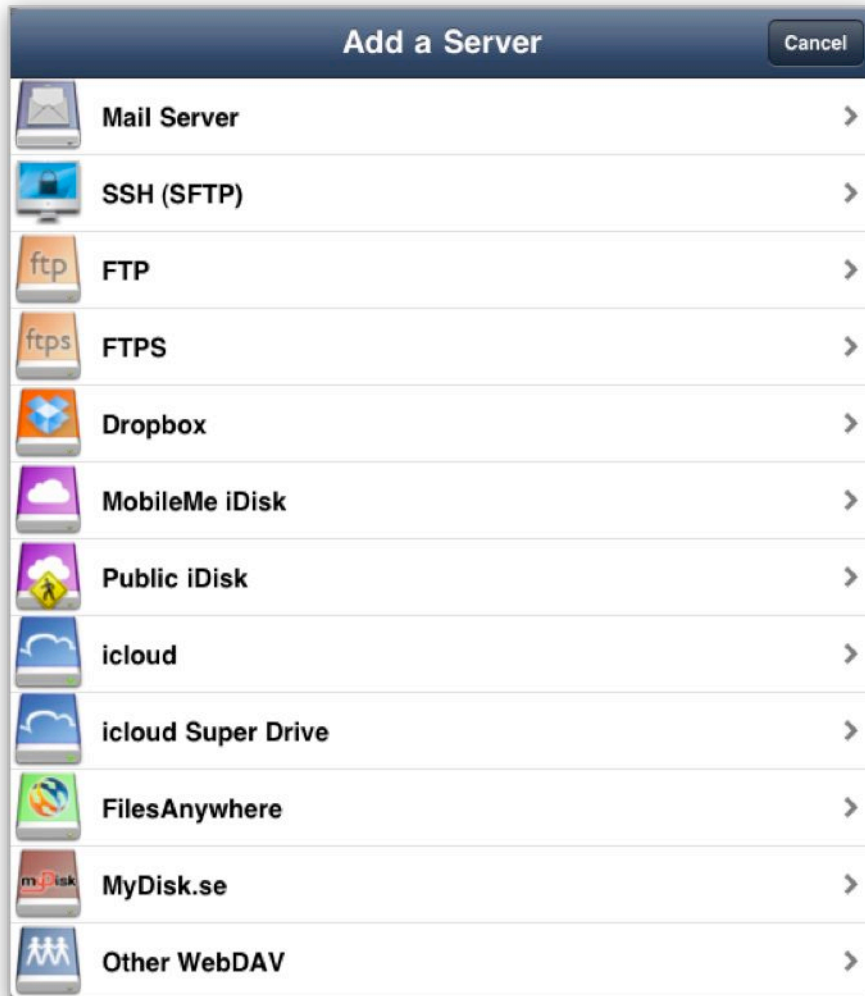


Figure 41: Air Sharing HD offers a cornucopia of server types, including three flavors of FTP, MobileMe, Dropbox, a few hosting services, and generic WebDAV, as well as Mail Server access (POP and IMAP).

For example, to add a mail server, follow these steps:

1. In the Add a Server view, tap Mail Server.

2. In the Add Account screen, choose the kind of email service (**Figure 42**). If you have a popular service, such Gmail or MobileMe, tap that button. Otherwise, tap Other.

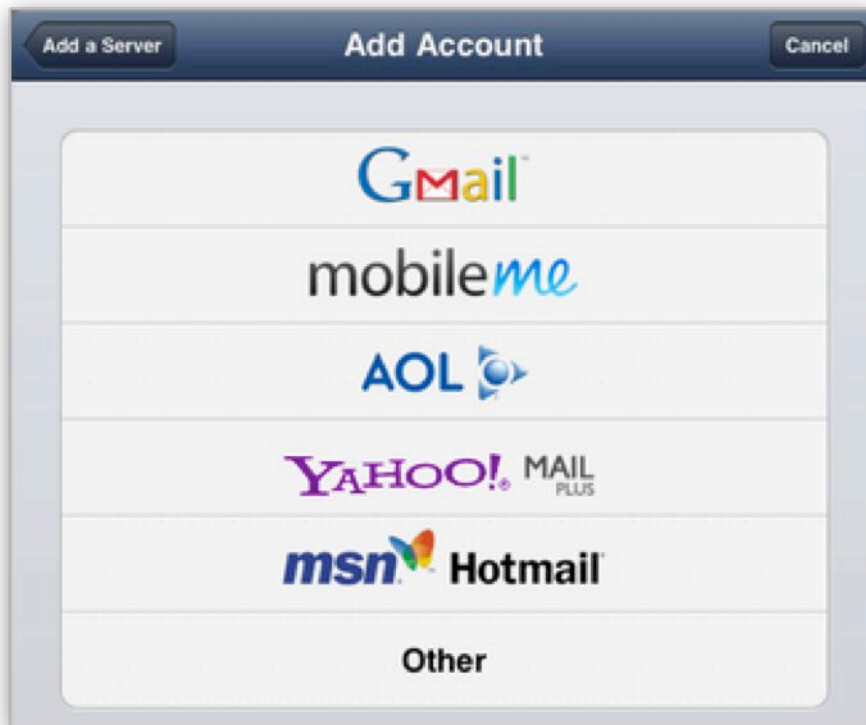


Figure 42: Choose the mail server type.

3. Enter the configuration details for the mail server (**Figure 43**).



Figure 43: Enter your email account's configuration details.

In this example, I'm entering details for an IMAP mail server using secure communications.

4. Tap Save.

You can now tap the server's item in the main Servers list to see what attachments are available for viewing for that account. A given message may have multiple attachments (**Figure 44**).

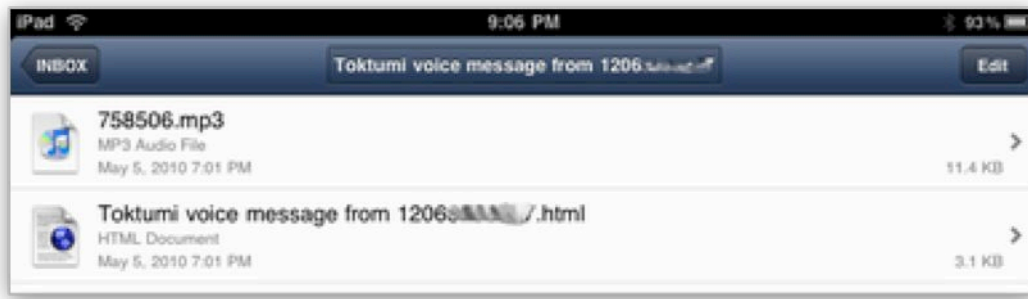


Figure 44: This message from the Toktumi calling service contains two attachments: the HTML that makes up the message text, and an MP3 of the voicemail audio.

Save Files Locally

Air Sharing HD stores files from remote servers oddly. When you view or play a file by tapping it in a remote server's directory, the app makes a temporary local copy, but doesn't store it.

To store a file locally in Air Sharing HD's My Documents file store, follow these steps:

1. In any file list view, either touch and hold down on a file in the list or tap the Edit button in the upper right corner.
2. Tap one or more items in the list.

A blue checkmark appears beside each selected item (**Figure 45**).

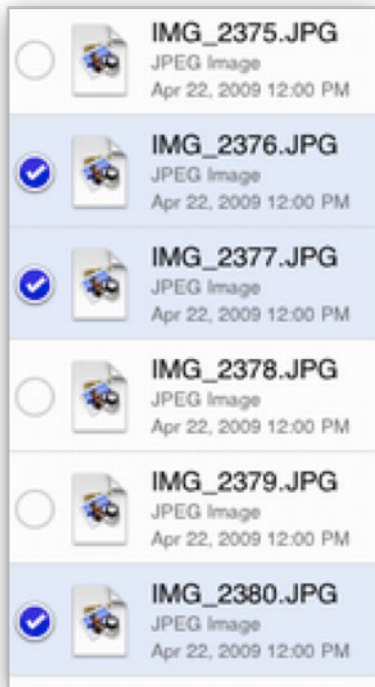



Figure 45: Items are selected for an action, such as copying.

3. When you've completed your selection, tap the gear  icon in the lower right corner.
4. From the pop-up menu that appears, Choose Copy or Move (**Figure 46**).

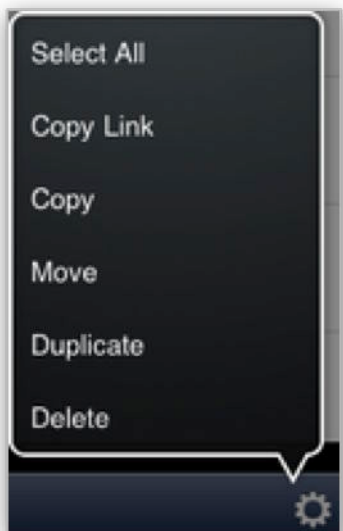


Figure 46: The menu lets you perform a variety of related actions on the files in the view.

Both Copy and Move create an internal list of items to copy; Move optionally deletes them (if you have permission) from the original source. A Clipboard icon appears to the right of items that are slated to be copied (**Figure 47**). An image of a clipboard with a paperclip appears in the upper right corner of the window, too.



Figure 47: A clipboard icon appears on files that have been marked for copying or moving (left); the upper-right corner of Air Sharing HD shows a icon to remind you that files are ready for placement.

5. Navigate to a location, such as the My Documents folder, into which you want to copy the files. (You can instead choose a directory on another service for which you have permission to add files).
6. Tap the clipboard icon, and then tap Paste *X* Items (**Figure 48**). The items are now copied or moved.

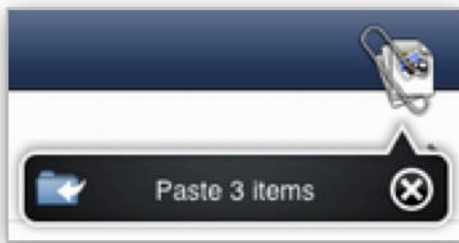


Figure 48: The Paste command lets you drop those files in any directory, including local storage or another server.

This process is a bit awkward if you simply want viewed files to be easily available in Air Sharing's iPad file store. A developer at Avatron Software told me that the company plans to simplify the process in the next release.

View or Play Files

To access a file so you can view it or play it:

- If the file is stored locally, from the main Air Sharing HD screen, tap My Documents and then navigate to and tap the file name.

- If the file is stored on a remote server listed on the Air Sharing Servers screen, select the server from the Servers page in order to connect to it, then navigate to and select the file (**Figure 49**). Air Sharing HD downloads it temporarily.



Figure 49: Browsing a folder on a file server.

In all supported document types where it makes sense, you can scroll, and pinch in and pinch out to zoom the display. But support for PDF goes a bit further (**Figure 50**).

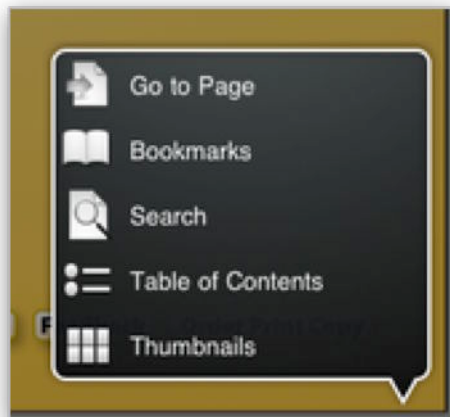


Figure 50: Air Sharing HD adds controls for looking through PDFs.

For example, you can search within a PDF file and tap on results to jump to that part in the document (**Figure 51**).

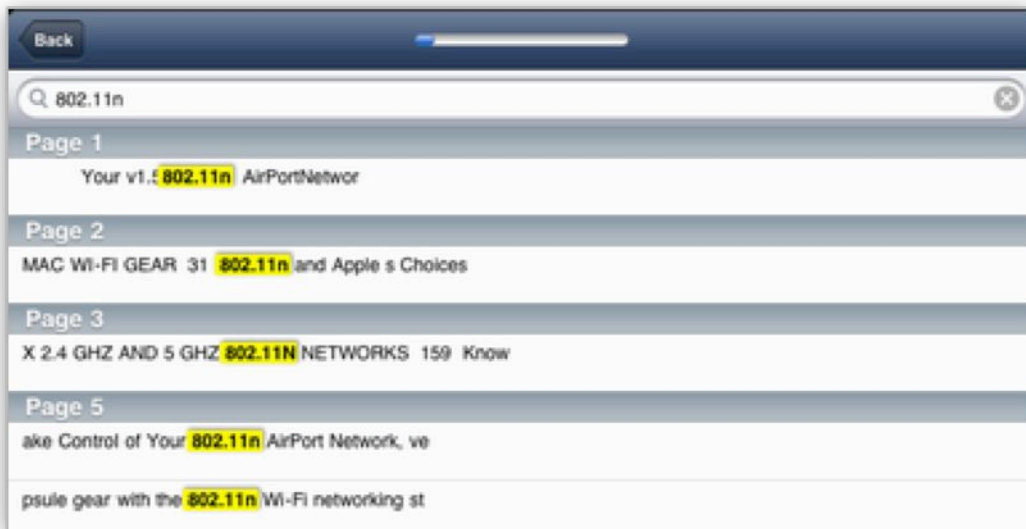


Figure 51: Search results on a PDF.

