Carl von Ossietzky
Universität
Oldenburg

Einrichten von KeePassXC

Universität Oldenburg - IT-Dienste
Tobias Kirstein
Version vom 05.04.2023

Inhaltsverzeichnis

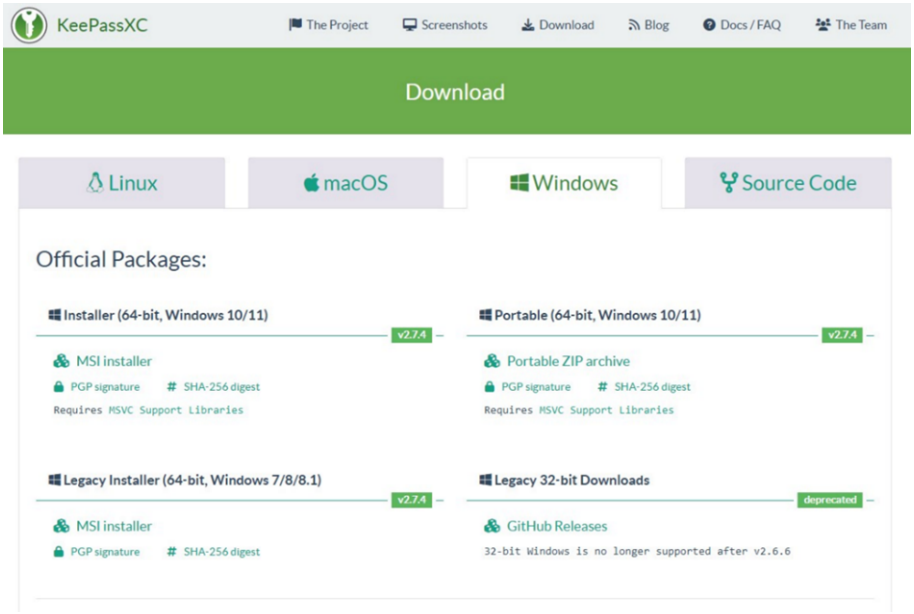
Allgemeine Informationen

KeePassXC ist ein quelloffener Passwort-Manager, der für alle gängigen Betriebssystem (Windows, MacOS, Linux usw.) angeboten wird. Das hat den Vorteil, dass die angelegte Passwort-Datenbank auch auf andere Systemübertragen und dort wie gewohnt mit KeePassXC gearbeitet werden kann. Des Weiteren ist es auch möglich, dass z.B. kdbx-Dateien von KeePass2-Datenbanken geöffnet und importiert werden können.

⚠ **Achtung:** Die Sicherheit der Passwortdatenbank hängt wesentlich davon ab, wie sicher Ihr selbst gewähltes Passwort für die Datenbankdatei selbst ist. Denn wenn jemand auf die Datenbank unbefugt zugreifen will, so hat der Angreifende beliebig viele Versuche, das Passwort zu knacken. Verwenden Sie also bitte für die Datenbank-Datei selbst ein besonders langes und sicheres Passwort (mindestens 20 Zeichen, gerne auch noch länger) und schreiben Sie sich dieses Passwort zur Sicherheit auch auf und verwahren Sie diese Papierkopie an einem sicheren Ort.
Bitte beachten Sie ebenfalls, dass es bei Verlust des Passworts für die Datenbank oder der eventuell eingesetzten Schlüsseldatei nicht mehr möglich ist, auf die Passwort-Datenbank zuzugreifen. Auch der Servicedesk kann Ihnen in dem Fall nicht weiterhelfen!

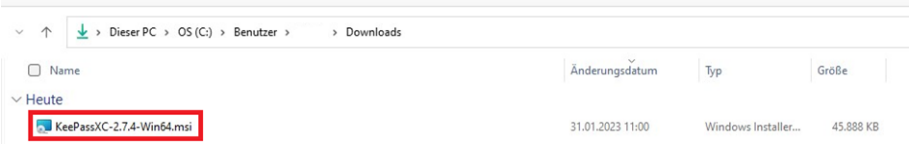
Herunterladen der Software

Die Installationsdatei für das jeweilige Betriebssystem laden Sie bitte von der Website des Herstellers herunter.
https://keepassxc.org/download/



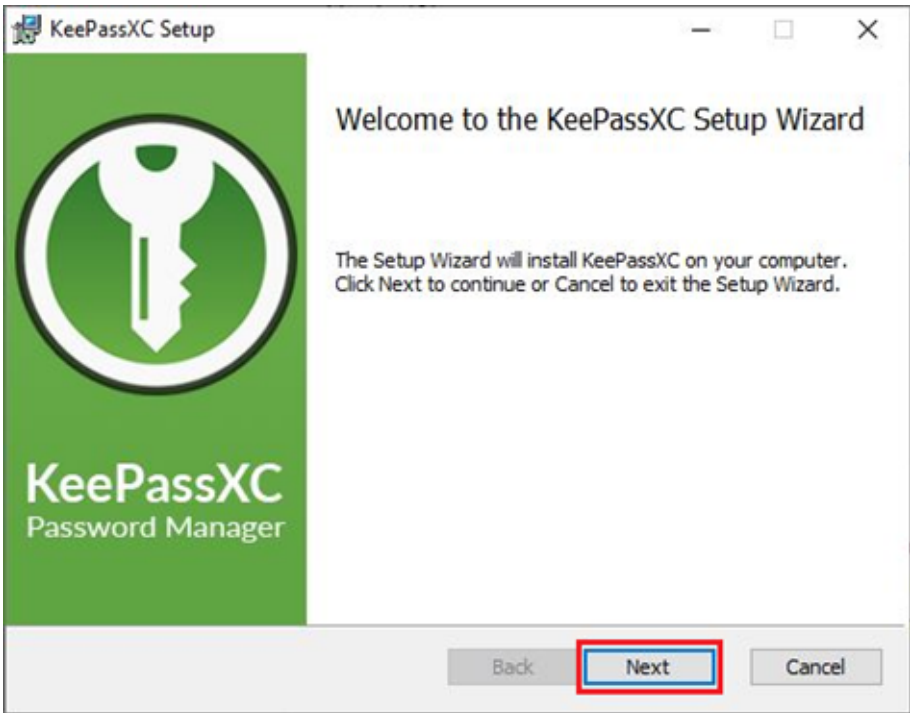
Starten der Installation

- Nach dem Download der Installationsdatei führen Sie diese bitte aus.



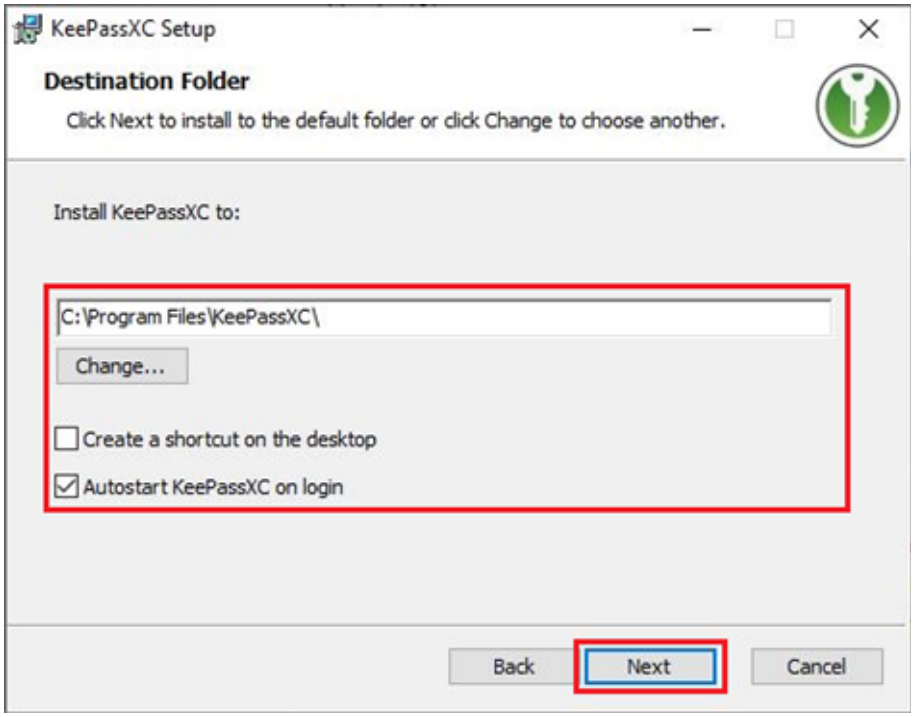
Installationsverlauf

- Das Setup startet mit einem Begrüßungsbildschirm, diesen überspringen Sie mit einem Klick auf „Next“.

