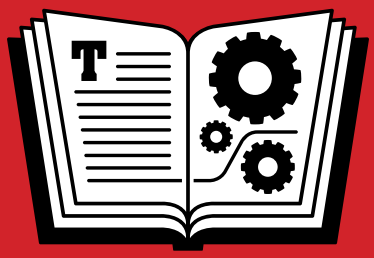
EBOOK EXTRAS: v2.2
Downloads, Updates, Feedback



TAKE CONTROL OF

1PASSWORD

by JOE KISSELL

$15

2ND EDITION

Table of Contents

Read Me First

Welcome to *Take Control of 1Password, Second Edition,* version 2.2, published in December 2016 by TidBITS Publishing Inc. This book was written by Joe Kissell and edited by Kelly Turner.

Find out how 1Password from AgileBits can simplify generating, storing, and inputting secure passwords and personal data so that you can sign in to Web sites quickly and click through Web shopping carts easily. Plus, learn how to use 1Password to store (and sync and share) many other forms of private data. Each 1Password platform (macOS, Windows, iOS, and Android) is covered, but the primary focus is 1Password 6 on the Mac.

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.

Updates and 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 on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

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

To review background information that might help you understand this book better, such as finding System Preferences and working with files in the Finder, read Tonya Engst's free *Read Me First: A Take Control Crash Course*.

In addition, please be aware of the following:

- **Application menu:** In 1Password for Mac, the application menu (which bears the app's name) is titled 1Password for the App Store version but 1Password 6 for the version purchased from the AgileBits Web site. For simplicity, I generally use the former term in this book—for example, "Choose 1Password > Preferences to open the Preferences window"—unless I'm explicitly talking about the version downloaded directly from AgileBits.
- **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.

What's New in Version 2.2

This version of the book contains numerous revisions to bring it up to date with the latest releases of 1Password. Some of the most noteworthy changes are these:

- Added a new topic, License 1Password, which discusses the various 1Password accounts (individual, family, and team) and stand-alone licenses for the 1Password app
- Included a detailed sidebar, 1Password Versions for Windows, which explains why there are three different Windows versions of 1Password and how they differ
- Added extensive clarifications throughout the book regarding the differences between 1Password 4 and 1Password 6 for Windows
- Expanded Make First-run Decisions and Install Browser Extensions to include information on steps for 1Password account holders, browser authorization codes, and other details
- Mentioned the 2016 MacBook Pro's Touch Bar in Lock or Unlock Manually with the Touch Bar
- Updated Set Up Syncing and other parts of the book to reflect the term "WLAN syncing" as a replacement for "Wi-Fi syncing"
- In Using Attachments and elsewhere, clarified that 1Password accounts use Documents as a replacement for attachments
- Updated Android to cover the features and usage instructions in the most recent version of 1Password for Android
- Massively revised the chapter Use 1Password Accounts (formerly "Use 1Password for Teams") to cover individual, family, and team accounts
- Updated the text to reflect the branding change from "1Password for Teams" and "1Password for Families" to "1Password Teams" and "1Password Families," respectively

- Removed text about 1PasswordAnywhere, which has been deprecated and is largely obsolete given the new 1Password accounts

What Was New in Version 2.1

Shortly after version 2.0 of this book was published, AgileBits made some significant improvements to 1Password.

The 2.1 revision addressed those changes and a few other small items:

- Added a clarification about sharing 1Password licenses with family members using iCloud Family Sharing; see Configure 1Password
- Rewrote the First Run for Mac Users description, as the process has changed considerably
- Updated the Watchtower and Heartbleed sidebar to clarify that Watchtower alerts you to other vulnerabilities besides Heartbleed (Watchtower is now available in 1Password 6.2 or later for iOS.)
- Described the new "Always open to" pop-up menu (for Mac only) in Configure Other Mac Preferences
- Revised the description and screenshots of the Android version to include the new features and revised user interface
- Updated the chapter Use 1Password Accounts to include information about 1Password Families
- Adjusted the wording of vault names for those using 1Password Teams; as of 1Password 6.0.2, the Everyone and Your Vault vaults have been renamed to Shared and Personal, respectively; see Create a Family or Team Vault

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. 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 an exhaustive 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—6.5.2 for Mac, 4.6.1 (and 6.1.308) for Windows, 6.5 for iOS, and 6.5 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 1Password 6 for Mac.

