

Kommunaler Versorgungsverband Sachsen

Anleitung

Sichere Nutzung von Passwörtern mit KeePassXC

vom 25.08.2025

Inhalt

1.	Einleitung	3
2.	Datenbank anlegen	3
3.	Datenbank füllen	7
3.1	Gruppen/Ordner anlegen	8
3.2	Einträge anlegen	9
4.	Einträge automatisch im Browser einfügen	12
4.1	Plugin aktivieren	12
4.2	Einträge einfügen	13
5.	Programm-Einstellungen	16

1. Einleitung

Sie als Mitarbeitende des KVS nutzen in der Regel eine Vielzahl von Passwörtern, um sich an diversen Anwendungen, Portalen oder Geräten anzumelden. Diese Passwörter sollen ausreichend lang, komplex und wenn möglich einmalig sein.

Da lange komplexe Kennwörter schwer zu merken sind, werden oft einfache Passwörter genutzt und/oder dasselbe Passwort für mehrere Dienste verwendet.

Um die Benutzung und Verwaltung von Zugangsdaten für Sie zu vereinfachen und gleichzeitig die Sicherheit beim Umgang mit Passwörtern zu erhöhen, stellen wir Ihnen die Anwendung KeePassXC zur Verfügung.

Mit diesem Passwortmanager können Sie unter anderem:

- Zugangsdaten und Kennwörter in einer verschlüsselten Datenbank ablegen,
- Passwörter in Gruppen/Ordern strukturiert verwalten,
- komplexe Kennwörter mit dem integrierten Passwortgenerator erstellen,
- Zugangsdaten mit wenigen Klicks in Webanmeldungen einfügen.

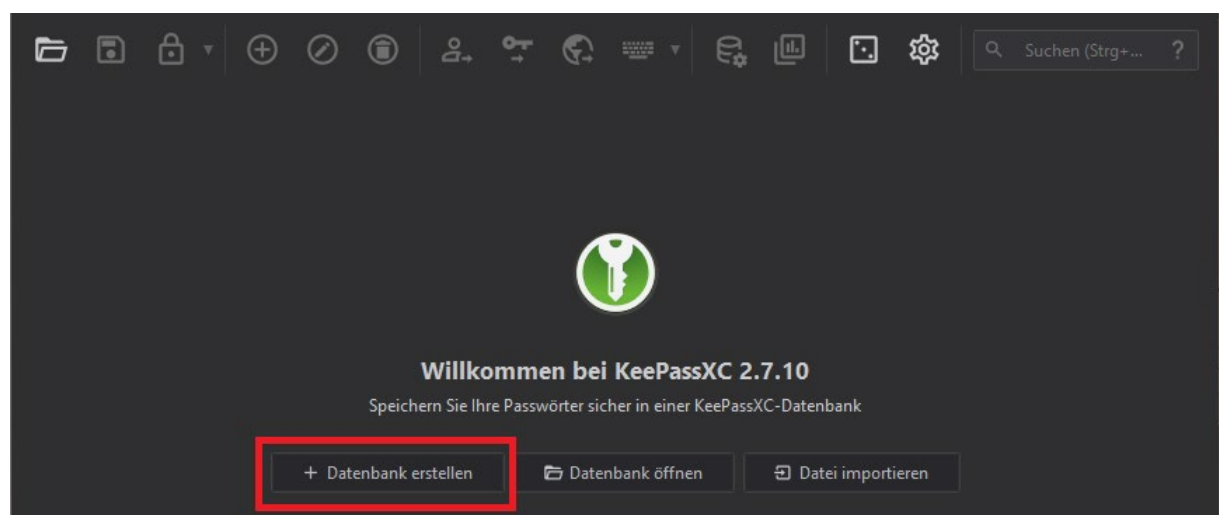
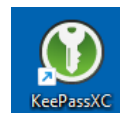
WICHTIGER HINWEIS:

Das Programm erstellt eine Datenbankdatei, die mit einem Masterpasswort geschützt ist. Dieses Kennwort kann NICHT wiederhergestellt oder zurückgesetzt werden.

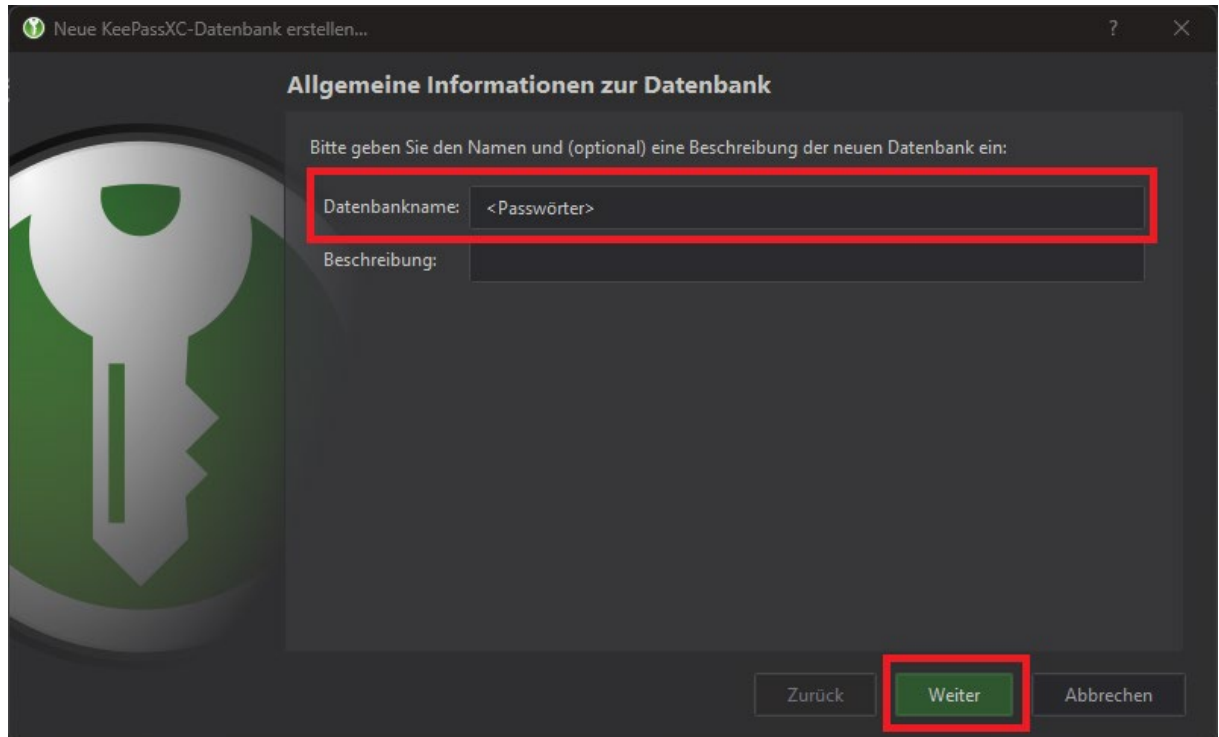
Wenn Sie das Masterpasswort vergessen, sind alle Kennwörter in der Datenbank unwiederbringlich verloren!

