Welcome to *Take Control of 1Password, Fourth Edition*, version 4.0, published in October 2018 by alt concepts 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 websites 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 7 for Mac and Windows.

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 © 2018, alt concepts inc. All rights reserved.

---

**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 website, 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

Please be aware of the following:

- **Application menu:** In 1Password for Mac, the application menu (which bears the app’s name) is titled 1Password 7, whereas in Windows, it’s just 1Password (without the 7). For simplicity, I generally use the latter term in this book—for example, “Choose 1Password > License to open the License window”—unless I’m explicitly talking about just the Mac version.

- **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.

- **Mac Basics:** If you’re a Mac user and you’d like to review other 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 book *Take Control of Mac Basics*.

## What’s New in the Fourth Edition

In the more than one year since the last version of this book, AgileBits has been hard at work on 1Password—adding features, changing the user interface, and bringing various platforms more closely into alignment. In particular, version 7 for Windows is much different from what I described in the previous version of this book, but 1Password for macOS, iOS, and Android have also changed in numerous ways. In addition, AgileBits has made 1Password accounts the primary way to both license 1Password and sync data, and the service’s user interface has undergone quite a few changes.
As a result, this book required hundreds of changes—a massive rewrite that touched almost every page of the book. A full list of changes would run for many pages, but here are some of the biggest ones:

- Updated the description of 1Password licensing options in License 1Password
- Revised Explore the 1Password Components to reflect 1Password’s new architecture on macOS and Windows
- Expanded the description of 1Password X, which now lets 1Password work on platforms such as Chrome OS and Linux
- Revised nearly every mention of the Windows version of 1Password to reflect its current features and interface, and removed all mentions of the old versions 4 and 6 for Windows
- Updated the discussion of autosubmit (see A Word About Autosubmit) to reflect 1Password’s new behavior starting in version 7.2
- Expanded and updated the instructions for setting up and generating One-Time Passwords
- Added a topic about Documents and Attachments to cover the various ways of storing files in 1Password
- Revised Use Tags to cover the new ways 1Password works with tags
- Completely rewrote Perform a Password Security Audit to reflect the major changes to 1Password’s Watchtower features
- Thoroughly updated the chapter Use 1Password on the Go to reflect current reality—especially the portion about iOS, which now describes the new mechanism for autofill in iOS 12
Nobody likes dealing with passwords. After all, they exist solely as barriers to keep unauthorized people from accessing websites, 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 website 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. (It also avoids security vulnerabilities that plague browsers’ built-in password managers.) 1Password can fill in other information on web forms, too (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—7.2 for Mac, 7.2 for Windows, 7.2 for iOS, and 7.0 for Android. I spend more time talking about the desktop (Mac and Windows) versions than the mobile (iOS and Android) versions.

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.
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.
- Use special features of 1Password for Families and 1Password for Teams; see Manage a Family or Team Account.

**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 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, 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 the company’s newer approach to licensing: subscription-based 1Password accounts for individuals, families, or business teams.

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

• **1Password account:** When you [sign up](#) online (or buy a subscription as an in-app purchase within 1Password for Mac or Windows), you pay a modest annual fee (starting at $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 standalone licenses would have to pay extra for. 1Password accounts also enable you to access your passwords securely from any web browser or using the [1Password X](#) extension for Firefox, Chrome, and Chromium-based browsers (which even works in Chrome OS and Linux), and include automatic syncing across all your devices. (If you later cancel your subscription, your data stays on your devices, but stops syncing.) 1Password accounts include unlimited app updates for as long as you continue paying for the service.

**Note:** I’ll repeat this later, but I want to make it clear up front: a 1Password account *permits* you to sync using 1Password’s servers, but does not *require* you to do so. 1Password account holders can opt to instead sync their data using Dropbox or another service—or store their data locally and not sync it at all. It’s up to you.

There are four 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.

‣ **1Password Families:** For $4.99 per month (again, billed annually), up to five family members can have all the benefits of a 1Password subscription. (But even with just two family
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, website, 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 ($52^9$).
A couple of chapters ago, in Learn How Logins Work, you learned how to save credentials for a few websites 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 websites. 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 7 > Preferences > Browsers; or, on a Windows PC, go to 1Password > Settings > Browsers. 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 website you’re developing), you can type those domain names into the exceptions list just below that checkbox.

If you use multiple local vaults (see Work with Multiple Vaults), 1Password’s automatic login saving feature defaults to your primary vault; otherwise, the default is your personal vault in your 1Password account. To change the default, go to 1Password 7 > Preferences > Vaults (Mac) or 1Password > Settings > All Vaults (Windows) and choose a vault from the Vault for Saving pop-up menu.

Regardless of your default setting, you can choose a different vault when saving any particular login. (The current vault’s name appears in the Save Login dialog as a reminder.) To save the credentials to a different vault, choose its name from the pop-up menu in the Save Login dialog.

