

# KeePassXC

## Getting Started

Die offizielle *englischsprachige* KeePassXC [Dokumentation](#) bietet einen sehr guten und umfangreichen "[Getting Started](#)" Artikel. Es empfiehlt sich diesen einmal durchzulesen um einen Überblick über die verfügbaren Funktionen zu bekommen!

Im Folgenden werden die unserer Meinung nach wichtigsten Punkte aus der oben verlinkten Dokumentation von KeePassXC zusammengefasst. Dabei wird immer wieder auf die einzelnen Stellen in der Dokumentation von KeePassXC verwiesen. Falls es Dir schwer fällt, so viel Text zu folgen, gibt es z.B. [dieses Video](#) (*auf YouTube*), das die Kernfeatures von KeePassXC ganz gut erklärt. Daran anknüpfend gibt es auch eine [Fortsetzung](#) für fortgeschrittene Anwendungsfälle.

## Datenbank anlegen

Die Datenbank ist im Grunde einfach nur eine Datei, in der die Passwörter verschlüsselt gespeichert werden. Sie endet immer mit `.kdbx`

KeePassXC ist das Program, um diese Datei dann entschlüsseln und benutzen zu können.

Wenn du noch keine Datenbank hast, musst du zu erst eine neue Datenbank anzulegen. Bevor du startest, könntest du dir aber noch die [Empfehlungen zu Schlüsseldatei](#) (Schlüsseldateien) anschauen. Falls dir das zusagt findest du im Folgenden eine Anleitung dazu.

Zum Anlegen einer neuen Datenbank ohne Schlüsseldatei kannst du dem Schritt in dieser Anleitung folgen: [Neue Datenbank anlegen](#)

## Schlüsseldatei

Beim Anlegen der Datenbank gibt es an der Stelle, wo das Passwort für die Datenbank festgelegt wird, einen Button `Zusätzlichen Schutz hinzufügen`.

Danach unter dem Feld `Schlüsseldatei` auf den Button `Schlüsseldatei hinzufügen`.

Hier kann jetzt entweder:

- eine neue Schlüsseldatei angelegt werden.
  - **Erzeugen**: einen Namen und Ort zum Speichern festlegen
- eine existierende Schlüsseldatei angegeben werden, die zum Verschlüsseln dieser Datenbank benutzt werden soll:
  - **Durchsuchen**: Datei auswählen

## Datenbank mit Schlüsseldatei und Passwort entschlüsseln

Hast du deine Datenbank mit einem Passwort und zusätzlichem Schlüsseldatei geschützt, brauchst du auch beides, um sie wieder zu entsperren:

- Datenbank mit KeePassXC öffnen
- **Ich habe eine Schlüsseldatei**
  - Im Dateimanager die Schlüsseldatei auswählen
- Passwort eingeben
- bestätigen

## Schlüsseldatei nachträglich hinzufügen

Falls du schon eine Passwortdatenbank hast, kannst du auch nachträglich noch ein Schlüsseldatei hinzufügen.

Wir empfehlen dringen vorher ein Backup deiner Datenbank zu machen. Damit verhindern wir den Verlust sämtlicher Passwörter, falls dabei etwas schief gehen sollte. *(Dafür einfach eine Kopie der Datenbank mit einem neuen Namen machen. Heißt die Datenbank z.B. "Passwords.kbdx" erstelle eine Kopie namens "Passwords-keyfile.kbdx" oder so.)*

- Öffne die (neue) Datenbank in KeePassXC
  - Jetzt kann es sein, dass du beide Datenbanken gleichzeitig geöffnet hast:  
multiple db tabs
  - Das ist nicht weiter schlimm, pass aber auf, dass du nicht durcheinander kommst und die falsche Datenbank bearbeitest. Schließe z.B die originale Datenbank, damit nichts schief geht.
- in der oberen Leiste auf **Datenbank**
- **Datenbanksicherheit...**
- von hier an folge der Anleitung des Abschnitts [hier drüber](#)
- Achtung: hast du nun ein Schlüsseldatei erzeugt und gespeichert, geht KeePassXC davon aus, dass du nun **nur** diese Schlüsseldatei zum Entsperren der Datenbank benutzen willst. Solltest du schon auf **OK** geklickt haben, hast du auch eine solche Warnung gesehen.

- Daher muss mit `Passwort ändern` das Passwort nochmal gesetzt und bestätigt werden.
- `OK`

# Passworteinträge

Hier ist erklärt, wie du einen Eintrag anlegen kannst: [Passworteintrag anlegen](#).

Du kannst existierende Einträge auch [nachträglich bearbeiten](#) (Doppelklick auf Eintrag).