2. Datenbank anlegen

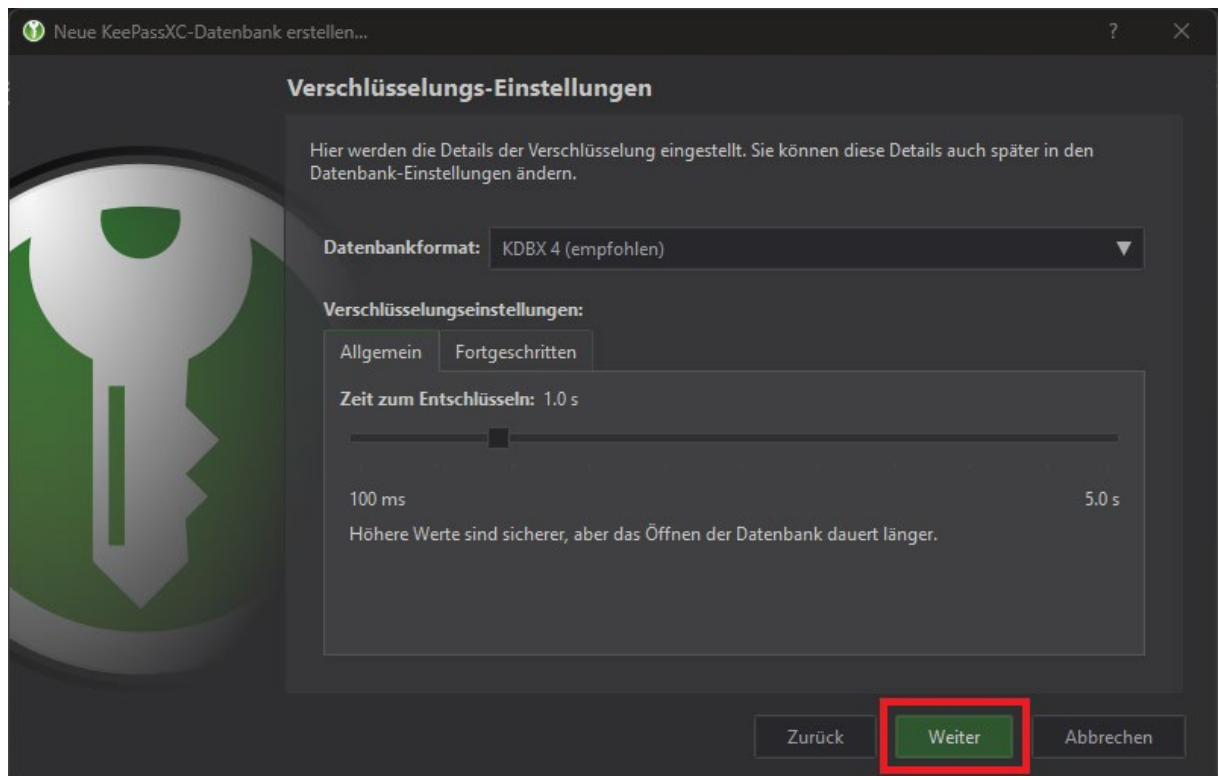
1. Starten Sie KeePassXC mit einem Doppelklick auf das Desktopsymbol
2. Klicken Sie auf die Schaltfläche *+Datenbank erstellen*.



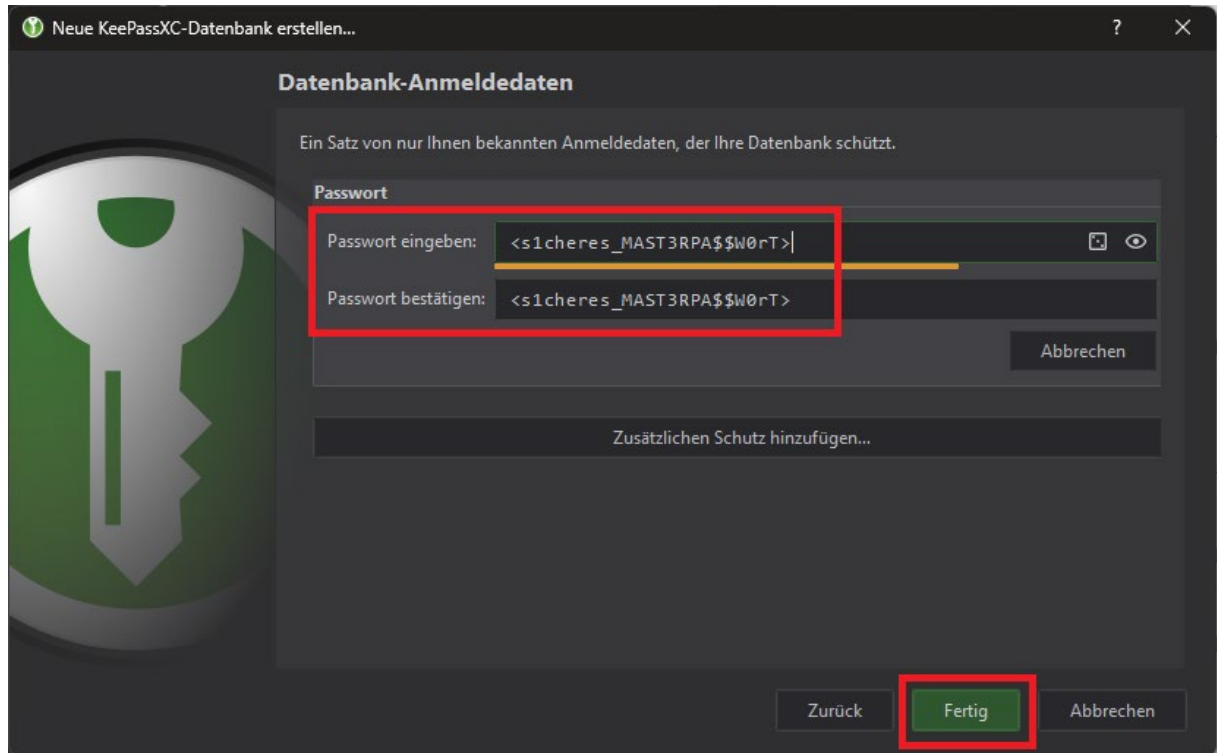
3. Geben Sie der Datenbank einen aussagekräftigen Namen und bestätigen Sie Ihre Angabe mit *Weiter*. Optional können Sie auch eine kurze Beschreibung angeben.



4. Im folgenden Bildschirm können Sie die Verschlüsselungsparameter der Datenbank ändern. Diese Einstellungen können Sie belassen und mit *Weiter* fortsetzen.



5. Vergeben Sie ein sicheres Masterpasswort zur Entsperrung der Passwortdatenbank.

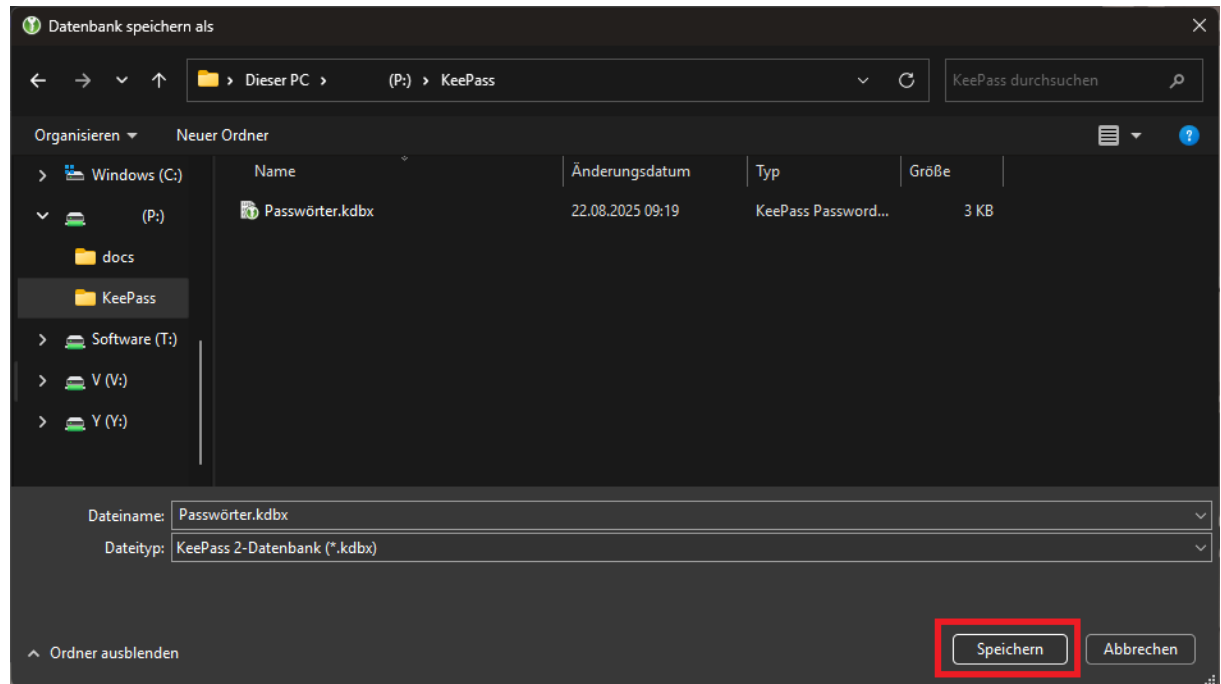


Nutzen Sie für das Masterpasswort ein ausreichend sicheres Kennwort, das Sie sich gut merken können. Laut BSI gelten folgende Arten von Passwörtern als sicher:

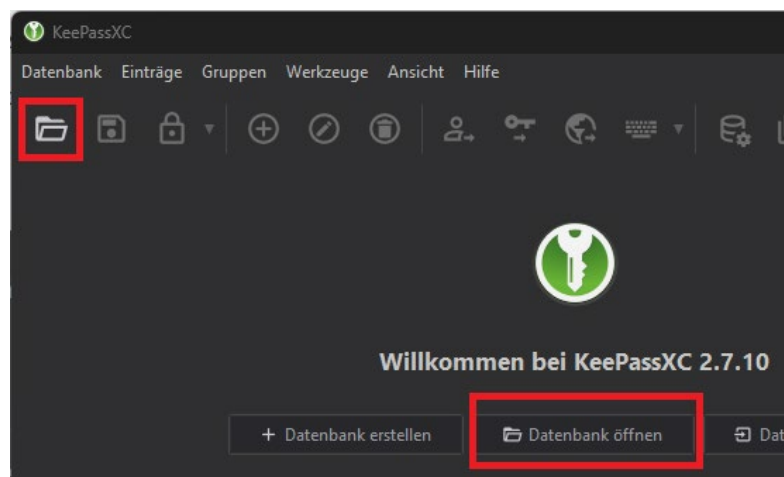
- 8 bis 12 Zeichen aus vier Zeichenarten (Großbuchstaben und Kleinbuchstaben und Ziffern und Sonderzeichen)
- 20 bis 25 Zeichen aus zwei Zeichenarten (z.B. große und kleine Buchstaben oder große Buchstaben und Ziffern usw.)

Allgemeine Hinweise zur Erstellung und Nutzung von Passwörtern finden Sie auf der [Webseite des BSI](#).

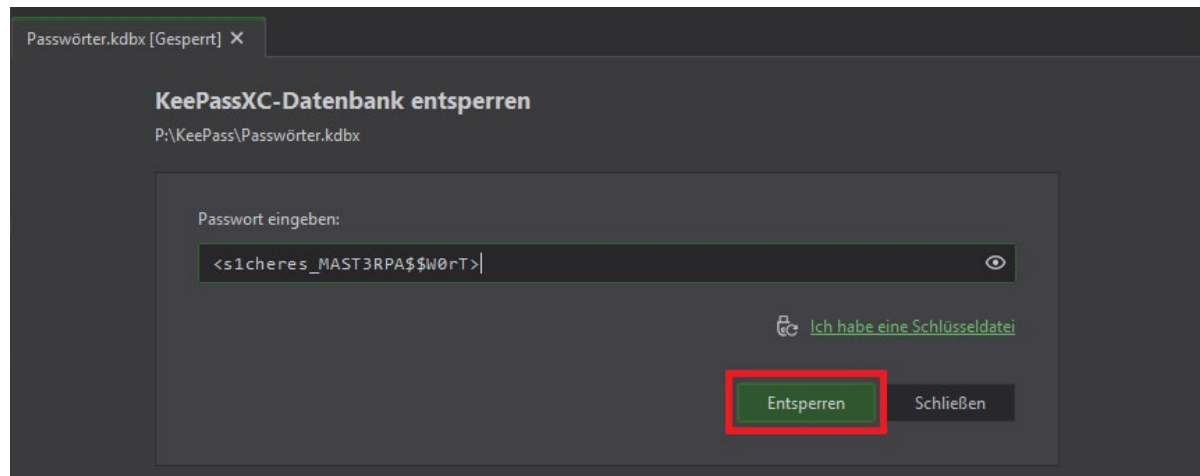
6. Speichern Sie die Datei auf Ihrem Laufwerk P:\, damit niemand außer Ihnen zugreifen kann. Erstellen Sie am besten einen eigenen Ordner – z.B. *KeePass* – und speichern Sie die Datei dorthin.



7. Um die Datenbank zu öffnen, starten Sie das Programm KeePassXC. Die zuletzt geöffnete(n) Datenbank(en) werden automatisch geladen. Sollte keine Datenbank geladen sein, können Sie Ihre Datei über das „Ordner“-Symbol oder über die Schaltfläche *Datenbank öffnen* öffnen.

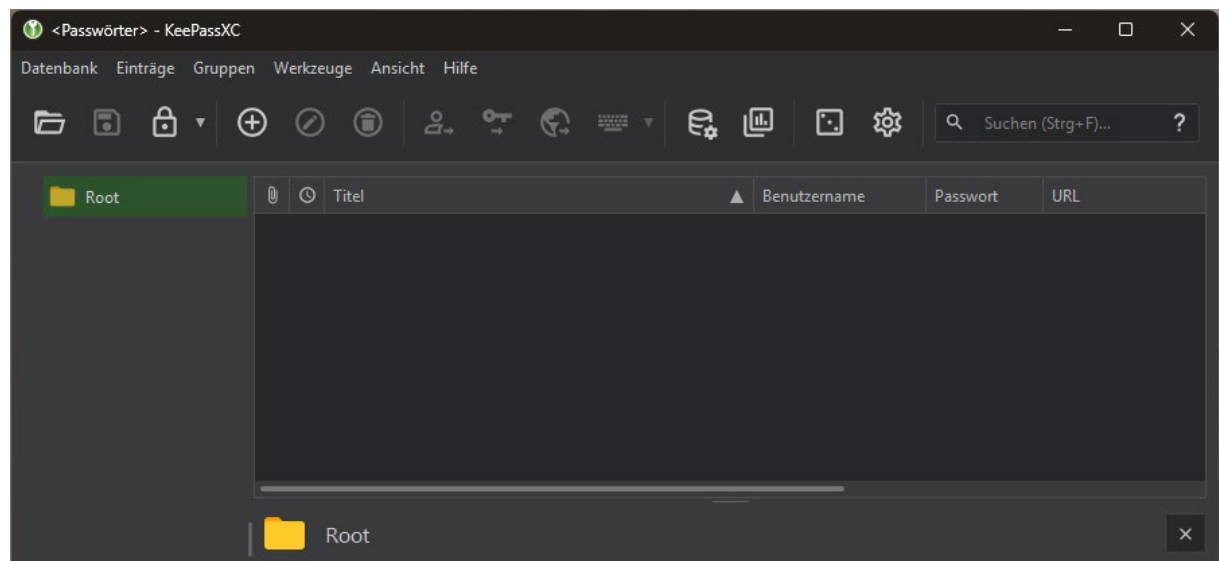


Geben Sie zum Entsperren Ihr Masterpasswort ein und Bestätigen Sie mit *Entsperren*.



