

KeePassXC Anleitung

Quelle: <https://wiki.ubuntuusers.de/KeePassXC/>

Konfiguration

Es wird ein Eintrag im Anwendungs-Menü unter "*Zubehör* → *KeePassXC*" angelegt. Über "*Werkzeuge* → *Einstellungen*" können einzelne Programmteile konfiguriert werden. KeePassXC speichert die Konfiguration im [Homeverzeichnis](#) in der versteckten Datei `~/.config/keepassxc/keepassxc.ini`.

Sicherheit

Unter "*Werkzeuge* → *Einstellungen* → *Sicherheit*" kann festgelegt werden, wie lange Daten in der Zwischenablage gehalten werden oder wann der Arbeitsbereich bzw. die Datenbank gesperrt wird. Auch kann dort eingestellt werden, ob Passwörter im Klartext oder als Sternchen dargestellt werden.

Unter "*Werkzeuge* → *Einstellungen* → *Allgemein*" kann zusätzlich eingestellt werden, ob, wie und wann die Datenbank nach Veränderungen gespeichert werden soll.

Allgemein

Systemtray

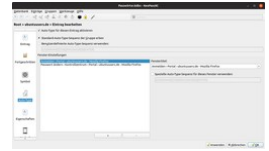
Unter "*Werkzeuge* → *Einstellungen* → *Allgemein*" kann eingestellt werden, ob ein  Symbol in der Leiste angezeigt werden soll sowie das Verhalten. Ein  *Linksklick* auf dieses bringt das Programm in den Hinter- bzw. Vordergrund. Ein  *Rechtsklick* öffnet ein weiteres Menü. Hier kann der Arbeitsbereich angezeigt/versteckt oder das Programm beendet werden.

Autotype

Man kann mit Auto-Type festlegen, Logins durch KeePassXC automatisch ausführen zu lassen. Über einen  *Rechtsklick* und "*Eintrag anzeigen/bearbeiten* → *Auto-Type*" ist diese Funktion bei den einzelnen Konten definierbar. Da die Zuordnung anhand von Fensternamen geschieht, kann dies nicht nur im Browser, sondern auch in anderen Fenstern genutzt werden. Außerdem ist es möglich, bei einer geöffneten Webseite mit einem Anmeldeformular die Datenbank nach passenden Einträgen mit einem globalen Kurzbefehl durchsuchen zu lassen. Existiert ein passender Eintrag, wird Autotype

automatisch ausgeführt. Voraussetzung ist auch hier, dass das Feld "Titel" und/oder das Feld "URL" des KeePassXC-Eintrages und der Fenstertitel der Website im Browser übereinstimmen.

Die einfachste Variante ohne sich mit den ganzen Einstellungen auseinandersetzen zu müssen ist es bei geöffneter Webseite im Browser bei KeePassXC auf die Schaltfläche *"Auto-Type ausführen"* zu klicken, die unter *"Einträge → Auto-Type ausführen"* zu finden ist. Dabei ist zu beachten das der Cursor im Anmeldeformular der Website im Feld Benutzername steht. Der globale Kurzbefehl für Autotype lässt sich unter *"Werkzeuge → Einstellungen → Allgemein"* festlegen.



Browser-Integration

Nach Installation der Browser-Erweiterung lässt sich die Browser-Integration unter *"Werkzeuge → Einstellungen → Browser-Integration"* für die gewünschten Browser aktivieren. Das [Verwenden der Browser-Integration](#) funktioniert nur bei geöffnetem KeePassXC.

Bedienung

Werkzeugleiste

Die Grundfunktionen von KeePassXC sind über die Werkzeugleiste oder das Menü zu erreichen.

Werkzeugleiste		
Symbol	Name	Beschreibung
	"Neue Datenbank"	Eine neue Datenbank wird erstellt.
	"Datenbank öffnen"	Eine bereits existierende Datenbank öffnen. Zum automatischen Öffnen Einstellungen ändern.
	"Datenbank speichern"	Datenbank wird gespeichert.
	"Neuen Eintrag hinzufügen"	Datensatz oder Gruppe neu erstellen.
	"Eintrag anzeigen/bearbeiten"	Datensatz anzeigen oder Veränderungen vornehmen.
	"Eintrag löschen"	Datensatz wird entfernt.
	"Benutzernamen in die Zwischenablage kopieren"	Der Benutzername wird zur weiteren Verwendung kopiert.
	"Passwort in die	Das Passwort wird zur weiteren Verwendung

	<i>"Zwischenablage kopieren"</i>	kopiert.
	<i>"URL in die Zwischenablage kopieren"</i>	Die URL wird zur weiteren Verwendung kopiert.
	<i>"Passwort Generator"</i>	Ein zufälliges, sicheres Passwort wird erzeugt ("gewürfelt").
	<i>"Arbeitsbereich sperren"</i>	Das Programm wird gesperrt. Hauptschlüssel wird zum Entsperren benötigt.