You can also navigate in the document by viewing and tapping thumbnails (**Figure 52**) or by tapping entries in the table of contents.




Figure 52: Air Sharing HD can show thumbnails of pages in a PDF.

Set Up Air Sharing HD as a Server

You can also add, retrieve, and remove files from Air Sharing HD's iPad file store using either a local file-sharing connection or iTunes via USB. iTunes details are explained earlier in [Manage and Copy Files via iTunes](#).

When you're connected to a Wi-Fi network, Air Sharing HD makes itself available as a WebDAV server to computers and other devices that can browse for WebDAV access.

Not over 3G: Air Sharing HD cannot share files when connected via 3G because it relies on a locally accessible IP address or Bonjour networking to let other computers or devices make a WebDAV connection.

Tap the Wi-Fi  icon at the bottom of the screen, and the four local network methods by which you can access the app's storage appear (**Figure 53**). It's really two methods—Bonjour and an IP address—doubled up between plain and secure (https for SSL/TLS) methods. I recommend using the secure forms, especially at a Wi-Fi hotspot. (See [Transfer Data Securely](#).)

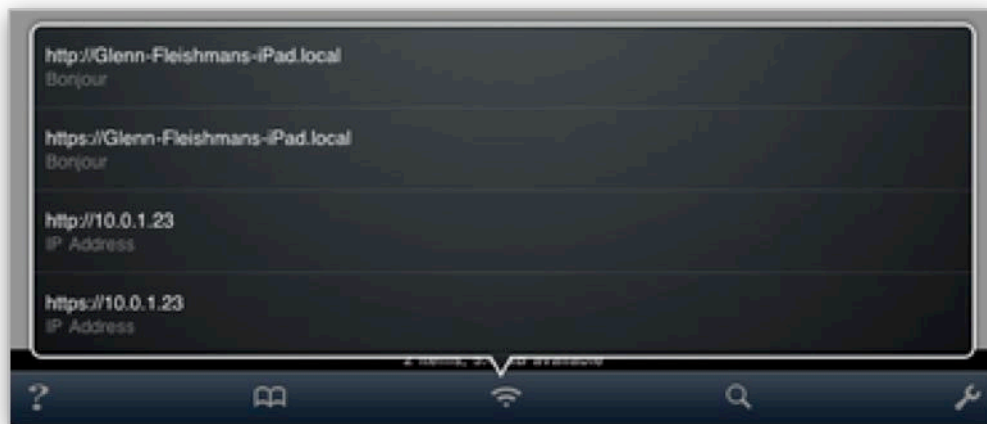



Figure 53: The various ways to connect over a local network appear when you tap the Wi-Fi signal icon.

This access can be restricted with a password, which I recommend if you are connecting in a public place. To set a password in Air Sharing HD, follow these steps:

1. Tap the Settings icon  at the right of the Air Sharing toolbar.
2. Tap Sharing Security.
3. Set Require Password to On.
4. Although filling in the User Name and Password fields is noted as optional, you should complete them for better compatibility for remote access.

5. Set Public Access On or Off. With Public Access enabled, anyone on the local network can connect and see files or put files in the Public Folder.

Now that you've set up Air Sharing HD as a server, you can connect to it over the local network, as I explain next.

GOODREADER

GoodReader for iPad, a \$0.99 app from Good.iWare, comes in several editions for different types of Apple devices, so be sure to get the iPad edition (<http://www.goodiware.com/>). GoodReader has the most features and options of any of the reader software I've tested, and this is both good and bad. Good, because the app can do most anything; bad, because it can be confusing to figure out which option you need at times (**Figures 54** and **55**).

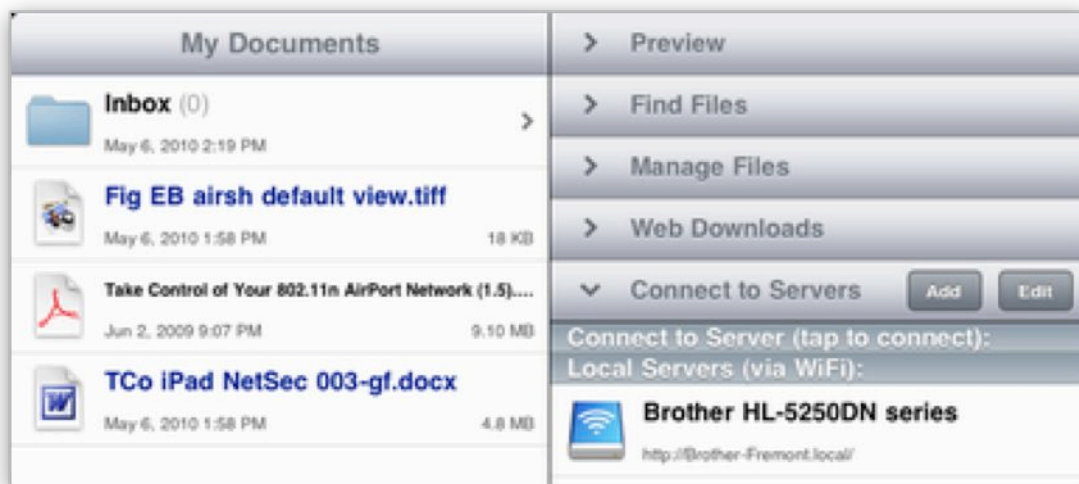


Figure 54: The top main view of GoodReader shows documents stored locally at left; at right are a set of stacked, collapsible views for interacting with local files (Preview, Find Files, Manage Files) and remote servers (Web Downloads, Connect to Servers).



Figure 55: An additional button bar at the bottom of the right pane lets you import images and videos from the Photos app, turn on a WebDAV server accessible from the local network, change settings, get help, and lock the iPad's rotation to the current orientation.

Like Air Sharing HD, GoodReader can access files in any of the standard iPhone OS [Supported Formats](#) (p. 86) from a variety of servers, store them locally on the iPad, and let you view them. GoodReader can serve as a viewer for many file types, but its particular skill is long PDFs. It can also open and store Google Docs.

Also like Air Sharing HD, the GoodReader app can act as a WebDAV file server, letting you access items in its iPad file store from other devices on your local network. Stored files can also be managed in iTunes.

Access Servers from the App

GoodReader can accept or retrieve files from WebDAV servers, Dropbox, mail accounts, MobileMe's iDisk, Google Docs, and FTP.

Warning! *Most remote access to servers isn't secured, and I don't recommend accessing servers from GoodReader on public networks. The exceptions are mail servers in which you have Use SSL enabled, Google Docs (for login but not file transfer), Dropbox (for all transactions), and WebDAV servers that have a URL starting with [https](#). See [Transfer Data Securely](#).*

The Connect to Servers list, in the right pane, shows any stored servers (below Connect to Server), and, if you're connected to a Wi-Fi network, any WebDAV servers that are advertising their availability via Bonjour (below Local Servers).

To add a server to the list, follow these steps:

1. Open the Connect to Servers list by tapping its name. The chevron (>) left of the Connect to Servers heading will point downward if the list is open.
2. With the list open, tap Add (at the right of Connect to Servers) to open the Create New Connection popover (**Figure 56**).

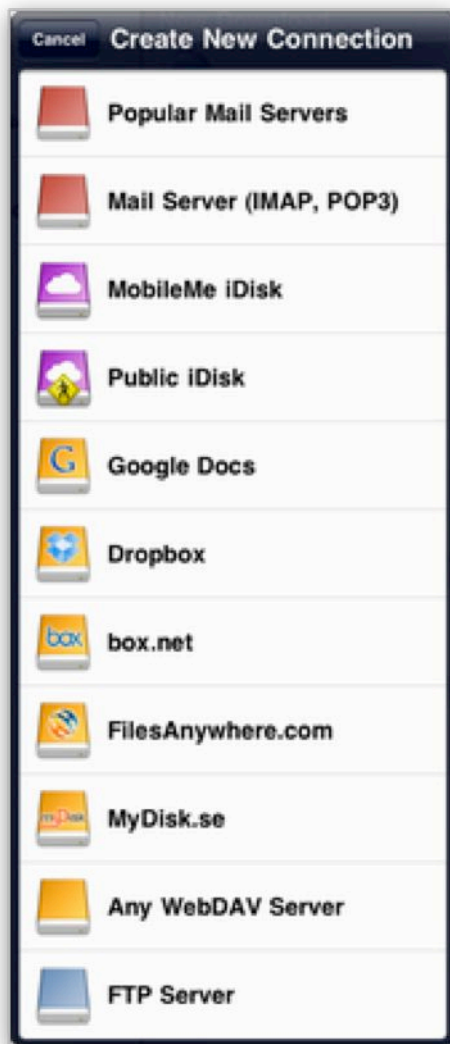


Figure 56: The list goes on, and on, and on.

3. Enter the necessary information for the particular connection method, typically a user name and a password.
4. Tap Add.
5. The server now appears in the Connect to Server list. Tap the server to connect and view files. GoodReader splits the view into one unfamiliar to Mac users, but common under Windows: folders at the top, files below (**Figure 57**).

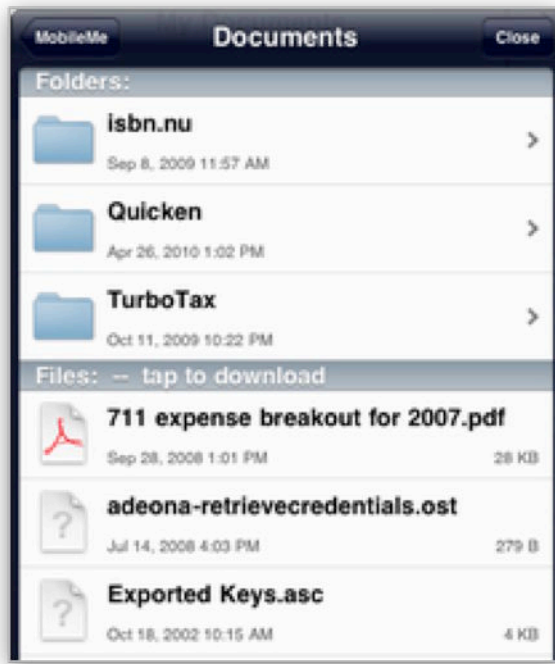


Figure 57: GoodReader shows the folders (top) and files (below) at a remote server.

6. Tap a folder to drill down further; tap a file to retrieve and store it.

GoodReader warns that the interface may freeze for a moment while a file is retrieved.

7. You must tap OK to proceed (**Figure 58**).

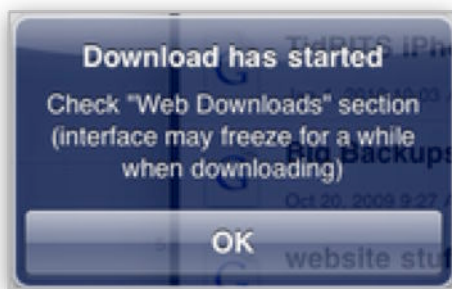


Figure 58: GoodReader alerts you to what might seem like a crash.

Warning! Unlike *Air Sharing HD*, GoodReader doesn't just temporarily store files; it downloads them and retains them until you delete them.

With Google Docs, GoodReader can access a conversion routine from Google to extract a stored document in one of many formats (**Figure 59**).

