

TAKE CONTROL OF
1PASSWORD

by **JOE KISSELL**
\$10

Table of Contents

Read Me First	5
Updates & More.....	5
Basics	6
Introduction	7
1Password Quick Start	9
Meet 1Password	10
Configure 1Password	10
Explore the 1Password Components	18
Learn How Logins Work	24
Find Your Usage Pattern	31
Set Up Syncing	33
Check for Updates	41
Learn What 1Password Isn't Good For.....	41
Understand Password Security	45
Learn Password Security Basics.....	45
Understand Optimal Password Length.....	48
Password Dos & Don'ts.....	50
Use 1Password for Web Browsing.....	52
Create & Save Logins.....	52
Log In.....	63
Deal with Multistep Logins.....	67
Fill Web Forms Using Identities	69
Shop Online Securely	71
Store Other Information in 1Password	73
Stand-alone Passwords.....	73
Software Licenses	75

Secure Notes	77
Other Data Types	78
Search & Organize Your 1Password Items	81
Make Your Life Simpler	81
Understand the Sidebar Sections	82
Use Favorites	85
Use Folders & Tags	85
Adjust the Sort Order	87
Perform a Basic Search	88
Perform an Advanced Search	89
Use Smart Folders	91
Work with Previously Generated Passwords	91
Use the Trash	93
Work with Multiple Vaults	93
Edit 1Password Items	97
Edit Saved Items	97
Work with Icons & Thumbnails	102
Update Old Passwords	105
Perform a Password Security Audit	108
Share 1Password Data	112
Import & Export Data	115
Customize 1Password	116
Set Security Preferences	116
Configure Other Mac Preferences	119
Use 1Password with Other Utilities	120
Use 1Password on the Go	123
iOS	123
Android	133
1PasswordAnywhere	135
Solve Problems	139
Don't Panic	139
Deal with Version 4 Changes	139

Troubleshoot Other Problems	141
Glimpse the Future of 1Password	142
About This Book	144
Ebook Extras	144
About the Author	145
About the Publisher.....	146
Copyright & Fine Print	147
Featured Titles	148

Read Me First

Welcome to *Take Control of 1Password*, version 1.0, published in September 2013 by TidBITS Publishing Inc. This book was written by Joe Kissell and edited by Tonya Engst and Kelly Turner.

This book shows you how to get the most from 1Password, the popular password manager for OS X, Windows, iOS, and Android. It explains the best ways to accomplish common tasks, explores new features, and helps you discover new ways to use 1Password.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: “lend” it for a quick look, but ask your friend to buy a copy for careful reading or reference. Discounted [classroom and Mac user group copies](#) are available.

Copyright © 2013, alt concepts inc. All rights reserved.

Sponsored by AgileBits

This book was sponsored by [AgileBits](#), makers of 1Password. Thanks to Jeff Shiner and Dave Teare for all their efforts to help bring this book to life, and especially for their able assistance with answering technical questions.



Updates & More

You can access extras related to this ebook on the Web (use the link in [Ebook Extras](#), near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.

- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading this ebook on handheld devices on our [Device Advice](#) page.)
- Read postings to the ebook’s blog. These may include new tips or information, as well as links to author interviews. At the top of the blog, you can also see any update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been added to your account, where you can download it in other formats and access any future updates. Otherwise, you can add it to your account manually; see [Ebook Extras](#).

Basics

Here are a few pointers that will help you read this ebook:

- **Links:** All blue text in this ebook is *hot*, meaning you can click (or tap) it, just like a link on the Web. If you click a link to switch to a different part of the ebook, you can return quickly to where you were if your ebook reader offers a “back” feature. For example, if you use iBooks in iOS to read the EPUB version of this ebook, you can tap the “Back to” link at the lower left of the screen. Or, if you use Preview on the Mac to read the PDF version of this ebook, you can choose Go > Back or press Command-[.
- **Menus:** Where I describe choosing a command from a menu in the menu bar, I use an abbreviated description that puts the name of the menu ahead of the command. For example, at the end of the previous paragraph, “Go > Back” means “choose the Back command from the Go menu.”
- **Credentials:** I frequently use the term *credentials* to refer to the complete set of information you need to log in to a site or service—typically a username (or email address) and a password.

Introduction

Nobody likes dealing with passwords. After all, they exist solely as barriers to keep unauthorized people from accessing Web sites, servers, and other digital resources. Entering the occasional password is no big deal, but when you're prompted for passwords dozens of times a day—forced to prove, over and over, that you are who you say you are—it can be mighty annoying.

Naturally, people take shortcuts to reduce that annoyance, such as picking short, easy-to-type passwords and reusing the same password everywhere. Unfortunately, those shortcuts also make it easier for another person (or, more likely, a computer) to guess your password, which can lead to all sorts of nasty consequences. And that sticky note or cheat sheet that makes it easier for you to find your passwords can make it equally easy for a thief or snoop.

