KeePassXC (Passwortmanager)

Zusammenfassung

Passwörter, **Passphrasen** und **Sicherheits-Keys** sind, als persönlicher Besitz zur Authentifizierung von IT-Diensten, integraler Bestandteil des täglichen Lebens geworden. Dabei nehmen nicht nur ihre Vielfalt, sondern auch deren Komplexität stetig zu. Dementsprechend hoch sollten die Anforderungen an Passwörter, Passphrasen, Sicherheits-Keys und deren Aufbewahrung sein.

Mit einem **Passwortmanager** (Kennwortverwaltung) können Sie **Zugangsdaten** für beliebig viele Anwendungen und Webseiten inklusive dazugehöriger Anmerkungen, Dateien etc. sicher speichern. Dadurch ist es einfach, für alle Zugänge unterschiedliche, komplexe und sichere Passwörter zu verwenden, da Sie sich die jeweiligen Passwörter nicht merken, sondern nur noch **ein einziges Passwort** für den Zugang zur **Passwort-Datenbank** wissen müssen. Die Verwendung sogenannter Passwortsafes/-manager, in denen die Zugangsdaten verschlüsselt abgelegt werden, kann bei geeigneter Wahl und sachgerechtem Umgang eine wesentliche Erleichterung darstellen.

KeePassXC ist eine Weiterentwicklung des Passwortmanagers (Passwort-Manager-Software) **KeePass**. Neu bei KeePassXC ist die **Internetbrowser-Integration**, wodurch die Anmeldung auf Webseiten direkt mit Daten aus KeePassXC unterstützt werden kann. Verfügbar ist dies u. a. für folgende Browser:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Chromium

Die Verwendung eines Passwortmanagers ist auch für den privaten Bereich sehr empfehlenswert.

Hier wird erläutert, wie KeePassXC installiert, eingerichtet und genutzt werden kann:

- Anforderungen an sichere Passwörter
- Installation
- Ersteinrichtung
  - Erstellen einer Datenbank
  - Einbindung bestehender Datenbanken
- Einträge anlegen
  - Einträge bearbeiten
  - Einträge verwenden
- Gruppen anlegen und verwalten
- Passwortgenerator (Automatische Passwörter oder Passphrasen generieren)
- Internetbrowser-Integration
  - Installation der Erweiterung im Internetbrowser
  - Aktivierung der Verbindung zwischen Internetbrowser und KeePassXC
  - Verwendung der Internetbrowser-Erweiterung
  - Anpassung von Einträgen über den Internetbrowser
- Allgemeine Tipps und Einstellungsmöglichkeiten
  - Autostart, Instanzen und Update-Prüfung
  - Datenbankzusammenführung, Export/Import, Backup
  - Automatisches Speichern und Laden
  - Suchfunktionen
  - Dauer Beibehaltung Zwischenablage und Sichtbarkeit Passwörter
  - Spaltenanpassung
  - Benutzername/Passwort per Doppelklick kopieren
  - Passwortstärke prüfen

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z. B. Fachschaftsräte)**
- **Gäste der Friedrich-Schiller-Universität**
- **alle sonstigen Zwecke**

Voraussetzungen

- KeePassXC-Installationen sind möglich auf folgenden Systemen:
  - **Microsoft Windows**
  - **Linux**

- **macOS**

Anforderungen an sichere Passwörter

- **Mindestlänge:**
  - Ein Passwort sollte eine Mindestlänge von **8 Zeichen** aufweisen.
- **Komplexität:**
  - Ein Passwort sollte aus **Kombinationen** von **Klein-** und **Großbuchstaben**, **Zahlen** sowie **Sonderzeichen** (z. B. :;?_!#§$%*,.+-/) bestehen.
  - Es sollten **keine Wörter** verwendet werden, welche in **Wörterbüchern** vorkommen (sprachenunabhängig).
  - Der zugehörige Anmeldename soll kein Bestandteil des Passwortes sein.
- **Verschiedene Passwörter:**
  - Für unterschiedliche **Dienste** oder **Webseiten** sind verschiedene Passwörter zu wählen. Auf keinen Fall sollte das gleiche Passwort immer wieder verwendet werden.
- **Aufbewahrung:**
  - Passwörter sind wie sehr persönliche Gegenstände zu betrachten, welche **nicht weitergegeben** werden sollten.
  - Eine **sichere Aufbewahrung** von Passwörtern ist unerlässlich. Keine andere Person sollte zu ihnen Zugang haben.
  - Es sollte sichergestellt werden, dass die Daten **nicht verlorengehen** können bzw. **Backupmöglichkeiten** bestehen (z. B. durch Speichern der Passwort-Datenbank auf dem **Home-Laufwerk**).
  - Die Speicherung sollte **verschlüsselt** erfolgen. Hierfür bietet sich der Einsatz von einem **Passwortmanager** an.

- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Umgang-mit-Passwoertern/umgang-mit-passwoertern_node.html
- https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/starke-passwoerter-so-gehts-11672
- https://www.it.tum.de/it/passwort/sichere-aufbewahrung/
- https://www.kaspersky.de/resource-center/threats/how-to-create-a-strong-password
- https://www.sueddeutsche.de/digital/sicherheit-im-internet-so-bewahren-sie-passwoerter-sicher-auf-1.2921743

Installation

> ⚠ **Hinweis für zentral verwaltete Arbeitsplätze:**
>
> Auf zentral verwalteten Arbeitsplätzen wird das Programm **KeePassXC** automatisiert über die Softwareverteilung Matrix42 zur Verfügung gestellt. Falls die Anwendung noch nicht auf dem genutzten PC installiert ist, bitte ein **Ticket** an den **IT-Support** unter Angabe der **PC-Inventarnummer** senden.

KeePassXC ist über den Link **https://keepassxc.org/download** zum **Herunterladen** verfügbar.

Achtung: Für die Installation werden **administrative Rechte** benötigt. Hierfür ist ggf. die **zuständige anschlussverantwortliche Person (AV)** zu kontaktieren.

Den Link **https://keepassxc.org/download/** aufrufen und unter ***Windows*** den passenden **Installer** (in der Regel ***64-bit, Windows 10/11 - MSI-Installer***) auswählen sowie den **Download** starten.

blocked URL

Sobald der Download durchgeführt wurde, ist die **MSI-Datei** per Doppelklick auszuführen. Je nach Browser-Einstellungen wird die Datei meist im Ordner ***Download*** abgelegt.

blocked URL

Mit ***Next*** die Installation beginnen.

blocked URL

Im Kästchen den **Haken** zum Akzeptieren der Lizenzvereinbarung (***I accept the terms in the License Agreement***) setzen und mit ***Next*** fortfahren.

blocked URL

Mit ***Install*** bestätigen.

blocked URL

Hier kann bei Bedarf der **Installations-Pfad** über ***Change...*** angepasst werden sowie optional **Haken** gesetzt werden zur

- **Erzeugung einer Desktopverknüpfung** (***Create a shortcut on the desktop***) sowie
- **KeePassXC beim Anmelden am PC automatisch starten zu lassen** (***Autostart KeePassXC on login***).

Die gewünschten Einstellungen hinterlegen und mit ***Next*** fortfahren.

blocked URL

Im nächsten Schritt ist die Installation durch die Eingabe von Zugangsdaten eines Kontos mit **administrativen Rechten** zu bestätigen. (Hinweis: Hierfür ggf. die **zuständige anschlussverantwortliche Person (AV)** kontaktieren.)

blocked URL

Mit ***Finish*** wird die Installation abgeschlossen. Optional kann mit Anhaken von ***Launch KeePassXC*** die Anwendung direkt geöffnet werden.

blocked URL

Die Anwendung kann über folgende **Desktop-Verknüpfung** geöffnet werden:

blocked URL

Ersteinrichtung

Erstellen einer Datenbank

Sofern bislang noch kein anderer Passwortmanager genutzt bzw. noch keine Passwort-Datenbank angelegt wurde, muss zunächst eine neue Datenbank erstellt werden, in welcher zukünftige Passwort-Einträge gespeichert werden können.

Hierfür die Schaltfläche ***Neue Datenbank erstellen*** (auch erreichbar über den Menüpunkt ***Datenbank***).

blocked URL

Die folgenden beiden Abfragen können mit den **Standardeinstellungen** über ***Weiter*** bestätigt werden.

blocked URLblocked URL

Für die Datenbank muss ein **sicheres Passwort** vergeben werden, welches bei **jedem Zugriff** auf die **Datenbank** benötigt wird. Es ist daher **wichtig**, sich dieses **Zugangs-Passwort gut zu merken**, da ohne dieses auch alle in der Datenbank gespeicherten Passwörter nicht abgerufen werden können.

blocked URL

Zum Abschluss erfolgt nach Klick auf ***Fertig*** die Aufforderung, die **Datenbank-Datei (.kdbx)** noch zu ***Speichern***. Es wird **empfohlen** hierfür einen **sicheren** und **verlässlich erreichbaren Ort**, wie z. B. die **Uni-Cloud (Nextcloud)** oder das **Home-Laufwerk**, zu nutzen.