Note: Wondering why I list two different version numbers for Windows? It's a bit complicated, as I explain in the sidebar 1Password Versions for Windows.

The core features of 1Password are similar on every platform, and I call attention to platform-specific differences as needed. Due to 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. 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.

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.

Learn the basics:

- Discover 1Password's components, walk through setting up and using its major features, and start syncing; see Meet 1Password.
- Learn password fundamentals 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, Apple Watch, or public computer; see Use 1Password on the Go.
- Share vaults securely with coworkers and family members; see Use 1Password Accounts.

Delve into the details of your 1Password data:

- Zip right to the information you need; see Search and 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.
- Get help with common troubleshooting tasks; see Solve Problems.

Meet 1Password

You'll have an easier time working with 1Password if you set it up correctly from the start and understand how it's designed to function. In this chapter, I help you decide which version of 1Password to buy (if you haven't already made up your mind), 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 for iOS and Android to Use 1Password on the Go, later.

License 1Password

By now you've most likely downloaded and installed 1Password. However, if you haven't yet made a purchase, you should be aware of several different licensing options. (And, even if you've owned a 1Password license for years, you should be aware of several newer options that could affect how you choose to license the app in the future.)

Note: If you've already purchased a license or subscription and don't need any further information about your options, you can skip ahead to Configure 1Password.

For most of 1Password's history, it was like most apps in that you licensed the software itself for one or more devices or platforms. Apart from any paid upgrades you might opt for, the software was then yours to use indefinitely. You *can* still license 1Password this way if you like, but it's expensive to do so, and you'll miss out on a number of benefits that come with an alternative approach to licensing: 1Password accounts for individuals, families, or business teams.

Here's an overview of how the two options compare:

- **Stand-alone license:** You pay a rather high one-time fee of $64.99, which lets you use 1Password on any number of Macs or PCs you own personally. You can also use the iOS or Android versions for free, but you'll need to pay an additional $9.95 to unlock the Pro features (see iOS for details) on the mobile platforms. (Stand-alone licenses have further qualifications depending on whether you obtain the app direct from AgileBits or from the Mac App Store, iTunes App Store, or Google Play—each of which has its own rules.) If you want to sync your data across multiple devices, you can use many different methods (see Set Up Syncing), including Dropbox, iCloud Drive, and direct WLAN (Wi-Fi) syncing.
- **1Password account:** When you sign up, you pay a modest annual fee (as low as $35.88 per year) to use 1Password on all your devices, on any platform—including all the Pro capabilities for iOS and Android that owners of stand-alone licenses would have to pay extra for. 1Password accounts also enable you to access your passwords securely from any Web browser, and include automatic syncing across all your devices—no need to mess with Dropbox or another cloud service. (If you later cancel your subscription, your data stays on your devices, but stops syncing.) 1Password accounts also include unlimited app updates for as long as you continue paying for the service. There are three varieties of 1Password accounts:
    - *Individual:* The most basic 1Password account, which costs $2.99 per month (billed annually), includes all the features I just mentioned for a single person.

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 one of your passwords is guessed, leaked, stolen, or hacked. That's bad news, but it 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 8 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 8-character password has about 53 trillion (52^8) possible combinations. Add just one character, and the number of combinations jumps to almost 2.8 quadrillion (52^9).

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 and 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 automatic login saving 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 and Export Data), but in my experience adding them as you go is the path of least resistance.