3. Datenbank befüllen

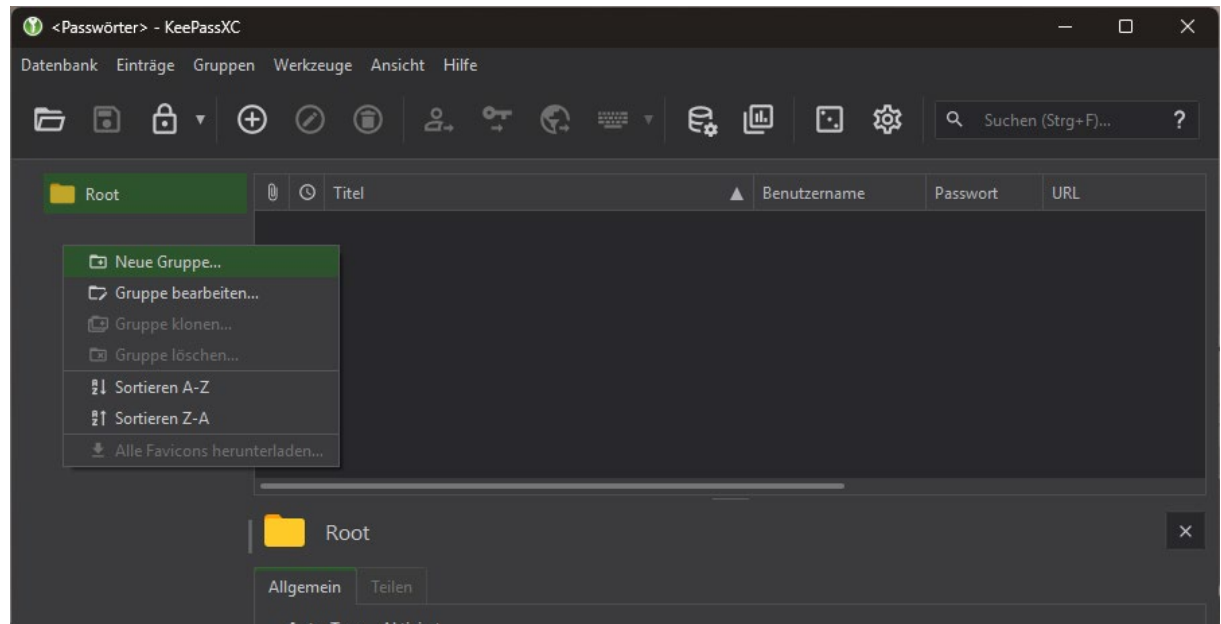
Wenn Sie die Passwortdatenbank nach der Erstellung zum ersten Mal öffnen, sehen Sie in der linken Spalte eine Gruppe *Root*. Das ist die Hauptgruppe. Unterhalb dieser können Sie Einträge oder weitere Gruppen anlegen.



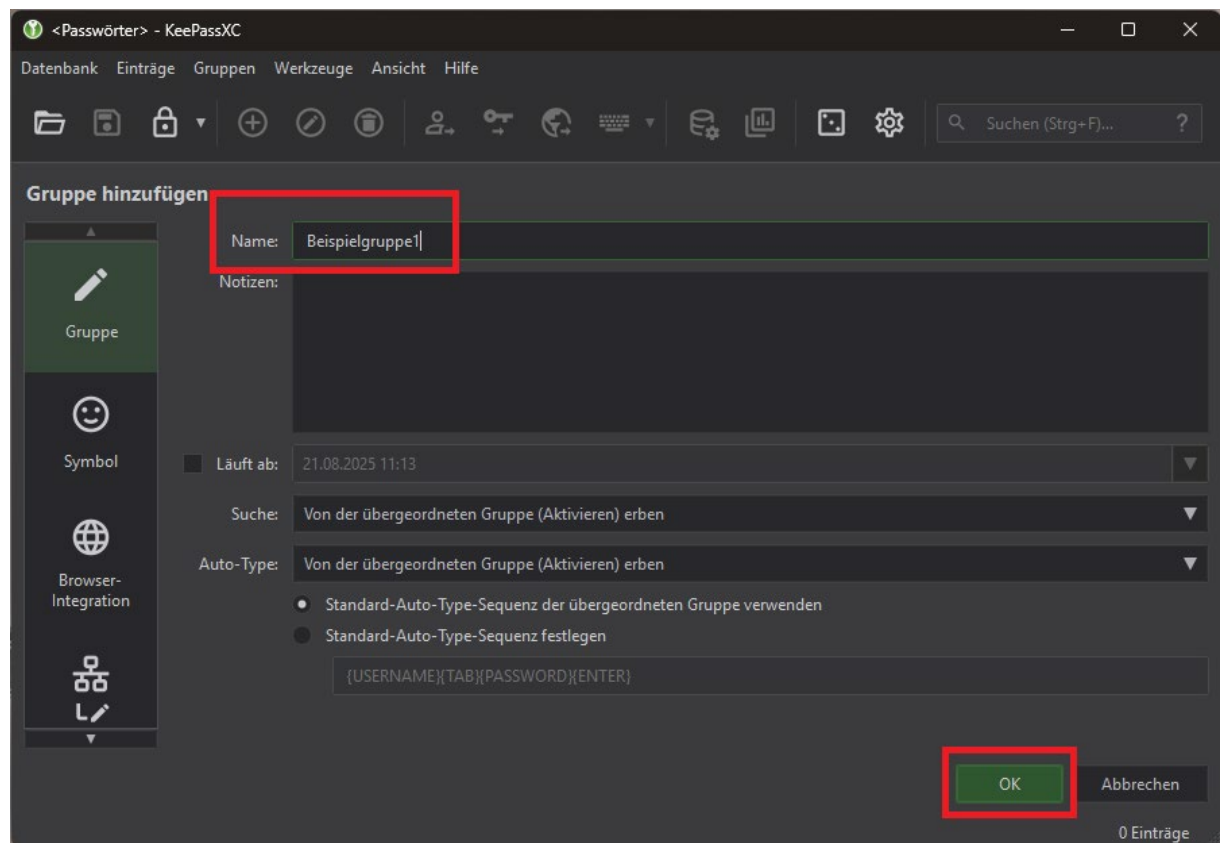
Wir empfehlen die Einträge für Zugangsdaten hierarchisch in Gruppen/Ordern zu strukturieren. Hierdurch erhalten Sie eine bessere Übersicht und können Zugangsdaten, welche thematisch zueinander passen, zusammenfassen (z. B. nach Fachanwendungen).

3.1 Gruppen/Ordner anlegen

1. Um eine neue Gruppe anzulegen, klicken Sie mit der rechten Maustaste auf die übergeordnete Gruppe und wählen Sie *Neue Gruppe*.



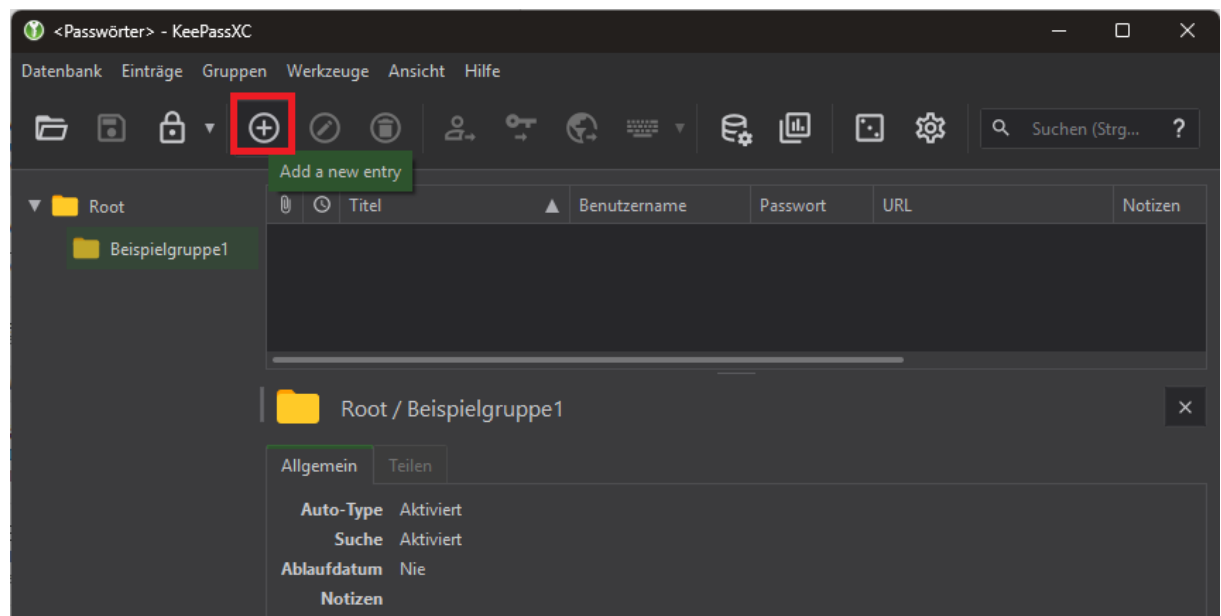
2. Geben Sie der Gruppe einen Namen und bestätigen Sie die Eingabe mit *Weiter*.