Vorteile der Home-Laufwerke:

(oder ggf. auch **Share-Laufewerke**, falls die Datenbank von mehreren Personen genutzt werden soll):

- Die Daten sind **jederzeit** über das **Netzwerk**, auch von mehreren Geräten aus, **erreichbar**.
- Die Datenbank geht **nicht verloren**, wenn z. B. der PC bzw. die Festplatte/USB-Stick (oder ähnliche Speichermedien) einen Defekt erleidet sowie wenn der PC neuinstalliert werden muss.
- Dateien werden über das **Backup regelmäßig gesichert** und können bei versehentlichem Löschen oder Ändern aus früheren Versionen zuverlässig **wiederhergestellt** werden.
- Es haben lediglich Personen **Zugriff** auf die Datei, welche für den **Zugang** auf das Laufwerk **berechtigt** sind.

blocked URL

Einbindung bestehender Datenbanken

Zuvor erstellte Datenbanken im **Datei-Format *.kdbx*** können sehr einfach in KeePassXC eingebunden werden (z. B. aus **KeePass**).

Hierfür die Schaltfläche ***Existierende Datenbank öffnen*** verwenden (alternativ erreichbar über den Menüpunkt ***Datenbank***).

blocked URL

Die bestehende **kdbx-Datei** im Dateibrowser **auswählen** und nach Eingabe des zugehörigen **Passworts** den Vorgang mit Klick auf ***Entsperren*** abschließen.

Alternativ kann auch eine ***Schlüsseldatei*** verwendet werden, **sofern vorhanden**.

blocked URL

Die Datenbank ist nun über KeePassXC vollständig verwendbar.

Hinweis: Sobald Datenbanken einmal in KeePassXC geöffnet wurden, werden sie beim zukünftigen Starten des Programms unter ***Zuletzt verwendete Datenbanken*** aufgelistet und können per Doppelklick direkt ausgewählt und anschließend nach Eingabe des zugehörigen Passworts entsperrt werden.

blocked URL

Info zur Verwendung mehrerer Passwort-Datenbanken:

Es ist problemlos möglich, mehrere Datenbanken **gleichzeitig** in KeePassXC **geöffnet** zu haben (z. B. die persönliche und eine Team-Datenbank).

Dazu einfach die gewünschten Datenbanken, wie vorab beschrieben, jeweils einbinden. Jede geöffnete Datenbank erhält einen eigenen **schließbaren Reiter** oben links. Per Klick kann zwischen diesen gewechselt werden.

Alternativ kann bei Bedarf in den Grundeinstellungen auch bestimmt werden, dass **mehrere** KeePassXC-**Programminstanzen** gleichzeitig geöffnet werden sollen, anstatt als mehrere Reiter in einer Instanz.

blocked URL

Einträge anlegen

Für jede Anwendung, Website etc. sollte ein **eigener Eintrag** im Passwort-Manager erstellt werden, um die zugehörigen Daten zu speichern.

Hierfür per **Rechtsklick** im rechten oberen Feld (ggf. nach Auswahl einer bestimmten **Gruppe**) ***+ Neuer Eintrag...*** aufrufen.
(Alternativ kann dies auch über das **Plus-Zeichen** im oberen Menüband, über den Menüpunkt ***Einträge*** oder per Tastenkombination ***Strg + N*** erfolgen.)

blocked URL

Dort den ***Titel*** und ***URL (Link)*** der Anwendung, Website o. ä. angeben sowie den zu verwendenden ***Benutzername*** und ***Passwort*** (ggf. automatisch generieren lassen) hinterlegen.

Hinweis: Das Passwort kann zur Prüfung über das **Auge-Symbol** rechts temporär **eingeblendet** werden. Durch den **Farbbalken** wird zudem visuell rückgemeldet, wie **stark** das eingegebene Passwort ist (s. **Farbbedeutungen**).

Optional können noch weitere Informationen wie ***Tags*** (Stichwörter), ***Ablaufdatum***, ***Notizen*** etc. eingetragen sowie über die linke Seite **weitere Kategorien** bestimmt werden, wie z. B.

- ***Fortgeschritten:*** Zusätzliche Eigenschaften, **Anhänge** (z. B. Text-Dateien), **Text-** sowie **Hintergrundfarbe**
- ***Symbol:*** Symbol auswählen/Icon importieren
- ***Auto-Type:*** Fenster-Zuordnungen
- ***Browser-Integration*** (sofern aktiviert): Verhalten und zusätzliche URLs
- ***Eigenschaften:*** Plugin-Daten/Schlüssel

blocked URL

blocked URL

blocked URL

blocked URL

blocked URL

Nach Hinterlegen der gewünschten Daten den Eintrag über ***OK*** gespeichern.

blocked URL

Tipp: Passwort automatisch generieren lassen:

Über das **Würfel-Symbol** rechts in der Zeile Passwort kann ein **zufällig erzeugtes** Passwort erstellt werden. Dies **vereinfacht** den Prozess, sich immer wieder neue Passwörter ausdenken zu müssen. Zudem sind automatisch generierte Passwörter meist **sicherer** als selbst ausgedachte Passwörter, da es sich um **komplexe Zeichenfolgen** handelt, die schwer merk- oder erratbar sind.