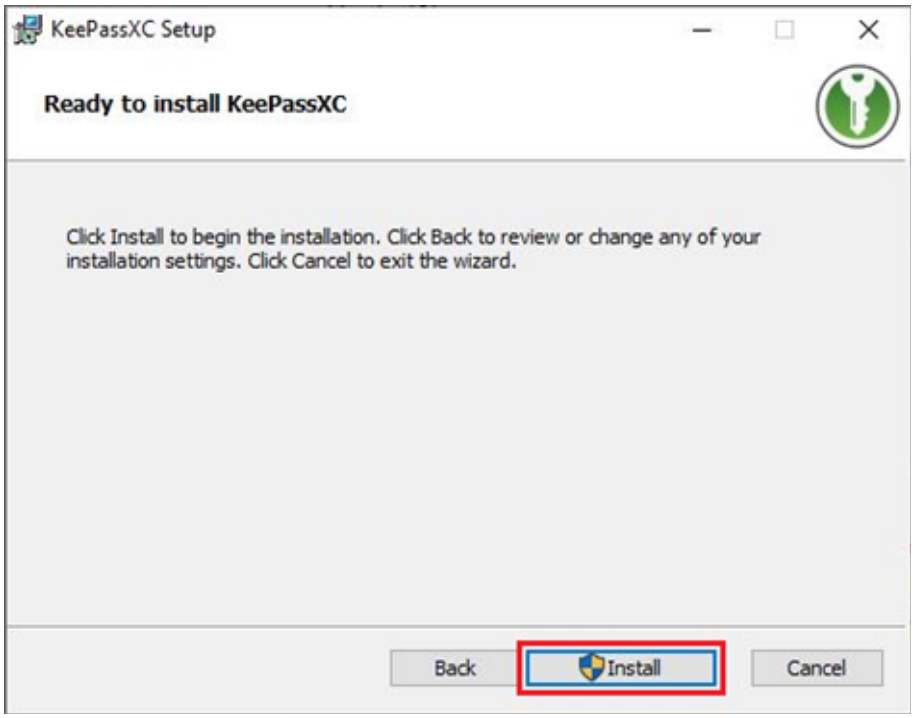


- Nachdem Sie die Lizenzbedingung sorgfältig durchgelesen und akzeptiert haben, klicken Sie auf **Next**.

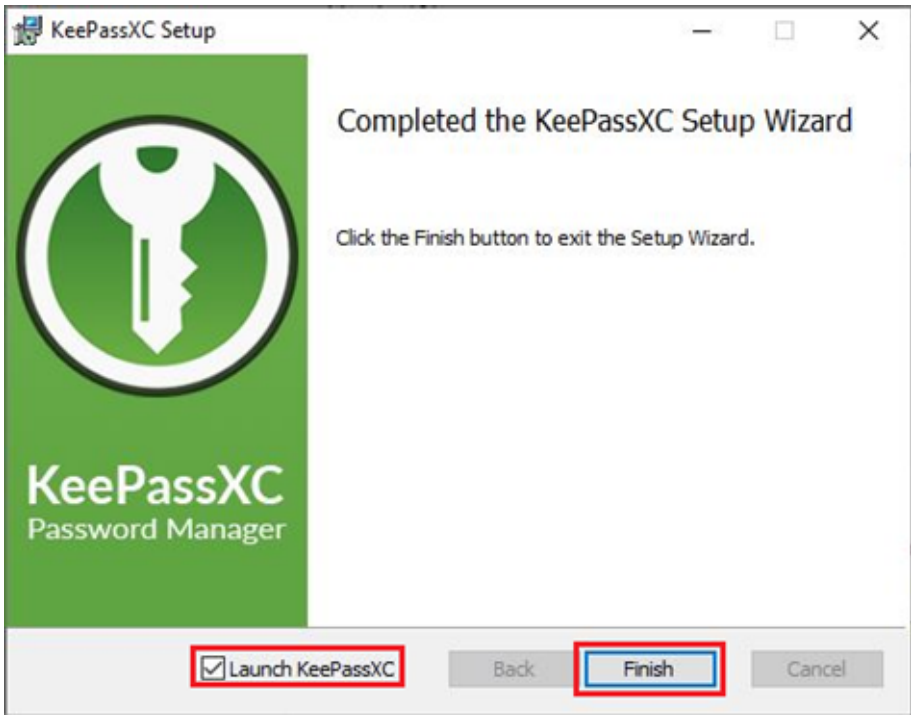
- In dem Fenster „Destination Folder“ können Sie, falls gewünscht, ein anderes Installationsverzeichnis festlegen und bestimmen, ob KeePassXC immer sofort beim Starten des Gerätes gestartet und ein Desktopsymbol angelegt werden soll. Im Anschluss klicken Sie dann auf **Next**.



- Klicken Sie, um die Installation zu beginnen, auf **Install**.

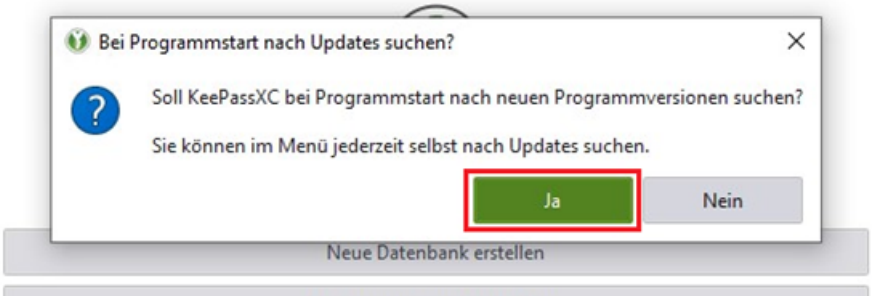


- Nach Abschluss der Installation kann man auswählen, ob KeePassXC sofort gestartet werden soll. Mit einem Klick auf „Finish“ wird das Setup abgeschlossen.

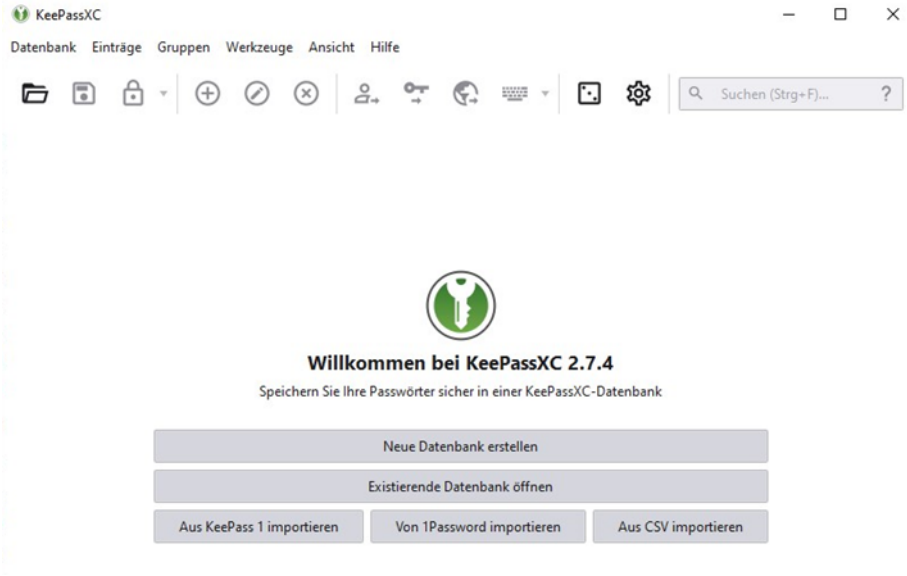


Konfiguration des Programmes

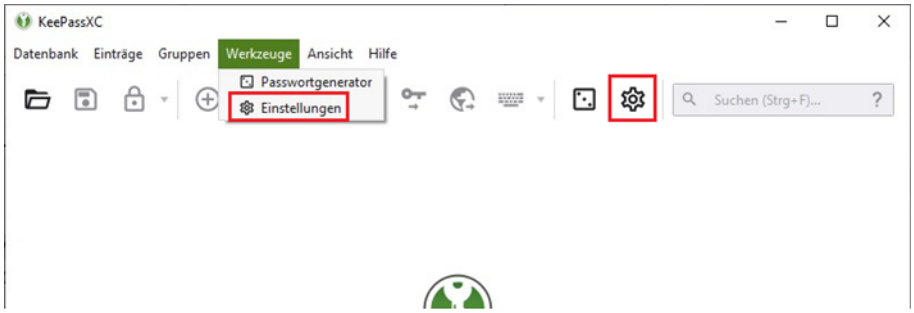
- Beim ersten Start von KeePassXC fragt das Programm ob es beim Starten automatisch nach Programmupdates suchen soll. Hier klicken Sie bitte auf „Ja“.



- Danach wird das Hauptmenü von KeePassXC angezeigt und zur Auswahl stehen:
  - ➢ Eine neue Passwortdatenbank anlegen
  - ➢ Eine bestehende Passwortdatenbank öffnen
  - ➢ Eine Passwortdatenbank aus KeePass 1, 1Password oder einer CSV-Datei importieren



- Weitere Einstellungen konfigurieren Sie unter dem Menüpunkt „Werkzeuge“ → „Einstellungen“ oder über den Button mit dem Zahnrad in der Symbolleiste.
  Die Einstellungen gliedern sich in die Bereiche:
  - ➢ Allgemein
  - ➢ Sicherheit
  - ➢ Browserintegration
  - ➢ SSH-Agent
  - ➢ KeeShare

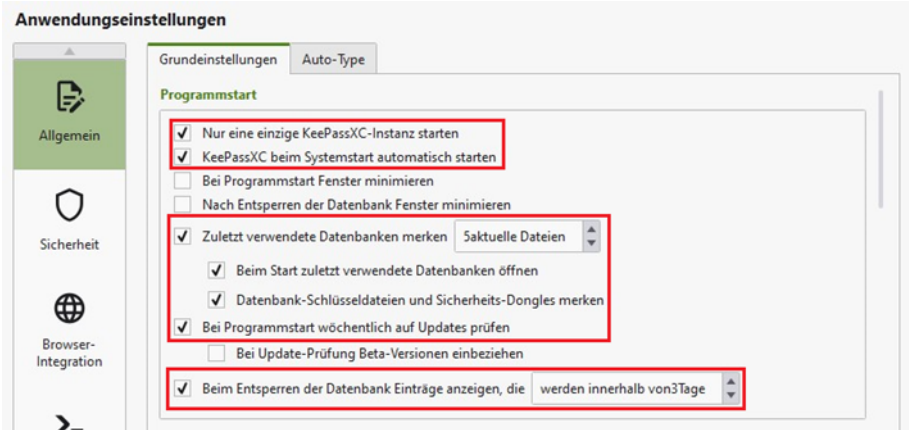


Für uns sind die Einstellungen „Allgemein“ und „Sicherheit“ wichtig.

