Windows

KeePassXC ist ein Passwortmanager, mit dem Sie Ihre Zugangsdaten für verschiedene Anwendungen und Webseiten sicher speichern können. Dadurch ist es einfach, für alle Zugänge sichere Passwörter zu verwenden, da Sie sich die Passwörter nicht merken müssen, sondern nur noch das Passwort für die Datenbank.

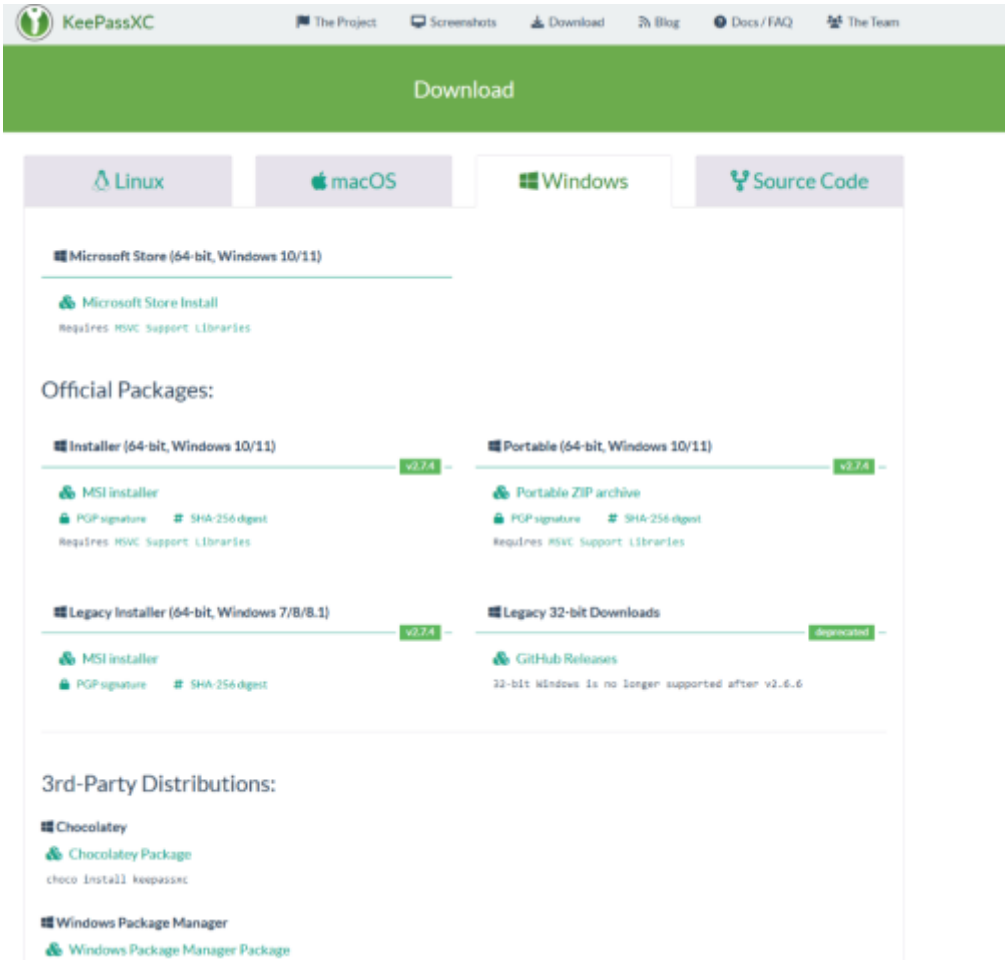
Zudem bietet KeePassXC eine Browser-Integration an, damit können die Anmeldedaten auf Webseiten direkt aus KeePassXC entnommen werden.

Installation

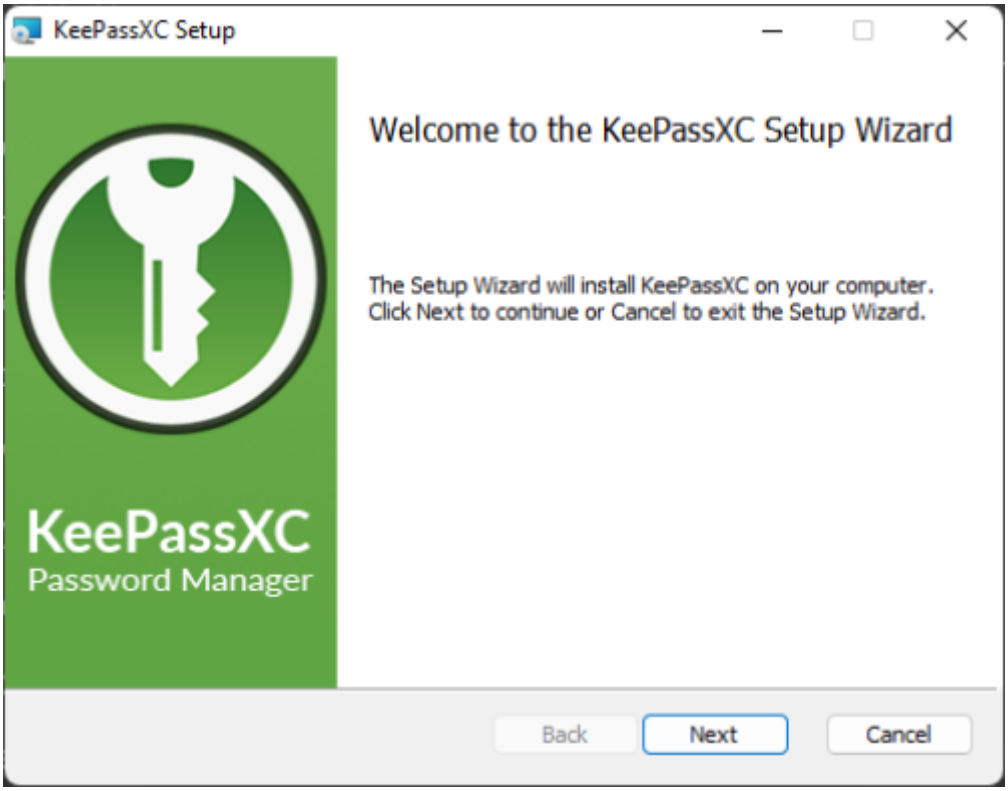
Im Folgenden wird gezeigt, wo Sie KeePassXC für Windows herunterladen und diesen auf Ihrem System installieren können.