Optional kann im Fenster ***Passwort erzeugen*** bei Bedarf noch die ***Länge*** geändert, ***Zeichentypen*** angepasst sowie über ***Fortgeschritten*** weitere **Spezifizierungen** vorgenommen werden. So ist es u. a. möglich, bestimmte **Zeichen auszuschließen**, wenn diese z. B. nicht von der betreffenden Anwendung akzeptiert werden. Zum Prüfen kann das generierte Passwort über das **durchgestrichene Auge-Symbol** temporär sichtbar gemacht werden.

Mit ***Passwort anwenden*** den Vorgang bestätigen.

blocked URL

Einträge bearbeiten

Eingegebene Daten können **nachträglich jederzeit** über **Doppelklick** auf den Eintrag geöffnet und **angepasst** werden.
(Alternativ den gewünschten **Eintrag markieren** und über das **Stift-Symbol** im oberen Menüband oder den Menüpunkt ***Einträge*** zur Bearbeitung bestätigen oder die Tastenkombination ***Strg + E*** nutzen.)

blocked URL

Es ist auch möglich, Einträge zu ***klonen*** (kopieren), falls z. B. mehrere Daten zu einem bereits erstellten Eintrag ähnlich sind. So brauchen nur noch Anpassungen zu erfolgen, ohne dass alle gleichbleibenden Daten erneut zu hinterlegen sind.

Dies funktioniert durch **Markieren** des **Original-Eintrags** und anschließendem Aufruf des Menüpunkts ***Einträge*** sowie der Auswahl ***Eintrag klonen...***
(Alternativ kann auch die Tastenkombination ***Strg + K*** verwendet werden.)

blocked URL

Einträge verwenden

Aus KeePassXC können nicht nur die **Passwörter herauskopiert** und in die zugehörige Anwendung eingefügt werden, sondern auch **Benutzername**, **URL** (Link) usw.

Für das **Kopieren** gibt es verschiedene **Möglichkeiten**:

- **Option 1:** In der Einträge-Übersicht die gewünschten **Daten-Zelle** in der entsprechenden **Spalte doppelt anklicken**.
  (Hinweis: Ggf. muss diese Funktion in den **Einstellungen** sowie die benötigte **Spaltenanzeige** noch aktiviert werden.)

- **Option 2: Rechtsklick** auf den benötigten Eintrag und auswählen, welche Daten kopiert werden sollen.
- **Option 3:** Den gewünschten Eintrag auswählen und die benötigten Daten über das **Personen-/Schlüssel-/URL-Symbol** in der Menüleiste bestimmen.
- **Option 4:** Den benötigten Eintrag auswählen und über den Menüpunkt ***Einträge*** auswählen, welche Daten kopiert werden sollen.

> **Achtung:**
>
> Zu beachten ist, dass die kopierten Daten immer nur für eine **kurze Zeit** in der **Zwischenablage** verbleiben und nur innerhalb der vorgegebenen Dauer an der benötigten Stelle wieder eingefügt zu werden können.
> Der **Standard** beträgt **10 Sekunden** und kann bei Bedarf in den ***Einstellungen*** verkürzt oder verlängert werden.

blocked URL

Gruppen anlegen und verwalten

Um **Einträge** besser sortieren und wiederfinden zu können, empfielt es sich, diese **thematisch gegliederten Gruppen zuzuordnen**.
Hierfür unterhalb des **Haupteintrags *Root*** per **Rechtsklick *Neue Gruppe*** aufrufen (alternativ oben über den Menüpunkt ***Gruppen***).

blocked URL

Im Fenster ***Gruppe hinzufügen*** einen passenden ***Namen*** sowie, falls gewünscht, ***Notizen*** und ein **Auflaufdatum** hinterlegen. Optional kann bei Bedarf noch ein besonderes ***Symbol*** gewählt werden. Anschließend mit ***OK*** die Anlage beenden.

blocked URL

Gruppeneinstellungen können **nachträglich** jederzeit per **Rechtsklick** über ***Gruppe bearbeiten...*** noch **geändert** werden, ebenso wie ***klonen*** und ***lösc hen***.