1Password solves these problems, making it convenient to be secure. It offers a painless way to create, store, and enter passwords—so every one of them can be unique and strong without any extra effort. Because all your passwords are protected with a single, master password, that's the only one you have to remember—hence the name 1Password. Once you've unlocked 1Password, logging in to any Web site is as simple as pressing a keyboard shortcut or clicking a button.

Nearly every Web browser can save and fill passwords, too, but 1Password is more versatile because it lets you use a single tool for all major browsers and platforms—and it safely syncs your data among them automatically. 1Password can also fill in other information on Web forms (such as your addresses and credit card numbers) and it can store software licenses, notes, and any other data you want to keep secure. It's not the only password manager out there, but I've tried many others and 1Password is my favorite by far.

Merely installing 1Password won't magically fix all your password problems, though. You'll need to configure it to meet your personal needs and tastes, add your existing passwords, and identify the

workflow that suits you best. In this book, I walk you through that entire process. Whether you're an absolute beginner or a seasoned 1Password user, I'll help you discover how to use 1Password to its best advantage.

This book isn't meant to replace the 1Password documentation or to be a comprehensive reference guide. Instead, I concentrate on the most common tasks you're likely to perform and help you find the quickest and easiest ways to accomplish them. In the process, I show you some cool features that you may have overlooked and share my favorite tips.

I cover *only* the latest versions of 1Password as of publication time—4.0 for Mac, 1.0.9 for Windows, 4.3 for iOS, and 1.8.5 for Android. I spend more time talking about the desktop (Mac and Windows) versions than the mobile (iOS and Android) versions, and I put particular emphasis on the recently released 1Password 4 for Mac. (If you're upgrading from an older Mac version, please see [Deal with Version 4 Changes](#) for help with the transition.)

The core features of 1Password are pretty much the same on every platform, and I call attention to platform-specific differences as necessary. As you'll see in [Glimpse the Future of 1Password](#), AgileBits has lots of major new features planned for future versions. As 1Password changes, I'll do my best to keep you up to date; be sure to follow the instructions in [Ebook Extras](#), near the end of this book, to check for new versions of this book and read posts to the book's blog. Because of the rapid pace of new releases, some aspects of the book may go out of sync with the newest versions of 1Password, so if you see something here that doesn't quite match what's on your screen, that's likely why—and I'll get to it as soon as possible.

Once you've mastered 1Password, you may want to learn more about password security—things like how password attacks work, what makes multi-factor authentication useful, how to deal with security questions, why everyone needs an emergency password plan, and how a password manager such as 1Password fits into a larger password strategy. I cover all this and much more in my book [Take Control of Your Passwords](#), which serves as a companion to this one.

1Password Quick Start

If you're new to 1Password, I suggest working your way through this book in linear order, or at least starting with the first two chapters ([Meet 1Password](#) and [Understand Password Security](#)), which provide important context for the rest of the book. If you're an experienced 1Password user, feel free to jump right to any topic of interest, such as [Deal with Version 4 Changes](#) in the [Solve Problems](#) chapter.

Learn the basics:

- Discover 1Password's components, walk through setting up and using its major features, and start syncing; see [Meet 1Password](#).
- Find out what makes a password strong or weak in [Understand Password Security](#).

Use 1Password for day-to-day tasks:

- Save and use Web credentials with ease—and shop online securely; see [Use 1Password for Web Browsing](#).
- Keep software licenses, secure notes, and other important info in 1Password; see [Store Other Information in 1Password](#).
- Access your 1Password data from a smartphone, tablet, or public computer; see [Use 1Password on the Go](#).

Delve into the details of your 1Password data:

- Zip right to the information you need; see [Search & Organize Your 1Password Items](#).
- Tweak saved items to correct mistakes and update old passwords; see [Edit 1Password Items](#).

Bend 1Password to your will:

- Adjust preferences to suit your needs; see [Customize 1Password](#).
- Find “missing” features in 1Password 4 and get help with common troubleshooting tasks; see [Solve Problems](#).

Meet 1Password

Whether you're entirely new to 1Password or upgrading to version 4 for OS X, you'll have an easier time working with the software if you set it up correctly from the start and understand how it's designed to function. In this chapter, I cover some preliminary configuration steps that are often ignored or misunderstood, make sure you know which components are supposed to do what and when, and then walk you through creating and using your first few Web logins, which for most people are 1Password's most crucial feature.

The chapter closes with important advice about identifying your best approach to using 1Password logins and some notes about a few tasks that 1Password does not handle.

This chapter is mainly about the Mac and Windows versions of 1Password. I do talk about syncing 1Password with other devices (including mobile devices), but I leave further discussion of 1Password on iOS and Android to [Use 1Password on the Go](#), later.