KeePassXC wird auf allen Windows-Arbeitsplatz-Rechnern, die vom Rechenzentrum betreut werden, mittels Zenworks zur Verfügung gestellt. Dadurch wird die Software automatisch installiert und aktualisiert.

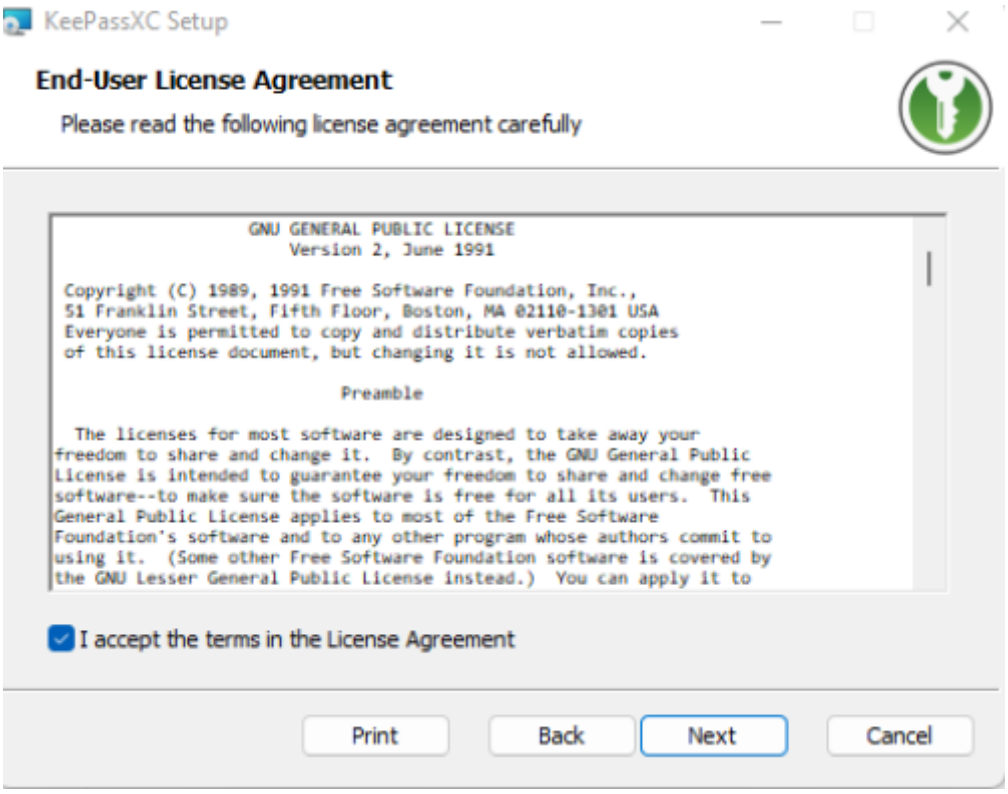
Laden Sie KeePassXC auf folgender Seite herunter: https://keepassxc.org/download/



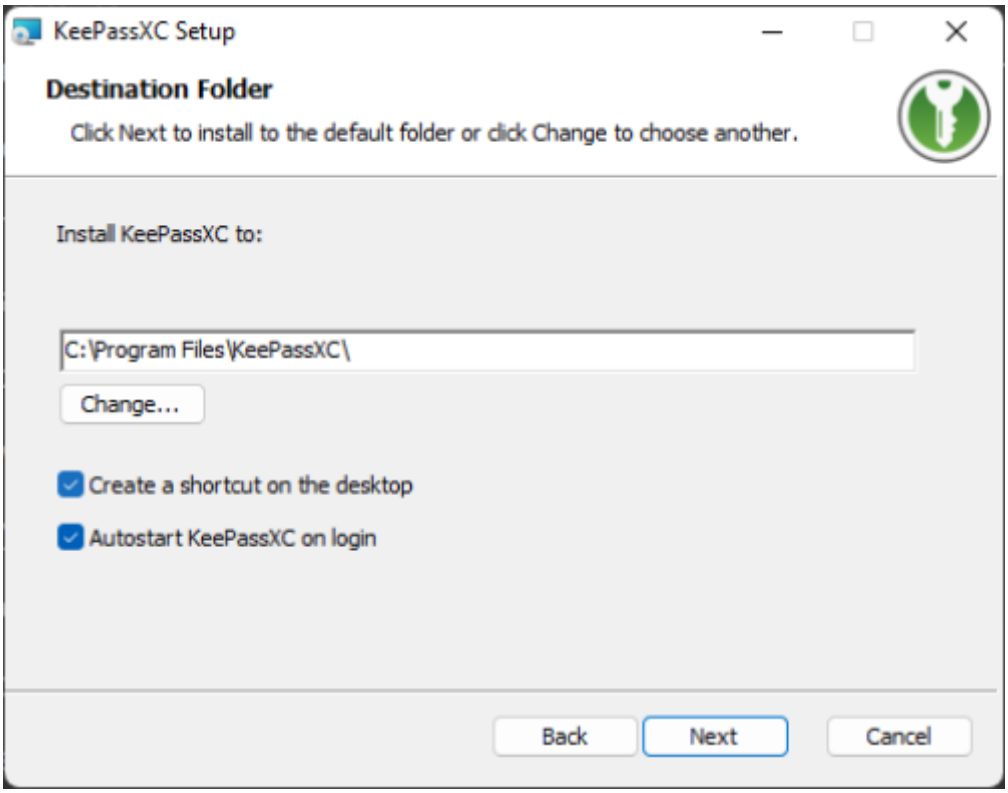
Führen Sie die heruntergeladene MSI aus und klicken Sie auf „Next“.



