Password-Manager

> [!toc] Table of Contents

> [!info] Info {static}
>
> A password manager is an essential tool for ensuring that you take the necessary precautions to keep your passwords secure. Here you can find out what makes a good password and how you should handle them:
>
> Countermeasure: Strong Passwords

KeePassXC and Bitwarden are both open source and have applications for all common operating systems/browsers.

KeePassXC works offline, Bitwarden online. However, KeePassXC can also be synchronized across multiple devices using external services.

Practical password managers for PCs:

- KeePassXC: Linux, Windows, MacOS
- Bitwarden: Linux, Windows, MacOS
  - Keep in mind, that for using Bitwarden, you will need a provider that runs a Bitwarden service and that you trust. Don't use untrusted providers.

The password managers integrated into browsers and operating systems are not necessarily recommended, as they are often proprietary and designed primarily for convenience. This regularly leads to security vulnerabilities. Browsers in particular are always a target for attackers and offer many attack vectors.

KeePass for mobile devices

Recommendation from the official KeePassXC documentation:

- Android: keepassDX, Keepass2Android

- iOS: Strongbox, KeePassium

KeePassXC

KeePassXC is one of the best-known and most widely used password managers. It is open source, regularly checked for vulnerabilities by experts, and offers a variety of very practical features. These enable us to bridge the gap between security and convenience.

Browser integration

There are plugins for KeePassXC for all common browsers *(except Safari)* to conveniently use the auto-fill function. This automatically suggests the correct login details on every website for which passwords have been saved.

This prevents you from accidentally entering your password when you click on a phishing link, because the plugin recognizes that you have landed on the wrong URL.

Key file

It is recommended to secure a password database with both: a password and a second factor. The easiest way to do this is with a key file. (See below for an example scenario.)

Key file as second factor

It is possible to encrypt the database with a separate key file in addition to the password. This means that you always need both the password and the key file to access the passwords.

Instructions for doing this can be found here.

Key file as master key

You can also encrypt your password database with just a key file, without a password. Then you must always select the key file when opening the database in KeePassXC.

Key file as master key with 2nd factor password

A common use case for this is to store the key file on an encrypted USB stick, which you always carry with you, e.g. on your key ring. This also ensures 2-factor authentication. The following is required:

1. factor: the password for the stick
2. factor: the stick (with the key file)

to access the passwords. It is essential to ensure that there is a backup USB stick in case the actual stick is lost!

Generate new passwords

One of the core features of a password manager is that it can generate strong passwords or passphrases according to your own specifications. This ensures that you don't reuse the same password out of convenience.

Synchronize and back up passwords in the cloud

Isn't that dangerous?

The password database is always encrypted, at all times. It is never decrypted in the cloud, so the cloud operators cannot read it. However, the police could potentially steal a copy of your database, as described in the following example scenario.

Example scenario

Let's assume that your password database is “only” protected with a (strong) password. If the police have access to your cloud (or obtain your database in some other way), they will only have the encrypted file and will not be able to do anything with it.

However, if they find out your password in the future (e.g., by secretly watching you type it in), they can retrieve the encrypted database and decrypt it.

If the database were also encrypted with a key file, it would not be enough to know the password; the key file would also be needed. If you were to destroy this key file, there would be no way to decrypt the stolen database.

How To

For example, you could store your database in the cloud and access it from all your devices.

The key file is stored **only locally** on your devices.

If you suspect that the authorities have obtained a copy of your password database

1. make a copy of your database
2. create a new password
3. and a new key file
4. and then delete the **old key file** from all your devices.

This will render the compromised database useless forever.

> [!warning] Warning {static}
>
> Before you delete your old key file, make sure:
>
> 1. that the new database works with the new key file
> 2. that you don't forget the new password!

In both cases, all your passwords would be irretrievably lost.

KeePassXC as a 2-factor app

KeePassXC can also be used as a 2FA app with TOTP. This even works on the apps for mobile phones.

Instructions

Here you will find instructions with further references.

Note

We consistently refer to KeePassXC here.

Older versions such as KeePassX and KeePass should no longer be used.

Version #2
Erstellt: 2026-02-15 16:16:31 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-03-18 13:28:19 UTC von ESC-IT Migration Bot