Keepassxc

> [!toc] Table of Contents

> [!info] Getting Started {static}
>
> The official *English-language* KeePassXC documentation offers a very good and comprehensive “Getting Started” article. We recommend reading it to get an overview of the available features!

Below, we summarize what we consider to be the most important points from the KeePassXC documentation linked above. Throughout the article, we refer back to the individual sections of the KeePassXC documentation. If you find it difficult to follow so much text, this video, *(on YouTube)*, explains the core features of KeePassXC quite well. Once you are familiar with the basic usage of KeePassXC, there is also a sequel for advanced use cases.

Create a database

The database is basically just a file in which passwords are stored in encrypted form. It always ends with `.kdbx`

KeePassXC is the program used to decrypt and use this file.

If you don't have a database yet, you must first create a new one. Before you create your first database, you need to consider the protection methods you want to use. The simplest form of protection is to use a strong password. For additional protection, you can consider adding another protection "layers", such as a key file (key files).

To create a new database without a key file, follow the steps in this guide: Create new database

Key file

When creating the database, there is a button labeled “Add additional protection” where you set the password for the database.

Then, under the “Key file” field, click the `Add key file` button.

Here you can now either:

- Create a new key file.
  - `Generate`: Specify a name and location for saving the new key file
- Specify an existing key file to be used to encrypt this database:
  - `Browse`: Here you can select your existing key file

Decrypt database with key file and password

If you have protected your database with a password and an additional key file, you will need both to unlock it again:

- Open the database with KeePassXC
- `I have a key file`
- Select the key file in the file manager
- Enter the password
- Confirm

Add key file later

If you already have a password database, you can also add a key file later.

We strongly recommend that you back up your database beforehand. This will prevent the loss of all passwords if something goes wrong. *To do this, simply make a copy of the database with a new name. For example, if the database is called “Passwords.kbdx,” create a copy called “Passwords-keyfile.kbdx” or something similar.*

- Open the (new) database in KeePassXC
  - Now you may have both databases open at the same time: multiple db tabs
  - This is not a problem, but be careful not to get confused and edit the wrong database. Close the original database, so that nothing goes wrong.
- In the top bar, click on `Database`
- Then click on `Database security...`
- From here, follow the instructions in the section on adding a key file
- Caution: Once you have created and saved a key file, KeePassXC assumes that you now want to use **only this key file to unlock the database. If you have already clicked `OK`,

you will have seen a warning message to this effect.
    - Therefore, you must reset and confirm the password using `Change password`.
    - `OK`

Password entries

Follow the official documentation to create a password entry.

You can also edit existing entries later (double-click on the entry).

Create strong password according to entropy

Click the dice icon in the tool bar. This opens the password generator. Here we have to options:

1. Create a password, out of selected character types

Screenshot of KeePass password generator character view

2. Create a password, out of a selected word list

Screenshot of KeePass password generator word list view

In both screenshots you can see the amount of entropy bits for the generated password. We recommend creating password with an entropy of 120 bits.

> [!tip] You can download word lists for various languages
>
> For example from here. You can also combine words from different languages, although you would have to do this manually, since KeePassXC only lets you select on word list at a time.

Browser integration

KeePassXC can be integrated into you browser. The integration makes it possible to automatically fill Browser Log-Ins for passwords that are saved in your Database. This saves a lot of time, as you don't need to manually copy-and-paste your passwords into the browser.

There are official instructions for installing the browser plugin (except for Safari).

TOTP

Official KeePassXC instructions with helpful screenshots.

TOTP is a form of two-factor authentication used by many web services, such as email or cloud access. To set up 2FA for a service, you need two things:

1. The appropriate setting in the web service, e.g. in the email settings.
2. The configuration of the corresponding KeePassXC entry for this web service.

The settings for web services all look slightly different, of course, but in most cases you will find the following in the account settings:

- A section with `Security` or `Privacy`.
- Here you should find the `2FA` or `TOTP` settings.
- “Enable TOTP” or similar

Now a QR code and, in the best case, a random string should appear (see KeePassXC instructions). The QR code is useful if you set up TOTP on your mobile phone, as you can easily read the `Secret` with the mobile phone apps using the camera. On a PC, we need the character string for this.

If only the QR code appears here without the character string, we have to read the “Secret” from the QR code.

> [!info]
>
> Read Secret from QR code This works with all common mobile phone cameras that can read QR codes. It is very likely that more than just the `Secret` will appear here, but rather a URL that is actually intended for mobile apps, e.g.: `otpauth://totp/example.org:username?secret=PABRSLZNHFLAIENT&issuer=Example` The `secret` is hidden here between `secret=` and the next special character, in this case `&issuer...`.
>
> Our `secret` is therefore: `PABRSLZNHFLAIENT`.

- `Copy secret`

Now we go to the KeePassXC database:

- Right-click on the corresponding password entry
- `TOTP`
- `Set up TOTP`
- Paste `Secret`
- `OK`

Now you should see a small clock next to the password entry. *This symbolizes the temporary nature of the TOTP codes.* totp clock symbol

Finally, we need to synchronize the TOTP setup. To do this, the current TOTP token must be re-entered in the web service settings. The TOTP token can be copied in two ways:

- `Control` + `T`, or
- `Right-click` > `TOTP` > `Copy TOTP`

Go back to the web service settings:

- Paste the TOTP token
- Confirm

You should now see a message indicating that the setup was successful.

Backup

KeePassXC offers an automatic backup feature. This ensures that you always have an up-to-date version of your password database in a different “location” than the one you mainly use.

Under Settings `(gear icon)` > `General` > `File Management`, you will find the option `Create backup of database before saving`. There you can specify a path where the replacement file should be saved.

It may be a good idea to specify cloud storage if you are not already synchronizing the database via cloud storage.

> [!warning] Warning {static}
>
> Although the database is always encrypted, even in the cloud, there are scenarios that need to be considered. Read the example scenario of a potential

> threat here!

Synchronization/backup in Nextcloud

At aktivismus.org you will find links to instructions for all platforms on how to synchronize files via Nextcloud.

The principle works the same with iCloud, OneDrive, Dropbox, etc.

Version #4
Erstellt: 2026-02-15 16:16:01 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-05-23 14:48:49 UTC von ESC-IT Migration Bot