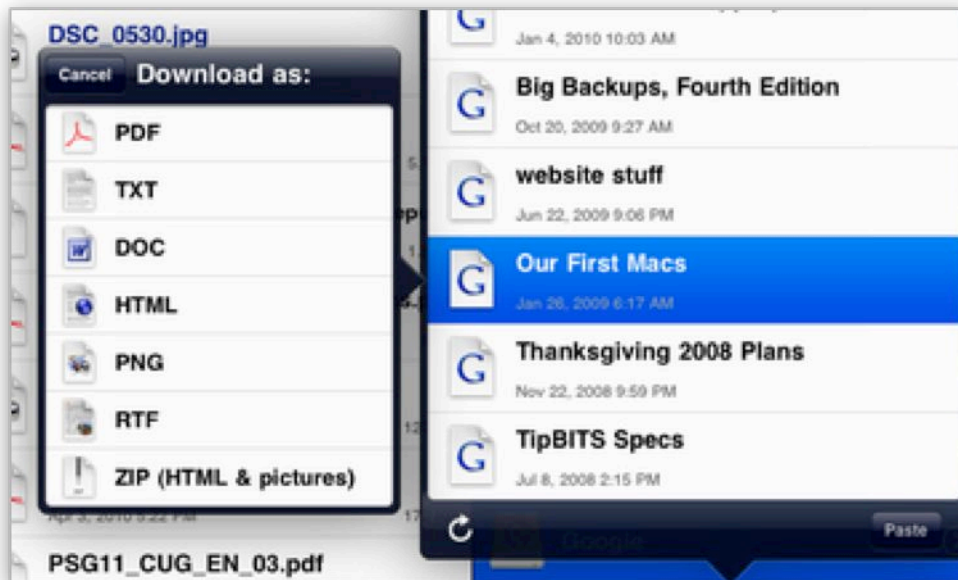


Figure 59: After selecting a Google Docs file, you choose in which format you want to retrieve the document.

Download Files from Web Pages

GoodReader has an additional trick up its sleeve: it can connect to a regular Web server and display Web pages from which you can download files. This is useful when there's a PDF or other file that you want to retrieve quickly into a better viewing environment than Safari.

There are two ways to pull this off:

- Use the Web Downloads option in GoodReader.
- Use a trick in Safari.

Web Downloads Option in GoodReader

For the first method, inside GoodReader, open Web Downloads in the right pane of the main view. Then tap either Browse the Web to open GoodReader's browser and navigate to a Web page or Enter URL to type (or paste) a URL for a specific file to download from a Web site.

Copy a URL in Safari and Paste It in GoodReader

You can copy a URL from a page in Safari by holding down on a link, waiting a moment, and then tapping Copy (**Figure 60**). To copy the current page URL, tap the URL area, tap again, tap Select All, and tap Copy.



Figure 60: Use Copy in Safari to grab the link you need to download a document in GoodReader, such as a PDF file.

To paste the URL in GoodReader, return to GoodReader, access the Browse the Web option and paste the URL by tapping the URL field and then choosing Paste. (There is an even faster way to do this: [A Trick in Safari](#), next page.)

If you tap Browse the Web, you start by entering (or pasting) a URL in a blank browser window, and then you navigate from there. Each time you tap a link, instead of being taken directly to the resulting page, you are prompted through a transparent menu: Follow the Link, Download Linked File, or Cancel (**Figure 61**).

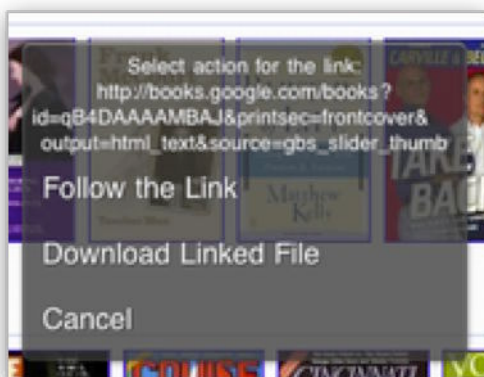


Figure 61: Choose to navigate (Follow the Link) or retrieve (Download Linked File). Cancel keeps you on the page.

A Trick in Safari

Because Safari doesn't let you choose an alternate app to open files, it would seem you were limited to the copy-and-paste advice in the sidebar a page or so earlier. However, GoodReader has a nifty trick you can take advantage of.

GoodReader registers a special URL identifier with iPhone OS so that when the pattern occurs, Safari automatically launches GoodReader to open that URL. GoodReader's trick? The developer added a **g** for GoodReader's registered identifier to the beginning of [http](#) and [https](#), as in [ghttp](#) and [ghttps](#). This lets you edit a URL in Safari to change it to a GoodReader format.

For instance, if you wanted to download a PDF while viewing the PDF in Safari you would touch the location field and hold down until the magnifying glass appears. Drag left to get the insertion point to the left of the **h** in [http](#) or [https](#). Now type **g** and tap Go.

***G not working?** During a last-minute check of this manuscript, we found that this trick wasn't working for us in the latest version of the GoodReader for iPad app. Perhaps it works only with some URLs or perhaps it will work once again in a future version.*

Access GoodReader Storage Remotely


You can use several techniques to transfer files between GoodReader's iPad file store and another computer or device. As with Air Sharing Pro HD, you can transfer files when the iPad is connected to iTunes with USB; for more details, read [Manage and Copy Files via iTunes](#), earlier in this section. Also like Air Sharing Pro HD, GoodReader has a built-in WebDAV server. Unlike its competitor, however, GoodReader's WebDAV server has two distinct limitations:

- It operates only when the WiFi-transfer [sic] window is displayed. You can't use other GoodReader features on the iPad in this mode.
- It doesn't offer secure modes of WebDAV for moving files over an open network. (Why is that a problem? See [Transfer Data Securely](#).)

Nonetheless, GoodReader's WebDAV server works just as expected, and is a perfectly reasonable way to move files in and out.

Only over Wi-Fi: The WebDAV server works only over a local network to which an iPad is connected via Wi-Fi.

To use this feature, follow these steps:

1. Tap the Wi-Fi signal icon  at the bottom of the right column.
2. The WiFi-transfer [sic] window appears. It shows the information you need to enter on another system to gain access to the files and folders available from GoodReader (**Figure 62**).

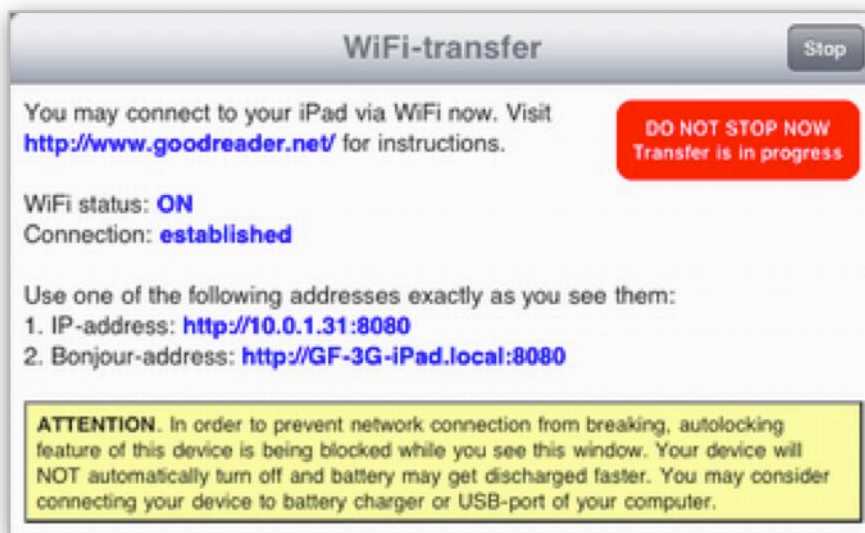


Figure 62: The details above let you access GoodReader's file store from elsewhere on a local network. A red warning appears if the network connection is in active use.

Until you tap Stop, disconnect from a Wi-Fi network, or exit GoodReader, its WebDAV server is available on the local network.

For how to connect to a WebDAV server from a desktop computer, see [Connect to an iPad WebDAV Server](#), later in this section.

View Files

When you tap most types of files in the left-hand My Documents list, GoodReader displays them without any special editing or navigation features. However, when you tap a PDF file, GoodReader overlays a template over a PDF for more efficient navigation (**Figure 63**). It takes a little getting used to, but it's available to view when you tap Help > Show Tap Zones.

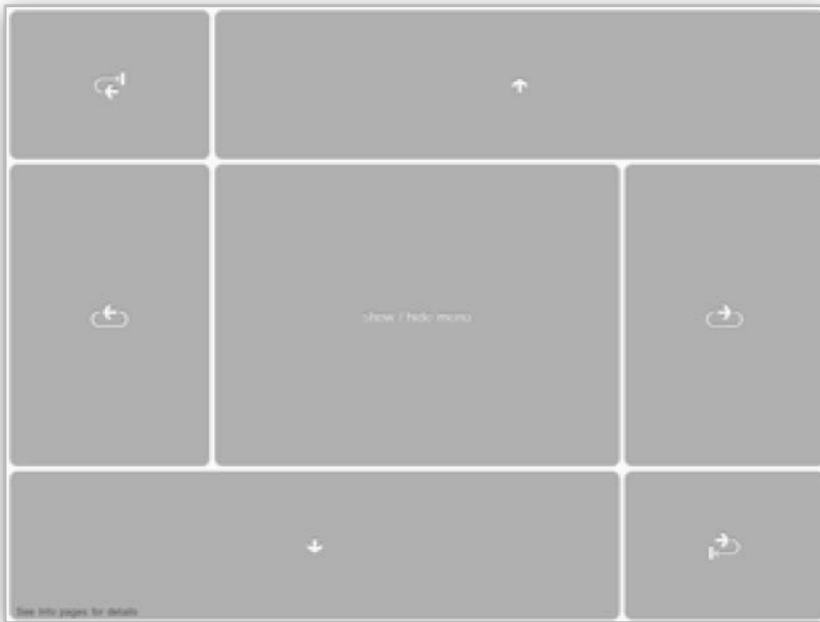


Figure 63: The Tap Zones overlay allows navigation based on where on the page you tap (landscape orientation shown).

Don't miss the show/hide menu zone: Perhaps the most important tap zone to keep in mind is the vertically and horizontally centered box in the middle: the show/hide menu zone. You must tap this zone to reveal the interface around the page, and go beyond reading the PDF and turning its pages.

To search within a PDF, follow these steps:


1. In the toolbar at the bottom, tap the Search  button.
2. Enter search terms (**Figure 64**), and tap Search.



Figure 64: Enter search terms and tap Search.

GoodReader searches through the PDF (**Figure 65**) until it finds a matching result, then displays the page with the result highlighted.

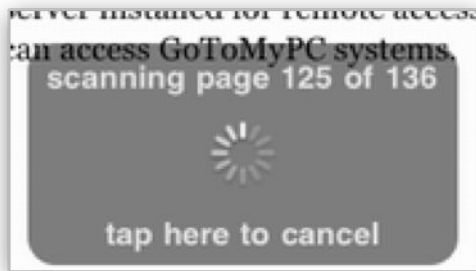



Figure 65: GoodReader scans for the next match.

You can now navigate back and forth through results (**Figure 66**).



Figure 66: The magnifying glasses with up arrow (for back) and down arrow (for forward) step you through matches. Tap the glass with an X in the corner to cancel the search.

To access the table of contents or any bookmarks, tap the Bookmarks  button on the toolbar to open the Bookmarks popover (**Figure 67**). Tap an item in the popover to jump to the location in the PDF. You can also create and then open your own bookmarks.