Alle Menüpunkte sind im jeweiligen Fensterbereich über einen  *Rechtsklick* ebenfalls erreichbar.

Datenbank

Eine vorhandene  *"Datenbank öffnen"* bzw. [importieren](#). Sofern keine Datenbank vorhanden ist, ist diese mit  *"Neue Datenbank"* zu erstellen. Diese wird beim ersten Speichern unter dem angegebenen Namen als KeePass-Datenbank (**.kdbx**) angelegt. Es können mehrere Datenbanken gleichzeitig geöffnet werden, die dann über entsprechende Reiter (Tabs) auswählbar sind.

Passwort

Der Hauptschlüssel sollte sicher gewählt sein, da ein unsicheres Passwort Tür und Tor öffnet. Dieses sollte einfach zu merken sein, aber trotzdem ein Höchstmaß an Sicherheit mit sich bringen [\[3\]](#).

Im Nachhinein kann dieses unter *"Datenbank → Hauptschlüssel ändern"* geändert und eine [Schlüsseldatei](#) hinzugefügt bzw. entfernt werden.

Unter *"Datenbank → Datenbankeneinstellungen"* kann man die Verschlüsselungsdurchläufe für den Hauptschlüssel einstellen. Je höher der Wert, desto sicherer. Die Voreinstellung (100000) ist eher konservativ gewählt. Daher sollte über den Button "Benchmark" der Wert (abhängig von der eingesetzten Hardware) für jede Datenbank neu festgelegt werden.

Schlüsseldatei

Für eine höhere Sicherheit sorgt die Verwendung einer Schlüsseldatei (**.key**), welche bei der Datenbankerstellung angelegt werden kann. Es ist ebenfalls möglich Dateien anderer Formate zu wählen. Bei jedem weiteren  Öffnen der Datenbank ist diese Schlüsseldatei erforderlich.

Gruppen

Zur besseren Übersicht können Einträge in Gruppen (vergleichbar mit Ordnern) kopiert werden. Standardmäßig werden alle Einträge innerhalb der Gruppe "Root" angelegt. Neue Gruppen erstellt man über "Gruppen → Neue Gruppe hinzufügen". Nach Eingabe eines aussagekräftigen Titels, z. B. "WLAN", kann man der Gruppe noch ein eigenes Gruppensymbol zuweisen. Mit "OK" wird die neue Gruppe erstellt. Um Gruppen zu löschen oder zu bearbeiten einen  Rechtsklick auf die gewünschte Gruppe ausführen und die Operation auswählen.

Eintrag

Um einen Eintrag zu erstellen wählt man die gewünschte Gruppe im linken Fensterbereich, durch einen  Linksklick, aus. Im rechten Fenster einen  Rechtsklick ausführen und  "Neuen Eintrag hinzufügen" auswählen. Die erforderlichen Daten eingeben, ggf. ein Symbol zuordnen und mit "OK" übernehmen. Bestehende Einträge können durch einen Doppelklick oder über die **Werkzeugleiste** angezeigt und bearbeitet werden.

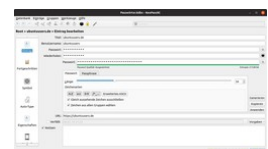
Weitere Funktionen:

- Ein **Passwortgenerator** hilft beim Erstellen von Passwörtern.
- Definieren eines Ablaufdatums, ab dem der Eintrag als veraltet markiert wird.
- Mitführen einer Historie (Verlauf), die das Datum und einige Werte (Titel, Benutzername, URL) der letzten Änderungen speichert (Anzahl der Einträge konfigurierbar über "Datenbank → Datenbankeneinstellungen").
- Einzelne Anhänge (Dateien wie z.B. Client-Zertifikate) können ebenfalls mit aufgenommen und nachträglich bearbeitet/gelöscht werden.
- Automatisches Mitführen von Datumsinformationen (Erstellt, Bearbeitet, Zugriffen)
- Hinzufügen zusätzlicher Informationen (Notizen, URL)
- Zuordnen von benutzerdefinierten Attributen



Passwortgenerator

Diese Funktion ist über das Erstellen eines neuen Eintrages oder bei einem schon vorhandenen Eintrag über einen  Rechtsklick "Eintrag anzeigen/bearbeiten" zu erreichen. Hier kann ein Passwort oder eine Passphrase beliebiger Stärke und Länge zufällig erzeugt werden.