Configure 1Password

By now you've undoubtedly downloaded and installed 1Password—and if not, this is a great time to do so. Visit [this page](#) on the AgileBits Web site to find links to purchase it on your platform(s) of choice. You install it the same way as any other app, so I won't bore you with those details. I do want to point out, however, that for Mac users, only the version of 1Password sold in the Mac App Store (not the version sold directly by AgileBits) officially supports iCloud syncing.

Before you can start using the software, you must choose a master password (unless you're upgrading from a previous version, in which case you can continue using the same master password). You should also install extensions for any browsers you may use, as well as understand (and perhaps adjust) the way locking and unlocking works.

If you use 1Password on more than one device, synchronizing your 1Password data file between those devices is also a key configuration step. I discuss that later in this chapter, in [Set Up Syncing](#).

Make First-run Decisions

If you've never used 1Password before on a given device—or if you're upgrading from version 3 to 4 on a Mac—the first time you run the app, 1Password displays a Welcome window and then presents a series of choices to help you get up and running quickly. You shouldn't agonize over any of these decisions, because you can always change your mind later. But you should be aware of your options.

Here's an overview of the first-run experience for new and upgrading Mac users, new and upgrading iOS users, and new Windows users.

First Run for Mac Users

When you open 1Password 4 for the first time on a Mac, it checks to see if you already have a [1Password Data Vault](#) in one of the default locations (such as the top level of your Dropbox folder). If so, it prompts you to enter your master password—but if you want to choose a different data source (or start over with a new vault), you can click the pop-up menu shown to choose a different option.

If 1Password doesn't find an existing vault, it displays two buttons: "I'm new to 1Password" and "I've used 1Password before." Click the former and you're prompted to create a new vault and select a master password (see [Choose a Master Password](#)). Click the latter and you can select the type and location of your data (for example, in a nonstandard spot on your disk or in Dropbox).

Whether or not you're a new user, once you've opened and unlocked your vault, you'll go through three more screens:

- **Security:** There are two options: Lock after Computer Is Idle for *x* Minutes (selected by default) and Lock When 1Password Window Is Closed (deselected by default). For new installations, the idle time is set to 5 minutes; if you previously had a version of 1Password installed with a different idle time, it'll show that instead. I suggest

Understand Password Security

To use 1Password effectively, you should know a few basics about what makes passwords more or less secure. This information will help you choose a good master password (which protects all your other passwords) and make smart decisions about using 1Password's password generator.

If you've already read my book [*Take Control of Your Passwords*](#), which discusses password security in detail, you can skip this chapter. If not, read on for a brief overview of the major points you need to know when choosing passwords.

Learn Password Security Basics

The whole idea of a password is that it's private—something known only to you and to the entity with which you have an account (a bank, Web site, cloud service, etc.). If someone else learns your password, that person can access your data, which could mean stealing your money, impersonating you online, taking over your computer, and worse. So, your main goal when picking a password should be to select one that won't be guessed.

Most people think of “guessing” as a strictly human activity. For example, a friend or colleague might guess that your password is the name of your dog, your anniversary, or your favorite ice cream flavor, and that's why you should never use words, names, or numbers someone might associate with you as passwords.

However, most of the time it's not people doing the guessing directly, but rather computers. A friend might never guess `poiuytrewq` as a password, but it would be among the first guesses by a program designed to crack passwords, because that string follows a pattern (in this case, a keyboard pattern). Cracking software is great at identifying

the patterns people commonly use to help them remember passwords, including patterns based on words, names, numbers, and shapes, not to mention substituting numbers for similar-looking letters (3 for E, 4 for A, and so on).

Now, suppose the worst happens and one of your passwords is guessed, leaked, stolen, or hacked. That's bad news, but it suddenly becomes much worse if you used the same password in lots of different places. For example, hackers probably don't care about your Facebook password as such, but they'd still love to know what it is, on the theory that you use the same one for your email account, bank accounts, PayPal, and other services that they could then access instantly. And that's exactly what hackers do—they immediately try stolen passwords on lots of different sites. The moral of the story is that you should never reuse passwords in more than one place. Make every one unique!

Even if you choose a unique, random password—a meaningless string of letters, numbers, and symbols—you're not necessarily safe. I know of cracking systems based on ordinary, off-the-shelf computer hardware that can try every single possible password of up to eight characters in just a few hours. This is called a *brute-force attack*, and it's guaranteed to succeed eventually. The only way to defeat a brute-force attack is to make every password so complex that “eventually” is longer than the attacker can afford to spend trying.

Fortunately, that's easier than it sounds. Cryptographers use the term *entropy* to mean a mathematical approximation of how strong a password is—that is, how well it can resist guessing. It turns out that you can increase a password's entropy, thereby increasing the average time it would take for a brute-force search to crack it, in any of three ways:

- **Make it longer.** Every character you add to a password exponentially increases the number of possible passwords that must be checked. For example, if each character in a password can be one of 52 possible choices (upper- and lowercase letters), then an eight-character password has about 53 trillion (52^8)

Use 1Password for Web Browsing

A couple of chapters ago, in [Learn How Logins Work](#), you learned how to save credentials for a few Web sites and use 1Password to fill them in. Although you can get lots of mileage out of the simple procedures I explained there, 1Password has lots of other options for working with Web sites. In this chapter I explain when you might need these extra features and how to use them when you do.