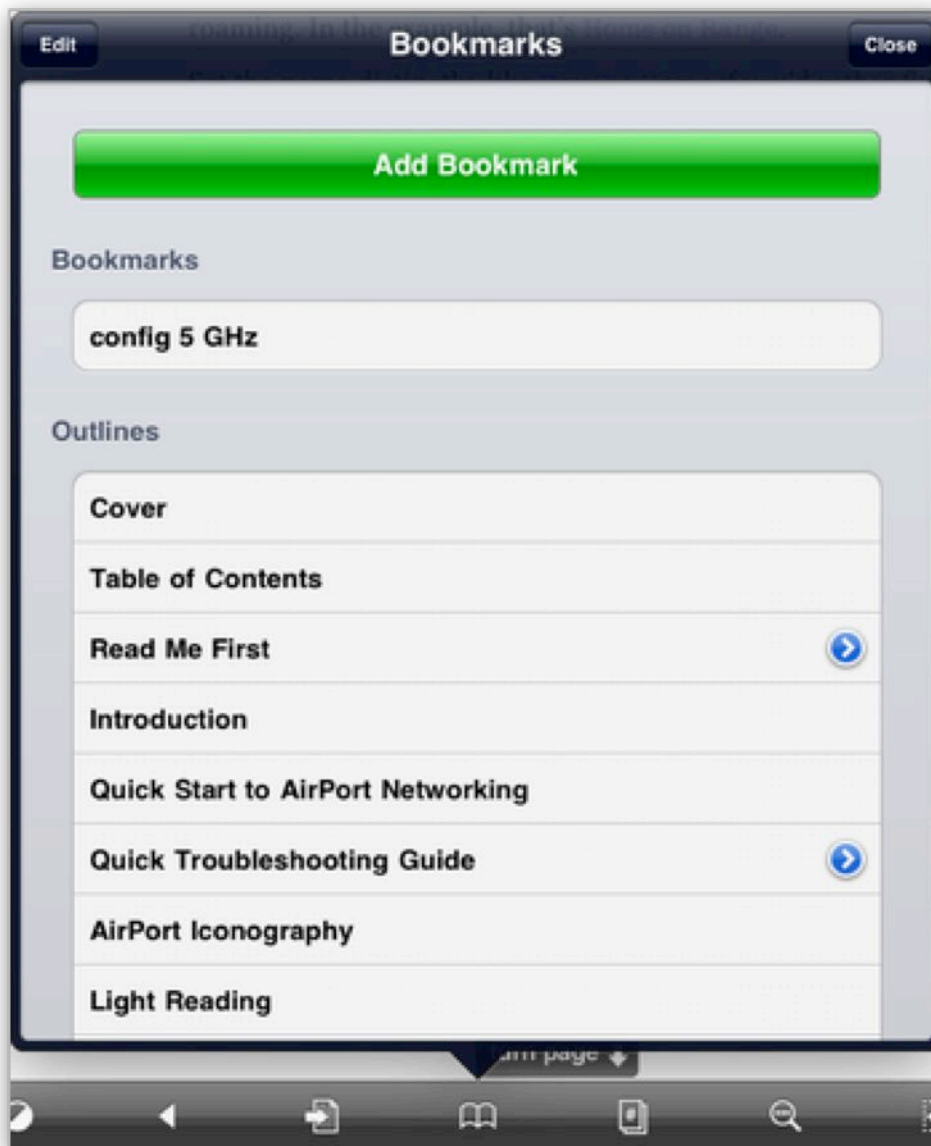



Figure 67: You can navigate via a table of contents developed by the PDF file’s creator, or set bookmarks for yourself.

Tip: You can also tap the Go to Page  button to enter and jump directly to a page number in the PDF.

CONNECT TO AN IPAD WEBDAV SERVER

On a Mac, you access WebDAV servers from the Finder. Follow these steps:

1. In the Finder, choose Go > Connect to Server (Command-K).


2. Type in precisely the name or number provided by the iPad app running the server to which you are connecting. Typically you can find this information by tapping a Wi-Fi  button on a toolbar in the app (entering the name, while it takes more keystrokes, lets you bookmark the iPad for later access while the app's server is active.)
3. In the login dialog, enter the details you set in the app's Sharing Security settings (**Figure 68**) and click Connect.



Figure 68: Log in with the details you set in the app, if any.

Invalid certificate? If you connect with either secure (https) address offered by Air Sharing HD, Mac OS X warns you about an invalid certificate. That's because Air Sharing HD uses a digital identity that's not registered with an external certificate authority. But you know it's fine, because you're controlling both ends of the connection. Click Continue to bypass the warning, or if to also skip the warning in the future, click Show Certificate, expand the Trust section, and from the When Using This Certificate pop-up menu choose Always Trust.

4. The app's file store appears as a volume on the Desktop (**Figure 69**).

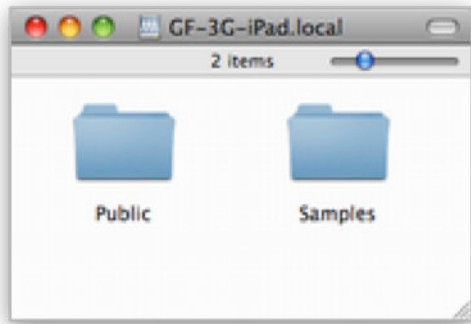


Figure 69: The app’s storage mounts and appears on the Desktop.

You Can Connect from Any Apple Device!

On another Apple networked device, including another iPad, you can also connect to your iPad’s WebDAV server and then transfer files between the devices using Air Sharing HD, GoodReader, or other software that handles WebDAV serving and access. One device is set to share; on the other, you connect using the information provided. Nifty!

In Windows, there are several ways to access an iPad app’s WebDAV server; here is some general advice.

To make the connection:

- In Windows XP, from the Start menu, click My Network Places. In the My Network Places dialog, in the “Network Tasks” section near the upper left, click Add a Network Place.

Windows XP note: *The folks at Good.iWare and Avatron recommend that XP users install the Microsoft Software Update for Web Folders; find it at <http://support.microsoft.com/kb/907306>.*


- In Windows Vista or 7, from the Start menu click Computer. From the toolbar at the top of the Computer window, click the Map Network Drive button. Click the “Connect to a Web site...” link.

Now, follow the prompts in the Add Network Place wizard, making sure (if it comes up) to uncheck Log On Anonymously.

DROPBOX

The Dropbox ecosystem lets you store files in a folder on any computer on which you have Dropbox software installed, and have any changes to items in that folder immediately synchronized, not only to Dropbox's cloud-based servers, but also to all registered computers.

You can also share individual folders within the Dropbox folder on your computer to another person or a group of people, thus making a "local" copy of that folder on the computer of each person it is shared with. Changes in any such local folder are copied right away to a Dropbox server and then relayed to each corresponding local folder as fast as each Internet connection allows. Dropbox includes 2 GB of free storage and charges monthly fees for larger quantities (<http://dropbox.com/>).


Inherently secure: *Dropbox uses only secured transfers. There's no need to worry about files being seen in the clear on open networks when you use the service. However, for maximum security, you'll want to protect your Dropbox files in case your iPad is borrowed or stolen by the wrong person. To do so, in the Dropbox app, tap the Settings  button and then tap Passcode Lock. Of course, the best protection in the case of theft will be to wipe the iPad with Find My iPad (see [Find My iPad via MobileMe](#)), and change your Dropbox password on the Dropbox site.*

It's natural to want a window into Dropbox from an iPad, and Dropbox obliges. You can access Dropbox files using the free, universal [Dropbox](#) app, which works well on any iPhone OS device.

Warning! *The Dropbox app cannot automatically update its iPad file store. See <https://www.dropbox.com/help/82> for details. You use the Favorites popover to check for updates and update files, described later.*

Alternately, some iPad apps have added Dropbox support, allowing you to access Dropbox files via the Internet, without the Dropbox app. In particular, Air Sharing HD and GoodReader for iPad both support Dropbox. Compared to the Dropbox app, they both have superior reading features, so you may prefer to use them.

Access Files

When you first launch the Dropbox app, you enter the user name and password associated with your account. That information is stored for later logins. (To make the app forget your login credentials, tap the Settings  button and then tap Unlink iPad from Dropbox.)

To access available files, put the iPad in landscape orientation and navigate in the left pane. Or, in portrait orientation, tap the My Dropbox icon to open the My Dropbox popover (**Figure 70**).

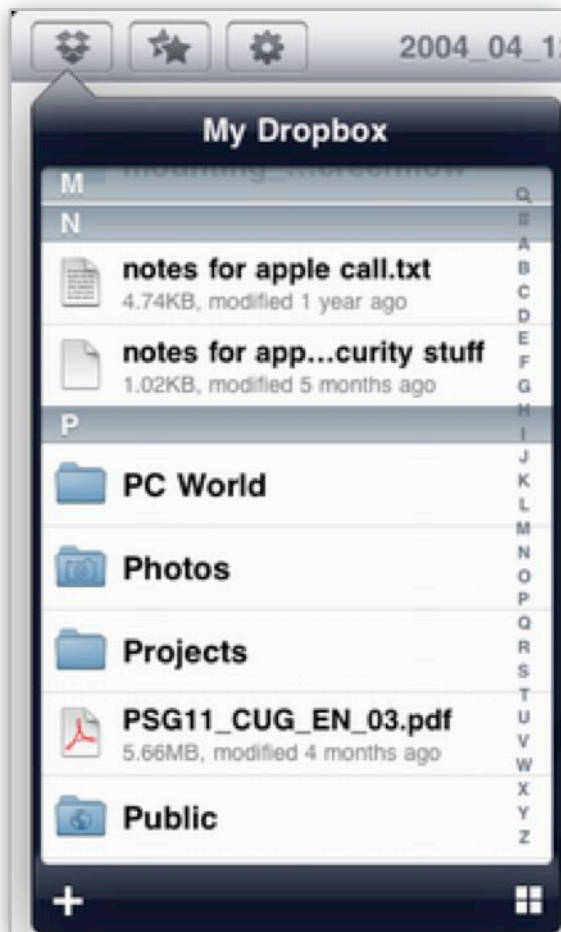


Figure 70: The My Dropbox pop-over shows you the contents of your synchronized Dropbox storage.

Tap folders to drill down. In longer file lists, tap letters on the right to zip through the list. (A sort by date or category option would be welcome!) Tap a document to view it. Dropbox's viewer lets you scroll through multi-page documents, but it has no search or other features for PDF or other file formats.

Here are a few important Dropbox tips:





- To share a file, tap  in the toolbar (top, right). Dropbox lets you email a public link to the file, or copy that link to the Clipboard.
- To add photos or videos stored in the Photos app to your file list, tap the plus  button at the left, below the file list.
- When working with the file list, you can preview a folder of images or PDFs as thumbnails by tapping the Thumbnails  button at the bottom of the file list (**Figure 71**).



Figure 71: In landscape mode, the image preview gallery appears as a popover. Tap an image or any supported file format, and it's downloaded (if not already cached locally) and displayed at right.

Keep Files Locally

Dropbox temporarily downloads any file you tap to view (if it's a supported file format), but you can store that download by tapping the Make Favorite  button in the upper right of the view.



Tap the Favorites  button in the upper left to see items you've marked to keep downloaded. Files that are downloading have a blue rotating badge (just as with Dropbox in desktop operating systems); a green checkmark badge indicates a fully downloaded file (**Figure 72**). Tap X  to cancel a download in progress.



Figure 72: Files with a green checkmark are fully downloaded.

Files aren't automatically updated due to restrictions in how Dropbox can operate under iPhone OS, the company says. But you can update manually via the Favorites list, and the app does note files that need updating.

The Favorites list has three features bundled into two actions:

- Tap Edit to delete files (removing them from the local data store) or change the order in which they appear in the list.
- Files that are out of sync are marked with a green arrow. Tap an individual file to download its latest version, or tap Update All to refresh the contents of all stored files.

iDISK

The free [MobileMe iDisk](#) app provides a view into your MobileMe iDisk storage. Apple has not updated it as an iPad app, but it works in compatibility mode. Because iDisk files can be accessed with apps like GoodReader and Air Sharing HD, there's no compelling reason to use

the iDisk app unless you frequently need to share iDisk files or you want to delete items from your iDisk using an app.

The main screen lists the folders on your iDisk. Tap a folder to navigate down; tap a file to view it (**Figure 73**). Files that you view aren't stored locally, just downloaded temporarily.



Figure 73: You can view photos stored on your iDisk.

Three other iDisk features extend the app's usefulness:

- **Share a file:** You can share a file stored on your iDisk by sending an email message containing a download link to that file. To do so, either tap the Share icon to the right of the filename in the list view, or view the file and tap the Sharing icon at the bottom of the screen. Files you've shared via the iDisk app or via Me.com are shown in the Shared Files view. You can re-share items for which the expiration date has passed from that view, too.
- **Delete a file:** You can delete a file either in the list view (tap Edit) or while viewing the file (tap the Trash icon).
- **Connect to other MobileMe public folders:** Tap the Public Folders button.

Transfer Data Securely

Any networked mobile device, whether an iPad, laptop, Nintendo game player, or what have you, can be in constant communication with a network, which means that you could unintentionally reveal a lot about yourself—including passwords and private data—as it flows between a central hub and the device. With an iPad, that hub is either a Wi-Fi router or a 3G base station on a cell tower nearby.

On an open public network, such as the Wi-Fi found in hundreds of thousands of restaurants, cafés, and airports worldwide, anyone in your vicinity can use free, simple *sniffing* software to capture all the data passing by, extract passwords and personal information, and use it to wreak havoc, commit identity theft, and order goods and services for themselves. While it may sound paranoid, there's no built-in protection for some of your data, and you thus have to assume from the perspective of risk that someone is always trying steal your data.

