

EBOOK EXTRAS: v7.0
Downloads, Updates, Feedback



TAKE CONTROL OF

1Password

by **JOE KISSELL**

\$14.99

7TH
EDITION

[Click here to buy the full 190-page "Take Control of 1Password" for only \\$14.99!](#)

Table of Contents

Read Me First	5
Updates and More	5
Basics	6
What's New in the Seventh Edition	7
Introduction	9
1Password Quick Start	11
Meet 1Password	12
License 1Password	12
Understand 1Password Accounts	14
Learn About 1Password 8	16
Set Up 1Password	17
Lock and Unlock 1Password	22
Explore the 1Password Components	27
Learn How Logins Work	39
Find Your Usage Pattern	46
Check for Updates	48
Learn What 1Password Isn't Good For	49
Understand Password Security	52
Learn Password Security Basics	52
Understand Optimal Password Length	55
Password Dos and Don'ts	56
Passkeys and the Passwordless Future	58
Use 1Password for Web Browsing	62
Create and Save Logins	62
Log In	73
Deal with Multistep Logins	76
Use Passkeys in 1Password	79
Fill Web Forms Using Identities	85
Shop Online Securely	87

Store Other Information in 1Password	90
Standalone Passwords	90
One-Time Passwords	91
Security Questions	94
Software Licenses	95
Secure Notes	97
Documents and Attachments	98
SSH Keys	99
Other Data Types	100
Search and Organize Your 1Password Items	102
Make Your Life Simpler	102
Understand the Sidebar Sections	103
Use Favorites	106
Use Tags	106
Adjust the Sort Order	107
Perform a Search	107
Use Previously Generated Passwords	111
Use the Archive	112
Work with Multiple Vaults	113
Edit 1Password Items	117
Edit Saved Items	117
Work with Icons and Thumbnails	123
Update Old Passwords	125
Perform a Password Security Audit	128
Share Individual 1Password Items	134
Import and Export Data	136
Customize 1Password	138
Configure Desktop Settings	138
Configure Browser Extension Settings	153
Set Up a Recovery Code	159
Configure 1Password Account Settings	160
About 1Password and Mac Launcher Utilities	163

Manage a Family or Team Account.....	165
Create a Family or Team Vault	165
Invite Users to Your Family or Team	166
Specify Permissions	167
Suspend or Revoke Vault Access	168
Share Items with Family or Team Members	169
Manage Family Access in the 1Password App	170
Use 1Password on the Go	171
Mobile Version Basics	171
iPhone/iPad	173
Android	179
1Password for Apple Watch	182
Solve Problems	184
Don't Panic	184
Troubleshoot Common Problems	184
About This Book.....	186
Ebook Extras	186
About the Author and Publisher	187
Credits	187
Also by Joe Kissell	188
Copyright and Fine Print	190

Read Me First

Welcome to *Take Control of 1Password, Seventh Edition*, version 7.0, published in February 2026 by alt concepts. This book was written by Joe Kissell and edited by Glenn Fleishman (seventh edition) and Kelly Turner (first through sixth editions).

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/iPadOS, Android, and watchOS) is covered, but the primary focus is 1Password for Mac, Windows, and Linux.

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 © 2026, Joe Kissell. 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.
- Access the book in both PDF and EPUB formats. (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.

Basics

Please be aware of the following:

- **Settings:** With a few exceptions, which I note throughout the book, the settings you can adjust in the 1Password desktop app are the same across platforms. To open the Settings window in Windows or Linux, click the Menu ☰ icon and choose Settings from the pop-up menu. To open this window in macOS, choose 1Password > Settings. Throughout this book, rather than repeat those instructions each time, I simply say “go to the Settings window” or words to that effect; to direct you to a specific pane, I say something like “go to Settings > Security.”
- **Keyboard shortcuts:** 1Password includes a number of built-in keyboard shortcuts, some of which are customizable. In general, shortcuts involve the Command (⌘) key in macOS or the Control (Ctrl) key in Windows and Linux, but are otherwise the same. In this book, I use a compressed notation where feasible to indicate when a keyboard shortcut differs across platforms only in the use of that modifier key, like “press ⌘/Ctrl-Shift-Space.” All that means is: press the ⌘ key on a Mac, or the Ctrl key anywhere else, along with the other listed key(s). Similarly, only Macs have an Option key; on PCs, you’ll see an Alt key instead.
- **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 or passkey.
- **Log in vs. sign in:** The terms “log in” and “sign in” mean exactly the same thing: to gain access to an account by supplying your credentials. Each site has its own reasons for choosing one expression or the other. As much as I’d like to pick one term and stick with it, even 1Password itself isn’t consistent—for example, it refers to

items that store your credentials as “logins” while using “sign in” for what you do to authenticate on 1Password.com (and elsewhere). Apart from sticking with whatever terminology shows up on the screen at specific spots, I use the terms interchangeably in this book.