Einstellungen „Allgemein“

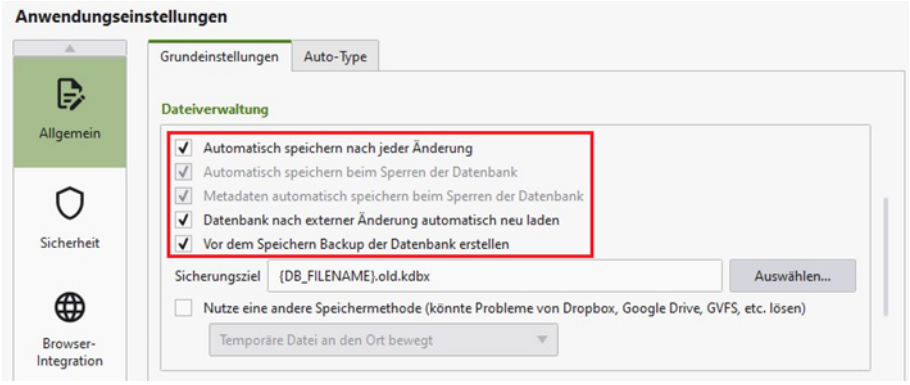
➢ Im Bereich „Programmstart“ sollten folgende Einstellungen aktiviert werden:

1. Nur eine einzige KeePassXC-Instanz starten
2. KeePassXC beim Systemstart automatisch starten (optional)
3. Zuletzt verwendete Datenbanken merken
   - Beim Start zuletzt verwendete Datenbanken öffnen
   - Datenbank-Schlüsseldateien und Sicherheits-Dongles merken
4. Bei Programmstart wöchentlich auf Updates prüfen
5. Beim Entsperren der Datenbank Einträge anzeigen, die …



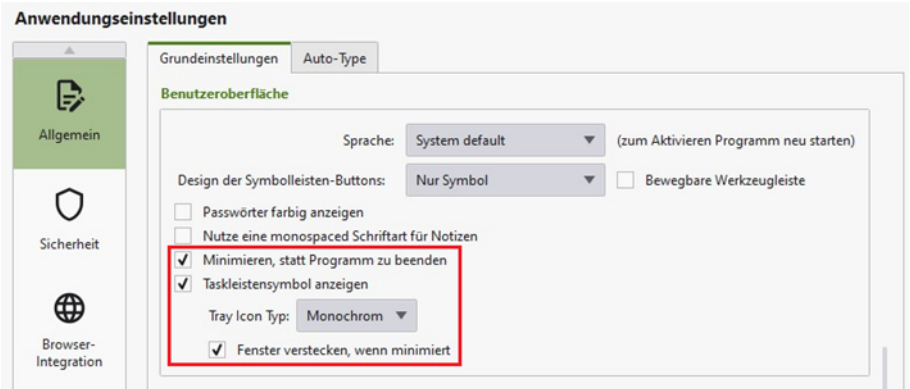
➢ Im Bereich „Dateiverwaltung“ sollten folgende Einstellungen aktiviert werden:

1. Automatisch speichern nach jeder Änderung
2. Datenbank nach externer Änderung automatisch neu laden
3. Vor dem Speichern Backup der Datenbank erstellen



➢ Im Bereich „Benutzeroberfläche“ kann optional folgende Funktionen aktiviert werden:

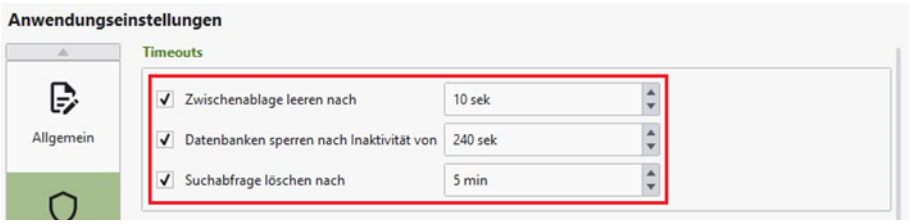
1. Minimieren, statt Programm zu beenden
2. Taskleistensymbol anzeigen
3. ggf.: verstecken, wenn minimiert (KeePassXC läuft dann im Hintergrund in der Statusleiste neben der Uhr)



Einstellungen „Sicherheit“

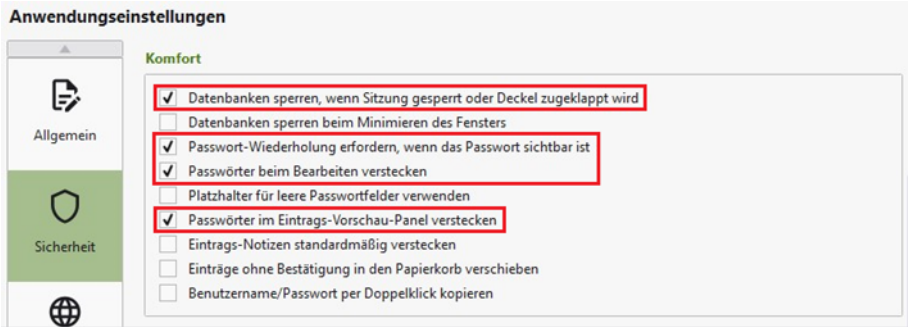
➢ Im Bereich „Timeouts“ sollten die Einstellungen wie folgt gesetzt werden:

1. Zwischenablage leeren nach: 10 sek
2. Datenbanken sperren nach Inaktivität von: 240 sek
3. Suchabfrage löschen nach: 5 min



➢ Im Bereich „Komfort“ sollten die folgenden Einstellungen aktiviert werden:

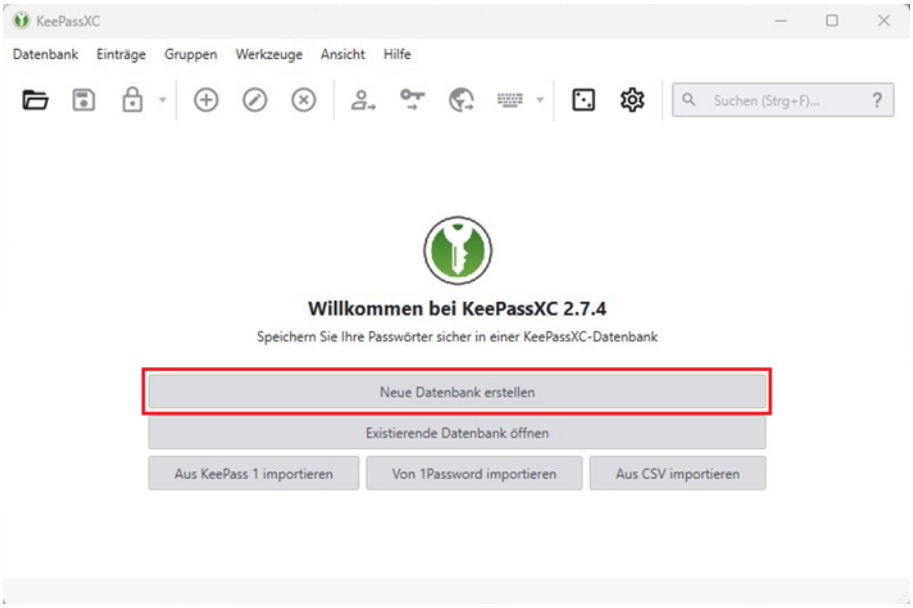
1. Datenbanken sperren, wenn Sitzung gesperrt oder Deckel zugeklappt wird
2. Passwort-Wiederholung anfordern, wenn das Passwort sichtbar ist
3. Passwörter beim Bearbeiten verstecken
4. Passwörter im Eintrags-Vorschau-Panel verstecken



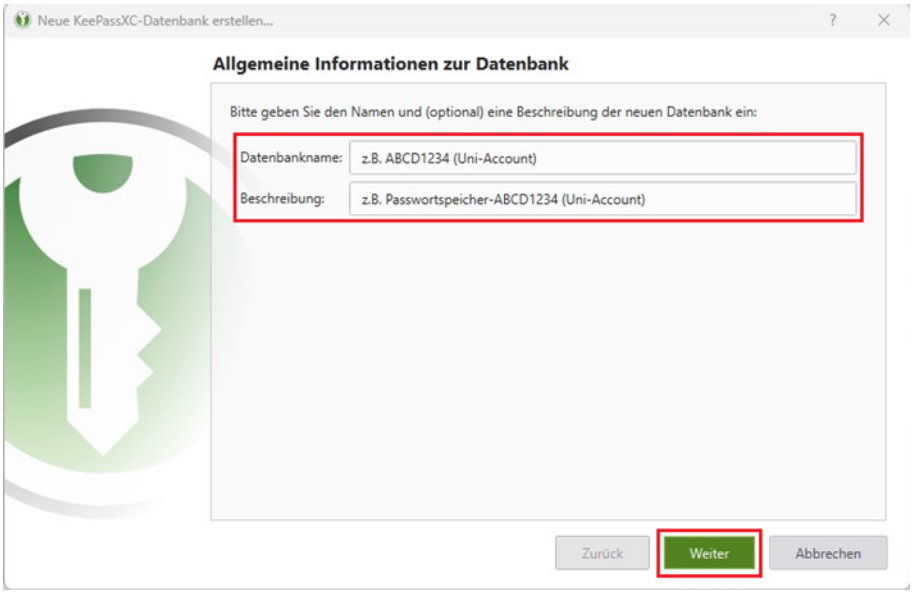
➢ Im Bereich „Datenschutz“ kann optional eingestellt werden, dass die Icons für die Passwort-Einträge über die Suchmaschine „DuckDuckGo“ heruntergeladen werden. Diese Suchmaschine legt großen Wert auf Datenschutz und Privatsphäre.