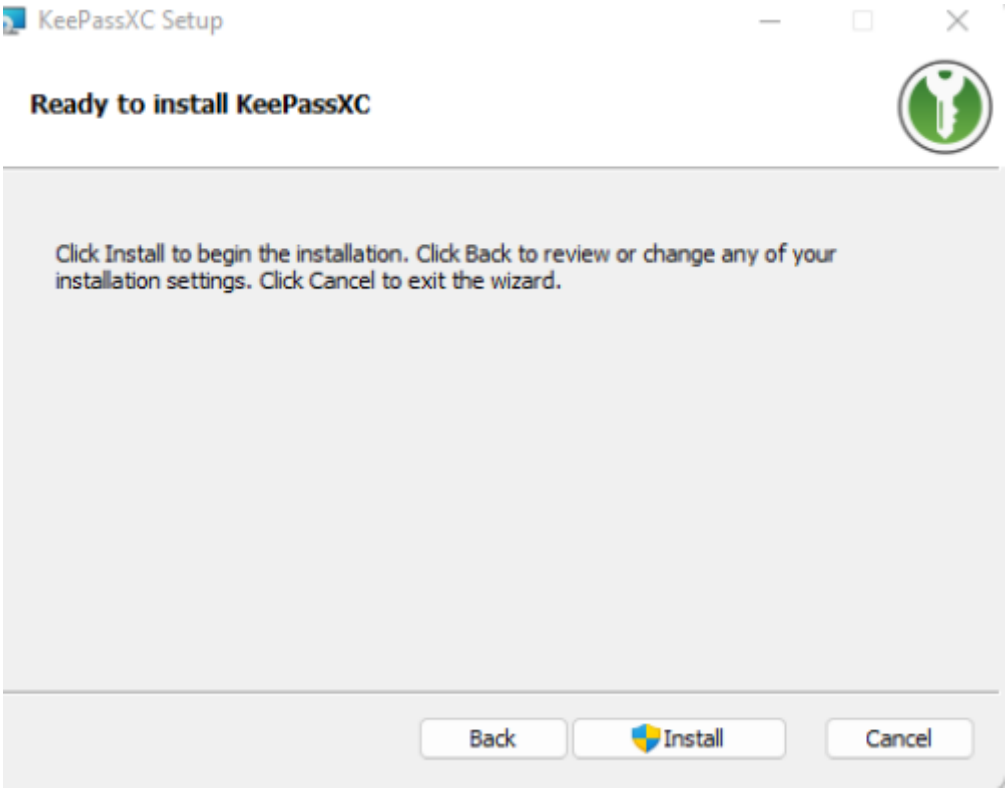
Akzeptieren Sie die Lizenzvereinbarung.



Bei Bedarf kann eine Desktopverknüpfung erstellt und das Programm in Autostart gepackt werden.



Klicken Sie auf „install“ und warten Sie, bis die Installation fertig ist.