Es ist zudem möglich, durch Ziehen mit gedrückt gehaltener Maustaste, Gruppen **anderen Ordnern über-/unterzuordnen**. Des Weiteren steht das auf-/absteigende ***Sortieren A-Z*** der Gruppen zur Verfügung.

blocked URL

Passwortgenerator (Automatische Passwörter oder Passphrasen generieren)

Abseits der Option, während der Anlage eines neuen Eintrages ein Passwort automatisch generieren zu lassen, besteht jederzeit die Möglichkeit, den ***Pas swortgenerator*** universell zu nutzen.

Hierfür entweder das **Würfel-Symbol** im oberen Menüband nutzen oder über den Menüpunkt ***Werkzeuge*** aufrufen. Das zufällig erzeugte Passwort kann entweder direkt (über das **Blatt-Symbol** rechts oben) kopiert oder, wie zuvor beschrieben, angepasst werden.

blocked URL

Alternativ ist auch die Erzeugung von **zufällig zusammengestellten Wörtern**, einer sogenannten ***Passphrase***, möglich. Hierfür den gleichnamigen Reiter auswählen und die gewünschten Optionen spezifizieren.

blocked URL

Das über den Passwortgenerator erzeugte Passwort/Passphrase wird nicht als Eintrag gespeichert, es ist lediglich herauskopierbar. Der Vorgang kann abschließend über ***Schließen*** beendet werden, um in die Eintragsübersicht zurückzugelangen.

Internetbrowser-Integration

Mithilfe der Integration von KeePassXC per **Erweiterung** in **Internetbrowser** können bereits im Passwortmanager gespeicherte **Anmeldedaten automatisch** auf Webseiten **eingetragen** werden, ohne dass diese manuell herauskopiert und eingetragen werden müssen.

Folgende vorbereitenden Schritte sind hierfür notwendig:

Installation der Erweiterung im Internetbrowser

Je nach verwendeten Internetbrowser ist zunächst die benötigte **KeePassXC-Erweiterung** (ggf. auch **Add-on** genannt) zu installieren. Dieser Menüpunkt befindet sich in der Regel in den jeweiligen **Browser-Einstellungen**.

Das ***Anwendungsmenü*** über das **3 Striche-Symbol** oben rechts öffnen sowie den Menüpunkt ***Add-ons und Themes*** aufrufen (Tastenkombination: **Strg + Shift + A**).

blocked URL

In der Kategorie ***Erweiterungen*** den Suchbegriff ***KeePassXC*** eingeben und mit **Enter** den Suchvorgang starten.

blocked URL

Aus den Ergebnissen den ***KeePassXC-Browser*** per Klick auswählen.

blocked URL

Die Schaltfläche ***Zu Firefox hinzufügen*** verwenden.

blocked URL

Die Erweiterung wird durch Klick auf ***Hinzufügen*** installiert.

blocked URL

Bei Bedarf kann die Option ***Ausführen der Erweiterung in privaten Fenstern erlauben*** gewählt und der Vorgang mit Klick auf ***OK*** abgeschlossen werden.

blocked URL
Da mitunter die KeePassXC-Erweiterung in Google Chrome über den üblichen Weg (3 Punkte-Symbol oben rechts (*Google Chrome anpassen und verwalten*) => Weitere Tools => Erweiterungen => Suchbegriff KeePassXC eingeben) oft nicht gefunden wird, bietet es sich an, in der **Adresszeile** direkt folgenden **Link** aufzurufen:

https://chrome.google.com/webstore/search/KeePassXC

blocked URL

Nach Auswahl des ***KeePassXC-Browser*** mit ***Hinzufügen*** bestätigen.

blocked URL

Die Schaltfläche ***Erweiterung hinzufügen*** verwenden.

blocked URL

Die nachfolgende Meldung kann über das **x** geschlossen werden, die Einrichtung ist damit durchgeführt.

blocked URL

Optional: Falls das **KeePassXC-Symbol** nicht in der Menüleiste angezeigt wird, kann dieses per Klick auf das **Erweiterungen-Symbol** und anschließend auf das **Pinnadel-Symbol** dauerhaft eingeblendet werden.

blocked URL
Das ***Einstellungsmenü*** über das **3 Punkte-Symbol** oben rechts öffnen und ***Erweiterungen*** auswählen. Alternativ kann der Aufruf auch direkt über das **Er weiterungen-Symbol** in der Menüzeile erfolgen.

blocked URL

Anschließend ***Erweiterungen verwalten*** öffnen.

blocked URL

Hier den Suchbegriff ***KeePassXC*** eingeben und mit Enter bestätigen. Falls nichts gefunden werden kann, die Schaltfläche ***Erweiterungen für Microsoft Edge abrufen*** verwenden.