However, even though saving new logins 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: automatic login saving is enabled globally by default, but you can toggle it if the need arises:

- On a Mac, go to 1Password > Preferences > Browsers and select or deselect "Detect new usernames and passwords and offer to save them." If you want to save logins automatically most of the time but exclude certain domains (for example, when you're testing a Web site you're developing), you can type those domain names into the exceptions list just below that checkbox.
- On a Windows PC running 1Password 4, go to File > Preferences > Auto-Save and select or deselect Auto-Save New Logins. To exclude a domain from Auto-Save, click Add, type the domain name, and click OK; repeat as needed.

Note: Automatic login saving does not yet work properly in 1Password 6 for Windows.

If you use multiple vaults (see Work with Multiple Vaults), 1Password's automatic login saving feature defaults to your primary vault. (On a Mac, its name appears in the Save Login dialog as a reminder.) To save the credentials to a different vault on a Mac, click the 1Password icon in the Save Login dialog and choose a different vault from the pop-up menu. (1Password 4 for Windows does not currently offer a way to choose a different destination vault on the fly.)

You can also disable automatic login saving for a particular domain on the fly. When you submit a login form and the 1Password Save Login dialog appears (much to your irritation), do this:

- On a Mac, click the gear  icon in the lower left of the dialog and choose Never Autosave for This Site from the pop-up menu.
- On a Windows PC, click Never for This Site at the bottom of the Auto-Save dialog box.

This adds the domain in question to 1Password's exceptions list on the Browser preference pane.

Store Other Information in 1Password

In the previous chapter I talked about using 1Password with a Web browser—storing and filling in usernames, passwords, contact data, credit card numbers, and so on. That combination of features may be 1Password's main focus, but the app can do many 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.

Note: Later, in Search and 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 several 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 can't find an appropriate category, you can create a password item.

Note: In Windows, the command to create a stand-alone password appears only if the Generated Passwords items appears in the sidebar. If it's not there, choose View > Generated Passwords before following these steps.

Since you generally won't be looking at a Web page when you need to create or save stand-alone passwords, automatic login saving won't help. Instead, open the main 1Password app, click File > New Item > Password (Mac) or New Item > Password (Windows), 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 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 app).
3. Later, at your convenience, open the main 1Password app and select Passwords in the sidebar.
4. Find the password you created (sorted by default according to Title), and edit its title or other attributes to identify its purpose (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 and 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 feature not yet available for Android).

But, before I get into any of this, I want to share my Professional Opinion, which is that you should ignore most of the features discussed in this chapter. 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 tell you about folders, tags, favorites, advanced searches, smart folders, and 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 1,500 items in my copy of 1Password (including more than 800 logins), accumulated over about 9 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 26**) 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.