Einrichten einer Passwortdatenbank

- Im Hauptmenü klickt man auf „Neue Datenbank erstellen“.

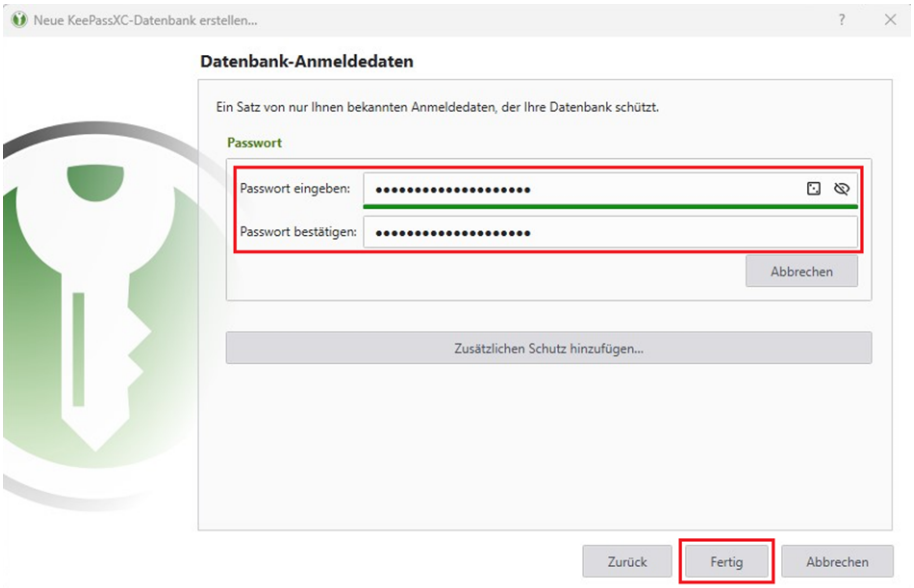


- Im ersten Schritt werden Sie aufgefordert einen Namen und eine Beschreibung für die neue Datenbank zu vergeben. Mit einem Klick auf „Weiter“ bestätigen Sie die Eingabe.

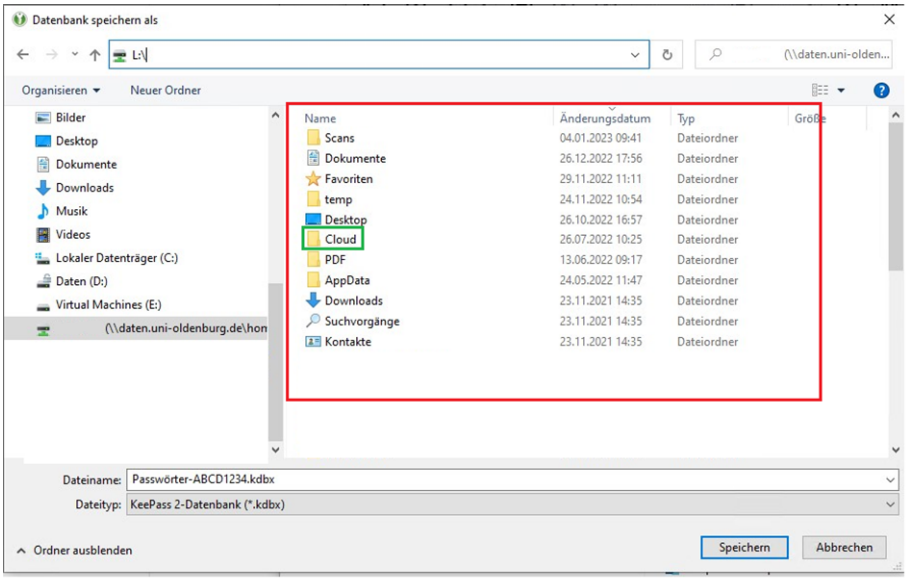


- Im nächsten Schritt müssen die Verschlüsselungseinstellungen gewählt werden. Je länger die Verschlüsselung dauert, umso stärker ist die Verschlüsselung, als Kompromiss zwischen Zeit und Stärke sollten Sie 2,5 s verwenden. Als Datenbankformat wählen Sie das empfohlene Format (KDBX4).

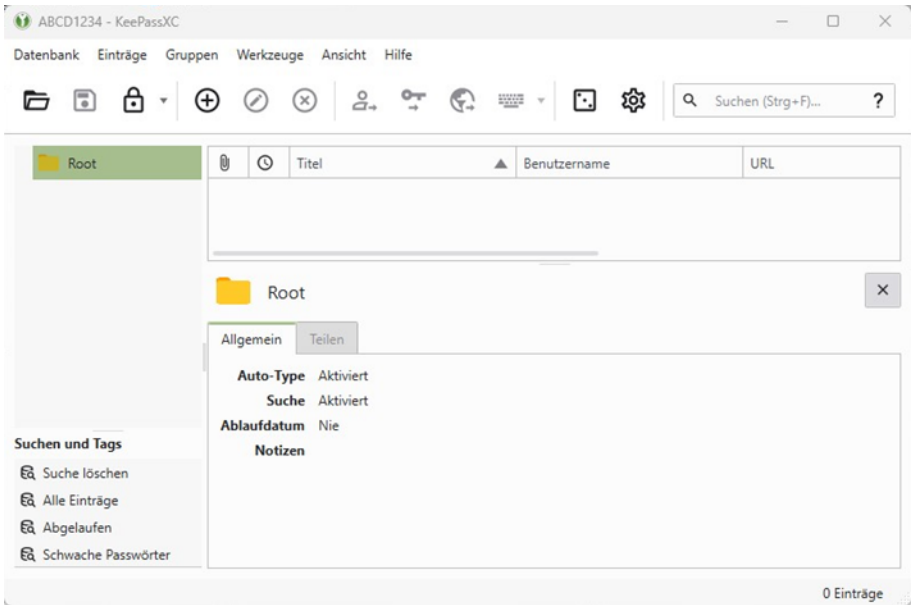
- Im nächsten Schritt müssen Sie die Anmeldedaten (Passwort) für die Passwortdatenbank festlegen. Verwenden Sie bitte ein komplexes Kennwort (grüner Fortschrittsbalken) und nicht das gleiche Passwort wie für Ihren Universitäts-Account.



- Mit einem Klick auf „Fertig“ wird die Datenbank erstellt und Sie werden aufgefordert auszuwählen, wo die Datenbank abgespeichert werden soll. Am besten eignet sich Ihr persönliches Home-Laufwerk (L:\). Wenn Sie auch über die Nextcloud auf die Passwortdatenbank zugreifen möchten, verwenden Sie den Ordner „Cloud“ auf Ihrem L-Laufwerk.

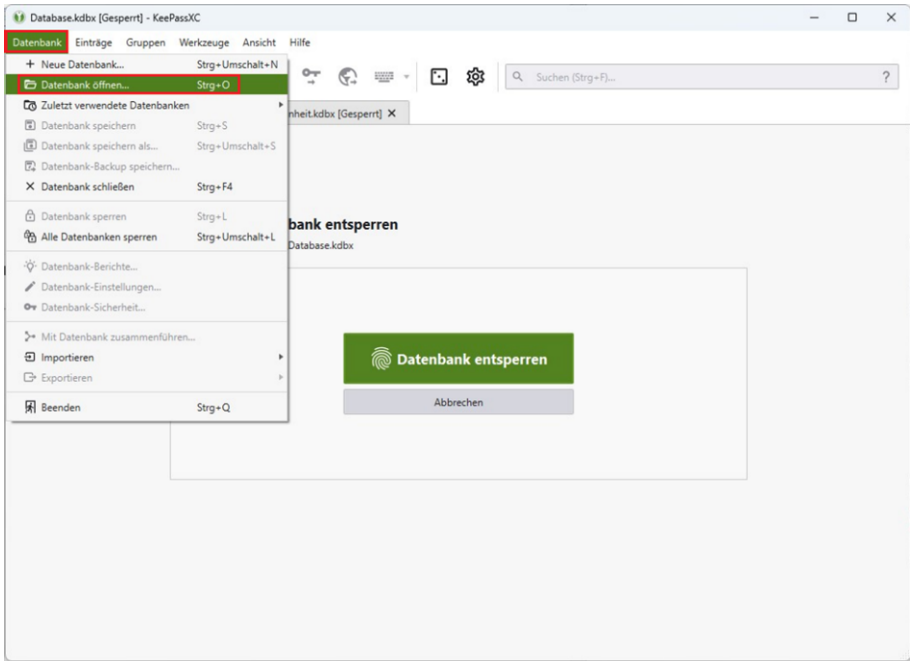


- Das Programm zeigt nun die Ordner und Einträge der Datenbank an. Es ist ein „Root“ genannter Ordner vorhanden, ansonsten ist noch nichts angelegt.

