Why ditch your expensive password manager for the free KeePass?

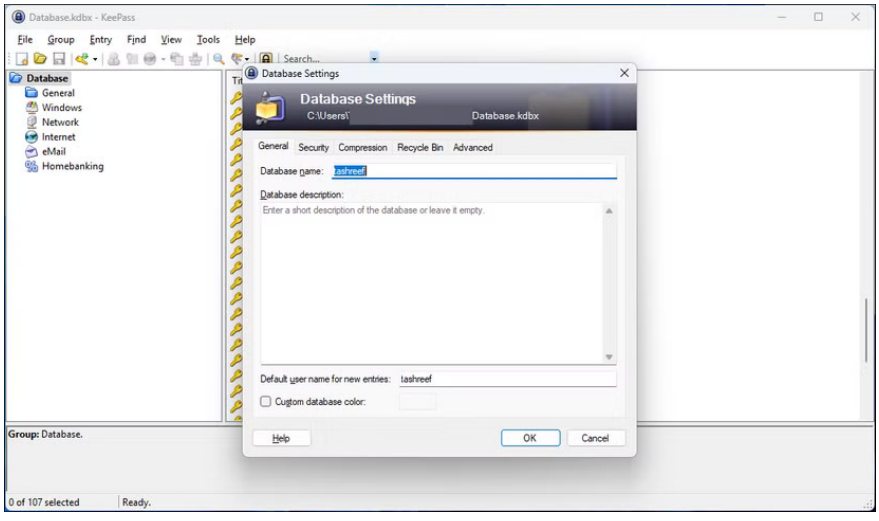
After 5 years and $300 spent on 1Password, many people have finally switched to the excellent free password manager: KeePass. The only thing they regret is not doing it sooner.

After 5 years and $300 spent on 1Password , many people have finally switched to the excellent free password manager: KeePass. The only thing they regret is not doing it sooner.

1. Complete control of data

1Password's move away from local storage isn't a huge deal, but it does change the deal. Paying $60 a year is increasingly pointless when every password, note, or license key has to live in the cloud, whether you like it or not.

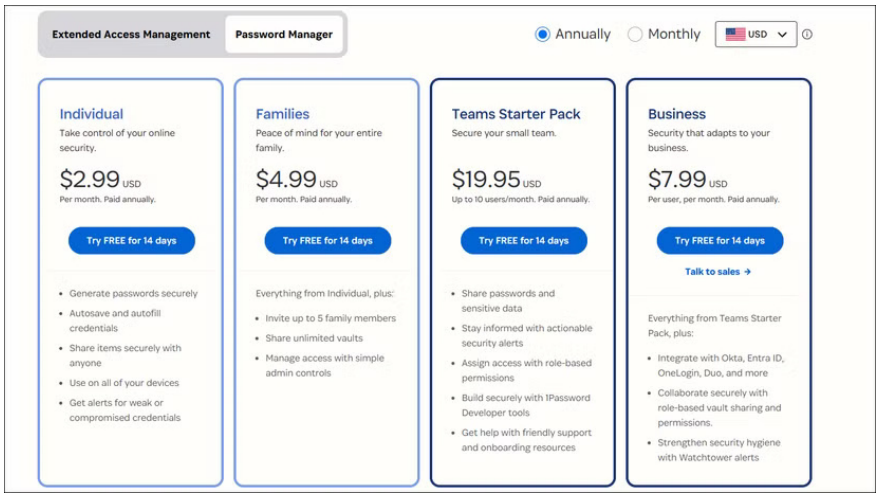
With KeePass , your password database lives exactly where you want it—on your laptop's SSD and synced via your Dropbox account. The KDBX file is yours, encrypted with AES-256, and KeePass encrypts the entire database, including passwords, usernames, notes, and attachments.



2. The cost is no longer reasonable

Another reason people are switching to KeePass is the rising cost of premium password management. 1Password's family plan costs $60 a year. Unlike LastPass or Bitwarden , which offer limited free plans, 1Password doesn't have a free option, so you have to pay starting on the 15th day after your trial ends. Over five years, that's $300—enough for a midrange tablet or a weekend trip.

You pay for features you rarely use and the privilege of renting access to your own passwords. As for the essentials, KeePass covers them well. The current Dropbox plan includes cloud sync. Browser add-ons work through the KeePass plugin, and the password generation works better with KeePass because you can customize more options than with 1Password.



3. Open source transparency is important

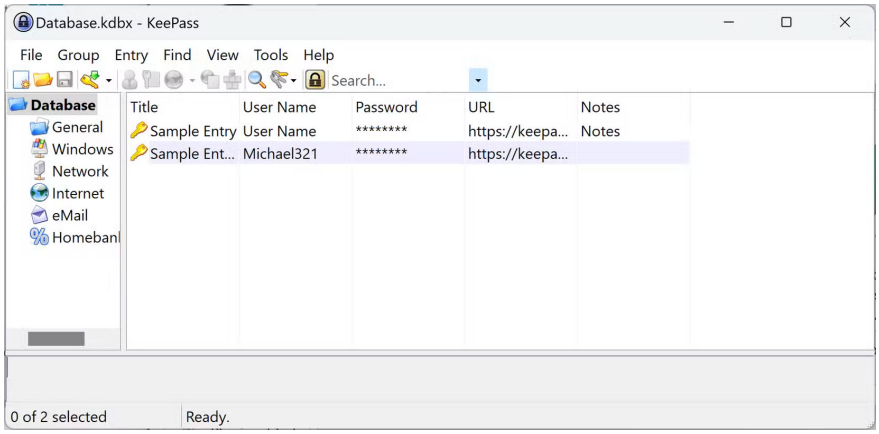
Open source tools are open to public scrutiny, meaning anyone can inspect and audit the source code. A comprehensive EU-FOSSA audit examined KeePass code in 2016 and found no critical or high-risk vulnerabilities, no hidden telemetry, no usage analytics, or anonymous data collection.

