**KeePass**

**INTRODUCTION**

**KeePass Password Safe** is a [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source) [password manager](https://en.wikipedia.org/wiki/Password_manager) primarily for [Windows](https://en.wikipedia.org/wiki/Windows). It officially supports [macOS](https://en.wikipedia.org/wiki/MacOS" \o "MacOS) and [Linux](https://en.wikipedia.org/wiki/Linux) [operating systems](https://en.wikipedia.org/wiki/Operating_system) through the use of [Mono](https://en.wikipedia.org/wiki/Mono_(software)).

Additionally, there are several unofficial [ports](https://en.wikipedia.org/wiki/Porting) for [Windows Phone](https://en.wikipedia.org/wiki/Windows_Phone), [Android](https://en.wikipedia.org/wiki/Android_(operating_system)), [iOS](https://en.wikipedia.org/wiki/IOS), and [BlackBerry](https://en.wikipedia.org/wiki/BlackBerry) devices.

KeePass stores usernames, passwords, and other fields, including free-form notes and file attachments, in an encrypted [file](https://en.wikipedia.org/wiki/Computer_file).

This file can be protected by any combination of a master password, a key file, and the current Windows account details. By default, the KeePass database is stored on a local [file system](https://en.wikipedia.org/wiki/File_system) .

KeePass supports a number of [plugins](https://en.wikipedia.org/wiki/Plug-in_(computing)).[[9]](https://en.wikipedia.org/wiki/KeePass#cite_note-9) It has a [password generator](https://en.wikipedia.org/wiki/Random_password_generator) and synchronization function, supports two-factor authentication, and has a *Secure Desktop* mode.

It can use a two-channel auto-type obfuscation feature to offer additional protection against [keyloggers](https://en.wikipedia.org/wiki/Keystroke_logging" \o "Keystroke logging).[[10]](https://en.wikipedia.org/wiki/KeePass#cite_note-Rubenking-Review-10) KeePass can import from over 30 other most commonly used password managers.

A 2017 [Consumer Reports](https://en.wikipedia.org/wiki/Consumer_Reports) article described KeePass as one of the four most widely used password managers (alongside [1Password](https://en.wikipedia.org/wiki/1Password), [Dashlane](https://en.wikipedia.org/wiki/Dashlane" \o "Dashlane) and [LastPass](https://en.wikipedia.org/wiki/LastPass" \o "LastPass)), being "popular among tech enthusiasts" and offering the same level of security as non-free competitors but being more difficult to install.

A 2019 Independent Security Evaluators study described KeePass as well as other widely used password managers as being unable to control Windows 10's tendency to leave passwords in cleartext in RAM after they are displayed using Windows controlled GUI.

 In addition, several github projects (KeeFarce, KeeThief, Lazanga) specifically attack a running KeePass to steal all data; when the host is compromised, KeePass cannot prevent password theft.

Note that "neither KeePass nor any other password manager can magically run securely in a spyware-infected, insecure environment.

|  |  |
| --- | --- |
| [KeePass icon.svg](https://en.wikipedia.org/wiki/File:KeePass_icon.svg) | |
| [KeePass 2.x Main Window](https://en.wikipedia.org/wiki/File:KeePass_Main.png)  KeePass 2.x Main Window | |
| [**Developer(s)**](https://en.wikipedia.org/wiki/Software_developer) | Dominik Reichl |
| **Initial release** | November 16, 2003; 16 years ago |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | 2.44[[1]](https://en.wikipedia.org/wiki/KeePass#cite_note-1) (January 20, 2020; 46 days ago) [[±]](https://en.wikipedia.org/w/index.php?title=Template:Latest_stable_software_release/KeePass&action=edit) |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [sourceforge.net/p/keepass/code/](https://sourceforge.net/p/keepass/code/)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q762660#P1324) |
| **Written in** | [C#](https://en.wikipedia.org/wiki/C_Sharp_(programming_language)) (2.x version), [C++](https://en.wikipedia.org/wiki/C%2B%2B) (1.x version) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista) and later (plus other platforms in [unofficial derivatives](https://en.wikipedia.org/wiki/KeePass#Unofficial_KeePass_derivatives)) |
| [**Platform**](https://en.wikipedia.org/wiki/Computing_platform) | [.NET Framework](https://en.wikipedia.org/wiki/.NET_Framework), [Mono](https://en.wikipedia.org/wiki/Mono_(software)) |
| **Available in** | English |
| [**Type**](https://en.wikipedia.org/wiki/Software_categories#Categorization_approaches) | [Password manager](https://en.wikipedia.org/wiki/Password_manager) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [GNU GPLv2](https://en.wikipedia.org/wiki/GNU_General_Public_License)+ |
| **Website** | [keepass.info](https://keepass.info/) [Edit this at Wikidata](https://www.wikidata.org/wiki/Q762660#P856) |

**HISTORY**

* k[eePass Password Safe](https://keepass.info/" \t "_blank) is a free open source password manager for Windows ; ports of the password manager are available for Linux, Mac OS X, Android, iOS, and other systems as well.
* The review focuses on the Windows version of KeePass, and here in particular version 2.x as it offers more features.
* Passwords are used nearly everywhere on today's Internet and even on local devices.
* you log in on your devices using a password, pin or other authentication options, and need passwords for nearly any service on the Internet.
* Some Internet programs, web browsers for instance, come with password saving functionality.
* Users may install browser extensions to improve the core functionality and use desktop programs or applications for that as well.
* Password managers can be divided into three groups: online, local, or mixed. Online password managers use cloud storage to sync data.
* [LastPass](https://www.lastpass.com/) is a typical example of an online service. Local password managers run on the local device and store the data on the device by default and not the cloud.
* Mixed password managers support both features and give the user the choice to pick the most suitable option. KeePass falls into the mixed category even though it stores its databases locally by default.

Gjgj

**HOW THIS KEEPASS WORKS?**

KeePass is a popular and free password management tool. As frustrating as they can be, passwords are still a way of life when authenticating to most systems and accounts.

The worst thing you can do from a security perspective is use the same password for all of your accounts (and remembering the breadth of your accounts can be challenging as well).

* You can reduce the headaches by using a password manager utility like [KeePass](https://keepass.info/) or [Password Safe](https://pwsafe.org/).

**ADVANTAGES**

* Your information is protected by a very high level of encryption.
* You only have to remember one master password.
* You can use this single password to unlock a database that contains all your stored passwords.
* You can organize passwords into groups.

**DISADVANTAGES**

* Not user-friendly: **KeePass** is designed for utility, not ease of use.
* No security breach alerts: **KeePass** merely stores your passwords, but it doesn't do anything else to protect your credentials online.
* No form fill-in: Unlike traditional password managers, **KeePass** won't automatically fill in forms for you.

**CONCLUSION**

The easiest way to put in your passwords is to export them into a CSV file from your browser.

I only saw **one plugin that allowed you to import passwords from a browser directly, and that was for Firefox.**

 If you don’t choose either of these options, you’ll have to type in each password manually, which could be a bit tedious.

One all of your passwords are in, KeePass will **tell you which ones are weak, repeated, or old.** It can offer replacements from the **password generator** that will be a lot harder to figure out than what you’d come up with (no offense!).