Sie können nun unterhalb der Gruppe weitere Gruppen oder Einträge anlegen.

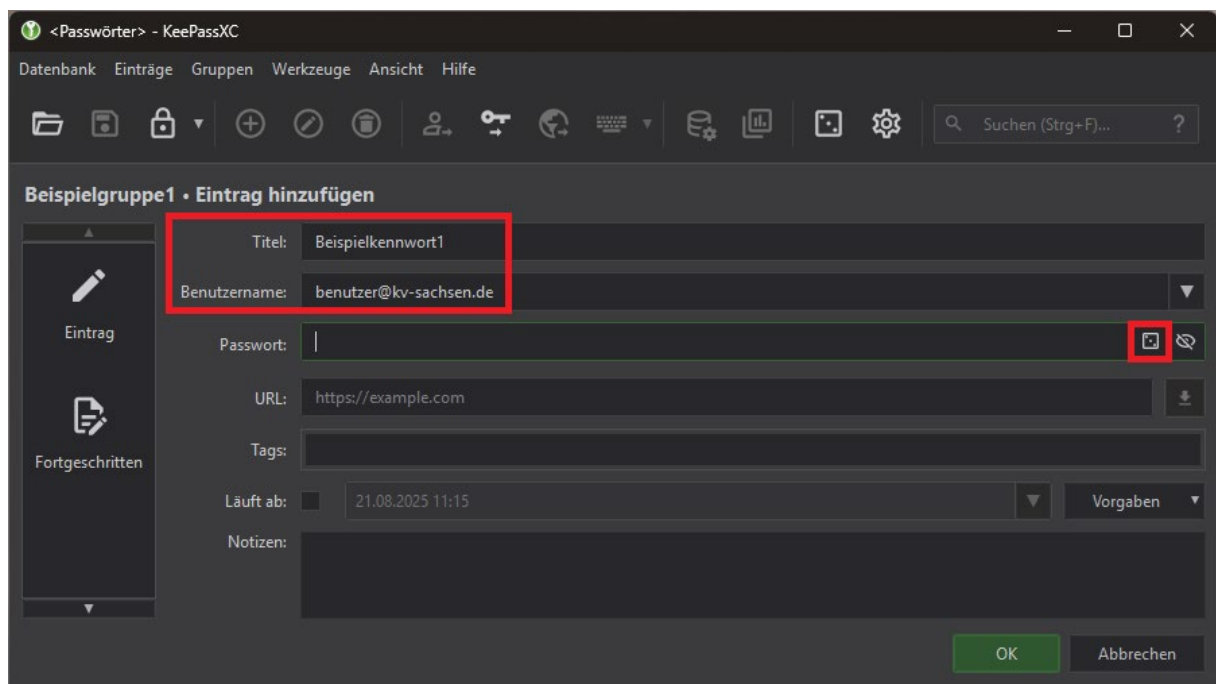
3.2 Einträge anlegen

1. Um einen neuen Kennworteintrag anzulegen, markieren Sie die Gruppe, in der der Eintrag angelegt werden soll. Klicken Sie anschließend auf das „+“-Zeichen und auf *Add a new entry*.

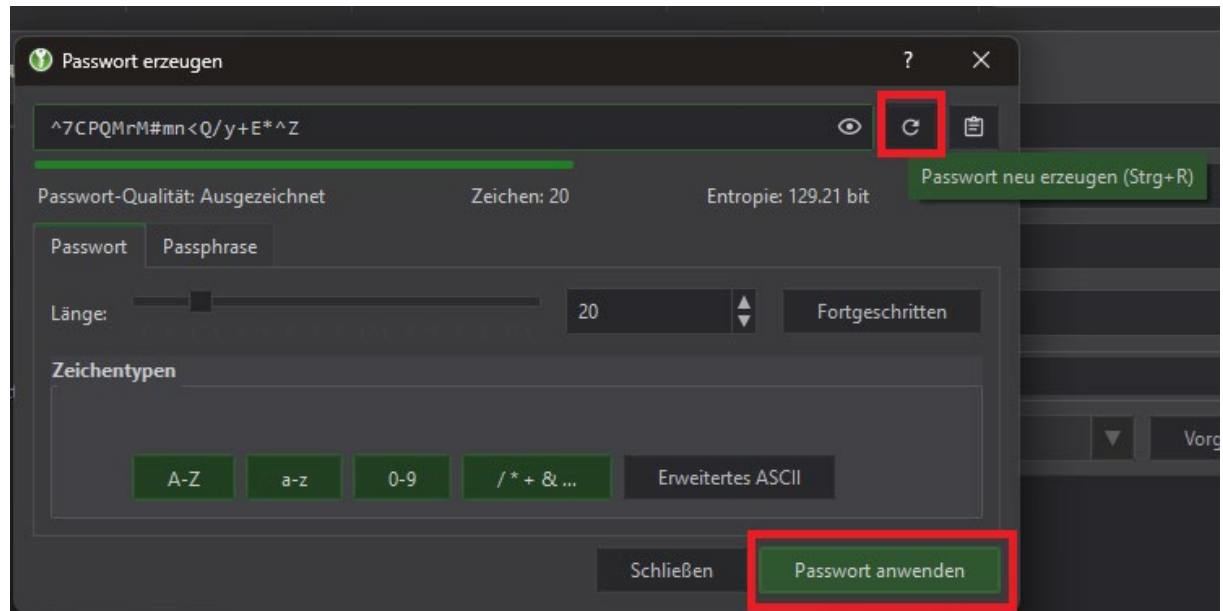


2. Tragen Sie nun einen Titel und die entsprechenden Zugangsdaten ein. Wenn Sie bereits ein sicheres Kennwort haben, können Sie es direkt in das Feld *Passwort* eintragen.