blocked URL

Aus den Sucherergebnissen den Eintrag ***KeePassXC-Browser*** über ***Abrufen*** auswählen.

blocked URL

Mit ***Erweiterung hinzufügen*** den Vorgang bestätigen.

blocked URL

Die Erfolgsmeldung kann über das **x** geschlossen werden. Die Einrichtung ist damit durchgeführt.

blocked URL

Optional: Falls das **KeePassXC-Symbol** nicht in der Menüleiste angezeigt wird, kann dieses per Klick auf das **Erweiterungen-Symbol** und anschließend auf das durchgestrichene **Auge-Symbol** dauerhaft eingeblendet werden.

blocked URL

Aktivierung der Verbindung zwischen Internetbrowser und KeePassXC

Im Programm KeePassXC die ***Einstellungen*** über das **Zahnrad-Symbol** in der Menüzeile öffnen. Über die linke Seitenleiste in den Menübereich ***Browser -Integration*** wechseln.

Anschließend den Haken im Kästchen ***Browserintegration aktivieren*** setzen. Je nach **verwendeten Browser** ist nun noch das zugehörige Kästchen unter ***Integration für diese Browser aktivieren*** anzuhaken, bei Bedarf auch mehrere.

Mit ***OK*** die Einstellungen bestätigen.

blocked URL

Für den nächsten Schritt in den gewünschten **Internet-Browser** wechseln und das **KeePassXC-Symbol** in der Menüleiste anklicken. Dort die Schaltfläche ***Verbinden*** verwenden.

blocked URL

In dem Fenster ***Neue Schlüsselverbindungsanfrage*** muss ein ***Name*** für die herzustellende Verbindung eingegeben werden. Dieser ist frei wählbar, es wird jedoch empfohlen, eine Bezeichnung zu verwenden, die u. a. **eindeutige Rückschlüsse** auf den zugehörigen **Browser**, **PC** und ggf. die **Datenbank** (falls z. B. verschiedene verwendet werden) zulässt.

Die Benennung mit ***Speichern und Zugriff erlauben*** bestätigen.

blocked URL

Verwendung der Internetbrowser-Erweiterung

Vor jeder Verwendung von KeePassXC im Browser muss zunächst das **KeePassXC-Programm gestartet** sowie die **anzuwendende Datenbank geöffnet** bzw. durch **Eingabe** des **Datenbank-Passwortes entsperrt** werden.

⚠ **KeePassXC-Status im Internetbrowser:**

Das KeePassXC-Symbol im Browser zeigt immer den **aktuellen Status** an. Es gibt 3 **Bedeutungen**:

blocked URL Das **KeePassXC-Programm** wurde **nicht gestartet** bzw. es konnte **keine Verbindung** hergestellt werden.

blocked URL Der Browser konnte eine Verbindung mit KeePassXC herstellen, jedoch ist die **Datenbank** noch **gesperrt**.

blocked URL KeePassXC ist **bereit** zur Verwendung im Browser.

Anschließend einfach die **gewünschte Webseite öffnen**. Im Eingabefeld für den Benutzernamen erscheint das anklickbare **grüne KeePassXC-Symbol**.

Bei erstmaliger Verwendung pro Webseite erfolgt eine ***KeePassXC-Browser-Zugriffsanfrage***. Hier können ggf. **nicht passende Einträge** durch die Schaltfläche ***Für diese Seite deaktivieren*** abgewählt werden.
Der **korrekte Eintrag** ist durch Anhaken des Kästchens ***Merken*** und Klick auf ***Auswahl erlauben*** zu verifizieren.

blocked URL

Sofern die zugehörigen Daten in KeePassXC eindeutig hinterlegt und im Internetbrowser bestätigt wurden, können mit Klick auf das **grüne KeePassXC-Symbol** die **Anmeldedaten automatisch eingefügt** und mit der **Anmeldung fortgefahren** werden.

blocked URL

Optional im Fehlerfall:

Wird hier ein Fehler gemeldet, sollten die **Daten** in der KeePassXC-Anwendung auf Richtigkeit **überprüft** und ggf. angepasst werden. Möglicherweise wurde lediglich die **URL** (Webseiten-Link) nicht korrekt im KeePassXC eingetragen.