Commercial password managers love to brag about their security. They'll tell you about their zero-knowledge architecture and secure cloud infrastructure, but you have to take their word for it. With KeePass, thousands of security researchers have reviewed the code. Even when vulnerabilities are discovered, the community identifies them, reports them, and fixes them promptly.

4. KeePass offers the multi-device flexibility you need

Many people run Windows on their PCs and Android on their phones. Most password managers handle this setup well, but KeePass lets you do it exactly the way you want.

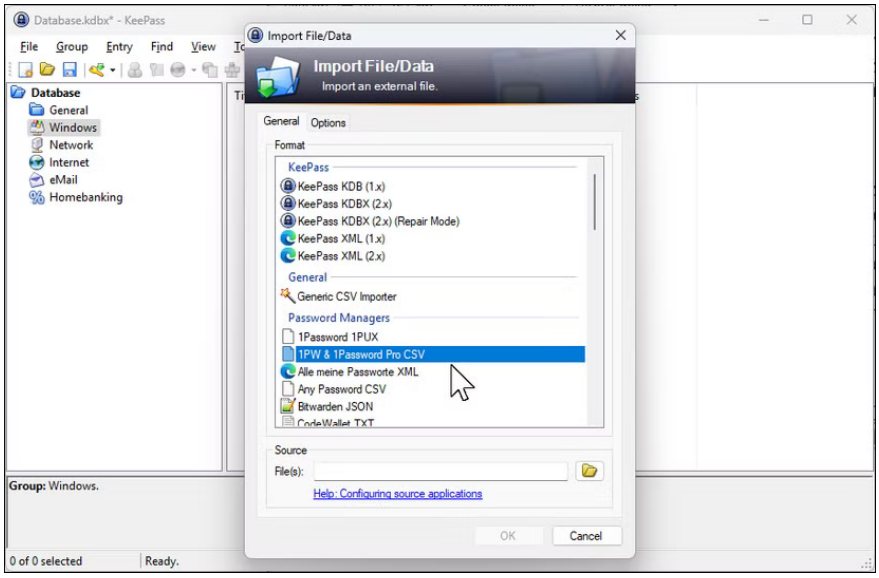
On Windows, you can use the original KeePass 2.x with some plugins. The interface looks like it was ripped from Windows XP, but it works well. You'll find KeePass runs significantly faster than 1Password 7. Android phones run KeePass2Android, which integrates with the system's autofill feature and even works offline. If you're on an iPhone, you can choose between KeePassium or Strongbox.



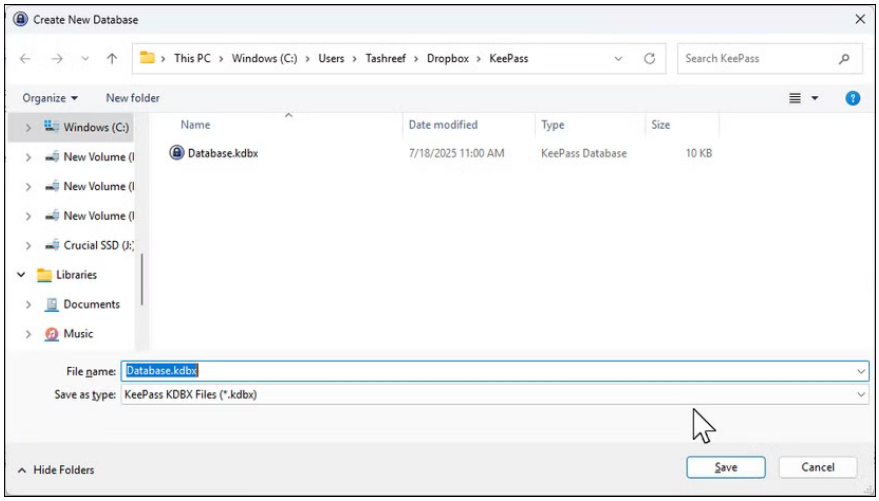
However, if the outdated interface puts you off, KeePassXC might be a better fit for you. It's a community fork that reads KDBX files similarly but doesn't look like the old version from 2003. You'll lose some plugin compatibility, but you get browser integration and TOTP support without the hassle of setting it up. Setting up KeePassXC is even simpler than the original KeePass—it took about 10 minutes, compared to the hour it took to configure the plugin.

5. The transition was easier than expected

The entire migration took about two hours. First, you exported your data from 1Password to CSV and imported it into KeePass, which supports over 35 formats, including 1Password, Dashlane , LastPass, and Bitwarden. Then you spent another hour organizing your entries into folders and setting up AutoType for the sites you use most.



The only real challenge was configuring sync, since KeePass doesn't have built-in cloud sync. I followed the KeePass documentation to save my database to a Dropbox folder, and then assigned the same folder as my Android phone's database folder to KeePass2 Android. Once configured, it worked so well that I forgot it wasn't built-in. When I edited on my phone, my laptop showed my changes within seconds.



Just remember, to ensure changes don't get lost or conflicted, it's best not to edit the database on multiple devices at once, and to always let Dropbox finish syncing before editing elsewhere.

1Password is great. But with KeePass, you truly own your passwords, control your data, and save money every month. If anything, many people wish they had made the switch sooner.