Among the things I cover here is generating new passwords, which you'll probably need to do more often when browsing the Web than in any other situation. I also discuss the way 1Password uses *identities* (sets of contact details) and credit cards, both of which you're likely to use regularly while browsing.

Create & Save Logins

The more logins you store in 1Password, the more powerful and handy it becomes. The easiest way to add your existing logins to 1Password is to browse the Web normally, enter your credentials for the sites that you encounter in whatever way you previously did, and then let 1Password's Autosave feature add them one at a time, just as you did earlier in [Learn How Logins Work](#). It's also possible to add them manually to the main 1Password app (see [Edit 1Password Items](#)) or import them from certain other repositories (see [Import & Export Data](#)), but in my experience adding them as you go is the path of least resistance.


However, even though Autosave is mostly self-explanatory, I want to cover a few less-obvious points. Then I'll tell you how to [Generate Random Passwords](#), which you'll do when registering for new accounts (which you'll also want 1Password to save for you).

Save New Logins

First things first: Autosave is enabled globally by default, but you can toggle it if the need arises:

- On a Mac, choose 1Password 4 > Preferences, click Browser, and select or deselect Automatically Ask to Save New Logins. If you want to use Autosave most of the time but exclude certain domains (for example, when you're doing testing on a Web site you're developing), you can add those domain names to the exceptions list.
- On a Windows PC, choose File > Preferences, click Logins, and select or deselect Ask to Save New Logins in Browsers. (The Windows version doesn't have an exceptions list.)

Note: If you use multiple vaults (see [Work with Multiple Vaults](#)), be aware that as of version 4.0, 1Password's Autosave feature always saves credentials to the currently active vault. (Its name appears in the Autosave dialog as a reminder.) This may change in a future update.

On a Mac, you can also disable Autosave for a particular domain on the fly. When you submit a login form and the 1Password Autosave dialog appears (much to your irritation), click the gear  icon in the lower left of the dialog and choose Never Autosave for This Site from the pop-up menu. That adds the domain in question to the exceptions list on the Browser preference pane.

Generate Random Passwords

When a site or service asks you to come up with a new password, 1Password is ready to supply one that meets your desired criteria. You can access the password generator in any of the following ways:

- In 1Password mini, hover over Password Generator with your pointer—or select it using the Up or Down arrow keys (if it's not already selected) and press Return, Enter, or the Right arrow key (**Figure 12**).

Store Other Information in 1Password

In the previous chapter I talked about using 1Password with your Web browser—storing and filling in usernames, passwords, contact information, credit card numbers, and so on. That combination of features may be 1Password’s main focus, but the app can do lots of other powerful things too. In this chapter, I talk about the types of information 1Password can work with that have nothing to do with Web browsing. Later, in [Search & Organize Your 1Password Items](#) and [Edit 1Password Items](#), I cover some of the ways you can work with this and other 1Password data beyond the basics.

Stand-alone Passwords

Passwords are needed for many reasons other than logging in to Web sites. I talk about a number of other categories, such as wireless routers, reward programs, and memberships, later in this chapter—see [Other Data Types](#). But sometimes you need to create a password and nothing more—no username, URL, or other fields. Just a password. For example, you may need:


- Passcodes for smartphones or tablets
- Passwords for full-disk encryption, disk images, and other encrypted files
- PINs for alarms and keyless entry systems

In these and other cases where you need to store a password (perhaps with other data) in 1Password and you can’t find an appropriate category, you can create a password item.


Since you generally won’t be looking at a Web page when you need to create or save stand-alone passwords, Autosave won’t help. Instead,

open the main 1Password app, click File > New Item > Password, and fill in the form (using the built-in password generator when you get to the Password field). Be sure to give the item a descriptive title that will help you find it later. Then click Save (Mac) or OK (Windows).

On a Mac, as an alternative, you can use 1Password mini:

1. Press Command-Option-\\ or click the 1Password key  icon in your menu bar to display 1Password mini.
2. Use the password generator (see [Generate Random Passwords](#)) to create a new password, and click Copy. Paste the password into the desired location (such as an encryption program).
3. Later, at your convenience, open the main 1Password app and select Passwords in the sidebar.
4. Locate the password you created (sorted by default according to Date Created), and edit its title or other attributes to show what you used it for (see [Edit Saved Items](#)).

Your password item is now ready for use.

When it comes time to retrieve your password later, you can again go to the main 1Password app—or, on a Mac, call up 1Password mini and search for it there. Then, on a Mac, you can quickly copy the password by clicking the Password field or reveal it temporarily by holding down the Option key. On a PC, click the Copy to Clipboard  button next to the Password field to copy it.