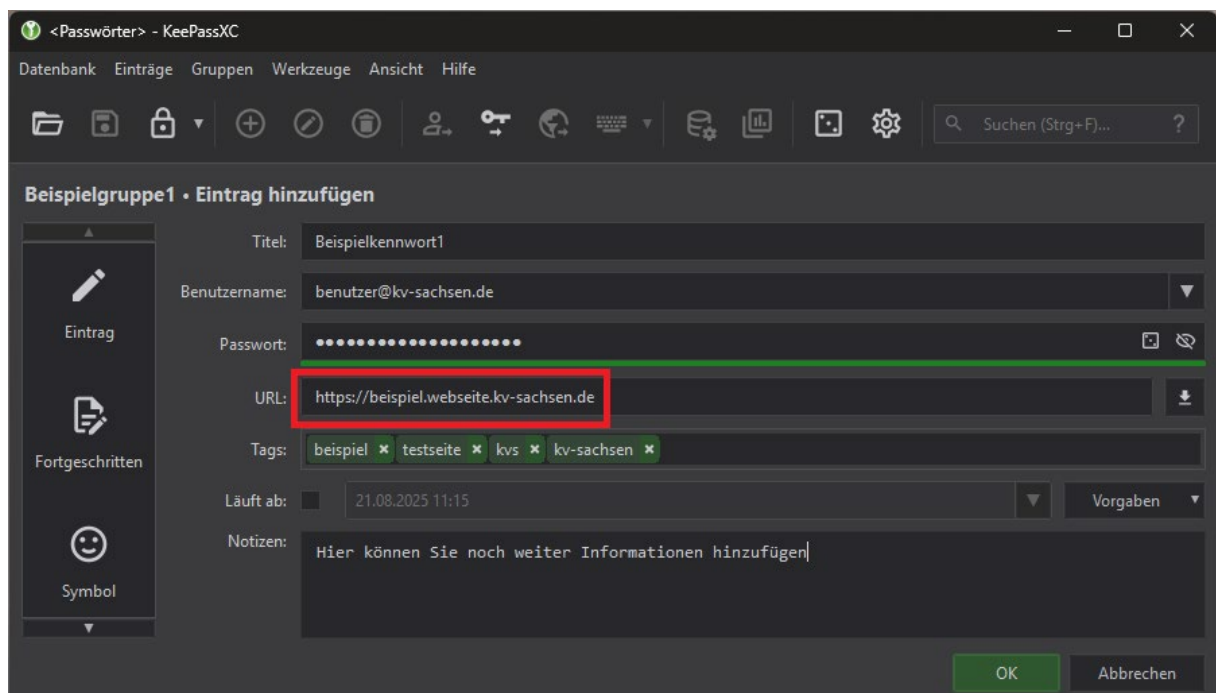
Wenn Sie ein Passwort generieren möchten, klicken Sie auf das „Würfel“-Symbol. Andernfalls fahren Sie mit Schritt 4 fort.



- Wählen Sie in dem sich öffnenden Fenster die Passwortparameter aus und klicken Sie auf das „Kreis“-Symbol.
Wenn Sie mit dem erzeugten Kennwort zufrieden sind, bestätigen Sie mit *Passwort anwenden*.



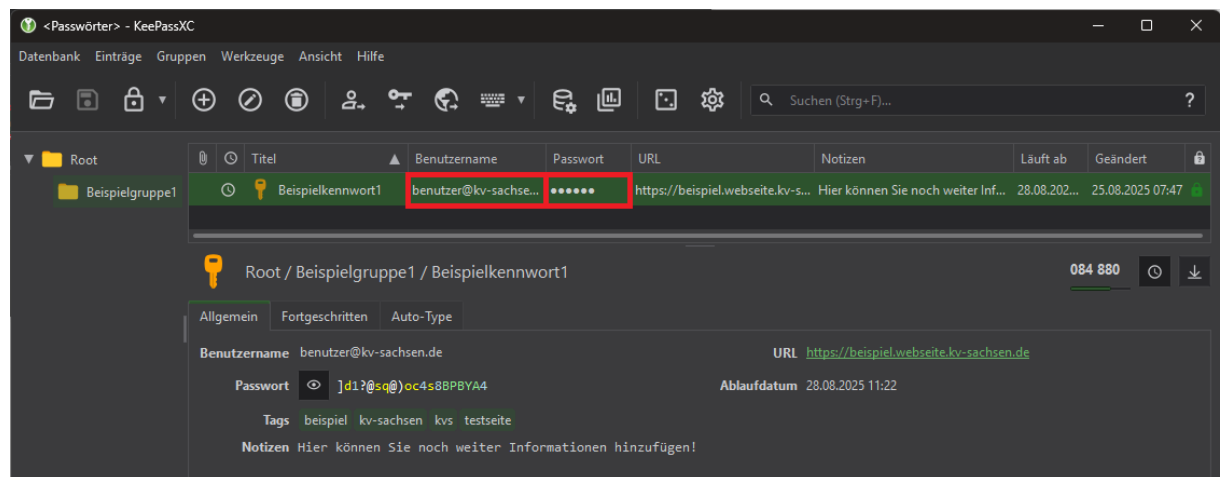
- Wenn Sie das Kennwort gewählt haben, können Sie unter *URL*: die Webadresse einer Webanwendung oder eines Webportals eintragen.
Das ist wichtig, wenn Sie Zugangsdaten automatisch in den Browser einfügen möchten.



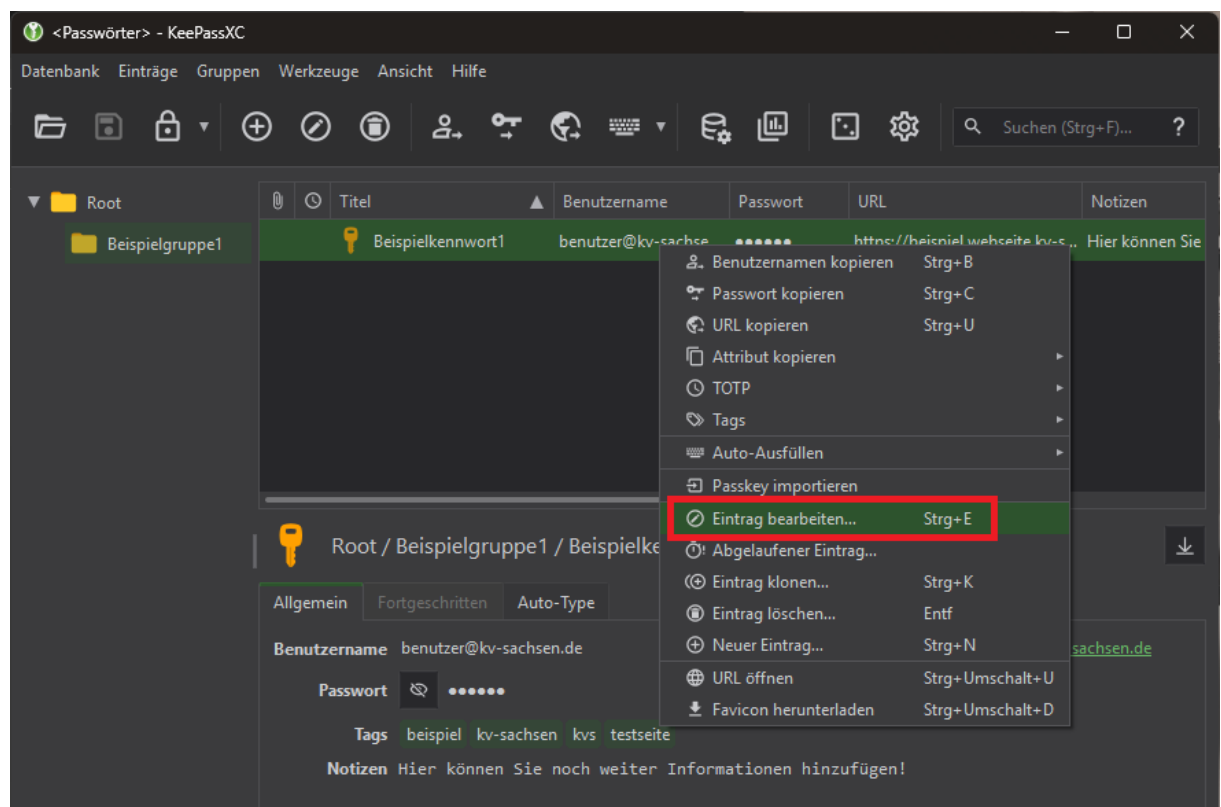
Tipp: Nutzen Sie bei der Erstellung von Einträgen aussagekräftige Tags. Dadurch können Zugangsdaten über die Suchfunktion durch die vergebenen Schlagworte besser gefunden werden.

- Wenn Sie alle relevanten Daten eingetragen haben, können Sie den Eintrag mit **OK** speichern.