Fortunately, it's easy to overcome this problem with a small amount of preparation and configuration. Here's what you need to know to stay protected while using local networks and the Internet.

EXPOSURE

To figure out how to respond to the risk of data being captured as you transfer it, let's first consider what precisely is at risk and not at risk.

Cellular data is far less risky: *Cellular data is encrypted by default, and cell networks have far less risk for use. See [2G](#) and [3G Data Networks](#) for more details, later in this section.*

What's at Risk?

When you're connected via Wi-Fi, the risk is both in data passing over the air from the iPad to the Wi-Fi router, and data passing between the Wi-Fi router and a broadband modem over Ethernet. Malicious software that's found its way onto a computer that's

connected via Ethernet to a Wi-Fi router could sample all information coming and going between Wi-Fi–connected devices and the Internet.

Here’s a short list of what a sniffer could extract from capturing all the data passing over a Wi-Fi network and beyond to and from your iPad:

- Email passwords for accounts that aren’t protected with SSL/TLS
- WebDAV accounts, used for file-server access in many iPhone OS apps (including accessing MobileMe), unless the WebDAV server’s URL starts with [https](#)
- The contents of Web pages viewed and forms submitted, unless the URL starts with [https](#)
- Screen sharing via VNC, unless SSH encryption is also enabled (see [Remote Access and Control](#))
- FTP has various risks:
 - Passwords and data sessions are exposed with plain FTP.
 - Data sessions are exposed with FTP over SSH (which is distinct from Secure FTP and FTP over SSL, explained just ahead).

More generally, unless a developer discloses the information, we don’t know whether an app that communicates with remote servers encrypts logins and data in transit.

Logins protected: *Most Web sites and apps are smart enough to encrypt logins, even if they aren’t consistent enough to protect data exchanges after login.*

What’s Not at Risk

There’s a large set of data that’s not at risk, because it’s protected by strong encryption that prevents anything but the server on the other end of a connection (a mail server, Web server, Internet telephony node, and so on) from deciphering and interpreting the results.

Ask the developer: *If you don’t know whether or not a particular app or service uses encryption and it’s not described ahead, ask the developer! If you don’t get an answer, or find that it’s not secured to your liking, find an alternative.*

Let's take note of three types of communications that you don't have to worry about.

SSL/TLS-protected Sessions

Hey, you say, that's a mouthful! Let me break it down. *SSL* (Secure Sockets Layer) is the older name for what's now known as *Transport Layer Security*. It's a basic means of protecting a connection between two parties, usually a client (like a mail program) and a server (like a mail server). SSL/TLS connections use certificates and outside verification of those certificates' validity. This makes SSL/TLS connections quite secure and reliable.

SSL/TLS is used for the following kinds of things:

- **Email connections:** On the iPad, the default mail services that Apple lists in the Add Account pane of the Settings app (except Microsoft Exchange) are secured by default. Exchange may or may not be secured depending on your network administrator. You can also create an email connection to other mail hosts and enable SSL/TLS.

Dump non-secure hosts: *If your mail provider doesn't offer secure email connections, switch providers. There's no excuse.*

- **Web sessions:** If the URL in your browser's location field starts with [https](https://) and there's a lock icon somewhere in the Web browser's interface, then you're on a secure site (**Figure 74**). Any data sent and received is secure from prying eyes.

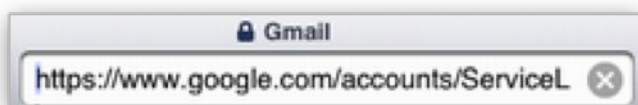


Figure 74: The lock by the title of the page and the [https](https://) in the location field indicate that this site uses SSL/TLS to protect data in transit.

Smart sites use protection: *Ecommerce sites, pages on which you enter credit cards, banking sites, stock-trading sites, and many email hosts use encryption by default, and have no other way to access information.*

- **WebDAV:** The file-transfer protocol used by MobileMe and other sites, WebDAV is widely supported in file-viewing apps (see [Access Documents](#)). It can work in a plain, unprotected mode or over SSL/TLS. The URL for an SSL/TLS-protected site will start with [https](#), just like a secure regular Web site.

Warning! *Some WebDAV servers may use a certificate that was generated without verification by a third party (called a certificate authority). If you access one of these on an iPad or desktop operating system, the device will warn you to make sure there's no skull-duggery involved. When connecting between two machines right in front of you, there's no risk in accepting a so-called self-signed certificate.*

- **FTPS:** *FTP*, a file-transfer standard, comes in many forms. *FTPS* (FTP over SSL/TLS) is a secure method for transferring files, but not in nearly as wide use.

SSH-protected Sessions

SSH (Secure Shell) was developed for terminal sessions, where you control a system through command-line instructions. Its use is now widespread for certain kinds of session-based software, especially when two computers, neither of them used as network servers, connect to one another.

No certificates: *SSH doesn't require a third-party signed certificate to start up a connection as does SSL/TLS, which removes some of the overhead of having a third-party involved in verifying the connection. SSH security can be just as strong as SSL/TLS.*

On an iPad, typical uses of SSH include:

- **VNC (Virtual Network Computer) remote access:** VNC itself lacks strong encryption (it uses a breakable password method), but programs like iTeleport allow a connection to open first using an SSH session, after which VNC starts up inside an encrypted *tunnel*.
- **SFTP:** SFTP isn't really FTP; it's a different protocol that's widely supported. SFTP uses SSH to handle file transfer securely.

- **Terminal connections:** There are a handful of terminal apps for the iPad that you might use for command-line sessions for Unix and Mac OS X systems that support SSH.

Proprietary Services

Several apps that connect to special services feature end-to-end encryption, although that must be enabled in some cases. Here's a partial list, based in part on services I've tested on an iPad:

- Dropbox uses strong encryption for data transfer. SSL/TLS is used for file transfers, and files are stored in encrypted format locked with your account password (<https://www.dropbox.com/help/27>).
- Google logins are protected, but not necessarily the contents of Google-browsing sessions. See [Secure Solutions](#), next page.
- iTunes purchases and downloads are protected by Apple, likely using SSL/TLS for logins. Apple doesn't disclose its methods.
- LogMeIn remote access sessions are secured by SSL/TLS, layered with other security methods (<https://secure.logmein.com/US/security.asp>).
- Skype's voice and other communications tools are secured by a proprietary system which involves several components to secure logins and the contents of sessions (<https://support.skype.com/faq/FA145/What-type-of-encryption-is-used>).

What Networks Are Risky?

As I noted in the introduction to this section, public hotspots are risky. Outside of public Wi-Fi networks, however, you have enormously lower general risk, and very little practical risk of having data intercepted.

Wi-Fi at Home or Work

At home your data will likely remain safe as long as you have WPA Personal or WPA2 Personal enabled; at an office, either of those or WPA2 Enterprise will protect your data.

Offices that handle sensitive data should opt for WPA2 Enterprise because it allows individual user names to be set for network access, access can be tracked and revoked, and it likely conforms to rules

requiring extra protection for firms handling legal, medical, and financial records.

For someone to capture data at home or at your work, that person would have to stake out the network, break your encryption method, and get something useful during the period of time he or she is observing. If someone were targeting you personally due to a grudge, a court case, or another reason, WPA/WPA2 encryption would protect your networks.

Warning! *WEP is effective only as a no trespassing sign. It's quick and simple to use free software to crack a WEP-protected network, so WEP is no good even as a thin shield.*

Tip: See [Connect to a Secure Wi-Fi Network](#) for more details.

2G and 3G Data Networks

2G and 3G GSM data networks always secure all the data passing over them, partly using information on the SIM (Subscriber Identity Module) that's part of any phone or device, such as the iPad.

There have been exploits that allow 2G data to be cracked and read, but it requires a fair amount of concerted effort, unlike a sniffer at a hotspot. Someone has to target you or a particular area for a period of time and have a reasonable amount of gear.

The encryption system used for 3G GSM networks has some flaws, but they are not broken yet (and can be improved for flaws that were found). Even if broken, someone would need to exercise serious and specific scrutiny to obtain your data.

SECURE SOLUTIONS

In cases in which some kind of security isn't in place by default, you can turn on protection. Let me start with an overall method, and then look at individual switches and controls for particular services.

Umbrella Protection with a VPN

A *virtual private network* (VPN) 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, creating a *tunnel* that

extends between the iPad 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 provide a way to extend the aegis of corporate security to remote devices and computers. 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, 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 methods described earlier), but that's typically just fine. The point of risk is the local link. Before you can get the iPad set up, however, you need to find a VPN service.

There are several kinds of VPN protocols, and the iPad (and all iPhone OS devices) support some of the most popular.

VPN Protocols in iPhone OS 3 and iOS 4

iPhone OS 3 handles L2TP, PPTP, and IPsec. The first two are generic, widely used standards. The IPsec label actually works only with a specific Cisco VPN version, even though the term *IPsec* is a standard term in the security industry. (Apple, like many companies, spells IPsec with a capital S, even though that's the wrong capitalization.)

SSL-based VPNs are not supported in iPhone OS 3, but Apple plans to add two SSL types (from Cisco and Juniper) in iOS 4.

Mac OS X Server and Microsoft Windows Server in any recent vintage (since about 2004), include VPN server software you can use without turning to a third party. Ask your network administrator (if one exists), or find a consultant to help configure the VPN services securely.

Find a VPN Service

Several firms offer "VPN for hire," letting you pay a monthly or yearly fee for VPN service to their data center servers. Here are two that I've had experience with:

- **WiTopia's personalVPN:** WiTopia offers a PPTP-based VPN service for the iPhone OS. Some hotspots block PPTP for reasons

that are unclear to me. That said, I've rarely had trouble using PPTP on the road (<http://www.witopia.net/index.php/products/>, \$39.99 per year).

- **PublicVPN.com:** This firm uses another popular VPN method called L2TP-over-IPsec (L2TP in the iPad's interface). L2TP seems to be more broadly passed through public networks than PPTP (<http://publicvpn.com/>, \$6.95 per month or \$69.95 per year,).

Set Up a VPN Profile

It's quite easy to set up VPN profiles on an iPad. 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 > Network > VPN.
2. Tap Add VPN Configuration (**Figure 75**).

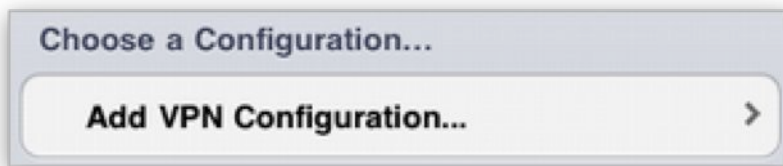


Figure 75: Add a VPN configuration here.

3. In the Add Configuration screen (**Figure 76**), fill in the settings:
 - Pick L2TP, PPTP, or IPsec, whichever is appropriate. The choice here affects which options appear below the header, as each standard has different requirements for configuration.
 - The description appears in the VPN view after you create the configuration, so enter something short and expository.
 - Server, Account, and Password tell the iPad which Internet host to connect to using which credentials.
 - RSA SecurID (L2TP and PPTP) should always be set to 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 (not shown) can be ignored unless you've been told otherwise.



Figure 76: Enter the details you were given.

4. Tap Save.

You now have a configuration profile that you can use.

Make a VPN Connection

In the General > Network > VPN pane of the Settings app, set VPN to On, and the iPad will connect using the profile; if there's more than one VPN profile, you'll be prompted to choose one.

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

- A VPN indicator appears in the status bar beside the network connection icon (**Figure 77**, top).
- A Status entry appears in the VPN pane in the Settings app and shows how long you've been connected (**Figure 77**, bottom).



Figure 77: The status bar shows an active VPN connection (top), while the VPN view shows how long you've been connected (bottom).

To check the status of your VPN connection, tap the current connection time in the VPN pane to view the Status pane (**Figure 78**). The IP Address field is a clue to the facility at which your VPN terminates.



Figure 78: Connection details reveal a little more information about where the VPN terminates.

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.*

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 settings pane. Disable a VPN connection by setting VPN to Off in the left pane of Settings or in General > Network > VPN.

Note: With a VPN profile configured, the VPN switch appears in the Settings app's left pane near the top, below Airplane Mode and Wi-Fi. You may have to exit and return to the Settings app to see the switch.

Protecting Particular Services

You can avoid the cost and configuration needed for a VPN by making sure each service you need is secured, or by only using secured services on public Wi-Fi networks.