Search & Organize Your 1Password Items

Over time, you'll store hundreds—maybe thousands—of things in 1Password. But they're only useful to you there if you can find them quickly and easily when you need to. So in this chapter, I review many of the ways in which you can search, organize, and view your 1Password items. I also tell you how to work with multiple vaults, a new feature in 1Password 4 for Mac.

But, before I get into any of this, I want to share with you my Professional Opinion, which is that you should ignore most of the features discussed in this chapter. And since I know a lot of people skim right over these chapter lead-ins, I'm going to emphasize this point by putting it in a nice bold heading:

Make Your Life Simpler

In the next several pages, I'm going to tell you about folders, tags, favorites, advanced searches, smart folders, and all sorts of other tools that you *could* use to manage your 1Password data. But you don't have to use any of them, and most people—even power users—will merely waste time and effort in the care and feeding of information that can take care of itself.

I have well over 1,200 items in my copy of 1Password (including more than 600 logins), accumulated over about 7 years. I don't use folders, tags, or favorites—a simple search virtually always turns up exactly what I'm looking for—and I feel as though the time I could pour into organizing and categorizing would be better spent doing something enjoyable or enriching.

So, before you do *any* organizing at all, try using 1Password for a while without it, merely searching (see [Perform a Basic Search](#)) for what you

need. If you find that searching isn't cutting it for you, then start using the other tools—slowly. Don't overdo it just because you can.

Nevertheless, even if you take no action now, you should be aware of what 1Password can do—especially how it sorts and displays your data—so you're never confused about where something may be.

Understand the Sidebar Sections

1Password's sidebar (**Figure 20**) lets you filter the display of your stored items in the main list. Click an item in the sidebar, and only the matching items show up in the list.

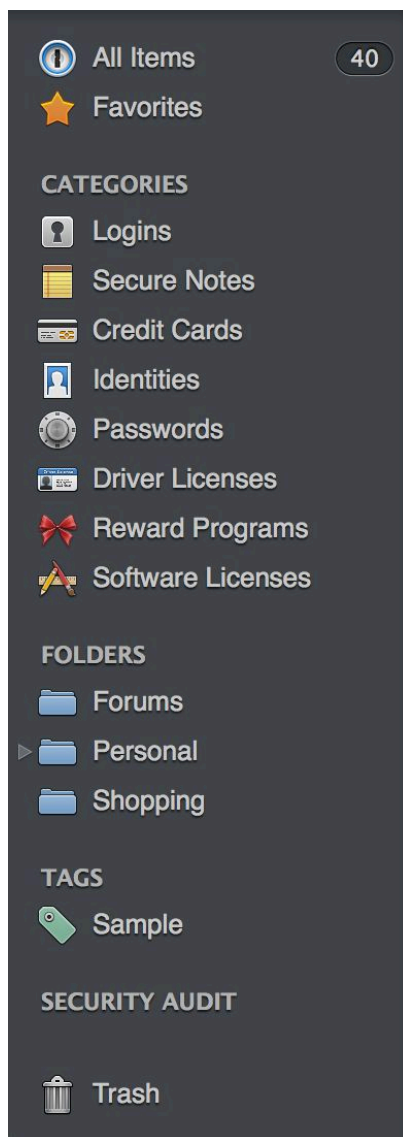


Figure 20: The sidebar in 1Password for Mac. (The Windows version is a bit different.)

Edit 1Password Items

If you've been reading in linear order, you've already encountered numerous situations where you may need to edit 1Password items, which requires nothing more than clicking the Edit button, making your changes, and clicking Save (Mac) or OK (Windows). However, in this chapter I address a variety of changes that may not be obvious at first glance—including modifying labels, using custom fields, tweaking URLs for better results, and dealing with icons and thumbnails.

I also explain exactly what to do when you need to change a password and how to audit passwords that have accumulated over time to make sure they're unique—and as strong as they should be. And I tell you about the new features in 1Password 4 for Mac that enable you to share individual passwords or even entire vaults with other people. I close the chapter with brief pointers on importing and exporting data.

Edit Saved Items

When 1Password's Autosave feature saves your login credentials, it usually has all the information it needs to log you in on future visits to the site. However, in certain situations it can get confused, and even if it doesn't, you may want to modify its behavior. For example, you may want to change the URL so it points at the sign-in page rather than the sign-up page (if they're different). And, if 1Password fails to fill in your credentials, identity, or credit card information correctly, some minor tweaks may be needed.

Modify Item Attributes

Three attributes of 1Password items—especially login items—have a significant effect on how 1Password processes them in a Web browser:

- **URLs:** The URL in a login item's Website (Mac) or Location (PC) field is the one for the page on which 1Password's Autosave feature

was used. If that's the site's regular sign-in page, you shouldn't need to modify it. But if it points to a page used only for registration, then clicking the URL (or accessing it in any of the numerous other ways discussed in [Log In](#)) could produce an error message, since you've already signed up! The easiest way to handle this is to navigate manually to the page on the site where you normally sign in, copy its URL from your browser's address bar, and paste it into the Website/Location field, overwriting the one that's already there.