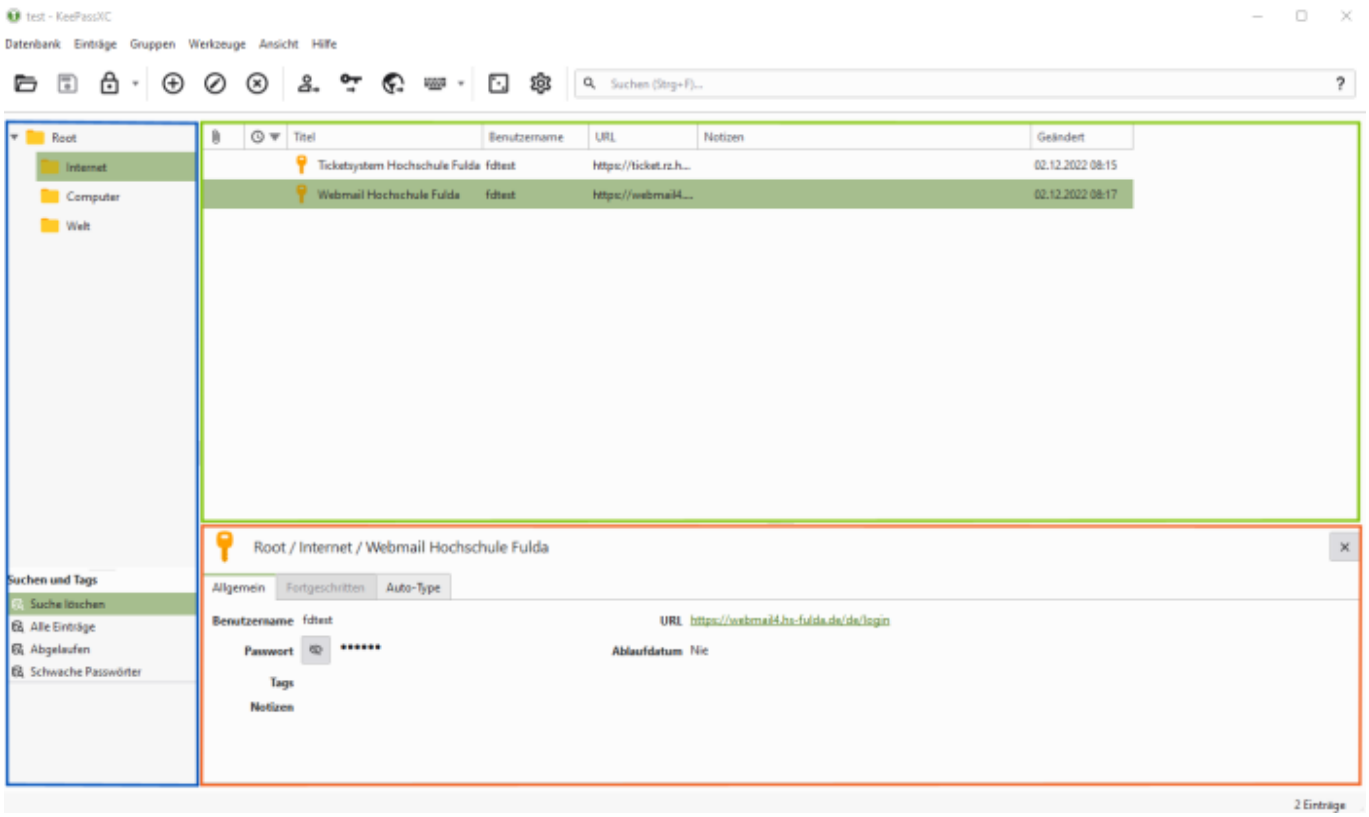
Symbolleiste

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.

(1) **Datenbank** - Datenbank öffnen, Datenbank speichern
(2) **Einträge** – neuen Eintrag erstellen, ausgewählten Eintrag bearbeiten, ausgewählten Eintrag löschen
(3) **Eintragsdaten** - Benutzername kopieren, Passwort kopieren, URL kopieren, Auto-Type durchführen
(4) **Alle Datenbanken sperren**: die Anwendung KeepassXC läuft weiter, aber zum Zugriff auf die Datenbank muss das Passwort erneut eingegeben werden
(5) **Werkzeuge** - Passwort-Generator, Anwendungseinstellungen
(6) **Suchen**

Aufbau der Anwendung

Die Hauptansicht der Datenbank ist in drei Bereiche aufgeteilt.

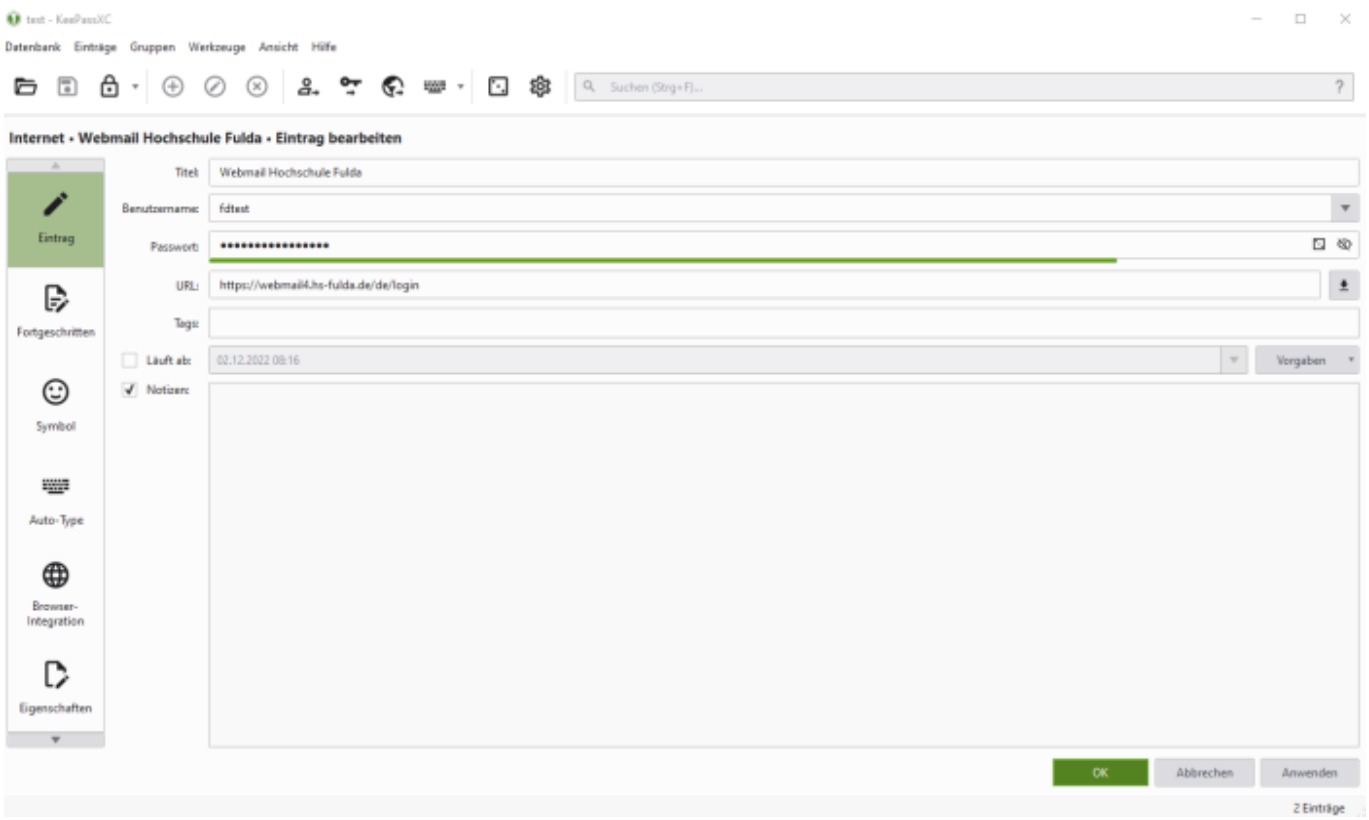


(1) **Gruppen** - unterhalb des Haupteintrags können Einträge und Gruppen liegen. Es empfiehlt sich, Einträge nach Themen in Gruppen zu ordnen. Innerhalb von Gruppen können wiederum Gruppen angelegt werden. Einstellungen aus übergeordneten Gruppen vererben sich auf darunterliegende Ebenen.