What’s New in the Seventh Edition

1Password is rapidly evolving, with new features and user interface updates appearing regularly. As a result, version 7.0 of this book is a gigantic revision, with many hundreds of changes. The most significant are:

- Shortened the topic [Learn About 1Password 8](#) from nine pages to one, since 1Password 7 is now in the distant past
- Overhauled the entire [Meet 1Password](#) chapter to reflect the current state of the app and browser extensions
- Updated instructions throughout the book for working with [1Password in Your Browser](#), whose interface has changed quite a bit
- Rewrote [A Word About Autosubmit](#), now that 1Password follows a new approach
- Updated [Use Passkeys in 1Password](#) to talk about additional setup steps and details, including a new sidebar [About Importing and Exporting Passkeys](#)
- Updated [Set Up a One-Time Password Generator](#) with current details
- Added information about additional sidebar entries to [Understand the Sidebar Sections](#)
- Explained the use of locations in 1Password items; see [Add a Location](#) and [The Home Screen](#)
- Updated [Import](#) to include numerous additional details

- Thoroughly revised the entire [Customize 1Password](#) chapter, as a huge number of settings are either new or different; this includes a new topic, [Set Up a Recovery Code](#)
- Updated [Configure 1Password for iPhone/iPad](#) with new instructions

Introduction

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 account 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.

Note: This book is meant primarily for individual and small-business users. I deliberately omit features intended only for corporate/enterprise users, such as the [1Password SCIM Bridge](#) and single sign-in (SSO) capabilities.

I cover *only* 1Password 8 in this edition—not earlier versions, even though they're still available on some platforms. I say more about this in [Learn About 1Password 8](#).

The core features of 1Password are similar across platforms, and I call out the few, minor 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, or Apple Watch; see [Use 1Password on the Go](#).
- Use special features of 1Password Families and 1Password Business; 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 settings 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 subscribe to (if you haven't already made up your mind), cover some preliminary configuration steps, explain locking and unlocking, 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, like most of this book, primarily describes the Mac, Windows, and Linux versions of 1Password, although most of what you learn here also applies to the mobile versions. To learn more details about 1Password for iPhone/iPad and Android, see [Use 1Password on the Go](#), later.

License 1Password

By now you've most likely subscribed to, downloaded, and installed 1Password. However, if you haven't yet subscribed, you should understand your licensing options.

Note: If you've already purchased a subscription and don't need any further information about your options, you can skip ahead to [Learn About 1Password 8](#).

When you [sign up](#) for a 1Password account online or buy a subscription as an in-app purchase on supported platforms, you pay a modest annual fee (starting at \$35.88 per year) to use 1Password on all your devices, on any platform. 1Password accounts (described more fully

just ahead) also enable you to access your passwords securely from any web browser, and include automatic syncing across all your devices. (If you later cancel your subscription, a local copy of 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.

1Password accounts come in several varieties (see [Understand 1Password Accounts](#), just ahead, for further details):

- *Individual*: The most basic 1Password account, which costs \$3.99 per month (billed annually), includes all the features I just mentioned for a single person.
- *1Password Families*: For \$5.99 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 members, you'll save money over the cost of individual accounts.) Each family member gets a personal vault that isn't shared, but family accounts also make it possible to share individual passwords and other pieces of data securely with other family members, manage family members' permissions, and help a family member recover a forgotten password—all things you can't do with an individual account.
- *1Password Business*: Businesses and other non-family groups can pay as little as \$2.00 per user per month for features comparable to those available to families—plus additional administrative controls. There are three [business categories](#):
 - ▶ *Teams*: Small businesses normally pay \$3.99 per user per month, but a Teams Starter Pack costs \$19.95 per month for up to 10 users, making the per-user price only \$2.00 per month.
 - ▶ *Business*: Large businesses needing advanced capabilities such as automated deployment, usage reports, and audit trails can opt for 1Password Business accounts, which start at \$7.99 per user per month, but also include free family accounts for each employee. (This book doesn't cover any of the features exclusive to 1Password Business accounts.)