Mitunter sind ***benutzerdefinierte Anmeldefelder*** für jene Webseite im Internetbrowser zu definieren, falls die automatischen Einstellungen durch KeePassXC fehlerhaft sind.
Hierfür im Browser das **KeePassXC-Symbol** anklicken und anschließend das **gelbe Symbol** oben links wählen.

blocked URL

Durch Auswahl der jeweiligen Kategorien wie ***Benutzername***, ***Passwort*** etc. kann das **zugehörige Feld** durch Klick auf das **passende Eingabefeld** korrigiert und mit ***Bestätigen*** abgespeichert werden.

blocked URL

Anpassung von Einträgen über den Internetbrowser

KeePassXC realisiert in der Regel, wenn sich manuell eingegebene Daten in einer Anmeldemaske von den in der Datenbank gespeicherten Daten **unterscheiden** und bietet durch eine **Einblendung** an, diese **anzupassen**.

Hierfür ***Aktualisieren*** verwenden, der zugehörige Datenbank-Eintrag wird nun automatisch geändert.
(Bei Bedarf kann die Anpassung mit ***Verwerfen*** abgelehnt werden.)

blocked URL

Alternativ kann stattdessen auch die Erzeugung eines **weiteren Datenbank-Eintrages** mit Klick auf ***Neu*** veranlasst werden, wenn der bisherige Eintrag nicht überschrieben werden soll.

blocked URL

Der **neu erzeugte Eintrag** ist anschließend im KeePassXC-Programm im Ordner ***Root*** auffindbar und kann bei Bedarf noch einer **passenden Gruppe** zugeordnet sowie im Detail **angepasst** werden.

blocked URL

Allgemeine Tipps und Einstellungsmöglichkeiten

Autostart, Instanzen und Update-Prüfung

Es ist möglich, KeePassXC direkt beim Hochfahren des PCs **automatisch starten** zu lassen sowie das **Updateverhalten** anzupassen. Auch besteht die Option, bei der Nutzung von **mehreren Datenbanken** diese anstatt über Reiter innerhalb einer Programminstanz in **verschiedenen Programminstanzen** zu öffnen.
Dies ist jeweils konfigurierbar über die ***Anwendungseinstellungen*** (**Zahnrad-Symbol** oben im Menüband), im Bereich ***Allgemein*** unter ***Programmstart***.

- Für den **Autostart** den Haken setzen bei ***KeePassXC beim Systemstart automatisch starten***.
- Die Bestimmung der **Instanzen** erfolgt über ***Nur eine einzige KeePassXC-Instanz starten***.
- Eine **automatische** wöchentliche **Prüfung** auf **Updates** wird über ***Bei Programmstart wöchentlich auf Updates überprüfen*** gesteuert. Standardmäßig ist die Option aktiv.

> **Achtung:**
>
> Für **Updates** sind, wie bei der Installation, **administrative Rechte** erforderlich.
>
> Hinweis für zentral verwaltete Arbeitsplätze: Die Prüfung ist hier generell deaktiviert, da Updates zentral über die Softwareverteilung Matrix42 erfolgen.

Die gewünschten Einstellungen mit ***OK*** bestätigen.

blocked URL

Datenbankzusammenführung, Export/Import, Backup

Datenbanken können vielseitig verwaltet, gesichert, wiederhergestellt etc. werden. Hier werden einige **Beispiele** vorgestellt:

- ***Datenbank-Backup speichern...*** : Ermöglicht die Sicherung einer Backup-Datei im **kdbx-Dateiformat**, aus der die jeweilige Datenbank später (ggf. auf anderen Geräten) wiederhergestellt werden kann.
- ***Mit Datenbank zusammenführen...*** : Eine Option, um **Daten** aus mehreren Datenbanken in einer Datei **zusammenzulegen**, so dass zukünftig nur noch jene zusammengestellte Datenbank geöffnet werden muss, anstatt mehrerer.
- ***Importieren***: Diese Funktion ähnelt der Option, Datenbanken zu öffnen, jedoch ist es hierüber möglich, sie **aus verschiedenen Formaten** zu **öffnen**:
  - ***CSV-Datei...***
  - ***1Password-Tresor...***
  - ***KeePass 1-Datenbank...***
- ***Exportieren****:* Über diese dem Backup ähnelnden Funktion (.kdbx) kann die Datenbank in **weiteren Datei-Formaten gespeichert** werden:
  - ***CSV-Datei...***
  - ***HTML-Datei...***
  - ***XML-Datei...***

blocked URL

Automatisches Speichern und Laden

KeePassXC bietet verschiedene Funktionen bzgl. der **Dateiverwaltung** an. So gehört es z. B. nun zu der **Standardeinstellung**, dass **Änderungen sofort automatisch gespeichert** werden, ohne dass dies, wie z. B. noch bei *KeePass* üblich, manuell erfolgen muss. Diese Einstellungen können natürlich nach Bedarf angepasst werden.