Mit einem Doppelklick auf den Benutzernamen oder auf das Passwort, können Sie diese jeweils automatisch in die Zwischenablage kopieren, um sie in einem Eingabefeld einfügen zu können.



- Um einen bestehenden Eintrag zu bearbeiten, klicken Sie mit der rechten Maustaste auf diesen Eintrag und wählen *Eintrag bearbeiten*.

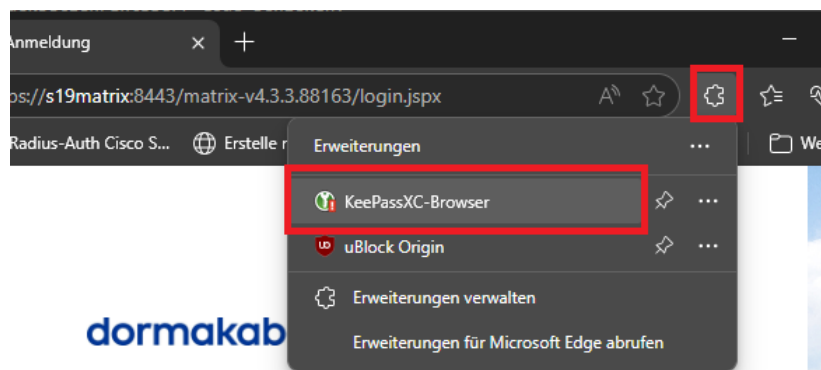


4. Einträge automatisch im Browser einfügen

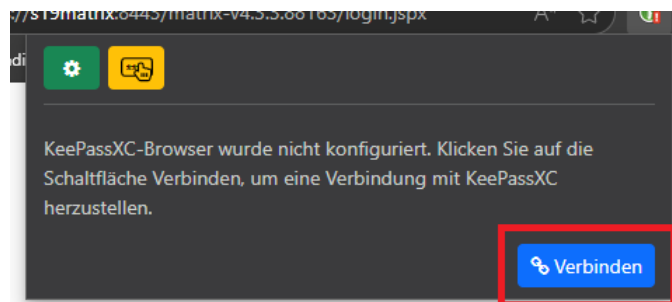
Für den Passwortmanager gibt es ein Browser-Plugin, mit dem Sie häufig benötigte Zugangsdaten mit einem Mausklick automatisch in Anmeldeseiten von Webseiten einfügen können. Das Plugin ist standardmäßig installiert, aber noch nicht aktiviert.

4.1 Plugin aktivieren

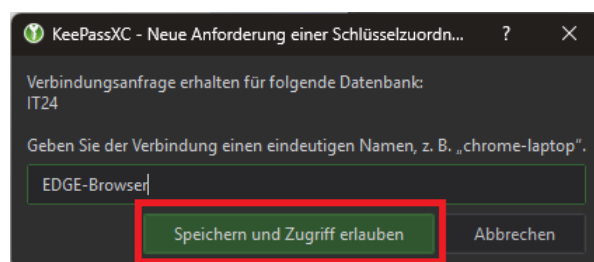
1. Öffnen Sie KeePassXC und entsperren Sie die Datenbank.
2. Starten Sie Ihren Browser (Microsoft EDGE) und klicken Sie oben rechts neben der Adressleiste auf das „Puzzle“-Symbol (Erweiterungen) und anschließend auf den Eintrag *KeePassXC-Browser*.



3. Um das Plugin nun mit der geöffneten KeePass-Datenbank zu verbinden, klicken Sie auf *Verbinden*.



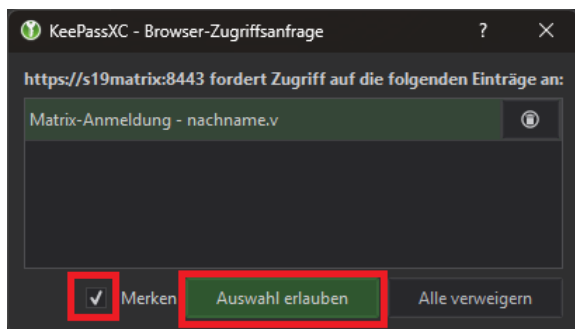
4. Geben Sie der Verbindung einen aussagekräftigen Namen und genehmigen Sie den Zugriff mit *Speichern und Zugriff erlauben*.



4.2 Einträge einfügen

Wenn Sie über den Browser eine URL zum ersten Mal anfragen, müssen Sie den Zugriff auf den Eintrag nochmal explizit erlauben. Diese Genehmigung gilt für alle Einträge, die mit dieser URL verknüpft sind.

1. Setzen Sie den Haken vor *Merken* und bestätigen Sie den Zugriff über *Auswahl erlauben*.



Sollte die Anfrage für die Browser-Zugriffsanfrage nicht automatisch kommen, klicken Sie bitte auf der Anmeldeseite auf das KeePassXC-Symbol in den Anmeldefeldern.



Anmeldung

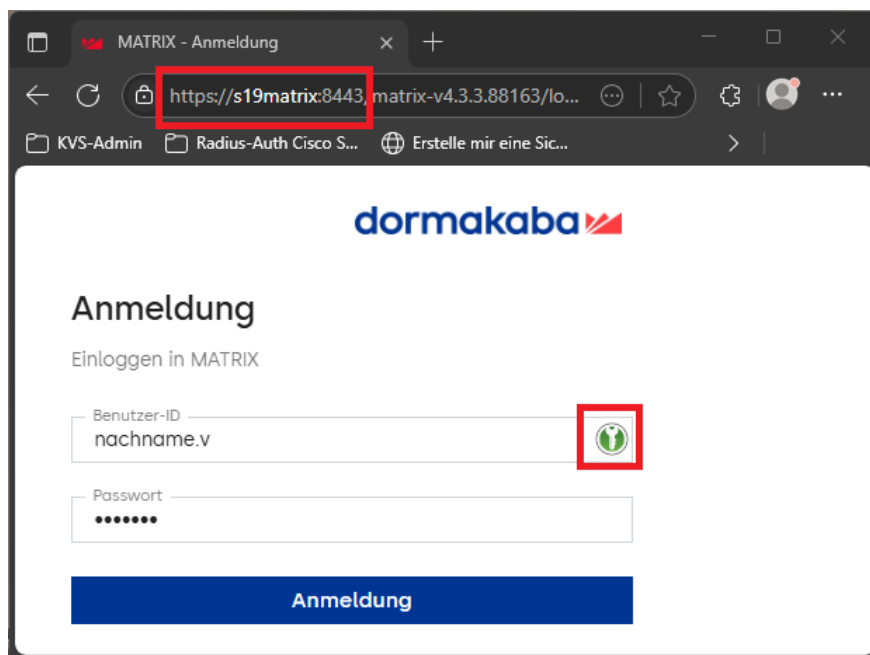
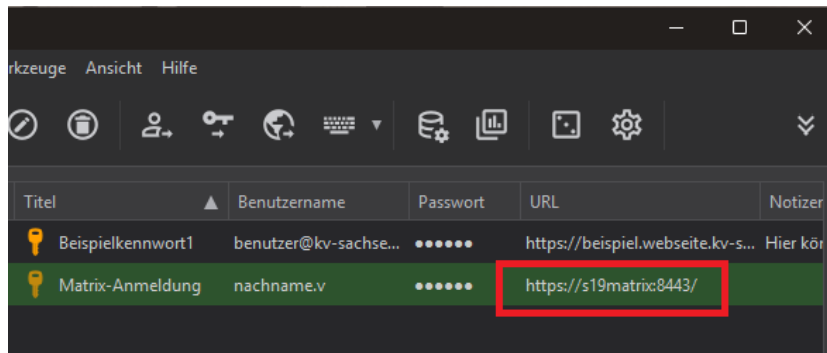
Einloggen in MATRIX