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 account 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).

Use 1Password for Web Browsing

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.

Reminder: In this chapter I focus mainly on the desktop (Mac, Windows, and Linux) versions of 1Password, though nearly everything here also applies to iPhone, iPad, and Android versions, too—just with a slightly different interface (see [Use 1Password on the Go](#)).

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 [Save a Login](#). It's also possible to add them manually to the 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).

Check Your Settings

To save logins in your browser, you must have the 1Password browser extension installed (see [Browser Extensions](#)). Automatic login saving is enabled in the extension by default, but you can toggle it if needed (which also toggles filling in passwords). To do so, click the 1Password  icon on the toolbar, then click the Account Menu followed by Settings. On the Settings page, select “Autofill & save” and turn on “Offer to save and fill logins and other items.”

While you're on the settings screen, you should check to see that the default vault for saving new passwords is the one you want: choose your desired vault from the “Save new items in” pop-up menu under General. To save the credentials for a particular site to a different vault, choose its name from the pop-up menu in the Save dialog (refer back to **Figure 11**).

Note: If you have not only multiple vaults but also multiple accounts (for example, a home account and a business account), 1Password tries to guess which account you want to use for saving new logins based on the email address you entered.

Generate Random Passwords

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

- In your browser, click in the password field and, in the 1Password pop-up menu, click Use Suggested Password. (If you're unsatisfied with the suggested password, see the next bullet point.) Click the Save button when prompted.

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.

Reminder: Like most of this book, this chapter concerns itself mainly with the desktop (Mac, Windows, and Linux) versions of 1Password, though nearly everything here also applies to iPhone, iPad, and Android versions, too—just with a slightly different interface (see [Use 1Password on the Go](#)).

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, in the 1Password app, click + New Item > Password; in the Mac app, choose File > New Item > Password; in Windows or Linux, choose the Menu ⋮ > New Item > Password; or in 1Password in Your Browser, click the plus  icon > Password. Fill in the form (using the built-in password generator when you get to the password field), being sure to give the item a descriptive title that will help you find it later. Then click Save.

When it comes time to retrieve your password later, you can go to the 1Password app or 1Password in Your Browser and click the password to copy it. Or, after finding the item in Quick Access, you can press ⌘/Ctrl-Shift-C to copy it, and then paste it where it's needed.

One-Time Passwords

Countless 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 log in. Dropbox, Facebook, Google, Microsoft, and Slack are among the many companies that use this approach.

Sometimes this one-time password is sent to your mobile phone via SMS, which is insecure and prone to hacking. But most frequently, the way to generate it is to use an authenticator app that you set up in advance for each of your accounts. Google Authenticator and Authy are perhaps the two best-known examples of authenticator apps, but 1Password can generate these one-time passwords for you too, eliminating the need for a separate app. As a bonus, 1Password automatical-

Search and Organize Your 1Password Items

Over time, you'll store hundreds—maybe thousands—of things in 1Password. But they're useful to you there only if you can find them quickly and easily when you need them. 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, searches, collections, 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 2,000 items in my copy of 1Password (including more than 1,000 logins), accumulated over 18 years. I don't use tags or favorites—a simple search virtually always turns up exactly what I'm looking for. I choose not to make extra work for myself.

So, before you do *any* organizing at all, try using 1Password for a while by merely searching (see [Perform a 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

The sidebar (**Figure 33**) in desktop versions of 1Password lets you filter the display of your stored items in the main list. Click a header to expand > or collapse ▼ it. Click a non-header item in the sidebar, and only the matching items appear in the list.