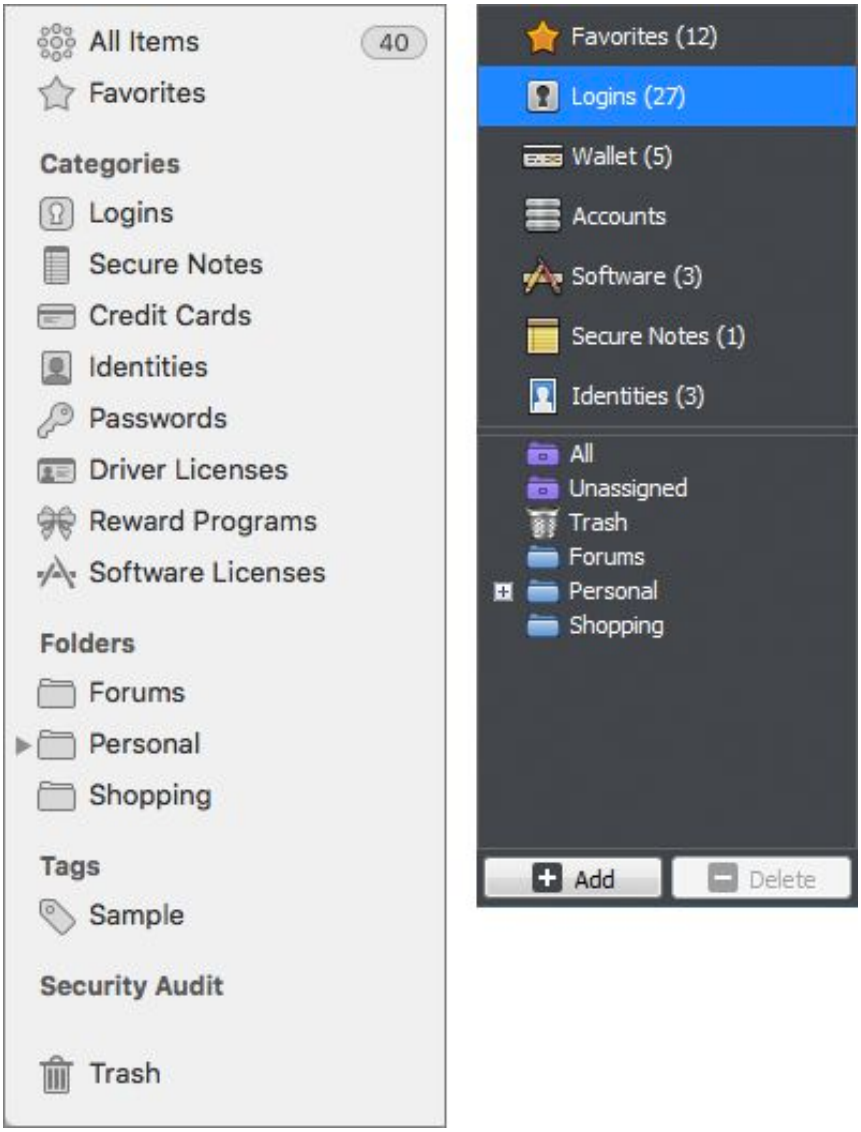


Figure 26: The sidebar in 1Password for Mac (left) and version 4 for Windows (right). (Version 6 for Windows looks more like the Mac version, but currently has fewer items.)

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; version 6 for Windows) or OK (version 4 for 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. In Share 1Password Data, I tell you about the features in 1Password for Mac that enable you to share individual passwords with other people, and about one method of sharing entire vaults with others using either the Mac or Windows version of 1Password. I close the chapter with brief pointers on how to Import and Export Data and Print 1Password Data.

Edit Saved Items

When 1Password's automatic login saving 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; version 6 for Windows) or URL (version 4 for Windows) field is the one for the page on which 1Password's automatic login saving 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 other ways discussed in Log In) could produce an error, since you're 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/URL field, overwriting the one that's there.

  You can also add more URLs to tell 1Password that there are other pages on which you can log in with the same credentials (see Add Multiple URLs to a Login). 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

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 go to 1Password > Preferences > Security (Mac), File > Preferences > Security (version 4 for Windows), or Settings  > Options > Security (version 6 for Windows).

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 (on a Mac only) enter a hint. Then click Change Password (Mac or version 6 for Windows) or OK (version 4 for Windows).

Changing your master password on one device changes it on your other devices too, once your data has synced among them.

Display

In the Mac version of 1Password and in 1Password 6 for Windows, 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 (on a

Mac) in 1Password mini. You can show the passwords on a Mac 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 on a Mac 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 (version 4 for Windows):** This self-explanatory option should remain selected for most people.
- **Lock When the Screen Saver Is Activated (Mac; version 4 for Windows):** 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; version 4 for Windows):** 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 When Web Browser Is Closed (version 4 for Windows):** To lock the 1Password helper app (which, in turn, locks all 1Password browser extensions) when you close your last

Use 1Password Accounts

Earlier, when I introduced the concept of 1Password accounts for individuals, families, and teams (see License 1Password), I said that *almost* everything about the way you use 1Password works the same with accounts as it does with a stand-alone license. This chapter is about the bits that *aren't* the same. The initial setup process is different, for example. You'll lose at least one feature (folders), and a couple of things will change (in particular, Documents replace attachments). And, if you have a 1Password Families or 1Password Teams account, you'll have access to new features, including secure sharing and permissions control.