On a Mac, you can also add more URLs—fields labeled Website 2, Website 3, and so on appear as needed—to tell 1Password that there are other pages on which you can log in with the same credentials. If you have multiple login items for a given site—one for each page or subdomain where you log in with the same credentials—you can simplify things by combining all those URLs in a single login item.

Tip: What if a site has only a combined sign-up/sign-in page? If the field names are the same in both parts of the form, 1Password fills them all in, but that's a problem only if Autosubmit "clicks" the wrong button. Your best bet on such sites is to disable Autosubmit (see the Submit bullet point ahead). However, if the field names are different in each part of the form, you can [Change Web Form Details](#) to make 1Password use the right ones.

- **Display:** The fact that a login item, identity, or credit card appears in the main 1Password app doesn't mean that it has to show up in 1Password mini (Mac) or in your browser extensions (PC). Preventing an item from appearing while you're in your browser means it won't autofill or appear on the list if you press Command-\ or Control-\. You might opt for this feature, for example, if you've disabled or deleted an account, moved to a new address, or canceled a credit card—you can keep a record of your old data in 1Password without cluttering your browsing experience. To keep an item from displaying in your browser on a Mac, choose Never Display in Browser from the Display pop-up menu when editing an item. On a PC, select the item, click Edit, and deselect the Display in Web Browser(s) checkbox.

Customize 1Password

Throughout this book I've mentioned a variety of preferences that you can change to modify 1Password's behavior. In this brief chapter, I want to mention a few preferences I didn't cover elsewhere and provide more detail about some that I did. (I don't cover every single 1Password preference—only the ones you're most likely to need. If there's a preference you're curious about that I don't discuss, consult the 1Password Help menu or [support Web site](#).)

I also talk briefly about other utilities, such as launchers and clipboard managers, that you can use in conjunction with 1Password.

Set Security Preferences

To set 1Password's security preferences, open the main app and choose 1Password 4 > Preferences (Mac) or File > Preferences (PC), and then click Security.

Master Password

To change the master password that protects all your 1Password data, click Change Master Password. Enter your current password (on a Mac only), enter and verify a new password, and optionally (on a Mac only) enter a hint. Then click Change Password (Mac) or OK (PC).

Display (Mac Only)

In the Mac version of 1Password only, the Display category has a single option: Conceal Passwords (selected by default). With this checkbox selected, your passwords will normally be represented by bullets (•) in both the main 1Password app and 1Password mini. You can show the passwords by holding down the Option key. To display passwords all the time in both environments—an unwise idea if someone might be able to look over your shoulder while you're using 1Password—deselect this checkbox.

Tip: You can also toggle concealing passwords by choosing View > Conceal Passwords in the main 1Password app.

Auto-lock

I introduced the Auto-Lock preferences earlier, in [Lock Automatically](#), and you may have selected some default options when you first ran 1Password. Here are the things you can change now (the order and wording differ by platform):

- **Lock on Sleep (Mac)/Lock When Your Computer Is Locked (PC):** This self-explanatory option should remain selected for most people.
- **Lock When the Screen Saver Is Activated:** Wait, there are people who still use screen savers? You know that LCD screens don't need saving, right? Well, if you use a screen saver as a security measure (so other people don't see what's on your screen when you're not there), it may be wise to select this option. If you don't use a screen saver, then it doesn't matter one way or the other!
- **Lock When Main Window Is Closed (Mac only):** Although you can manually lock 1Password at any time, even with the window open (see [Lock and Unlock 1Password](#)), some people don't want to expend any extra effort and feel safer knowing that if the app window is closed, the data is protected immediately. If you're such a person, select this option.
- **Lock after Computer Is Idle for ___ Minutes (Mac)/Lock after ___ Minutes of Inactivity (PC):** The default setting here is 5 minutes, but you can enter a longer or shorter time, or deselect this option altogether. In general, I think it's wise to leave this turned on if there's any chance someone else might be able to use your computer (including thieves), although depending on how you use your computer, locking after only 5 minutes may force you to type your master password more often than you like. (Keep in mind that "inactivity" refers to a period of time during which you don't use the keyboard or mouse at all—such as when you're watching a movie—not merely "time since I last did something in 1Password.")

Use 1Password on the Go

Most of this book has talked about the desktop versions of 1Password (for OS X and Windows). But 1Password also comes in versions for iOS and Android, both of which can sync data with a Mac or PC and enable you to access your crucial 1Password data from a smartphone or tablet. This chapter introduces you to those two versions, focusing on the key ways in which they differ from the desktop versions.