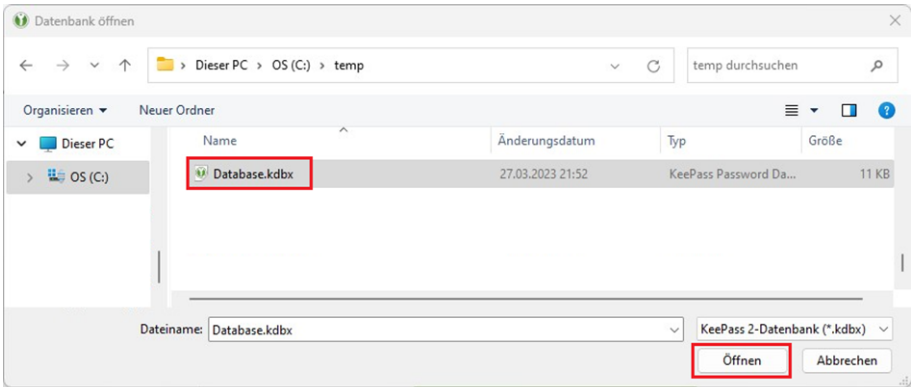


Bestehende Datenbank öffnen

- Sie können mit KeepassXC Datenbanken im kdbx-Format öffnen und benutzen, die Sie mit Keepass2 erstellt haben. Öffnen Sie die KeepassXC-Anwendung, klicken Sie auf die Schaltfläche Datenbank und wählen dann Datenbank öffnen.



- Nachdem Sie die Datenbank-Datei im Datei-öffnen-Dialog ausgewählt haben, können Sie im folgenden Fenster das Passwort für die Datenbank eingeben und Ihre Datenbank öffnen.



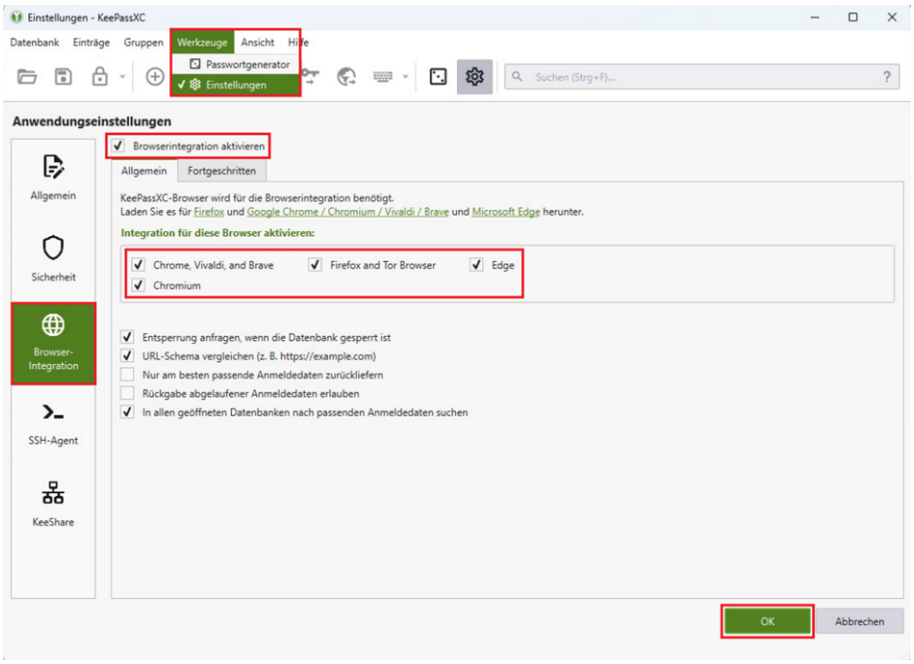
Browser-Integration

- Durch die KeePassXC-Browser-Integration können automatisch Benutzernamen und Passwörter aus KeePassXC abgerufen und direkt in die entsprechenden Felder auf Webseiten eingefügt werden. Sie müssen die Daten nicht manuell aus Ihrer KeePassXC-Datenbank kopieren und in die Felder einfügen.
- Voraussetzung ist, dass für Ihren Browser das Add-on installiert ist, das für die Verbindung zwischen KeepassXC und Browser sorgt.

➢ Installationslinks für die Browser-Erweiterungen:

1. Microsoft Edge
2. Google Chrome / Chromium
3. Mozilla Firefox

- Dann muss die Verbindung von KeePassXC zu Ihrem Browser in KeePassXC freigeschaltet werden. Dazu klicken Sie in KeepassXC auf „Werkzeuge -> Einstellungen -> Browser-Integration“ und kreuzen an, dass Sie die „Browserintegration aktivieren“ möchten. Darunter kreuzen Sie an, welchen Browser Sie benutzen: Firefox, Chrome oder Edge. Die restlichen Einstellungen lassen Sie, wie sie sind, und klicken auf OK.



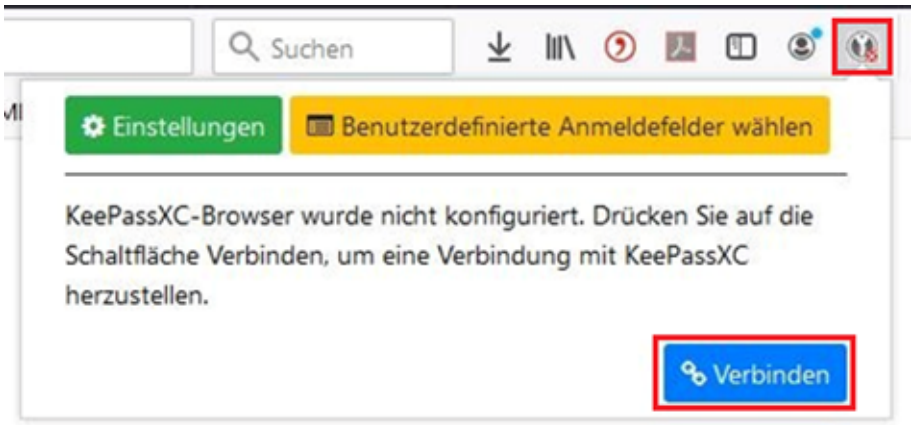
- Nach dem (Neu-)Start des Browsers können Sie jetzt in der Symbolleiste oben rechts ein KeePassXC-Symbol sehen. Das Symbol kann unterschiedlich aussehen:

➢ KeePassXC läuft nicht oder ist nicht verbunden

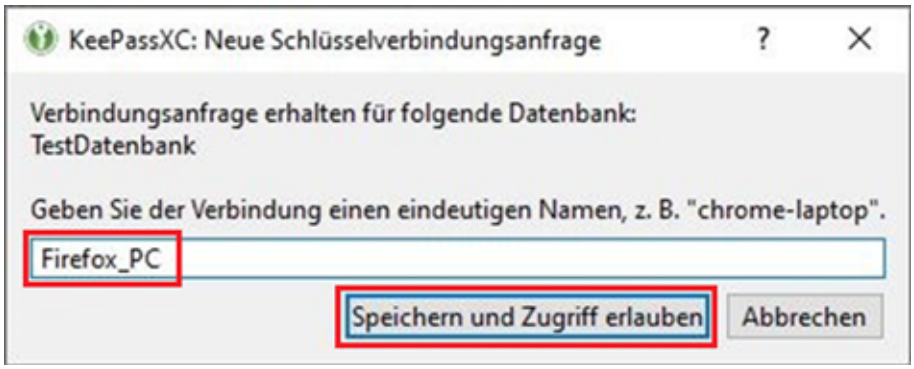
➢ Mit KeePassXC verbunden, aber die Datenbank ist gesperrt

➢ Verbunden mit KeePassXC und bereit zur Verwendung

- Klicken Sie auf das Symbol. Wenn eine Fehlermeldung erscheint, überprüfen Sie, ob KeePassXC läuft und Ihre Datenbank entsperrt ist. Nur dann funktioniert die Verbindung. Wenn die Verbindung nicht möglich ist, erscheint eine Meldung, dass diese noch eingerichtet werden muss. Klicken Sie auf „Verbinden“.



- KeePassXC meldet sich mit einem kleinen Fenster und fragt, ob Sie die "Neue Schlüsselverbindungsanfrage“ zulassen wollen. Wählen Sie einen eindeutigen Namen für diese Verbindung, z.B. „Firefox_PC“ und klicken Sie dann auf Speichern und Zugriff erlauben.



- Damit ist die Verbindung hergestellt. Firefox kann jetzt auf die Passwörter zugreifen, die Sie in KeePassXC gespeichert haben.