Here are three tips:

- Make sure you're always using SSL/TLS email connections. There's no good reason not to. If your mail host doesn't provide secured email for your incoming email (POP or IMAP, likely IMAP on an iPad) and for your outgoing email (SMTP), find a new host. Email programs otherwise may send passwords in the clear or with weak encryption, and likely send all data in the clear. Refer back to [What's Not at Risk](#), earlier in this section, for a few more details.
- Set Google to use secure services for Web access, something the company doesn't provide by default.
 - With Gmail, start in Safari by entering <https://mail.google.com/> to connect to your account. Log in. If the Settings link does not appear at the top right of the screen (it won't on the iPad), at the bottom of the screen, tap Basic HTML to access settings.

Now tap Settings at the top right of the page. In the General settings tab, in the Browser connection option, tap the Always Use https radio button. Tap Save Changes.

- For other Google services that aren't secured by default in a browser, precede the address with <https>, as in <https://docs.google.com/>. Google then uses a secure connection.
- Only use a secured alternative to plain FTP. FTP programs otherwise send passwords and data in the clear.

Keep Data Safe

Someone using a completely unprotected iPad can access any precious information stored on it and access accounts related to apps and Web sites. You can prevent other people from having access to that data, whether you leave an iPad on your living room table or in your office cubicle and walk away for an hour, or if your iPad is stolen.

EXPOSURE

Let's start with your exposure. The iPad keeps relatively little data accessible; rather, what's at risk is access to resources. A person who uses your iPad without permission cannot, for instance, recover your email account password, but could use your email account to read your email and send email purporting to be from you, or view any document in a word-processing program and view your photos.

What's at Risk?

Here are examples of data that could be accessed by someone else:

- If you use programs like Air Sharing HD and GoodReader, a finder or thief could access—and potentially change or delete—files on any server you linked in to those programs for remote file access.
- Access to email accounts for sending and receiving email.
- Access to the content provided by apps that store passwords for access, such as Netflix (but not the passwords)
- Access to Web sites for which you have stored login information in Safari. (See [The Danger of Safari's AutoFill](#), two pages ahead.)

In the above two cases, if you've set up those accounts using an email address that is also receiving email on the iPad, the person using your iPad could likely change your password. And, in some cases, that person could pretend to be you, a drama that you might not appreciate in your Facebook account.

Real World Example

A friend recently had her Gmail account hacked—probably by having the password sniffed—and the hackers sent out a scam message to all her friends asking for them to help her by wiring £1,500 to London where all her stuff had been stolen. The scammers changed her Gmail settings to forward email to an address of theirs, too. It took her days to get things back under control. This could easily happen with an iPad with a stored email password either in Safari (where Gmail can be set to “remember” you) or via the Mail app.

Further, if you save your login information in Safari for an ecommerce site, and then a thief logs in to that site, orders items, and changes the delivery address, even if the site confirms the address change via email, the thief could access your email to acknowledge that confirmation.

Amazon’s clever approach: *Even if you’ve stored your login data for Amazon.com, the company uses extra security checks for orders when addresses are changed. Sometimes, you have to re-enter some credit-card information, or log in again on a different secure page on which a password might not be cached for use. That’s what 15 years of experience selling on the Web brings to an ecommerce site.*

This is also why Apple prompts you to enter your password again when you’re already logged in to access certain features at MobileMe via me.com, such as Find My iPad and billing settings.

What’s Not at Risk?

Here’s a quick list of data that’s not at risk of being accessed by the wrong person:

- Passwords for App Store, iBookstore, and iTunes Store purchasing. Apple prompts for your password if it hasn’t been entered recently.
- Your stored passwords. Mail, Safari, and all the apps I’ve used over the last few years store passwords but don’t reveal them.
- Purchases on your AT&T 3G account on a 3G iPad. AT&T doesn’t cache the password needed to make changes to a 3G data account. And, even if someone had the password, the only actions that are

possible are to renew, cancel, or make a one-time (if expensive) international data plan purchase.

The Danger of Safari's AutoFill

With AutoFill turned on, you can save a lot of time by not re-entering the same routine login information for Web sites. The iPad retains information that you enter with your permission. However, someone who gains access to your iPad can also log in to your account on the various sites for which you've used AutoFill to store user name, password, and other authentication data.

You can disable this option in the Settings app. Tap Safari > AutoFill, and set Names and Passwords to Off.

MITIGATION

There are two ways to lock down your iPad's data. The first is the built-in passcode system that can prevent unauthorized access to the iPad overall. The second is a third-party password safe that can lock away information from prying eyes.

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 iPad.

To set the passcode lock, follow these steps:

1. In Settings, tap General > Passcode Lock.
2. Tap Turn Passcode On.
3. Enter a four-digit passcode, and re-enter when prompted.

You can also enable the passcode lock remotely if you have an active MobileMe account and Find My iPad enabled on the device. See [Find My iPad via MobileMe](#), ahead.

Tip: Is four digits not good enough for you? You can set a longer passcode, too. See [Advanced Passcode Configuration](#), next page.

Passcode Options

The Passcode Lock screen offers a few additional security options. You can set the interval for which you must enter a passcode from Immediately to After 4 Hours:

- Immediately means that you're always asked for the passcode any time the iPad goes to sleep. You can put the iPad to sleep manually, of course, by pressing the Sleep/Wake switch on its edge, but you can also set the iPad to sleep automatically, with the General > Auto-Lock option in the Settings app.
- Longer intervals let the iPad be unlocked without a passcode for up to the time duration you've chosen from the list.

The Picture Frame switch lets you enable or disable showing your photos when the passcode lock is required.

As a nuclear option, you can set your iPad to self-destruct—destroy its data, at least—if there are more than ten failed attempts to enter the passcode correctly. What do you lose? Only items created since the last backup and sync; see [Remote Wipe](#) in [When Your iPad Goes Missing](#).

Warning! *A dedicated cracker can use easily available tools to bypass the passcode—even a longer passcode like those I explain how to set up ahead—in a couple of minutes. Apple will encrypt email in iOS 4, making that unreachable even if the device is hacked.*

Advanced Passcode Configuration

For some of us, four digits isn't a strong-enough passcode. You can make (and even require) a longer code, if that's what you like. To do so, you use free software from Apple called iPhone Configuration Utility, which is primarily used for business configurations.

Download iPhone Configuration Utility (for Mac OS X or Windows) from <http://www.apple.com/support/iphone/enterprise/>, install it on your computer, and launch it. The utility lets you set up a configuration profile, which can then be applied to one or more devices.

Follow these steps to get started:

1. In the utility, in the sidebar at the left, select Configuration Profiles under Library.

2. In the toolbar at the top, click New.
3. In the General pane that appears, name the profile something memorable in the Name field (perhaps “severe password policy”) and assign an Identifier, which must be in the form *com.something.something*, such as *com.glennf.severeprofile*.
4. Beneath General in the list of options for the new profile, click Passcode.
5. Click Configure. (You can have multiple Passcode policies.)
6. Choose among the various options, including requiring a passcode, having a minimum passcode length, expiring passcodes after a period of days, and requiring a new passcode each time (up to 50 changes). You don’t need to save anything when done.

Warning! *If the computer on which iPhone Configuration Utility is running is not the one with which you sync your iPad, first launch iTunes, and make sure that in Preferences, in the Devices pane, the box is checked for “Prevent iPods, iPhones, and iPads from syncing automatically.” Otherwise, you could mess up your iPad’s media, apps, and other synced data.*

7. Now connect your iPad via USB to the machine on which the utility is running.

The iPad’s icon appears in the sidebar of iPhone Configuration Utility, under Devices (**Figure 79**).



Figure 79: The utility shows any connected iPhone OS devices.

8. Select the iPad in the sidebar, and click the Configuration Profiles tab.
9. In the listing for the new profile that you just created, click Install (**Figure 80**).

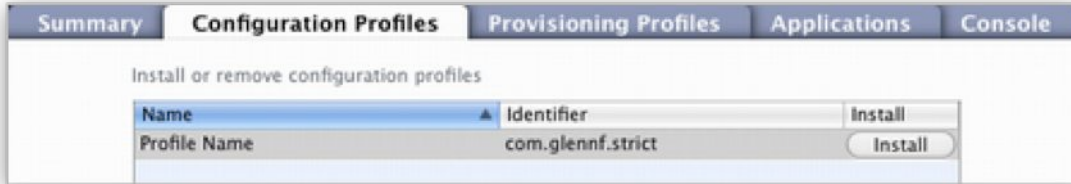


Figure 80: Click Install to add this profile to your iPad.

10. Your iPad now displays the profile in a pop-up dialog. Tap Install to proceed, and you're prompted to make sure you mean it (**Figure 81**). Tap Install Now.



Figure 81: Tap Install Now to add the stronger passcode configuration you set in the utility.

11. With the new profile, you must immediately set a password that conforms to your stronger settings (**Figure 82**). Enter such a password, tap Next, enter it again to verify it, tap Next, and you're finished.

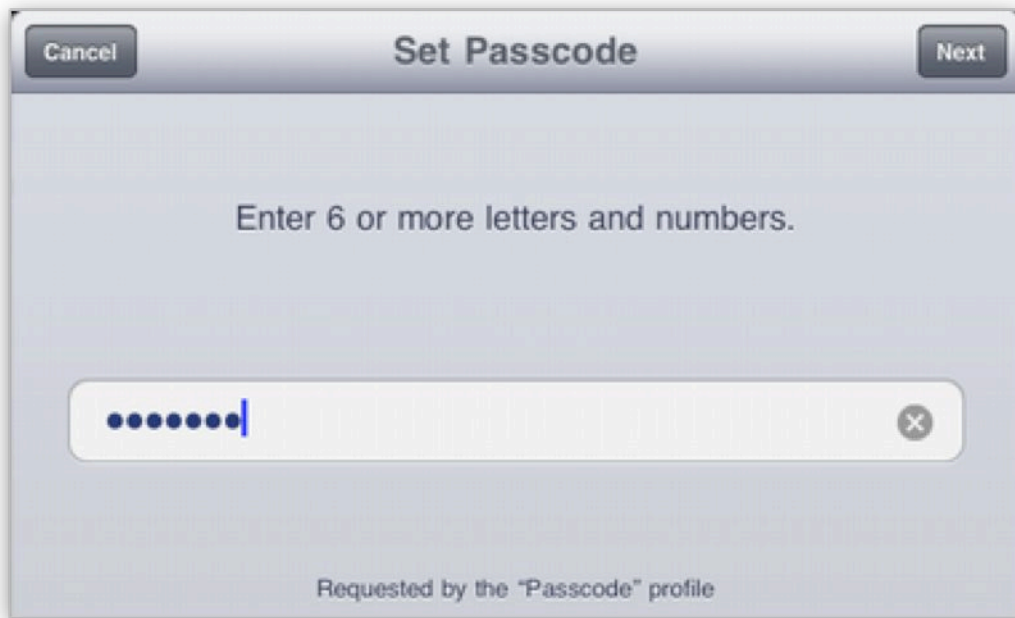


Figure 82: A note at the bottom of the Set Passcode pane reminds you that the new password is required by the profile you just installed. (It says “requested,” but it’s not optional.)

12. The profile is shown as installed. Tap Done to complete the process.

The next time you try to unlock your iPad, you will be shown the type of keyboard needed to enter the passcode (**Figure 83**). For instance, if you’ve chosen letters, numbers, and punctuation, you’ll see a full keyboard.

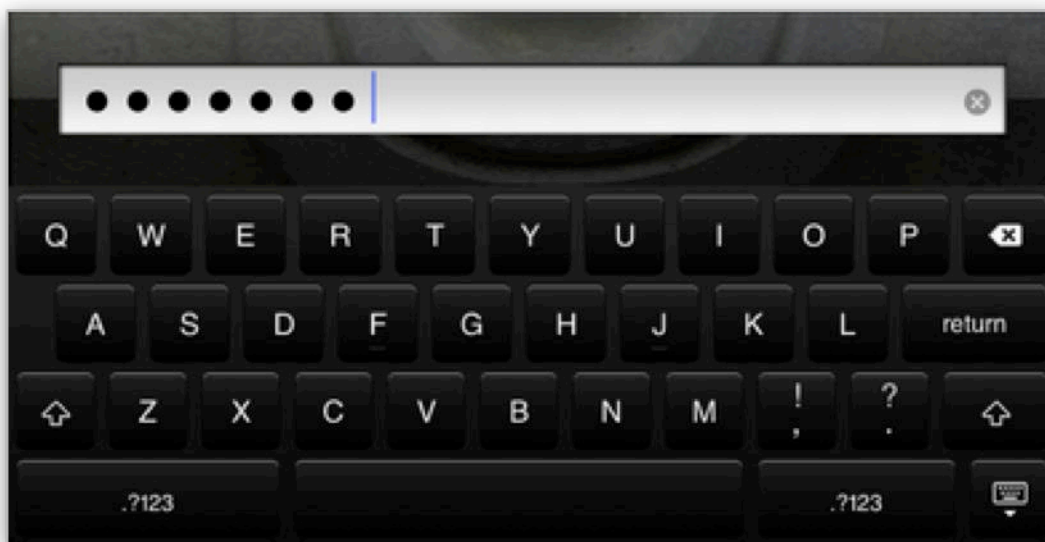


Figure 83: A full keyboard appears for you to enter a mixed-character password.