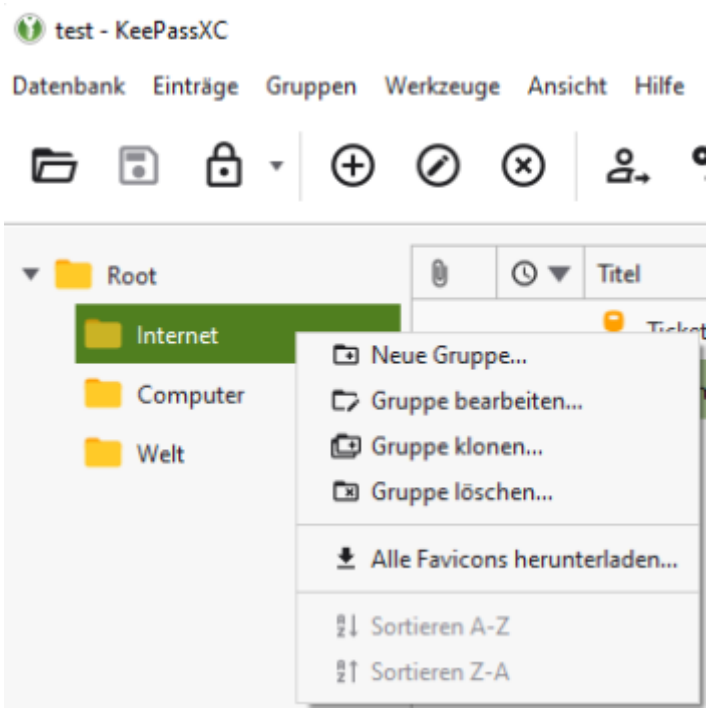
(2) **Einträge** – Für jede Website oder Anwendung, für die die Anmeldedaten in KeepassXC gespeichert werden sollen, wird ein Eintrag angelegt. Die Ansicht zeigt alle Einträge in der ausgewählten Gruppe an. Jede Spalte kann in der Größe verändert, neu geordnet und je nach Wunsch ein- oder ausgeblendet werden. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, um alle verfügbaren Optionen zu sehen.

(3) **Vorschau** - Zeigt eine Vorschau der ausgewählten Gruppe oder des ausgewählten Eintrags an. Die Vorschau kann mit der Schließen-Schaltfläche auf der rechten Seite vorübergehend ausgeblendet oder in den Anwendungseinstellungen komplett deaktiviert werden.

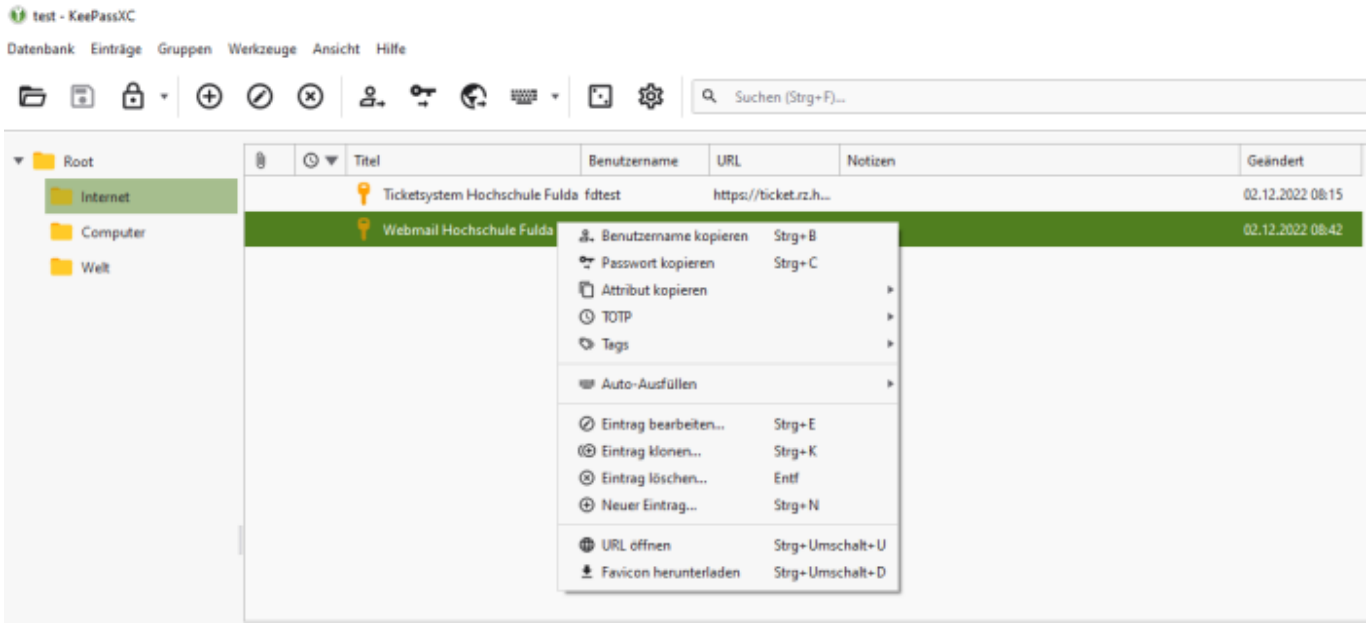
Nach einem Klick auf einen Eintrag in der Eintragsliste wird dieser in der Vorschau darunter angezeigt. Ein Doppelklick auf den Eintragstitel öffnet den Eintrag zur Bearbeitung. Unter „Titel“ wird ein Name für den Eintrag vergeben, der in der linken Spalte angezeigt wird, es folgen Benutzername und Passwort. Bei „URL“ kann man die Webseite eingeben, auf der man sich mit diesen Daten anmelden kann. Diese URL kannn direkt aus KeepassXC aufgerufen werden.