What exactly will you get if you sign up for a 1Password account? Here are the highlights, starting with those available to everyone:

- **Built-in syncing:** 1Password accounts include their own sync capability, so you won't have to rely on Dropbox, iCloud, or another third-party service. (You can continue to sync local vaults separately in whatever way you choose—or not at all—while using 1Password accounts.)
- **Web access to your 1Password data:** 1Password accounts let you (and, if applicable, any family or team member) view and edit vault data securely in a Web browser.
- **Item history:** Using the Web interface, you can view previous versions of each item (for example, before a password change) and restore them if necessary. For individual and family accounts, 1Password stores item history for a year. For Standard team accounts, it stores 30 days of history, while Pro team accounts get unlimited history storage.

In addition, family and team accounts offer the following:

- **Secure sharing:** Share a single item, or a vault containing an arbitrary group of items, with other family or team members. (If you like, you can still share local vaults manually, as described

in Share 1Password Data, but sharing vaults through your account is both easier and more secure.)

- **Simpler invitations:** Send an invitation to one or two people or even an entire organization, and the recipient(s) can join your family or team account quickly and easily.
- **Automatic deployment:** Once people have joined your family or team account, you can give them access to shared vaults, on all their devices, whenever you like, without their having to take any action whatsoever.
- **Total access control:** You can decide, for each user of each vault, which actions that person can perform—including viewing passwords, creating and deleting items, printing items, and more. (The options are considerably more granular for team accounts than for family accounts, however.) In addition, you can at any time suspend or delete a family or team member entirely, or revoke a person's access to a particular vault.
- **Account recovery:** If one of your family or team members forgets his or her master password for a shared vault, you can perform a procedure to recover that person's access.

1Password accounts currently require the use of Safari, Chrome, Firefox, or Opera to perform setup and administrative functions. (AgileBits has told me that eventually the administration features will be rolled in to the various 1Password native apps, which will eliminate the need for a browser altogether.)

The remainder of this chapter contains an overview of how to use the features unique to 1Password accounts. I don't offer complete details here (and the details I do offer could quickly go out of date), but I do include numerous links to AgileBits' online documentation for 1Password accounts.

Use 1Password on the Go

Most of this book has talked about the desktop versions of 1Password (for macOS 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. And, for iPhone users who also have an Apple Watch, this chapter explains how to get a handful of 1Password features on your wrist.

Note: The next major release of 1Password for Windows 10, which is currently in beta testing, will run on any Windows 10 device, including phones and tablets. Because the release is far from complete as of publication time, I don't cover it in this chapter.

iOS

1Password for iOS is a universal app that runs on the iPhone, iPad, and iPod touch. It features a reorganized user interface to suit the needs of small, touchscreen devices. You can download it for free from the App Store.

Although 1Password for iOS has most of the features of its desktop counterparts, some features are available only with an in-app purchase of 1Password Pro (or a paid 1Password account):

- Multiple vaults
- Additional categories, such as Bank Accounts, Software Licenses, Passports, and Wireless Routers
- File attachments
- Custom fields
- Multiple URLs per item

- Apple Watch support (see Use 1Password on an Apple Watch)
- Time-based one-time passwords
- Folders and tags

Note: This chapter covers the Pro version, so if you haven't made that in-app purchase, some of the options described here won't appear in 1Password on your iOS device.

You should also be aware that even with the Pro features, 1Password for iOS does not currently offer the following features:

- Creating new vaults
- Renaming or removing tags
- Changing the sort order
- Performing advanced searches and creating smart folders
- Performing a security audit
- Editing Web form details
- Adding or modifying icons/thumbnails

In addition, form filling is a bit different due to restrictions in the design of iOS. But while filling in credentials with 1Password for iOS is still *slightly* harder than doing so with iCloud Keychain, 1Password makes it reasonably easy—especially on devices with Touch ID—and offers greater security and flexibility than iCloud Keychain.

If you're willing to use the browser built into the 1Password app, you'll have a smoother form-filling experience (at the expense of losing many of the features in Safari and other browsers); see Use the Built-in Browser for details. If you want to stay in Safari or another browser, you'll use a different technique; see Use Another Browser.