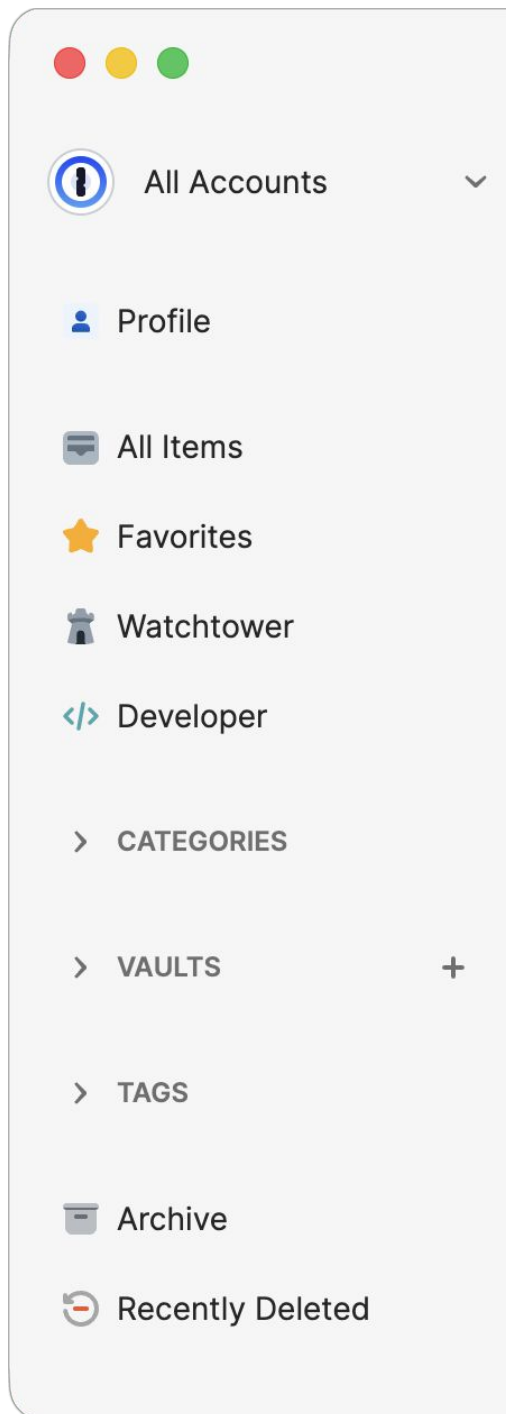


Figure 33: The 1Password sidebar, with all sections collapsed

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 Individual 1Password Items](#), I tell you about how to share credentials with other people. I close the chapter with brief pointers on how to [Import and Export Data](#).

Reminder: As before, in this chapter I focus mainly on the desktop (Mac, Windows, and Linux) versions of 1Password, though most of this also applies to iPhone, iPad, and Android versions, too—just with a slightly different interface (see [Use 1Password on the Go](#)).

Note: It is not possible to print from 1Password.

Edit Saved Items

1Password’s automatic login saving feature usually captures 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 to 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 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 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.

Use Custom Fields

You can add extra fields to an item and call them anything you like. This should rarely be necessary, since 1Password provides the most commonly needed fields, plus a generic Notes field. However, it could come in handy if, for example, you want a single software license item to contain license keys for multiple versions of the software, or if you want a login item to include both an email address and a separate username.

When editing an item in 1Password, you see a “+ add more” control like the one in **Figure 34**. Click it to display a pop-up menu with a variety of additional field types.

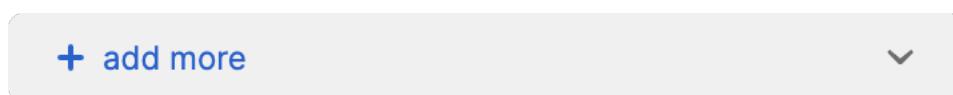


Figure 34: Use this pop-up menu to add your own custom fields and sections.

Customize 1Password

Throughout this book, I've mentioned a variety of settings that you can change to modify 1Password's behavior. Here, however, I want to provide a complete reference, which is broken down into the following subtopics:

- In [Configure Desktop Settings](#), I cover the settings in the 1Password app for Mac, Windows, and Linux.
- In [Configure Browser Extension Settings](#), I describe the settings available in 1Password in Your Browser (including 1Password for Safari).
- In [Set Up a Recovery Code](#), I tell you how to generate a code you can use to access your account if you lose your secret key or password.
- In [Configure 1Password Account Settings](#), I explain settings that are found when you sign in to your account at 1password.com, 1password.ca, or 1password.eu.

I round out the chapter with a brief mention of using 1Password on a Mac with launcher utilities; see [About 1Password and Mac Launcher Utilities](#).

Note: For settings in the mobile versions of 1Password, see [Configure 1Password for iPhone/iPad](#) and [Configure 1Password for Android](#).

Configure Desktop Settings

To open the Settings window in Windows or Linux, click the Menu  icon and choose Settings from the pop-up menu. To open this window on a Mac, choose 1Password > Settings. From there, select a category to display a pane with the corresponding settings.