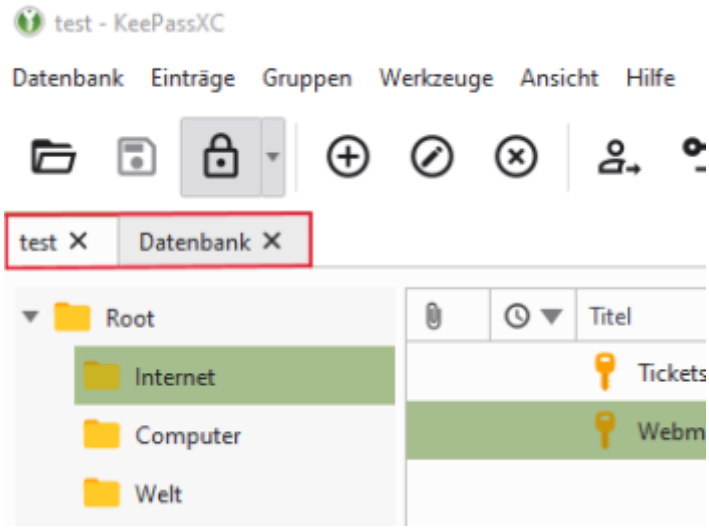
Bei einem Rechtsklick auf eine Gruppe öffnet sich das folgende Kontextmenü. Sie können neue Gruppen anlegen, die bestehende Gruppe bearbeiten oder löschen.



Bei einem Rechtsklick auf einen Eintrag wird das Kontextmenü für Einträge angezeigt. Wenn Sie die Webseite im Browser aufgerufen haben, für die Sie Zugangsdaten eingeben müssen, können Sie hier den Benutzernamen und anschließend das Passwort kopieren. Sie können auch den Eintrag bearbeiten oder einen neuen Eintrag anlegen.



Es können mehrere Datenbanken gleichzeitig geöffnet werden, sie werden dann in Registerkarten angezeigt.



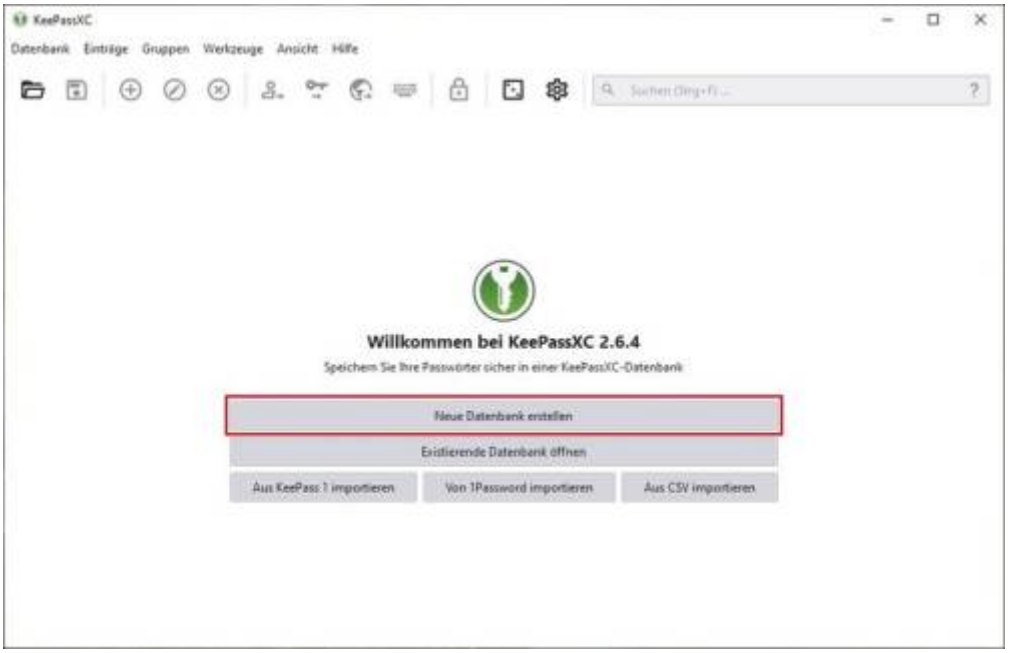
Datenbank erstellen

Eine Datenbank wird benötigt, um die Zugangsdaten der verschiedenen Programme und Webseiten in einer Datei zu speichern und bei Bedarf abzurufen.

Es ist empfehlenswert, die Datenbank auf eines Ihrer Netzlaufwerke zu sichern. Sollte die Datenbank ausversehen gelöscht werden, kann das Rechenzentrum bei Bedarf die Datei wiederherstellen.

Starten Sie KeePassXC und Klicken Sie auf die Schaltfläche „Neue Datenbank erstellen“. Die Funktion

finden Sie auch im Menüpunkt Datenbank.