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 corner of the dialog and choose “Never Autosave for this Site” from the pop-up menu.

- On a Windows PC, click the triangle on the right side of the Not Now button and choose “Never autosave for this site” from the pop-up menu.

This adds the domain in question to 1Password’s exceptions list on the Browsers 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.

### Standalone Passwords

Passwords are needed for many reasons other than logging in to websites. 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.
Since you generally won’t be looking at a webpage when you need to create or save standalone passwords, automatic login saving won’t help. Instead, open the main 1Password app, click File > New Item > Password (Mac) or plus + button > 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.

As an alternative, you can use 1Password mini:

1. Open 1Password mini in whichever way you prefer.

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 (they’re 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 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. In Windows, you can right-click it and choose password > Copy from the contextual menu.

---

**One-Time Passwords**

Increasingly, online services offer an optional security feature called two-step verification (or words to that effect), in which you need both your regular credentials and a time-based one-time password (TOTP)—typically a numeric code that changes every 30 seconds—to
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.

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 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 1,800 items in my copy of 1Password (including more than 900 logins), accumulated over more than 12 years. I don’t use smart 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 27) lets you filter the display of your stored items in the main list. Click a header (denoted by a tiny arrow to its right) to expand or collapse it. Click a non-header item in the sidebar, and only the matching items appear in the list.

Figure 27: The 1Password sidebar. Item counts (shown here) are optional in 1Password for Mac, but always visible in 1Password for Windows.
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. 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. 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 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, domains, or subdomains 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 entering 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 or in your browser extensions.

Preventing an item from appearing while you’re in your browser means it won’t autofill or appear on the list if you press ⇧-\ 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...
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 website.)

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) or 1Password > Settings > Security (Windows).

Master Password

To change the master password that protects all the 1Password data in your current local vault on a Mac (not applicable to Windows, or to 1Password accounts on any device), click Change Master Password. Enter your current password, enter and verify a new password, and (on a Mac only) enter a hint. Then click Change Password.

.helper::

| Note: For instructions on changing the master password for a 1Password account or on Windows, see [this 1Password support article](#). |

Changing your master password for a standalone vault on one device changes it on any other devices that sync with it (once the next sync has occurred).
Display

The Display category has a single option: “Conceal passwords” (selected by default). With this checkbox selected, your passwords will be represented by bullets (•) in both the main 1Password app and 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—disable this feature.

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 computer is locked (Windows):** This self-explanatory option should remain selected for most people.

• **Allow Windows Hello to unlock 1Password (Windows):** If your PC is compatible with Windows Hello and you have it set up to log you in to your computer using a camera or fingerprint sensor, it makes sense to let the same mechanism unlock 1Password. Note, however, that you must still enter your 1Password master password the first time you unlock it after turning on or restarting your PC.

• **Lock when the screen saver is activated (Mac):** 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!
Manage a Family or Team Account

Throughout this book, I’ve pointed out situations in which 1Password accounts behave differently from local vaults. (Refer back to Learn About 1Password Accounts for more details.) However, with perhaps one or two exceptions, I haven’t mentioned ways in which 1Password Families or 1Password Teams accounts differ from individual 1Password accounts—what unique things you can do when your account supports multiple people. So I’d like to spend a few pages here doing just that.

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. Read on to learn about creating additional group vaults, adding family or team members, setting up permissions, and other tasks.

Before you can do any of the activities in this chapter, you must open a web browser; go to your-account-name.1password.com; and log in with your email address, account key, and master password. Everything here happens in the web interface.

Create a Family or Team Vault

Each family or team member gets a personal vault automatically, plus access to a single shared vault. However, you can create additional vaults if you like, each one with different contents and its own set of permissions for who can access it and how.

In your browser, you should see at least three categories—All Vaults, Personal (for all the user-specific vaults in your group), and Shared or Team (the default shared vault for your group). If you’ve already created other vaults, they’ll appear here too.
**Note:** Every user in your family or on your team gets a personal vault that’s not shared—just like you. They can choose to use it in addition to or instead of any existing personal vaults, or they can ignore it.

To add a vault, click New Vault, enter a title and description for the new vault, and click Create Vault. Repeat as desired to add more vaults.

**Note:** For more details and options, consult [Administrators: Get started with 1Password](which applies to teams and families).

---

**Invite Users to Your Family or Team**

To invite people to your family or team account, click Invitations in the sidebar on the right in your browser window. Click the blue plus + icon, enter one or more email addresses (separated by commas) and an optional message, and click Invite.