Benutzer-ID 

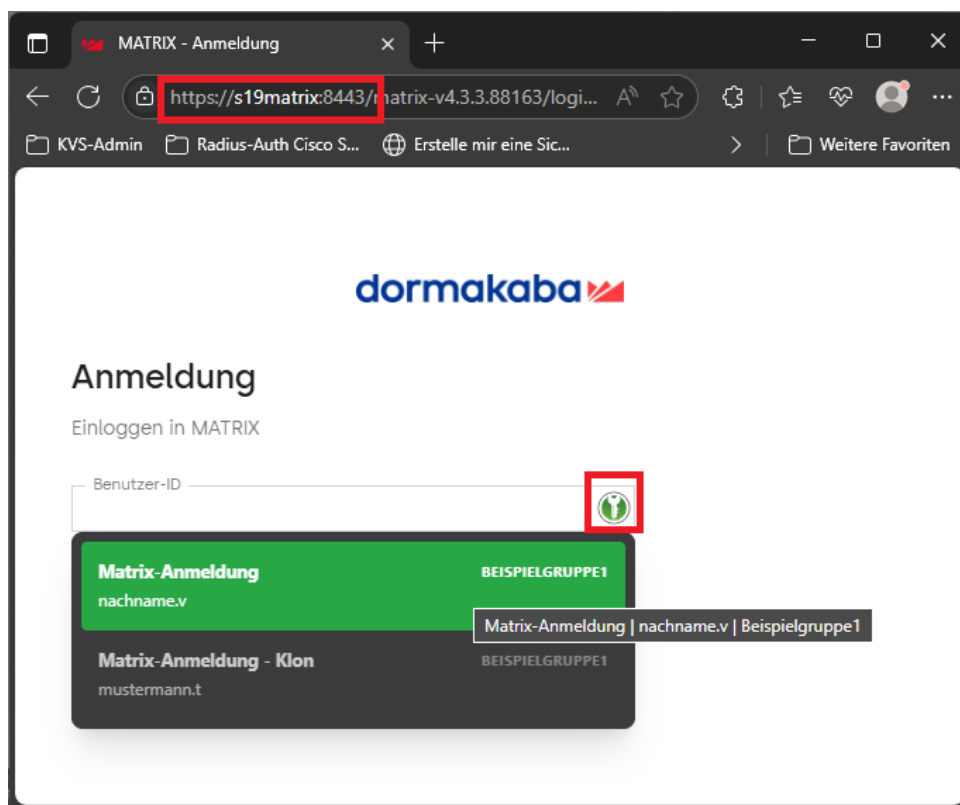
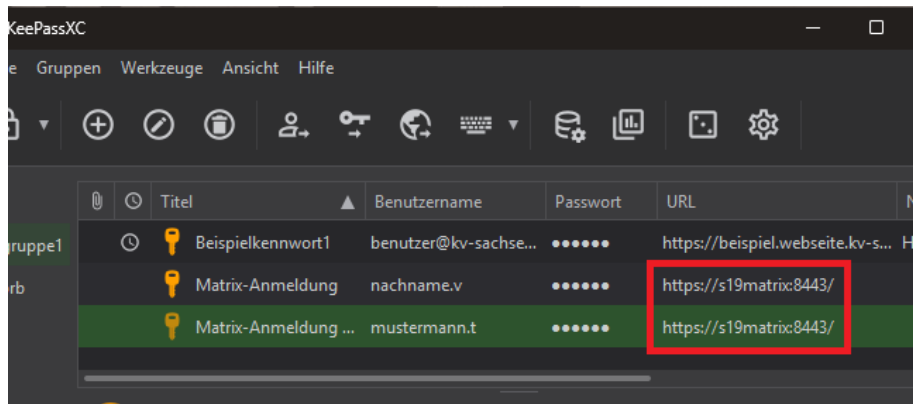
Passwort

Anmeldung

2. Wenn Sie einen Eintrag haben, der mit der URL im Browser übereinstimmt, kann der Eintrag über einen Klick auf das grüne KeePassXC-Symbol in die Eingabefelder eingefügt werden.



3. Wenn Sie zu einer URL mehrere Einträge haben, werden Ihnen alle Einträge mit der passenden URL angezeigt. Wählen Sie hier den Eintrag aus, mit dem Sie sich anmelden möchten.

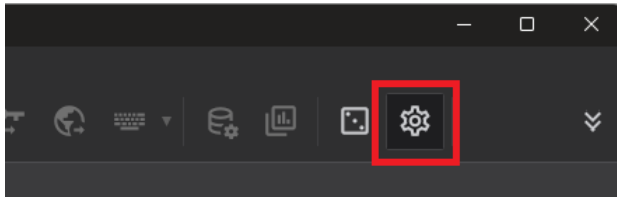


ACHTUNG: Um die Funktion des Browser-Plugins zu nutzen, muss die URL vom Beginn des Eintrages übereinstimmen. Teile der URL aus der Mitte, wie zum Beispiel nur „s19matrix“ oder „http://s19matrix“, werden nicht erkannt.

5. Programm-Einstellungen

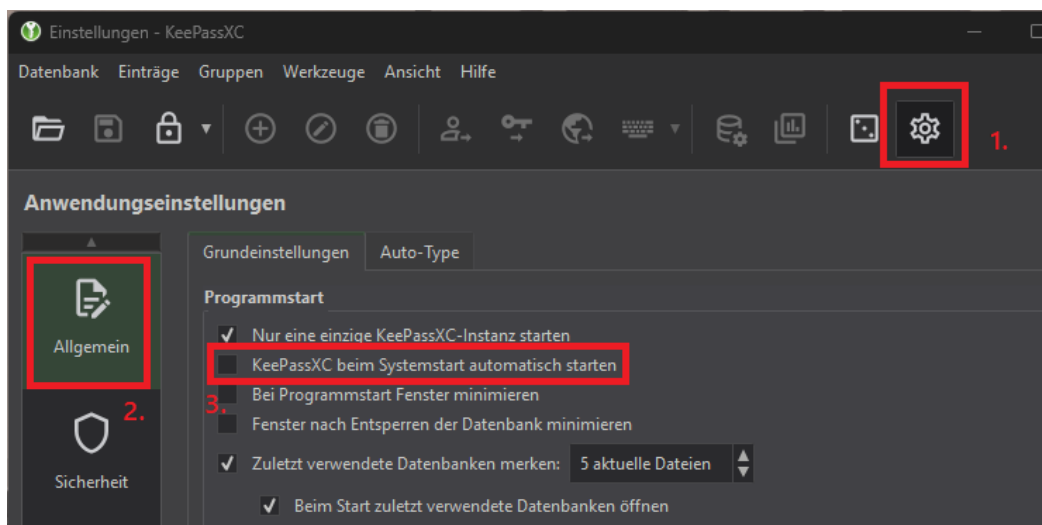
Bei der Erstinutzung von KeePassXC werden Einstellungen geladen. Diese wurden durch das Sachgebiet IT definiert und vorgegeben. Sie können diese Einstellungen ändern. Bitte beachten Sie, dass bei Änderungen von Einstellungen Funktionen gegebenenfalls nicht mehr wie oben beschrieben funktionieren oder Programmeinträge anders aussehen können.

Im Folgenden finden Sie einige Funktionen, welche nicht als Grundeinstellungen definiert sind, aber für Sie sinnvoll sein könnten. In die Einstellungen gelangen Sie über das Zahnradsymbol.



Automatischer Start mit Windows

Öffnen Sie die Einstellungen und setzen Sie unter *Allgemein* → *Programmstart* den Haken vor *KeePassXC beim Systemstart automatisch starten*.



Programm minimieren statt beenden

Wenn Sie verhindern möchten, dass sie das Programm aus Versehen durch einen Klick auf das „Schließen-X“ beenden, öffnen Sie die Einstellungen und setzen Sie unter *Allgemein* → *Benutzeroberfläche* den Haken vor *Minimieren, statt Programm zu beenden*.