I also describe 1PasswordAnywhere, which enables you to access your 1Password data securely from almost any computer with an Internet connection and a modern Web browser.

iOS

1Password for iOS is a universal app that runs on the iPhone, iPad, and iPod touch. It has most of the features in 1Password 4 for Mac, with a few notable exceptions—and a reorganized user interface, to suit the needs of small, touchscreen devices. You can purchase it from the [App Store](#).

One of the first things you'll probably want to do is sync the iOS version of 1Password with your Mac or PC; if you've already turned on Dropbox or iCloud sync, it's a matter of a few taps. (I cover all the details—as well as what to do if you prefer to avoid cloud-based sync—in [Set Up Syncing](#).)

Before you go any further, however, you should understand a few key concepts about the iOS app.

1Password for iOS: The Ins and Outs

Unlike OS X and Windows, iOS has no support for browser extensions or other mechanisms that enable one app to reach inside another to retrieve or enter data. Apple designed iOS this way for better security,

but it also limits the ways in which apps can interact, and is especially problematic when it comes to tools like 1Password.


So, when you're browsing the Web in Safari (or any other browser) on iOS and you come to a login page, you can't grab your credentials from 1Password without leaving your browser. Although you *could* switch to 1Password, enter your master password, find the login item, copy your password, switch back to your browser, and paste it (possibly repeating these actions with your username), that's more effort than most of us are willing to expend. Luckily, there are a few shortcuts, as I explain ahead, that make use of 1Password's built-in browser.

Even so, you may prefer to stay in another browser most of the time, and I wouldn't blame you. If you're using iOS 7 along with a Mac running OS X 10.9 Mavericks, the new iCloud Keychain feature that Apple plans to release later in 2013 may simplify your life—I discussed how that may interact with 1Password earlier, in [1Password & the Apple Keychain](#). Even with iCloud Keychain, however, you may want to switch to 1Password to fill in identities, choose among multiple sets of credentials for a given site, or fill in credit card information including your CVV number—not to mention sync password data across browsers and platforms.

Apart from Web browsing, 1Password for iOS lets you view, edit, add, and delete items, mark items as favorites, generate new passwords, and more.

One major difference from the desktop versions is the option to use a Quick Unlock Code. This is a convenience feature to prevent you from having to enter your master password (which, let's face it, can be a real pain on a tiny iPhone keyboard!) repeatedly in a short period of time. At your option, you can tell 1Password that if you leave the app and come back within a designated period of time (such as 2 minutes), you can unlock it with a much simpler, 4-digit code.

To set up a Quick Unlock Code:

1. Tap the Settings  icon.
2. Tap Security.

Solve Problems

Although I've found 1Password to be extremely reliable in the years I've used it, occasionally things go wrong. In particular, since 1Password 4 for Mac is brand new, it's more likely to provoke those "Hey, wait a minute..." moments. So, I want to close the book with a few brief pieces of advice about solving problems in 1Password.

Don't Panic

The first thing I want to say—notice the large, friendly letters—is that if something appears to be wonky, you shouldn't freak out. I know a number of the folks who work for AgileBits, and I'd interacted with them numerous times as a customer before I started writing about their software. I'm here to tell you, they pay attention to customers.

If you have a problem that isn't solved in this chapter, and for which you can't find a solution on the [1Password support site](#)—and especially if you're on the verge of panicking—feel free to [contact the AgileBits support department](#). A real live human being will read your message, take it seriously, and recommend steps to solve your problem.

If your query is less pressing, you may first want to peruse the [AgileBits discussion forum](#), where thousands of 1Password users (including yours truly) hang out and try to help each other with questions and problems—and yes, the AgileBits support staff hangs out there too!

Deal with Version 4 Changes

During the beta testing of 1Password 4.0 for Mac, I read hundreds upon hundreds of messages in the beta discussion forum, many of which amounted to a desperate "Oh no! What happened to (*my favorite feature from version 3*)?" If you're having that reaction, this section is for you.

Although 1Password 4 is an upgrade in the sense of having a higher version number, a different interface, and new features, the AgileBits engineers didn't create it by making changes to version 3.x. Instead, they rewrote the whole thing from scratch. Now, there were good reasons to do this, but the point I'm making is that if you notice a "missing" feature, it's not because it was *removed*, it's because it *wasn't added*. In some cases, AgileBits decided to go down a different path and modify, rename, merge, or (sometimes) remove features, but most "missing" features aren't there *yet* because there were higher priorities at first—and they will be back before long (see [Glimpse the Future of 1Password](#)).

Here are a few of the most commonly noticed "what about...?" features in 4.0:

- **Accounts and Wallet groups:** The item groups Accounts (of which there were 11 subtypes) and Wallet (of which there were 8 subtypes including Credit Card) no longer exist in 1Password 4.

In many cases, 1Password has merely promoted subtypes to full categories—for example, Database, Email Account, and Server, which were Account subtypes, are now full categories; and nearly all the Wallet subtypes (such as Bank Account, Driver's License, and Passport) are also stand-alone categories now. A few seldom-used item types (like FTP Account, MobileMe, and Membership) no longer exist as such, but when you upgrade from version 3 to 4, the data is preserved—anything that doesn't match an existing category is converted to a generic login.