Solve Problems

Although I've found 1Password to be extremely reliable in the years I've used it, occasionally things go wrong. 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 Support Forum, where thousands of 1Password users (including, occasionally, yours truly) hang out and try to help each other with questions and problems—and yes, the AgileBits support staff hangs out there too!

Troubleshoot Common Mac Problems

A few other issues pertaining to the Mac version of 1Password appear to be FAQs, so let me address them here:

- **1Password mini not working in browsers:** If the 1Password mini app on a Mac works on its own but behaves weirdly (or not at all) in your browser, the cause might be an antivirus program.

One in particular, Sophos Antivirus for Mac, is known to interfere with the communication between 1Password mini and Web browsers. For details on working around the problem, read the support article Configuring Sophos.

- **Launcher utilities unable to see 1Password bookmarks:** Make sure you have the latest version of your launcher utility (such as Alfred, LaunchBar, or Quicksilver). Then go to 1Password > Preferences > Advanced, and select Enable 3rd Party App Integrations. Flip back to Launcher Utilities for more details.
- **Clipboard utilities behaving incorrectly:** Read Clipboard Managers for a discussion of this problem.
- **1Password mini flaking out:** If 1Password mini starts acting erratically for any reason, open the main 1Password app and choose Help > Troubleshooting > Restart 1Password mini to restart it. That usually fixes the problem.

If you're having another sort of problem, you can search for answers in the 1Password knowledge base; choose Help > Frequently Asked Questions.

One final troubleshooting tip: AgileBits has a stand-alone Mac diagnostic app called 1Password Troubleshooting. It can generate an extensive report about your computer that will help AgileBits techs solve your problems, and it includes a few maintenance functions. To read about and download this app, choose Help > Troubleshooting > Troubleshooting Utility.

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 on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have 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 the author of numerous books about technology, including *Backing Up Your Mac: A Joe On Tech Guide* and *Take Control of Your Online Privacy*. He is also a contributing editor to TidBITS and a senior contributor to Macworld, 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, Joe likes to travel, walk, cook, eat, and practice t'ai chi. He lives in San Diego with his wife, Morgen Jahnke; their sons, Soren and Devin; and their cat, Zora. To contact Joe about this book, send him email and be sure to include `Take Control of 1Password` in the subject of your message so his spam filters won't intercept it. But please note: *Joe is unable to provide any technical support for using 1Password.* Refer all technical questions, bug reports, feature requests, and other comments about the 1Password software to AgileBits.

Shameless Plug

On my site Joe On Tech, I write about how people can improve their relationship with technology. The site also features my own series of ebooks on topics such as backing up and maintaining your Mac. I'd be delighted if you stopped by for a visit! You can also sign up for joeMail, my free, low-volume, no-spam mailing list, or follow me on Twitter (@joekissell). To learn more about me personally, visit JoeKissell.com.

About the Publisher

TidBITS Publishing Inc., publisher of the Take Control ebook series, was incorporated in 2007 by co-founders Adam and Tonya Engst. Adam and Tonya 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.

Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Editor: Kelly Turner
- Production Assistant: Lauri Reinhardt
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK

More Take Control Books

This is but one of many Take Control titles! Most of our books focus on the Mac, but we also publish titles that cover other Apple devices, along with general technology topics.

You can buy Take Control books from the Take Control online catalog as well as from venues such as Amazon and the iBooks Store. Our ebooks are available in three popular formats: PDF, EPUB, and the Kindle's Mobipocket. All are DRM-free.

Copyright and Fine Print

Take Control of 1Password, Second Edition
ISBN: 978-1-61542-465-8

TidBITS Publishing Inc. 50 Hickory Road Ithaca, NY 14850 USA

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM 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.

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

Caveat lector: 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 book 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.

It's just a name: Many of the designations in this ebook 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. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren't Apple: 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 registered trademarks or service marks of Apple Inc. If you're into that sort of thing, you can view a complete list of Apple Inc.'s registered trademarks and service marks.