Es ist empfehlenswert, die Einstellung ***Automatisch speichern nach jeder Änderung*** beizubehalten, damit Daten nicht versehentlich verlorengehen. Auch lohnt sich die Option ***Datenbank nach externer Änderung automatisch neu laden***, wenn die gleiche Datenbank z. B. an verschiedenen Geräten genutzt wird.

Anpassbar sind die Optionen in den ***Anwendungseinstellungen*** (**Zahnrad-Symbol** im oberen Menüband) unter dem Bereich ***Dateiverwaltung***.

blocked URL

Suchfunktionen

Über das **Suchfeld** oben rechts kann durch Eingabe eines Begriffes nach Einträgen und Inhalten gesucht werden. Ohne Spezifizierung werden nicht nur Eintragstitel, sondern auch Benutzernamen und sonstige Eigenschaften durchsucht.

Es ist jedoch auch **gezielteres Suchen** möglich. Eine **Übersicht** der genauen **Suchoptionen** und wie diese zu nutzen sind, kann über das **Fragezeichen-Symbol** in der Suchleiste aufgerufen werden:

- Eingrenzung der Suchergebnisse auf bestimmte ***Felder***
- Nutzung von ***Modifikatoren*** sowie ***Platzhalter***
- ***Beispiele***

Zudem können unten links bei ***Suchen und Tags***

- vorangegangene Suchvorgänge beendet (***Suche löschen***)
- ***Alle Einträge*** in einer Gesamtübersicht angezeigt
- oder weitere Suchfunktionen wie ***Abgelaufen*** (hierfür müssen Ablaufdaten in den Einträgen hinterlegt worden sein)
- und die Filterung auf ***Schwache Passwörter*** genutzt

werden.

blocked URL

Dauer Beibehaltung Zwischenablage und Sichtbarkeit Passwörter

Die Dauer, wie lange aus KeePassXC kopierte Daten in der Zwischenablage behalten werden und in der zugehörigen Anwendung wieder eingefügt werden können, ist anpassbar. Die **Standardeinstellung** beträgt **10 Sekunden**. Zudem kann eingestellt werden, ob **Passwörter** in Einträgen **sichtbar** sei n dürfen.

Beides kann bei Bedarf angepasst werden über die ***Anwendungseinstellungen*** (**Zahnrad-Symbol** oben im Menüband), Wechsel in den Bereich ***Sicherh eit*** (Seitenleiste links). Sobald die gewünschten Einstellungen unter ***Timeouts*** und ***Komfort*** an- bzw. abgehakt wurden, über ***OK*** bestätigen.

blocked URL

Spaltenanpassung

Um **Spalten** zu Einträgen **ein- oder ausblenden** zu können, muss das zugehörige Auswahlmenü per **Rechtsklick** auf die **Spaltentitelzeile** aufgerufen werden. Dort einfach per Klick **an- und abwählen**, welche Spalten gewünscht sind.

blocked URL

Benutzername/Passwort per Doppelklick kopieren

Damit Einträge wie Benutzername und Paswort direkt per Doppelklick aus der jeweiligen Zelle in der Eintragsübersicht kopiert werden können, ohne den Eintrag vorher öffnen zu müssen, ist zunächst folgende Einstellung zu tätigen:

Die ***Anwendungseinstellungen*** über das **Zahnrad-Symbol** im oberen Menüband aufrufen, in der Seiteleiste links zum Bereich ***Sicherheit*** wechseln und unter ***Komfort*** den Haken im Kästchen ***Benutzername/Passwort per Doppelklick kopieren*** setzen sowie mit ***OK*** bestätigen.

blocked URL

Passwortstärke prüfen

Bereits **während** der **Eintragserstellung** wird visuell durch den **Farbbalken** unter der Eingabezeile angezeigt, **wie sicher** das eingegebene **Passwort** ist.

Farbbedeutungen:

Grün = sicheres Passwort
Orange = schwaches Passwort
Rot = sehr schwaches Passwort

Nachträglich wird dies ebenfalls in der **Übersicht** für die jeweiligen Einträge angezeigt, sofern die zugehörige **Spalte** ***Passwortstärke*** aktiviert wurde.

blocked URL

Es lohnt sich, regelmäßig über die Funktion ***Schwache Passwörter*** ungenügend sichere Einträge ausfindig zu machen und diese zu verstärken und parallel in den jeweiligen Anwendungen bzw. Webseiten anzupassen.
Hinweis: Die ***Suchergebnisse*** werden zudem **gezählt** und das Ergebnis ober- sowie unterhalb der Eintrags-Übersicht angezeigt.

blocked URL

Titel: "KeePassXC (Passwortmanager)"

Stand: 16.05.2023

blocked URL