Dabei kann man auch angeben, aus welchen Zeichenkombinationen (z. B. nur Buchstaben, Buchstaben und Zahlen, Sonderzeichen usw.) das Passwort bestehen soll. Weitere Optionen:

- Gleich aussehende Zeichen ausschließen
- Sicher stellen, dass das Passwort Zeichen aller Gruppen (Zeichenkombinationen) enthält

Zwischenablage

 Benutzernamen und  Passwörter können zur weiteren Verwendung in die **Zwischenablage** kopiert werden. Je nach **Sicherheitseinstellung** werden diese nach kurzer Zeit aus dieser gelöscht. Zu erreichen ist die Funktion über einen  *Rechtsklick* oder die **Werkzeugleiste**.

Import/Export

KeePassXC kann unter verschiedenen Betriebssystemen genutzt werden. Es beherrscht den Import der Formate: KeePass 1 und (.csv). Als Exportformat steht ebenfalls (.csv) zur Verfügung. Die Punkte sind über *"Datenbank → Import"* bzw. *"Datenbank → als CSV Datei exportieren"* zu erreichen.

Tastenkürzel

Tastenkürzel	
Taste(n)	Bedeutung
Strg + O	Datenbank öffnen
Strg + S	Datenbank speichern
Strg + W	Datenbank schließen
Strg + Q	Beenden
Strg + ↑ + N	Neue Datenbank hinzufügen
Strg + K	Eintrag klonen
Strg + E	Eintrag anzeigen/bearbeiten
Strg + N	Eintrag hinzufügen
Entf	Eintrag löschen
Strg + B	Benutzername kopieren
Strg + C	Passwort kopieren

Strg + V	Auto-Type ausführen
Strg + U	URL öffnen
Strg + Alt + U	URL in Zwischenablage kopieren
Strg + F	Suchen
Strg + L	Datenbank sperren
Strg + M	Datenbank minimieren

Verwenden der Browser-Integration



Interaktives Ausfüllen von Login-Daten durch KeePassXC-Browser

Sollen regelmäßig Benutzer und Passwort in einem Browser-Fenster automatisch ausgefüllt werden, kann die Browser-Integration verwendet werden. Dafür muss die Browser-Erweiterung namens "KeePassXC-Browser" installiert werden (auf genau diesen Titel achten!). Die Erweiterung kann für Google Chrome, Firefox, Chromium und Vivaldi eingerichtet werden. Für Firefox findet man die Erweiterung unter [KeePassXC-Browser](#) .

Im nächsten Schritt klickt man (bei geöffnetem KeePassXC) auf das Symbol im Browser und dort auf "verbinden". Im sich nun öffnenden Fenster fragt KeePassXC nach dem einem eindeutigen Namen für die Verbindung. Greift man als Einzelperson auf die KeePassXC-Datenbank zu, kann man diese Verbindung bspw. nach dem Browser benennen. Ist die Verbindung hergestellt, verändert sich das Symbol.

Ruft man eine Internetseite auf, für die bereits ein Eintrag mit der gleichen URL existiert, bietet die Browser-Erweiterung nach Klick in das Benutzername-Feld Einträge aus der KeePassXC-Datenbank an. Meldet man sich zum ersten Mal an einer Internetseite an, kann die Browser-Erweiterung automatisch den Eintrag in der KeePassXC-Datenbank speichern. Die hierüber gesammelten Passwörter finden sich in KeePassXC in der Gruppe "*KeePassXC-Browser Passwörter*".

Problemlösung

Autotype

Unter manchen Umständen funktioniert das Ausfüllen der Felder über die Autotype nicht ganz zuverlässig (beobachtet unter [Kubuntu 18.04](#)). So landete im Test auch mal ein Benutzername im Passwortfeld. Das Benutzername-Feld blieb dabei leer. Mit der [Browser-Integration](#) wurde dies nicht beobachtet.