General Settings

The General pane of 1Password's Settings window contains the following settings:

- **Keep 1Password in the menu bar (Mac)/notification area (Windows)/system tray (Linux):** Although keyboard shortcuts are always available and 1Password in Your Browser provides easy-to-find icons for accessing 1Password, you may prefer to have yet another systemwide mechanism for opening and using 1Password. Check this box to display a 1Password / icon in the appropriate spot for your operating system. What exactly this icon does is determined by the next setting.
- **Click the icon to:** With the 1Password icon visible (per the checkbox above), you can use this pop-up menu to configure what happens when you click it: “Show a menu,” the default, displays a pop-up menu with options such as Open 1Password, Open Quick Access, and Lock/Unlock; Show Quick Access displays the Quick Access window; and “Show the main window” opens the 1Password app.
- **Start at login (Mac)/Open 1Password on startup (Windows):** Make sure this checkbox is selected to run the 1Password background process when you start, restart, or otherwise log in to your computer. (This does not open the 1Password app itself on login.)
- **Format secure notes using Markdown:** Leaving this checkbox selected gives you the option to use Markdown formatting to apply styles to your notes (see [Secure Notes](#)); if for some reason you want to ensure that they're always plain text, you can deselect this.
- **Prefill username when creating a new login:** When creating a new login, 1Password can make a guess at the username it thinks you'll want to use and fill it in, as long as this box is checked. 1Password starts by using your default email address, if it's set in your profile; otherwise, it uses the username you have chosen most frequently.

Manage a Family or Team Account

So far, 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.

Note: Although 1Password Business and 1Password Enterprise accounts include all the Teams features, this book doesn't cover features exclusive to Business or Enterprise 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. 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, secret key, and account password. Everything here happens in the web interface.

Note: If you live in Canada or the European Union, your domain name might end in 1password.ca or 1password.eu, respectively.

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 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 left in your browser window. Click “Invite by email,” 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

Use 1Password on the Go

Most of this book has talked about the desktop versions of 1Password (for macOS, Windows, and Linux), with occasional references to the mobile versions for iPhone/iPad and Android. This chapter provides a bit more detail about those latter 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.

Mobile Version Basics

The mobile versions of 1Password are nearly identical to each other in both features and interface, and also closely resemble the Mac, Windows, and Linux versions of the app. That means nearly everything you’ve learned in this book about using the desktop versions of 1Password applies to the mobile versions. It also means you can move between [iPhone/iPad](#) and [Android](#) versions of 1Password with barely a thought.

Nevertheless, it’s worth spending a moment noting some of the minor differences between the mobile and desktop versions of 1Password, and then reviewing unique characteristics of the iPhone/iPad and Android versions of the app.

The Home Screen

One interface element found in the mobile versions but not the desktop versions is a Home screen. If it’s not currently visible, tap Home to display it (and if you don’t see a Home icon, which may be the case on larger-screen devices, tap the sidebar  icon to display it).

The Home screen is a customizable dashboard that may contain elements such as tips, favorites, recently created logins, and frequently used items. To customize the Home screen, scroll down to the bottom

and tap Customize. Check or uncheck any section, and use the handles on the right to rearrange the order. Then click Done.

I mentioned in [Add a Location](#) that any item can have an associated geographical location. If you select the Nearby category at the top, then any items to which you've added a location appear automatically on your Home screen when you're near those locations.

You can also pin any 1Password field (such as a specific username or password field within an item) to the Home screen for quick access later. (Be sure to enable Pinned Fields when you customize the Home screen.) To pin a field, open an item, touch and hold (iPhone/iPad) or tap (Android) a field, and choose Pin to Home from the pop-up menu.

The Sidebar/Items List

On iPads and other tablets, 1Password displays a sidebar similar to the one in desktop apps. (On smartphones, the same information appears in the Items view—tap Items at the bottom of the screen.) Unlike desktop versions of 1Password, however, the mobile versions let you customize this view. To do so, scroll to the bottom and tap Customize. Just as when customizing the Home screen, check or uncheck any section, and use the handles on the right to rearrange the order. Then click Done.

Item Shortcuts

While viewing a single item, you can touch and hold (iPhone/iPad) or tap (Android) a password to display a menu with commands that may include Copy, Reveal, Show in Large Type, Pin to Home, and (if applicable) “View password history.”

Locating Settings

The Settings screen in mobile versions of 1Password is not as easy to find as it once was. Here's how to get there:

- **On an iPhone:** Tap Home, Search, or Watchtower at the bottom, then tap the icon in the upper-left corner of the screen, followed by Settings.