Verwenden der Browser-Erweiterung

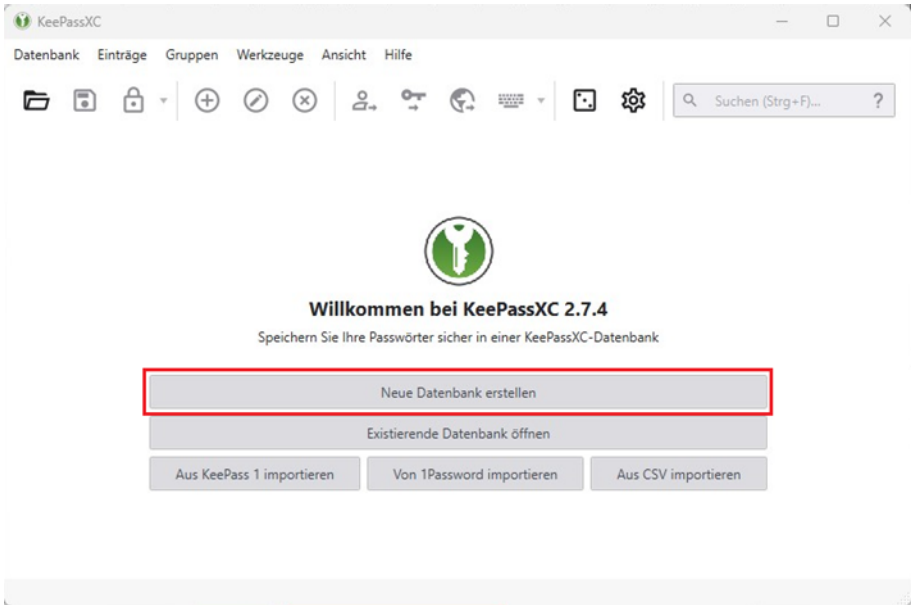
- Um die Browser-Integration zu nutzen, starten Sie die Anwendung KeepassXC und entsperren Ihre Datenbank. Im Webbrowser öffnen Sie die URL, die Sie mit Ihrer Datenbank verwenden möchten. Im Eingabefeld für den Benutzernamen ist das grüne KeepassXC-Symbol zu sehen.

- Wenn in Ihrer Datenbank ein Eintrag mit Anmeldedaten existiert, der zu dieser URL passt, werden nach einem Klick auf das grüne Symbol die Anmeldedaten automatisch hier eingetragen und Sie können sich anmelden.

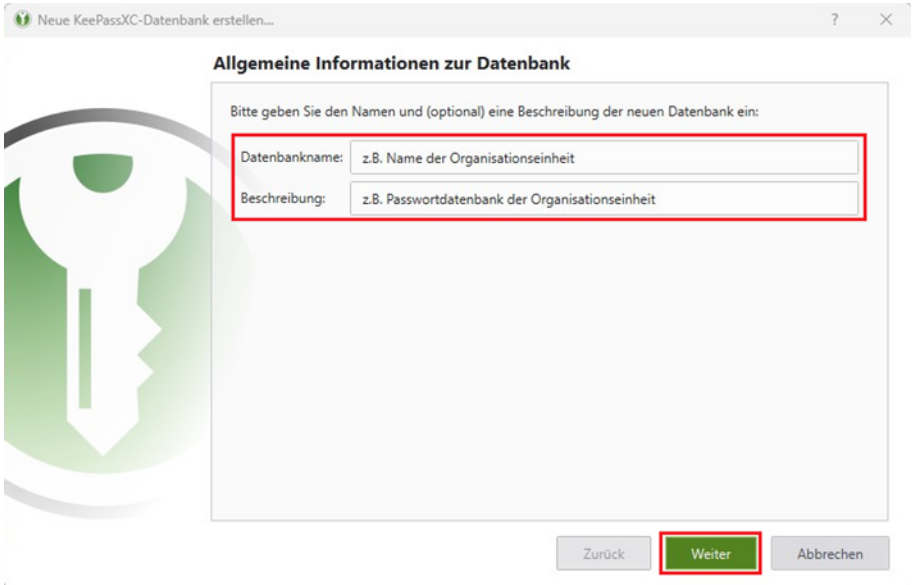
Einrichtung einer Gruppen-Datenbank

Erstellen der Gruppen-Datenbank

- Im Hauptmenü klicken Sie auf „Neue Datenbank erstellen“.

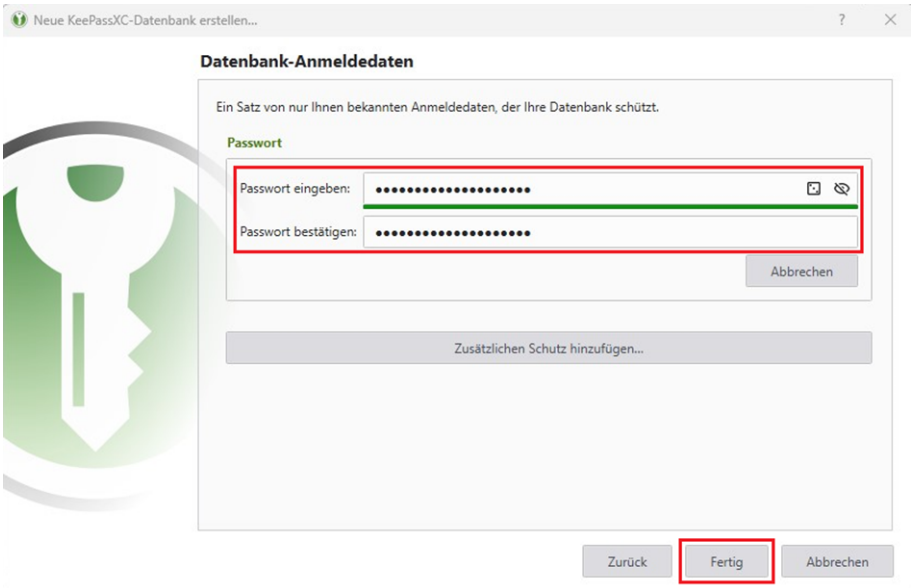


- Im ersten Schritt werden Sie aufgefordert einen Namen und eine Beschreibung für die neue Datenbank zu vergeben. Mit einem Klick auf „Weiter“ bestätigen Sie die Eingabe.

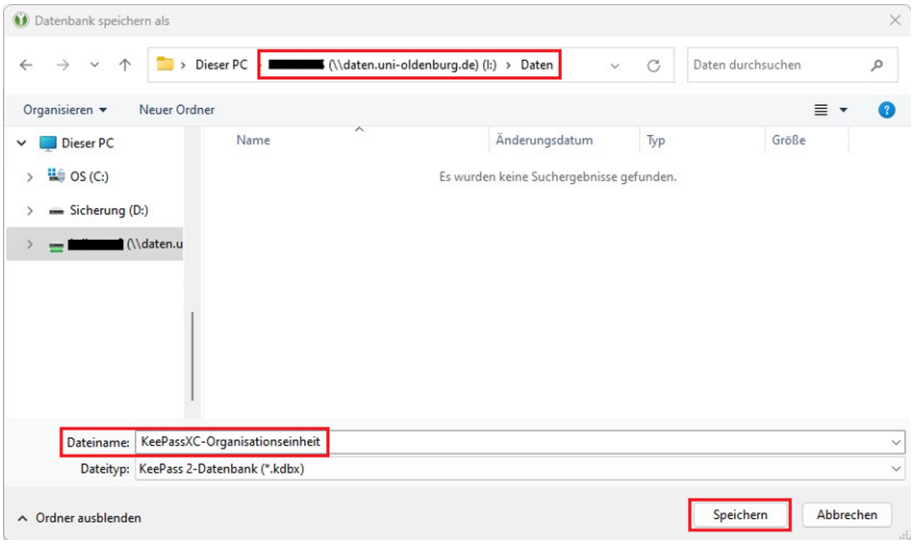


- Im nächsten Schritt müssen die Verschlüsselungseinstellungen gewählt werden. Je länger die Verschlüsselung dauert, umso stärker ist die Verschlüsselung, als Kompromiss zwischen Zeit und Stärke sollten Sie 2,5 s verwenden. Als Datenbankformat wählen Sie das empfohlene Format (KDBX4).

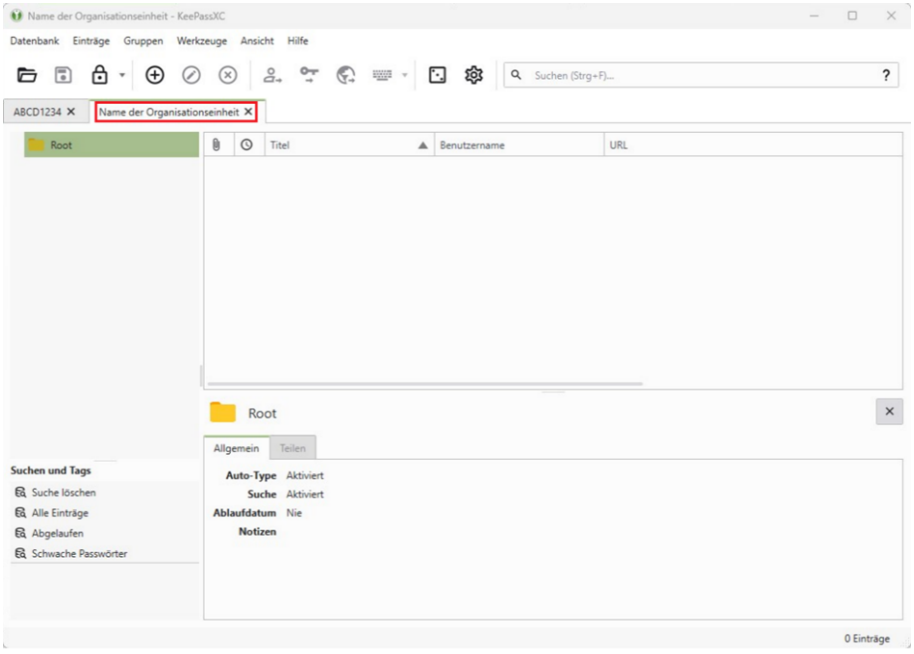
- Im nächsten Schritt müssen Sie die Anmeldedaten (Passwort) für die Passwortdatenbank festgelegen. Verwenden Sie bitte ein komplexes Kennwort (grüner Fortschrittsbalken) und nicht das gleiche Passwort wie für Ihren Universitäts-Account oder Ihre persönliche Passwortdatenbank.