To revert to the default four-digit passcode format, follow these steps:

1. In the Settings app, tap General > Profile.
2. Tap the passcode profile you installed.
3. Tap Remove.
4. Enter your passcode as prompted.
5. With the profile removed, in General, tap Passcode > Change Passcode.
6. You're prompted to enter your current passcode (the one associated with the profile you just removed).
7. Set a new four-digit passcode.

The next time you unlock your device, the regular four-digit keypad display appears for passcode entry.

Store Information in a Password Safe

Several apps let you store private data, including passwords for access to email, Web sites, and financial services. These include [mSecure](#), [eWallet](#), [1Password](#), and many more. The goal of each of these apps is to give you an easy and secure way to travel with data you need. (See [The Danger of Safari's AutoFill](#), earlier in this section.) The best of these apps work with desktop software, too, letting you regularly sync your data over a local Wi-Fi network with a desktop machine.

I'm most familiar with 1Password from Agile Web Solutions, which comes in three iPhone OS releases (<http://agilewebsolutions.com/>). My fellow Take Control author Joe Kissell, who wrote *Take Control of Passwords in Mac OS X*, recommends 1Password as his top pick.

1Password Editions

[1Password for iPad](#) (\$6.99) works only on the iPad, while plain old [1Password](#) (\$6.99) is compatible with the iPad, but uses only the iPhone/iPod touch screen size. [1Password Pro](#) (\$14.99) is the universal edition, so it works on whatever device you have, has better Safari integration than its cheaper siblings, and is slated to have synchronization that doesn't rely on a local network connection in a future release. If you own multiple iPhone OS devices, Pro makes sense since it will work on all units.

1Password (and similar apps) use internal encryption separate from anything Apple provides to lock your data away. You enter a password when launching the program; that password is stored only for a period of time you specify (**Figure 84**).



Figure 84: An impressive graphical lock guards your private data.

Stored passwords and information are divided into categories in 1Password. Web accounts are stored in the Logins field. You can select a login (such as Barnesandnoble.com, as shown in **Figure 85**), and tap the right arrow ➔. This opens a Web browser sheet inside 1Password and the app logs in to the site.

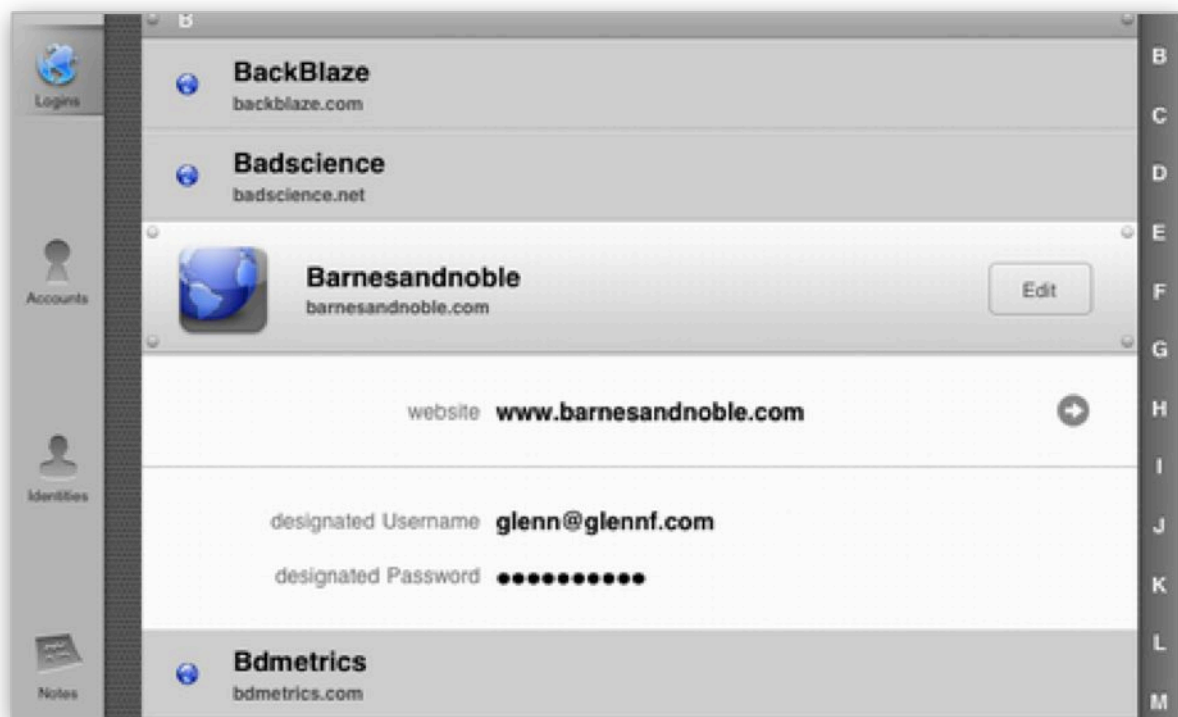


Figure 85: A login entry lets you tap the arrow and log in to the site using a browser sheet inside 1Password.

1Password Pro also lets you add a bookmark to Mobile Safari that can round trip through the program. When you're at a site for which you want to use a stored login in Safari, you tap the bookmark, which launches 1Password, looks up your stored information, lets you copy it, and then takes you back to Safari.

Whichever of these programs you use, you get the complementary advantages of exposing less to casual access while having what you need available wherever you go.

When Your iPad Goes Missing

Your iPad will be a desirable item for thieves, and unlike an iPod or iPhone, it will be more obvious that you have one, and easier to grab from you—you won't have it clutched tightly in one hand or shoved in a pocket. You are also more likely to leave it sitting on a table in front of you while turning away; being smaller than a laptop, it'll thus still be easier to filch.

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

SAFETY TIPS WHILE OUT AND ABOUT

The rest of this section looks at technology, but let me start with a few practical tips that may not be as obvious when you're carrying an iPad instead of a device like a mobile phone or a laptop:

- **Don't have an obvious computer bag:** A bag that can hold an iPad doesn't have to scream "I have a valuable computer inside!" Bags that look like they were designed to carry a computer are more likely to trigger untoward interest.
- **Don't pull out your iPad in public if you can be approached from behind:** I don't suggest always keeping your back to the wall, but if you're in a crowded railway station and whip out the unit, it would be easy work for someone to run by and snatch it.
- **Don't set it down and turn away:** The iPad is compact enough to hide and light enough to grab, so leaving it on a table at a café while you turn away to talk to someone could provide a thief with a good opportunity to relieve you of your iPad.
- **Lock your iPad when you're not using it:** The iPad is preset to keep its screen active for much longer than the iPhone and iPod touch. (You can tap Settings > General > Auto-Lock to change the

duration.) If you use the passcode lock described in [Set a Passcode](#) and hit the Sleep/Wake button when you're not using the iPad, it's more likely that a thief couldn't access your data.

Finding a Good Bag

My editor Tonya Engst recently purchased a [LeSportsac Classic Hobo](#) bag that turned out to be the perfect size to carry an iPad in the center compartment, along with a wallet and a few other small items. She gives it a big thumbs up for style and lightness, but puts the iPad in a light sleeve for extra protection.

I'm a big fan of the Timbuk2 line of messenger bags. While many people carry laptops and iPads and other devices in them, the bags are so prevalent (along with other messenger bag makers' gear) that they're hard to target. I found that a 13-inch MacBook bag I had fit the iPad neatly in a soft-lined inside compartment. (<http://www.timbuk2.com/tb2/products/laptop/>).

FIND MY iPad VIA MOBILEME

In 2009, Apple added a clever feature that combines the location awareness of iPhone OS devices with MobileMe: Find My iPhone. Despite that name, which is how it's labeled at the Me.com site, you can find the last reported position of any iPod touch, iPhone, or iPad, if you've set up a MobileMe account on the device and turned on the tracking feature. You can also take action remotely, choosing among options to play a message and optional sound, lock the device with a new four-digit passcode, or wipe all its data!

Note: A MobileMe account costs \$99 per year from Apple for a single user, but less if you buy a serial number in a box from Amazon.com for a new account or a renewal. Family packs are \$149 for five accounts from Apple, and less from online retailers.

How It Works

The feature relies on having a device send MobileMe's servers a regular update of location information derived from Wi-Fi (all iPhone OS devices), cellular (2G and 3G iPhones, some iPads), and GPS (iPhone 3G, 3GS, and iPad with 3G). You can enable the feature on multiple devices from one MobileMe account.

GPS built in: The 3G iPad has a GPS receiver built in for more precise positioning. GPS coordinates can be used by apps on the iPad whether or not a 3G plan is active. However, GPS information can't be sent to MobileMe unless there's either an active 3G plan or an active Wi-Fi network connection.

Wi-Fi positioning is derived by scanning for nearby networks and then using an online database from Skyhook Wireless to approximate a position based on network details, including the name and some less-apparent unique hardware identifiers. That lookup requires an active data connection, which is fine for an iPhone (which can use 2G or 3G data), or a 3G iPad with 3G service active.

But for a Wi-Fi-only iPad or a 3G iPad with inactive cellular data service, the iPad must be actively connected to a Wi-Fi network to retrieve Wi-Fi-based position information, as well as to send it or respond to queries from MobileMe.

Enable Find My iPad

Find My iPad requires that either Push or Fetch be enabled for interaction with MobileMe's servers. *Push* lets MobileMe and other servers connect to your iPad to transfer data such as email, calendar events, and contacts. It also enables MobileMe to obtain the current position for Find My iPad. *Fetch* allows you to set an automatic recurring interval at which your iPad retrieves new information and updates any remote settings.

Push is better than Fetch for finding a device: *Push is better here because it allows an instant request to get your device's location. With Fetch, Me.com waits until the next interval you chose before location data is updated.*

To configure your Push/Fetch settings:

1. In the Settings app, tap Mail, Contacts, Calendars.
2. Tap Fetch New Data.
3. Now, either set Push to On or set Fetch to Every 15 Minutes, Every 30 Minutes, or Hourly. (You can also set both.)

Now you need to set up your MobileMe account to use Find My iPad.

If you haven't set up a MobileMe account on your iPad:

1. In the Settings app, tap Mail, Contacts, Calendars > Add Account > MobileMe.
2. Enter your name, MobileMe email address, and password, along with an optional description of the account. Tap Next.

If you entered everything correctly, the iPad shows that the account has been verified, and you see an Edit screen that lets you choose to sync Mail, Contacts, Calendars, and Bookmarks, with the Find My iPad option last.

3. Tap the Find My iPad switch to enable the feature.

If you have set up a MobileMe account on your iPad:

1. In the Settings app, tap Mail, Contacts, Calendars.
2. Tap your MobileMe account name.
3. Set Find My iPad to On.
4. Tap Done.

Warning! *If you have Find My iPad turned on and disable both Push and Fetch, the iPad warns you that this turns off Find My iPad (Figure 86). Tap Turn Off, and Find My iPad is disabled along with Push and Fetch. Click Cancel to enable Fetch before disabling Push.*




Figure 86: You're warned if you make a Fetch New Data change that would disable Find My iPad.

View Your iPad's Location

To view your iPad's location, you use the Find My iPhone feature on the MobileMe Web site. Apple updated the feature recently to allow access via Mobile Safari, as well as with desktop Web browsers.

The steps for viewing your iPad's location are similar whether you are using Safari on the iPad or a desktop browser. Here are the specific steps for a desktop browser:

1. Go to <http://www.me.com/>.
2. Log in with your MobileMe account name and password.
3. Click the green Find My iPhone  icon at the top.
4. You're prompted for your password again; re-enter it.