# Browserintegration

Es gibt eine [offizielle Anleitung](#), um das Browser-Plugin zu installieren (außer für Safari).

# TOTP

[Offizielle KeePassXC Anleitung](#) mit guten Screenshots.

TOTP ist eine Form der 2-Faktor-Authentifizierung, die viele Webdienste wie z.B. E-Mail oder Cloud Zugänge nutzen. Um für einen Dienst die 2FA einzurichten, braucht es zwei Dinge:

1. Die entsprechende Einstellung im Webdienst, also z.B. in den E-Mail Einstellungen.
2. Die Konfiguration des entsprechenden KeePassXC Eintrages für diesen Webdienst.

Die Einstellung der Webdienste sehen natürlich alle etwas unterschiedlich aus, aber in den meisten Fällen gibt es in den Konto Einstellungen:

- eine Sektion mit `Sicherheit` oder `Privatsphäre`.
- Hier sollten sich die `2FA` bzw. `TOTP` Einstellungen finden.
- `TOTP aktivieren` oder ähnliches

Jetzt sollte ein QR-Code und im besten Fall eine zufällige Zeichenkette erschienen (Siehe KeePassXC Anleitung). Der QR-Code ist praktisch, wenn du TOTP auf dem Handy einrichtest, da du mit den Handy-Apps einfach per Kamera das `Secret` auslesen kannst. Am PC brauchen wir dafür die Zeichenkette.

Sollte hier nur der QR-Code, ohne Zeichenkette auftauchen, müssen wir das `Secret` aus dem QR-Code heraus lesen.

## Secret aus QR-Code herauslesen

Das funktioniert mit allen gängigen Handy Kameras, die QR-Codes lesen können.

Hier taucht sehr wahrscheinlich mehr auf, als das reine `Secret`, sondern eine URL, die eigentlich für mobile Apps gedacht ist, z.B.:

```
otpauth://totp/example.org:username?secret=PABRSLZNHFLAIENT&issuer=Example
```

Das `Secret` versteckt sich hier zwischen dem `secret=` und dem nächsten Sonderzeichen, hier `&issuer...`.

Unser `Secret` lautet somit: `PABRSLZNHFLAIENT`.

- `Secret kopieren`

Nun gehen wir in die KeePassXC Datenbank:

- Rechtsklick auf den entsprechenden Passworteintrag
- `TOTP`
- `TOTP einrichten`
- `Secret` einfügen
- `OK`

Jetzt sollte neben dem Passworteintrag eine kleine Uhr zu sehen sein. *Die symbolisiert den temporären Charakter der TOTP Codes.* totp clock symbol

Wir müssen abschließend die TOTP-Einrichtung synchronisieren. Dafür muss der aktuelle TOTP-Token wieder in den Einstellungen des Webdienstes eingegeben werden. Der TOTP-Token kann auf zwei Arten kopiert werden:

- `Steuerung` + `T`, oder
- `Rechtsklick` > `TOTP` > `TOTP kopieren`

Wir gehen wieder in die Einstellungen des Webdienstes:

- TOTP-Token einfügen
- Bestätigen

Jetzt solltest du angezeigt bekommen, dass die Einrichtung erfolgreich war.

# Backup

KeePassXC bietet eine automatische Backup-Funktion. Damit ist sichergestellt, dass Du immer eine up-to-date Version deiner Passwortdatenbank an einem anderen "Ort" hast, als die, die du hauptsächlich benutzt.

Unter [Einstellungen \(Zahnrad\) > Allgemein > Dateiverwaltung](#) findet sich die Option [Vor dem Speichern Backup der Datenbank erstellen](#). Dort kannst du einen Pfad festlegen, wo die Ersatz-Datei gespeichert werden soll.

Hier kann es sich anbieten, einen Cloud-Speicher anzugeben, wenn du die Datenbank nicht schon darüber synchronisierst: [Empfehlungen](#)

### Achtung

Obwohl die Datenbank immer verschlüsselt ist, auch in der Cloud, gibt es Szenarien die dabei mitbedacht werden müssen. Lies dich hier schnell ins [Beispiel Szenario](#) einer potentiellen Bedrohung ein!

# Synchronisation/Backup in Nextcloud

Bei [aktivismus.org](https://aktivismus.org) findest Du Links zu Anleitungen für sämtliche Plattformen, wie du Dateien über eine Nextcloud synchronisieren kannst.

Das Prinzip funktioniert genauso mit iCloud, OneDrive, Dropbox, etc ...

---

Version #1

Erstellt: 8 Februar 2025 09:33:19 von ESC-IT Migration Bot

Zuletzt aktualisiert: 8 Februar 2025 09:33:19 von ESC-IT Migration Bot