- Mit einem Klick auf „Fertig“ wird die Datenbank erstellt und Sie werden aufgefordert auszuwählen, wo die Datenbank abgespeichert werden soll. Am besten eignet sich ein separates Verzeichnis auf Ihrem Gruppenlaufwerk.



- Das Programm zeigt nun die Ordner und Einträge der Datenbank an. Es ist ein „Root“ genannter Ordner vorhanden, ansonsten ist noch nichts angelegt.



Zugriffsberechtigungen

- Der Austausch der Passwortdatenbank soll über zentrale, zugriffsbeschränkte Datenlaufwerke, bspw. ein interne Gruppenlaufwerke oder den uni-eigenen Cloudstorage erfolgen. Die Zugriffsberechtigungen auf die Datenspeicherorte der Datenbanken sind auf das minimal Notwendige zu beschränken und die Berechtigungen sind periodisch zu überprüfen und zu aktualisieren.
- Es gibt drei Arten von Berechtigungen: Vollzugriff, Ändern/Schreiben und Lesen. Bei allen Berechtigungen können Sie mit den Optionen „Zulassen“ und „Verweigern“ den Zugriff auf freigegebene Ordner oder Laufwerke steuern.
  - ➢ Lesen:
    Benutzer können die Datei öffnen, Daten in Dateien lesen und verwenden.
  - ➢ Ändern/Schreiben:
    Benutzer können dieselben Aufgaben ausführen wie mit der Berechtigung „Lesen“ und außerdem Daten hinzufügen, ändern und löschen.
  - ➢ Vollzugriff:
    Benutzer können dieselben Aufgaben ausführen wie mit den Berechtigungen „Lesen“ und „Ändern/Schreiben“ und zusätzlich können die Berechtigungen geändert werden. Der Gruppe „Administratoren“ und „System“ ist standardmäßig die Berechtigung „Vollzugriff“ zugewiesen diese sollten Sie nicht entfernen.
- Zum Ändern der Zugriffsberechtigungen wenden Sie sich bitte per Email an Servicedesk@uni-oldenburg.de
  - ➢ Betreff: KeePass-Berechtigungen
  - ➢ Nachrichtentext:
    Pfad\Dateiname: „Pfad und Dateiname der Passwortdatenbank“
    Berechtigungen: „Nutzername = Berechtigung“ (z.B. ABCD1234 = Lesen)

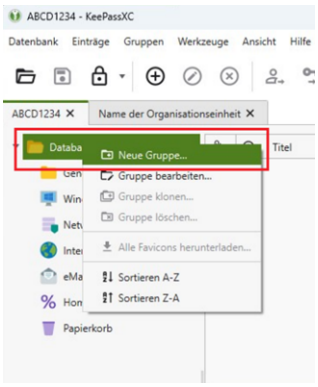
Austausch von Masterpasswörtern

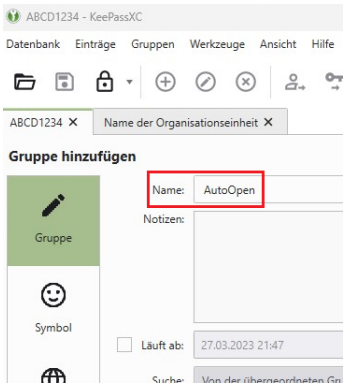
- Sofern der Austausch von Masterpasswörtern für Passwortdatenbanken notwendig ist, so sollte er über sichere Kanäle erfolgen. Zu präferieren sind nicht-technisch gestützte Übergaben der Masterpasswörter. Des Weiteren sollten zentrale, sichere Ablageorte in den Organisationseinheiten definiert werden, etwa ein Safe im jeweiligen Sekretariat.
- Erfolgt die Übergabe der Masterpasswörter über IT-Systeme, ist unbedingt auf eine Ende-zu-Ende-Verschlüsselung zu achten. Damit entfällt im Regelfall das Versenden per E-Mail.
- Es ist zu vermeiden, lokale Kopien von Passwortdatenbanken anzulegen, speziell ist es nicht gestattet, Passwortdatenbanken auf privaten Geräten vorzuhalten.

Tipps zur Bedienung

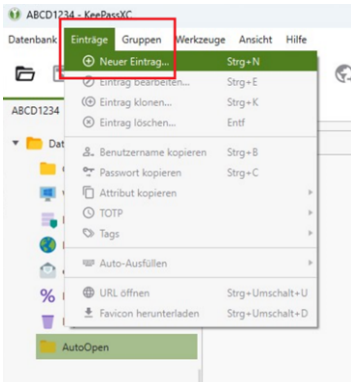
AutoOpen einer zusätzlichen Passwortdatenbank

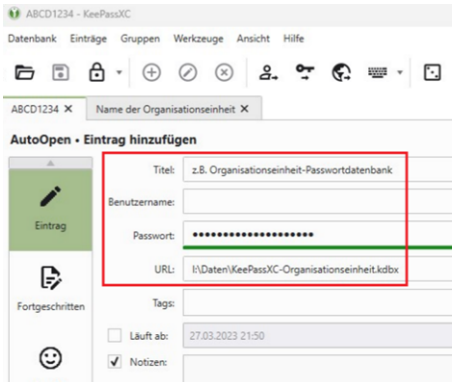
- Erstellen Sie in Ihrer persönlichen Passwortdatenbank eine Gruppe mit dem Namen "AutoOpen" direkt unter Root





- In dieser Gruppe erstellen Sie einen Eintrag wie folgt:
  - Titel: z.B. Abteilungspasswortdatenbank
  - Benutzername: lassen Sie leer
  - Passwort: das Passwort der weiteren Passwortdatenbank
  - URL: der Pfad, unter dem die Datenbank abgespeichert ist





- Nachdem KeePassXC neugestartet und Ihre persönliche Datenbank entsperrt wurde, werden im Anschluss automatisch die weiteren Datenbanken geöffnet, die in der Gruppe AutoOpen eingerichtet wurden.

Symbolleiste

Die Symbolleiste bietet eine schnelle Möglichkeit, allgemeine Aufgaben mit Ihrer Datenbank auszuführen. Einige Einträge in der Symbolleiste sind dynamisch deaktiviert, basierend auf den im ausgewählten Eintrag enthaltenen Informationen. Jede gängige Aktion in KeePassXC kann auch mit einem Tastaturkürzel gesteuert werden.

1. Datenbank:
   - Datenbank öffnen
   - Datenbank speichern
   - Datenbank sperren / Alle Datenbanken sperren
2. Einträge
   - neuen Eintrag erstellen
   - ausgewählten Eintrag bearbeiten
   - ausgewählten Eintrag löschen
3. Eintragsdaten
   - Benutzername kopieren
   - Passwort kopieren
   - URL kopieren
   - Auto-Type durchführen
4. Werkzeuge
   - Passwort-Generator
   - Anwendungseinstellungen
5. Suchen

Tastenkombinationen

Wenn Sie einen Passworteintrag in der Liste ausgewählt haben, können Sie folgende Tastenkombinationen verwenden:

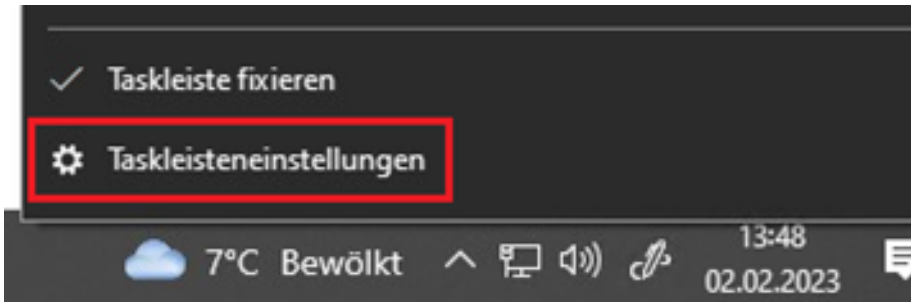
- Strg + C > Passwort in die Zwischenablage kopieren
- Strg + B > Benutzernamen in die Zwischenablage kopieren
- Strg + U > URL (Webadresse) in die Zwischenablage kopieren
- Strg + Umschalt + U > URL im Browser öffnen.

Unter macOS nutzen Sie statt der Strg-Taste die Command-Taste (⌘).

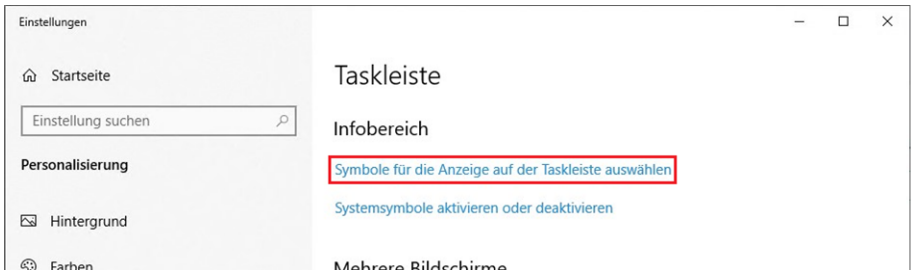
KeePassXC immer in der Statusleiste anzeigen lassen (Windows)

Wenn Sie KeePassXC immer in der Satusleiste/Taskleiste (links neben der Uhr) angezeigt bekommen möchten, müssen Sie wie folgt vorgehen.