Geben Sie einen Namen und eine Beschreibung für die neue Datenbank ein.

Es öffnet sich ein Fenster für die Verschlüsselungs-Einstellungen. Die Voreinstellungen können beibehalten werden. Klicken Sie auf weiter.

Vergeben Sie ein ein Passwort für Ihre Datenbank, das Sie im zweiten Feld wiederholen müssen. Sie können auch den Passwortgenerator benutzen, den Sie am Ende der ersten Zeile anklicken können.

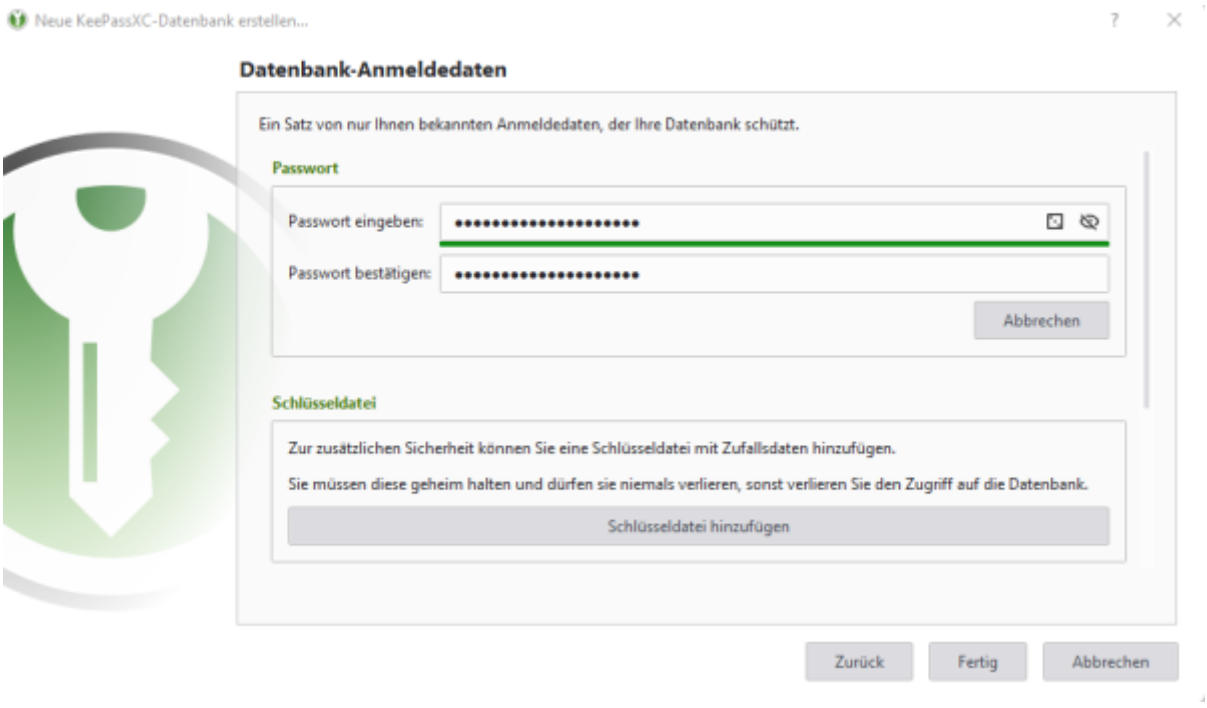
Um die Sicherheit zu erhöhen, kann **optional** eine Schlüsseldatei erzeugt werden. Diese wird bei Erstellung neben der Passworteingabe ebenfalls zwingend zum entsperren der Datenbank gebraucht!

Nach dem Klick auf Fertig, können Sie den Speicherort für Ihre Datenbank auswählen und die Datei speichern. Die Datenbank ist nun angelegt.

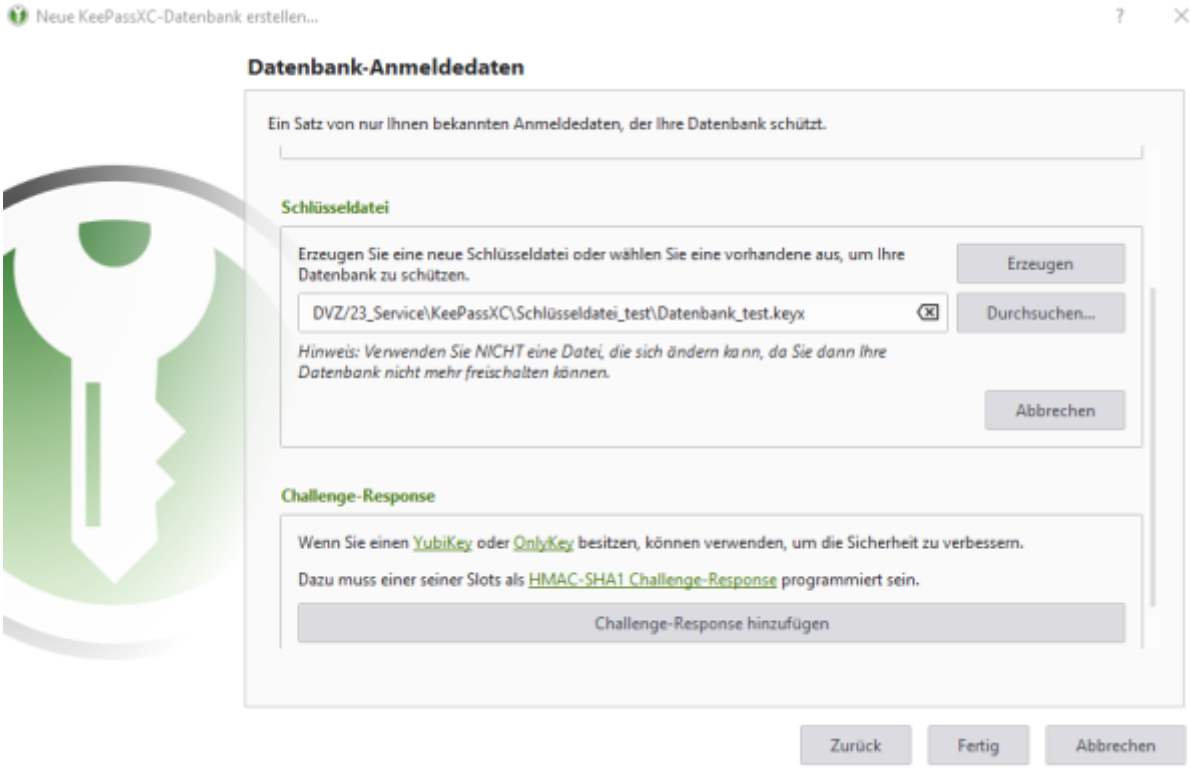
Wichtig Bewahren Sie dieses Passwort für Ihre Datenbank sicher auf. Am besten notieren Sie sich das Passwort und bewahren es an einem sicheren Ort auf. **Der Verlust des Datenbank-Passworts kann zu einer dauerhaften Sperrung Ihrer Datenbank führen** und Sie können die in der Datenbank gespeicherten Informationen nicht mehr abrufen.