**Note:** You can also invite someone *outside* your family or team as a guest. Guests have access to only a single shared vault of your choosing, but that is sufficient for some purposes. (AgileBits uses examples such as an accountant, realtor, or babysitter, each of whom may need only a small number of shared passwords.) For instructions on sharing vaults with guests, see [this support article](

Each invitee receives an email message with simple instructions they must follow to join your family or team account, which includes adding the family or team to their copy(ies) of 1Password. Once a family or team member accepts your invitation, you (the administrator) also receive an email message containing a link you must click to confirm the new member. (You can also find a button for confirming new members by clicking Invitations in the sidebar.)

Family or team members initially receive access to the Shared vault and to their personal vault within the 1Password account.
Use 1Password on the Go

Most of this book has talked about the desktop versions of 1Password (for macOS and Windows), with occasional references to the mobile versions for iOS and Android. This chapter provides a bit more detail about those two versions, as well as noting 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.

About the Pro Features

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

- 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
- Tags

**Note:** This chapter covers the Pro versions of the mobile apps, so if you aren’t using a 1Password account and haven’t made that in-app purchase, some of the options described here won’t appear in 1Password on your device.
iOS

1Password for iOS is a universal app that runs on the iPhone, iPad, and iPod touch. You can download it for free from the App Store; as noted above, you’ll need to either use a 1Password subscription or purchase the Pro features to unlock all its capabilities. You should also be aware that even with the Pro features, 1Password for iOS does not currently offer the following features:

- Creating new local vaults
- Renaming tags, or removing them from all items at once
- Changing the sort order
- Performing advanced searches and creating smart folders
- Performing a security audit (although individual items in the Compromised Logins category do display a banner to that effect, as long as Watchtower is enabled in Settings > Security)
- Editing web form details
- Adding or modifying icons/thumbnails

In addition, form filling is a bit different, though far easier in iOS 12 than it was previously—especially on devices with Touch ID or Face ID—and it offers greater security and flexibility than iCloud Keychain.

Configure 1Password for iOS

If you use a 1Password account (see Learn About 1Password Accounts), follow the prompts to log in when you first run 1Password for iOS. If not, 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.)

You’ll also want to configure certain security settings to make it easier to access your data. One major difference from the desktop versions
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 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:

• **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.

• **Browser extensions flaking out**: If 1Password’s browser extensions start acting erratically for any reason, open the main 1Password app and choose Help > Troubleshooting > Restart 1Password Extension Helper to restart this background process. 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 > Get Help.

One final troubleshooting tip: AgileBits has a standalone 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.
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 website, 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 website, contact us.
Joe Kissell is the author of more than 60 books about technology. As of May 2017, he also became the publisher of Take Control Books, when alt concepts inc.—the company he runs along with his wife, Morgen Jahnke—acquired the Take Control series from TidBITS Publishing Inc.’s owners, Adam and Tonya Engst.

Joe is also a contributing editor to TidBITS and a senior contributor to Macworld. Before he began writing full-time in 2003, Joe spent nearly eight years managing software development. He holds a bachelor’s degree in Philosophy and a master’s degree in Linguistics.

In his rare non-work hours, Joe likes to travel, walk, cook, eat, and practice t’ai chi. He and Morgen live in San Diego with their sons, Soren and Devin, and their cat, Zora. To contact Joe about this book, send him email and please include Take Control of 1Password in the subject. You can also follow him on Twitter (@joekissell) or visit his personal website, JoeKissell.com.

### Credits

- Publisher: Joe Kissell
- Editor: Kelly Turner
- Cover design: Sam Schick of Neversink
- Logo design: Geoff Allen of FUN is OK
Click any book title below or visit our web catalog to add more ebooks to your Take Control collection!

*Are Your Bits Flipped?:* Overcome common tech misconceptions with this collection of easy-to-read essays.

*Take Control of Apple Mail:* Learn the ins and outs of Apple’s email app in macOS and iOS.

*Take Control of Automating Your Mac:* Work more efficiently on your Mac with time-saving shortcuts of all kinds.

*Take Control of Backing Up Your Mac:* Protect your valuable data with a complete, bulletproof backup strategy.

*Take Control of iCloud:* Understand the many features, get set up properly, and enjoy iCloud!

*Take Control of Maintaining Your Mac:* Learn preventive maintenance steps to keep your Mac running smoothly.

*Take Control of the Mac Command Line with Terminal:* Master your Mac’s command-line interface and learn basic Unix skills.

*Take Control of Your Digital Legacy:* Make sure your important digital information is preserved for future generations.

*Take Control of Your Online Privacy:* Learn what’s private online (not much)—and what to do about it.

*Take Control of Your Paperless Office:* 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:* Overcome password overload without losing your cool.
Copyright and Fine Print

*Take Control of 1Password, Fourth Edition*
Copyright © 2018, alt concepts inc. All rights reserved.

alt concepts inc. 4142 Adams Ave. #103-619, San Diego CA 92116, 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, they 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 alt concepts 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 alt concepts 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.

Click here to buy the full 167-page “Take Control of 1Password” for only $14.99!