- **Table-like views:** 1Password 3 had Traditional and Widescreen views that let you display multiple columns at once and sort by various criteria by clicking column headers. 1Password 4 currently has only a single list view, which many people dislike because it takes up more space yet fits less information. AgileBits tells me other views are under consideration—they're just not something they could squeeze into the initial 4.0 release.
- **Customizable Web fields:** In [Change Web Form Details](#) I said that you can rename or delete Web form fields but you can't add

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](#).

Ebook Extras

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 buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading this ebook on handheld devices on our [Device Advice](#) page.)
- 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.

If you bought this ebook from the Take Control Web site, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the “access extras...” link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the “access extras...” link above. Then, once you are logged in to your new account, add your ebook by clicking the “access extras...” link a second time.

Note: If you try these directions and find that your device is incompatible with the Take Control Web site, [contact us](#).

About the Author

Joe Kissell is a Senior Editor of TidBITS, a Web site and email newsletter about Apple and the Internet, and the author of numerous books about technology, including [*Take Control of Your Passwords*](#), [*Take Control of Your Online Privacy*](#), and [*Take Control of Dropbox*](#).



He is also a Senior Contributor to Macworld, was the winner of a 2009 Neal award for Best How-to Article, and has appeared on the MacTech 25 list (the 25 people voted most influential in the Macintosh community) since 2007. Joe has worked in the Mac software industry since the early 1990s, including positions managing software development for Nisus Software and Kensington Technology Group.

When not writing or speaking, Joe likes to travel, walk, cook, eat, and dream (in both senses of the word). He lives in San Diego with his wife, Morgen Jahnke; their son, Soren; and their cat, Zora. To contact Joe about this book, [send him email](#). But please note: *Joe is unable to provide any technical support for using 1Password*. Please refer all technical questions, bug reports, feature requests, and other comments about the 1Password software to [AgileBits](#).

Shameless Plug

Although I currently write and speak about technology as my day job, I have a great many other interests. To learn more about me, read other things I've written, and find out what I'm up to beyond the realm of Apple products, visit my home page at [JoeKissell.com](#). You can also follow me on Twitter ([@joekissell](#)) or App.net ([@joekissell](#)).

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.

Adam and Tonya are known in the Apple world as writers, editors, and speakers. They are also parents to Tristan, who has reached the age where he can read, understand, and find mistakes in the Take Control series.



Credits

- Take Control logo: Geoff Allen of FUN is OK
- Cover design: Sam Schick of Neversink
- Editors: Kelly Turner and Tonya Engst
- Editor in Chief: Tonya Engst
- Publisher: Adam Engst



Copyright & Fine Print

Take Control of 1Password

ISBN: 978-1-61542-428-3

Copyright © 2013, alt concepts inc. All rights reserved.

[TidBITS Publishing Inc.](#)

50 Hickory Road

Ithaca, NY 14850 USA

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.

You have our permission to make a single print copy of this ebook for personal use. Please reference this page if a print service refuses to print the ebook for copyright reasons.

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 that are the registered trademarks of Apple Inc.; you can view a [complete list of the trademarks and of the registered trademarks of Apple Inc.](#)

Featured Titles

Click any book title below or [visit our Web catalog](#) to add more ebooks to your Take Control collection!

[*Take Control of Dropbox*](#) (Joe Kissell): Discover the many features—especially the non-obvious ones!—that make Dropbox an exceptionally useful and popular Internet service for file transfer and collaboration.

[*Take Control of iCloud*](#) (Joe Kissell): Understand the many features, get set up properly, and enjoy iCloud!

[*Take Control of iBooks Author*](#) (Michael E. Cohen): Plan your project, customize a template, set up a table of contents, lay out pages, add interactivity and glossary items, and publish your masterpiece!

[*Take Control of LaunchBar*](#) (Kirk McElhearn): See the [comic](#) to learn how LaunchBar can help you control your Mac from the keyboard.

[*Take Control of PDFpen 6*](#) (Michael E. Cohen): Create, edit, and manipulate PDFs with Smile's PDFpen 6!

[*Take Control of Your 802.11n AirPort Network*](#) (Glenn Fleishman): Make your 802.11n (or 802.11ac) AirPort network fly—get help with buying the best gear, setup, security, and more.

[*Take Control of Your Online Privacy*](#) (Joe Kissell): Learn what's private online (not much)—and what to do about it.

[*Take Control of Your Paperless Office*](#) (Joe Kissell): With your Mac, scanner, and this ebook in hand, you'll finally clear the chaos of an office overflowing with paper.

[*Take Control of Your Passwords*](#) (Joe Kissell) Overcome password overload without losing your cool—and [view the comic](#) that goes with this ebook!