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 [1Password Community](#) site, 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 Problems

The old “turn it off and back on again” cure for all manner of electronic devices applies, in its own way, to most 1Password problems too. To wit:

- If you’re having trouble with 1Password in Your Browser, first try quitting and reopening the browser. If that doesn’t solve the problem, try turning off the 1Password extension and turning it back on.

In my experience, one of those two procedures fixes the vast majority of in-browser issues.

Tip: On a Mac only, if 1Password for Safari is causing you grief that the above steps don't fix, try opening the 1Password app and choosing Help > Fix Missing Safari Extension. Then go back to Safari, go to Safari > Settings > Extensions, uncheck 1Password for Safari if it's checked, and then recheck it.

- If you're having trouble with the 1Password app, try quitting it and reopening it. If that doesn't do the trick, sign out of your 1Password account(s) and then sign back in.
- If even those fixes don't help, try restarting your device.

If all those suggestions seem a bit simplistic, well...they are! In my many years of using 1Password on six different platforms, I've found it to be quite solid, but on the few occasions when I've had problems, one of those steps *nearly always* fixed it (and when I was unsuccessful solving problems on my own, AgileBits tech support was able to help me out).

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.
- Access the book in both PDF and EPUB formats. (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.

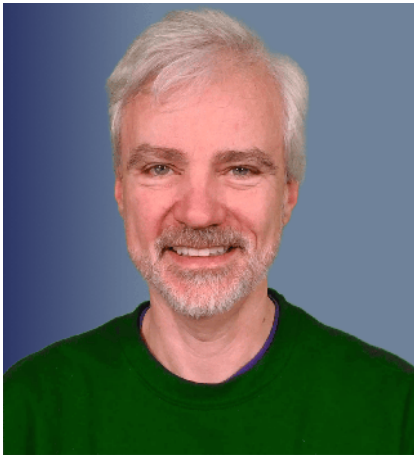
More Take Control Books

This is but one of many Take Control titles! We have books that cover a wide range of technology topics, with extra emphasis on Macs and other Apple products.

You can buy Take Control books from the [Take Control online catalog](#) as well as from venues such as Amazon and the Apple Book Store. But it's a better user experience and our authors earn more when you buy directly from us. Just saying...

Our ebooks are available in two formats, PDF and EPUB, which are viewable on any computer, smartphone, tablet, or e-reader. All are DRM-free.

About the Author and Publisher



Joe Kissell is the author of more than 75 books about technology. In 2017, he also became the publisher of Take Control Books, when alt concepts—the company he runs with his wife, Morgen Jahnke—acquired the Take Control imprint from TidBITS Publishing Inc.’s owners, Adam and Tonya Engst. Before he began writing full-time in 2003, Joe managed software development, a *totally normal* profession for someone with degrees in philosophy and linguistics.

In his rare non-work hours, Joe likes to walk, cook, read, and practice tai chi. He lives in Saskatoon, Saskatchewan, Canada, with Morgen and their sons. To contact Joe about this book, [send him email](#) and *please* include [Take Control of 1Password](#) in the subject. You can follow him on Mastodon ([@joekissell](#)) or Bluesky ([@joekissell.com](#)), or visit his personal website, [JoeKissell.com](#).

Credits

- Publisher: Joe Kissell
- Editor: Glenn Fleishman (7th edition), Kelly Turner (1st–6th editions)
- Cover design: Sam Schick of [Neversink](#)
- Logo design: Geoff Allen of [FUN is OK](#)

Also by Joe Kissell

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

[*Mac Basics*](#): Get to know your Mac inside and out with this detailed guide.

[*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 DEVONthink 4*](#): Master this powerful information management tool.

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

[*Take Control of MailMaven*](#): Discover how to use this powerful Mac email app from SmallCubed.

[*Take Control of the Mac Command Line with Terminal*](#): Master your Mac's command-line interface and learn basic Unix skills.

[*Take Control of Tahoe*](#): Discover what's new in macOS 26 and get all the information you need to upgrade safely.

[*Take Control of Solving Mac Problems*](#): Learn how to maintain, troubleshoot, and speed up your Mac.

[*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, you'll 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, Seventh Edition

ISBN: 978-1-990783-86-9

Copyright © 2026, Joe Kissell. All rights reserved.

[alt concepts](#), 419 8B-3110 8th St. East, Saskatoon, SK S7H 0W2 Canada

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 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 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.