***Apple's being smart about unattended machines:** Me.com lets you stay logged in for 2 weeks at a time, but it prevents unauthorized access to Find My iPhone by asking for your password first. The secondary login times out after 15 minutes.*

The Find My iPhone and Remote Wipe screen shows up with details about any devices you've registered to your MobileMe account, their current status (online or not), and the latest location information. Depending on the device and where it's located, you may receive a more precise location update within 3 minutes. A 3G iPad shows an approximate location first (**Figure 87**), and then (as long as the device can receive any satellite signals) an exact location via GPS.

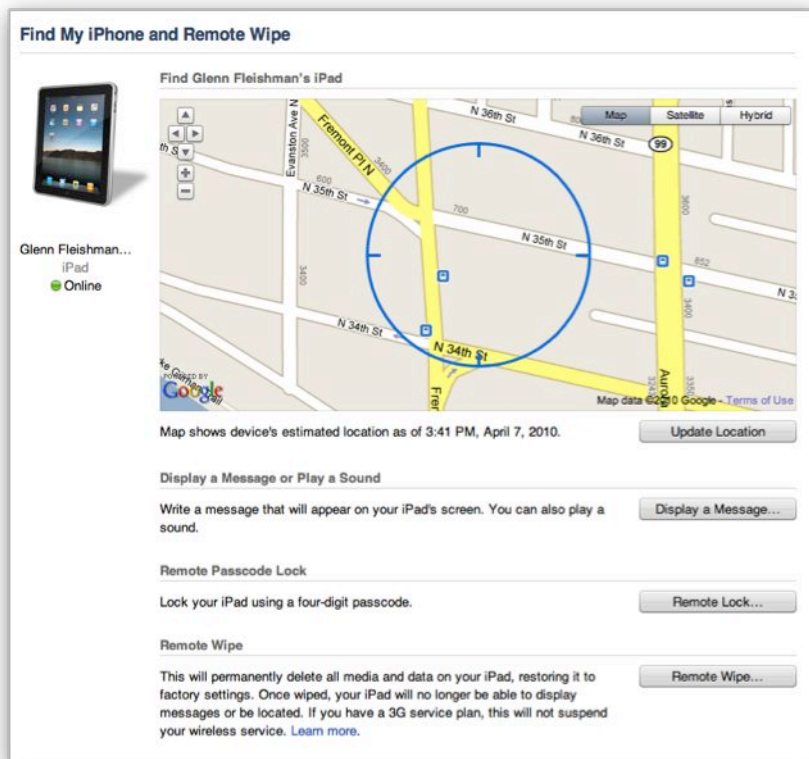


Figure 87: Me.com lets you see where your iPad was located the last time it sent coordinates. If you have attached multiple devices to one MobileMe account, scroll down to see them all.

Take Remote Action on Your iPad

You can now take action on your iPad, choosing one or more of three options that vary in utility based on whether your iPad has fallen behind a couch cushion, or was misplaced or stolen. Whatever action you take, MobileMe sends an email message to your me.com address, notifying you.

Call the police first! If you know your iPad was stolen, you should consider taking location information to the police—calling 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 acting the next time it's online: You can pick any of the below options even if the iPad is shown as offline, and MobileMe will trigger them whenever the device comes back online—if ever. Stolen hardware tends to be wiped as soon as it's practical, and an iPad without an active 3G plan would have to join a Wi-Fi network to report itself and be remotely reachable.

Display a Message or Play a Sound

Click Display a Message, and you can enter text that will display on the iPad's screen. You can also choose to play a sound for 2 minutes. This overrides any mute settings on the device. This option is designed for three purposes:

- If you left your iPad somewhere in your house or office, and can't find it, this lets you trigger a sound you can use to home in on it.
- If you left your iPad somewhere else, the sound and noise can provoke someone to take a look. You can offer a reward and provide your phone number. It also puts the finder on notice that you know approximately where it is.
- Were the iPad stolen, this is a way to tell a thief that you've got their location and other data, and advise them to give it up.

Even if you use the next feature to lock the iPad remotely, the message still appears on the locked screen.

Remote Lock

This option sets a four-digit passcode lock on the iPad. If a code has previously been set, the iPad changes to this new code. It also overrides any more complex passcode requirements you may have set through the iPhone Configuration Utility.

Use a passcode: See [Set a Passcode](#) for more details on how the passcode works.

You enter a code, click Next, and re-enter the same code (**Figure 88**). Click Done. The code is passed to the device, and email is sent to your MobileMe account confirming the action. The iPad's Passcode Lock setting is changed to Immediately (Settings > General > Passcode Lock), as well.



Figure 88: You can set a passcode via Me.com that overrides an existing one or imposes one if none was already set.

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

- If the iPad is online and asleep, the next time it's woken, the current possessor must enter the passcode to gain access.
- If the iPad is online and in use, the operating system drops the user into the Slide to Unlock standby screen.
- If the iPad is offline, the next time it accesses the network, the passcode lock is put into place.

Remote Wipe

The last resort in some cases (or first in others) is a *remote wipe*, in which all the user data on the iPad is quickly erased. Apple gives you a couple of chances to back out, asking you to check a box indicating that you understand there's no way out, and then having you click the Erase All Data button.

Hardware Encryption

Like the iPhone 4 and 3GS, Apple includes hardware encryption on the iPad. To “erase” all the device’s stored data, just the encryption key has to be thrown away and a few other settings rewritten. On the original iPhone and iPhone 3G, which lacked this hardware feature, each byte of data has to be reset, which can take hours. With hardware encryption, “erasing” takes only a minute or two.

However, wiping your iPad isn’t quite as bad for your data as it sounds. When you sync your iPad with iTunes, iTunes automatically backs up all your user data and syncs any media you bought on the iPad to the iTunes library on the computer.

If you wipe your iPad and either recover it or obtain a new one, when you sync it with the same copy of iTunes, you can restore the latest backup and sync any media stored in the computer’s iTunes library.

Data which you set iTunes to sync (via the iPad’s Info tab with the device attached), such as contacts and calendar entries, will sync to the recovered or new iPad via iTunes using the most up-to-date data in the computer.

If you were syncing any of that sort of data wirelessly through a MobileMe or Exchange account, you won’t have lost any data; once the account is back online on the iPad, your data will flow back to the iPad. You will lose any changes made between the last sync (whether push, fetch, or manual) for each account and the remote wipe.

REMOTE TRACKING SOFTWARE

The iPad doesn’t yet allow third-party software to work in the background, so you can’t run theft-recovery software as you can on certain cell phones and most computer operating systems. Those third-party packages on other platforms check at regular intervals to see whether a device has been reported missing. If so, the software goes into overdrive, snapping pictures (if there’s a built in Webcam), making screenshots, sending network data, and using Wi-Fi and GPS positioning to send location information.

Two firms have come up with ingenious ways around this:

- **GadgetTrak for iPhone** has an icon that makes it look like it might be a Web browser. The app uses Apple's WebKit software to seem just like Mobile Safari. A thief might launch this app, which causes it to send location information in the background. The software hasn't been updated for iPad at this writing, but it is compatible (GadgetTrak, free).
- Orbicule created the universal **Undercover** app, a mobile version of its Mac OS X software, which uses push notifications to provide location data. If your device is lost or stolen, you use Orbicule's recovery Web site to mark the unit as missing. You can then set a notification that tries to get the current possessor to tap the View button, such as saying that mobile banking credentials are available for viewing. If the View button is tapped, this launches Undercover, which then transmits the location to Orbicule's servers and provides it to law enforcement. The device's user sees a Web browser interface pointing to a Web site. It's a beautiful form of misdirection. (Orbicule, \$4.99).

Tracking Apps Coming in iOS 4

Tracking applications will be possible in iOS 4, coming in third-quarter 2010 to iPad, by allowing background requests from otherwise idle apps for location updates. A theft-recovery package can receive these requests and send lightweight location updates over a network—or so I believe from publicly available information provided by Apple.

Details are yet to emerge about automatic launches and keeping background processes running indefinitely. For a tracking package, you'd want it to auto-launch at startup, and never quit without warning, even if system resources were tight.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments at tc-comments@tidbits.com. Keep reading in this section to learn more about the author, the Take Control series, and the publisher.

ABOUT THE AUTHOR

Glenn Fleishman started writing about technology in the late 1980s for his college newspaper, where he had a lot to do with setting up and running Macs using PageMaker 1.0. His professional career began with *Aldus Magazine* in 1994, with a feature about font management. Glenn writes about technology and its implication for people in publications like the *Economist* and the *Seattle Times*. He contributes how-to and how-it-works articles along with reviews to *Macworld*, *Popular Science*, *Ars Technica*, and many others.



Glenn has been an editor at TidBITS for umpty-ump years, and runs the back-end technology. He developed a content-management system used for TidBITS editors to publish articles and that feeds out content on its live site. Glenn also edits his own blog, *Wi-Fi Networking News*, and runs isbn.nu, a book price shopping engine.

Glenn lives in Seattle with his wife and two sons. He has more computers than he can count and has written more books than he can remember.

AUTHOR'S ACKNOWLEDGMENTS

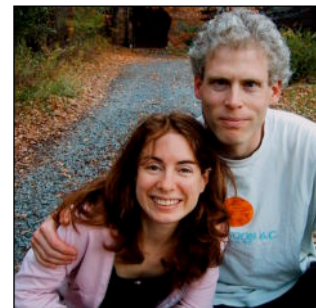
I dedicate this book to my wife, Lynn, and sons, Ben and Rex. They keep me sane and happy, and keep me from spending my entire day thinking about and using digital devices. A big thank you also to the tireless Tonya Engst, the driver behind this set of Take Control books

about the iPad, who had the foresight to think about what we might write about months before we had actual hardware.

ABOUT THE PUBLISHER

Publishers Adam and Tonya Engst have been creating Apple-related content since they started the online newsletter *TidBITS*, in 1990. In *TidBITS*, you can find the latest Apple news, plus read reviews, opinions, and more (<http://www.tidbits.com/>).

Adam and Tonya are known in the Apple world as writers, editors, and speakers. They are also parents to Tristan, who thinks ebooks about clipper ships and castles would be cool.



PRODUCTION CREDITS

Take Control logo: Jeff Tolbert

Cover design: Jon Hersh

Editor in Chief: Tonya Engst

Publisher: Adam Engst

Copyright and Fine Print

Take Control of iPad Networking & Security

ISBN: 978-1-61542-054-4

Copyright © 2010, Glenn Fleishman. All rights reserved.

TidBITS Publishing Inc.

50 Hickory Road

Ithaca, NY 14850 USA

<http://www.takecontrolbooks.com/>

Take Control electronic books help readers regain a measure of control in an oftentimes out-of-control universe. Take Control ebooks also streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

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. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Although the author and TidBITS Publishing Inc. 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 ebook is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. 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 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>.

Featured Titles

Take Control books have an easy-to-read layout, clickable links if you read onscreen, and real-world info that puts you in control. Click any book title below or [visit our Web catalog](#) to add more ebooks to your Take Control collection!

INCREASE YOUR iPad IQ

[Take Control of iPad Basics](#) (Tonya Engst): Patch any blank spots in your basic iPad know-how. Free!

[Take Control of Media on Your iPad](#) (Jeff Carlson): Maximize your iPad enjoyment by reading an ebook, listening to music, viewing photos, watching a video, or using your iPad as a remote control. \$10

[Take Control of Working with Your iPad](#) (Joe Kissell): Adopt a cutting-edge mindset while you take your iPad to meetings, create original documents, round-trip files to other devices, and print. \$10

[Take Control of Mail on the iPad, iPhone, and iPod touch](#) (Joe Kissell): Develop your mobile email strategy, and learn how to use email effectively on your Apple device. \$10

MORE TAKE CONTROL EBOOKS

[Take Control of Sharing Files in Snow Leopard](#) (Glenn Fleishman): Find friendly advice and steps for sharing files from your Mac, and get further ideas for using an Internet-hosted service. \$10

[Take Control of Passwords in Mac OS X](#) (Joe Kissell): Use strong passwords that keep your data safe without taxing your memory! \$10

[Take Control of Your 802.11n AirPort Network](#) (Glenn Fleishman): Make your AirPort network fly—get help with buying the best gear, set up, security, and more. \$15

[Take Control of Your Wi-Fi Security](#) (Engst & Fleishman): Learn how to keep intruders out of your wireless network and protect your sensitive communications! \$10