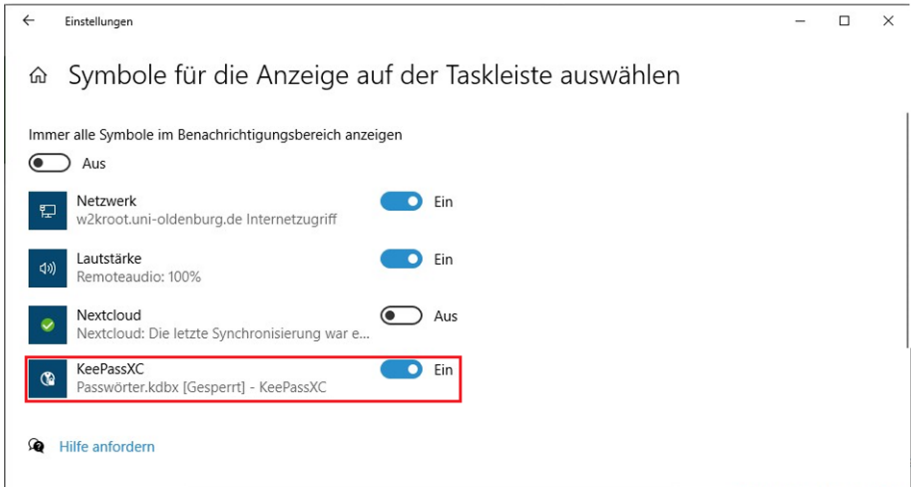
- Klicken Sie mit der rechten Maustaste auf die Taskleiste und wählen dann Taskleisteneinstellungen aus



- Scrollen Sie im Fenster Taskleiste bis zu Infobereich, dort klicken Sie auf "Symbole für die Anzeige auf der Taskleiste auswählen".



- In der Liste schalten Sie neben KeePassXC um auf Ein und schließen das Fenster.



- Das Symbol für KeePassXC wird dann in der Taskleiste neben der Uhr angezeigt

KeePassXC im Dock behalten (macOS)

Damit das KeePassXC Symbol immer im Dock angezeigt wird, müssen Sie wie folgt vorgehen.

- Halten Sie die [control]-Taste gedrückt und klicken auf das KeePassXC-Symbol um das Kontextmenu zu öffnen. Im Anschluss wählen Sie Optionen und aktivieren Im Dock behalten.

Gruppen anlegen

KeepassXC legt die Passworteinträge in sogenannten Gruppen an. Das sind „Kategorien“ die vom Benutzer selbst festgelegt werden können. In den Gruppen sind die eigentlichen Passwort-Einträge abgelegt.

- Über den Menüpunkt „Gruppen“ → „Neue Gruppe“ öffnet sich das Menü zum Anlegen einer Gruppe.
- Im Punkt „Gruppe“ wird der Name der Gruppe vergeben. Optional können Notizen (z.B. eine Beschreibung) angegeben werden. Weiters kann ein Ablaufdatum festgelegt werden – das ist jedoch in den meisten Fällen nicht notwendig.
- Hat man einen Namen für die Gruppe vergeben, kann mit einem Klick auf „Symbol“ ein Symbol für die Gruppe vergeben werden. Dabei kann ein vorhandenes Symbol verwendet werden oder ein eigenes Symbol.
- Mit einem Klick auf „OK“ wird die Gruppe gespeichert.

Passworteintrag anlegen

- Mit einem Klick auf die Schaltfläche mit dem „+“ öffnet sich ein Menü zum Anlegen eines neuen Passworteintrages.
- Es öffnet sich ein Menü, dort kann im Bereich „Eintrag“ der Name des Eintrages, der Benutzername (optional) und das Passwort, das gespeichert werden soll, eingegeben werden. Ebenso können eine URL (z.B. für die Login-Seite einer Website) und Notizen angegeben werden.
- Mit einem Klick auf das kleine Würfelsymbol neben dem Passwort-Feld gelangt man zum Passwortgenerator. Hier kann man sich ein zufälliges Passwort beliebiger Größe und mit verschiedenen Optionen erzeugen lassen.
- Im Reiter „Passwort“ können die Länge des Passwortes sowie die Zeichen, die verwendet werden sollen, ausgewählt werden. Die Option „Gleichaussehende Zeichen ausschließen“ verhindert, dass z.B. ein großes „i“ und ein kleines „l“ gleichzeitig im Passwort vorkommen. Damit können Eingabefehler aufgrund gleich aussehender Zeichen vermieden werden.
  Die Option „Zeichen aus allen Gruppen verwenden“ verwendet für das Passwort alle Arten von Zeichen.
  Über den Reiter „Passphrase“ kann ein Passwort aus einer Passphrase, also einem „Satz“ aus verschiedenen Wörtern, die aneinander gereiht werden, erzeugt werden. Es kann auch ein Trennzeichen für die Trennung der einzelnen Wörter verwendet werden.
    1. Das Menü erlaubt folgende Einstellungen:
       a. Festlegen wie viele Wörter aneinander-gereiht werden sollen
       b. Ein Trennzeichen, das zwischen die einzelnen Wörter gesetzt wird
       c. Nur Klein- / Großbuchstaben oder gemischt verwenden
- Mit einem Klick auf „Passwort anwenden“ wird das Passwort erzeugt. Mit einem Klick auf den Punkt „Symbol“ kann wieder ein Symbol für den Eintrag (Systemsymbol oder ein eigenes Symbol) ausgewählt werden.
- Mit einem Klick auf „OK“ wird das Passwort als neuer Eintrag angelegt.
- Mit einem Klick auf das Speichersymbol im Menü oder durch drücken der Tastenkombination „STRG+S“ wird die Datenbank gespeichert.
- Der Eintrag ist nun sichtbar und kann mit einem Doppelklick geöffnet und bearbeitet oder gelöscht werden.

Passwortgenerator

- Mit dem Passwortgenerator können Sie zufällige, starke Passwörter oder Passphrasen generieren, die Sie für Ihre Anwendungen und die von Ihnen besuchten Webseiten verwenden können.
- Die Oberfläche des Passwortgenerators öffnet sich nach einem Klick auf das Würfel-Symbol (in der Zeile für das Passwort beim Bearbeiten eines Eintrags oder in der Symbolleiste). Sie können die Zeichengruppen (z. B. Großbuchstaben, Ziffern, Sonderzeichen usw.), die in ihrem Passwort enthalten sein sollen, auswählen und die Länge des Passworts. KeePassXC wählt nach dem Zufallsprinzip Zeichen aus der Menge aus.
- Statt eines Passwortes können Sie auch eine Passphrase generieren. Das ist eine zufällige Folge von Wörtern, die mit einem Trennzeichen getrennt sein können.

Passwortdatenbank importieren

- Das Programm bietet die Möglichkeit Passwort-Einträge und auch Datenbanken aus diversen verschiedenen Dateiformaten zu importieren.
- Es ist möglich Passwörter als CSV-Datei zu importieren. Ganze Datenbanken können auch im Dateiformat kdbx (von Keepass) oder 1Password-Format importiert werden.

Backup

- Um die Datenbank zu sichern, gibt es zwei Möglichkeiten:
  - Export der Passworteinträge in eine CSV-Datei oder HTML-Datei
  - Sichern der Passwortdatei und des Keyfiles selbst
- Der sicherste Weg, um die Passwortdatenbank zu sichern, ist die Passwortdatei und (falls vorhanden) das zugehörige Keyfile regelmäßig auf eine externe Festplatte oder einen USB-Stick zu kopieren.
- Das Exportieren der Passwort-Einträge erfolgt unter „Datenbank“-“Export“ und der Wahl des gewünschten Datenformates.

Mobile Anwendungen

Leider ist das Programm KeePassXC selbst nicht für iOS und Android verfügbar. Es gibt jedoch Apps, mit denen Sie die Passwortdateien auch auf dem Mobilgerät öffnen können.

Android

Wir haben unter Android die kosten- und werbefreien Apps Keepass2Android und KeePassDX getestet. Diese können Sie im Google Play-Store herunterladen:

- Keepass2Android
- KeePassDX

iOS

Wir haben unter iOS die Apps Strongbox und KeePassium in der kostenlosen Basisversion getestet. Diese können Sie im Apple-Store herunterladen:

- Strongbox
- KeePassium

Datenbank und Arbeitsplatz beim Verlassen sperren

Beim Verlassen des Arbeitsplatzes sollten Sie zumindest die Datenbank, besser noch den gesamten Arbeitsplatz immer sperren.

- Das Sperren der Datenbank erfolgt im KeePassXC-Hauptfenster unter Windows mittels [Strg]+[L] und unter macOS mittels [command]+[L].
- Der Arbeitsplatz lässt sich unter Windows mittels [Windows]+[L] und unter macOS mittels [control]+[command]+[Q] sperren.

Weitere Informationen

- Documentation and FAQ - KeePassXC
- Liste Tastenkombinationen