Schlüsseldatei erzeugen

Wie bereits erwähnt, ist das Erzeugen der Schlüsseldatei optional. Klicken Sie im „Datenbank-Anmeldedaten“ Fenster auf „zusätzlichen Schutz hinzufügen“ und anschließend auf „Schlüsseldatei hinzufügen“.



Klicken Sie auf „Erzeugen“ und Sie werden gebeten, einen Speicherort und Dateinamen für die Sicherungsdatei auszuwählen.



Drücken Sie auf fertig und wählen denn Speicherort für Ihre Datenbank aus. Die Datenbank und die Schlüsseldatei sind nun erstellt.

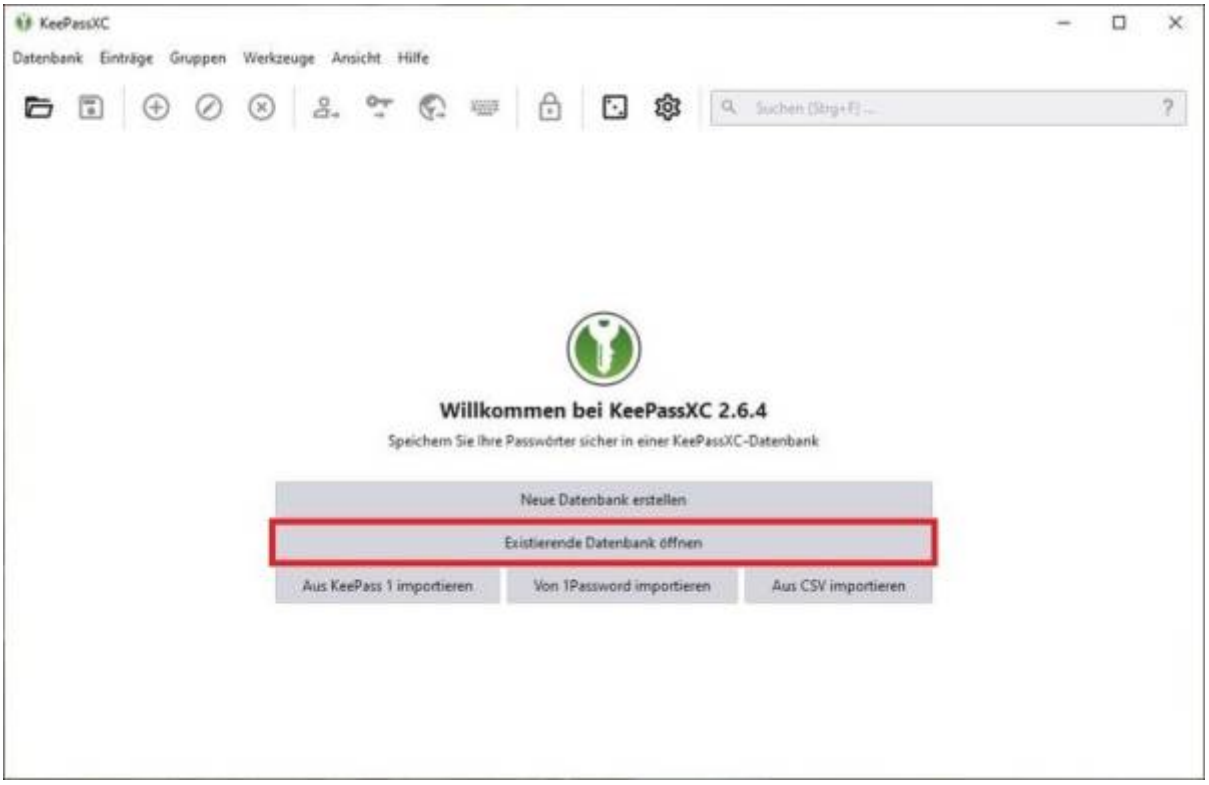
Auch hierbei ist es empfehlenswert, die Schlüsseldatei auf einem Netzlaufwerk zu sichern. Ebenso kann eine Kopie dieser Datei erstellt werden, um eine Backup-Datei zu haben, falls der Schlüssel gelöscht wird. **Bei Verlust der Sicherungsdatei verliert man dauerhaft den Zugriff auf die Datenbank!**

Existierende Datenbank öffnen

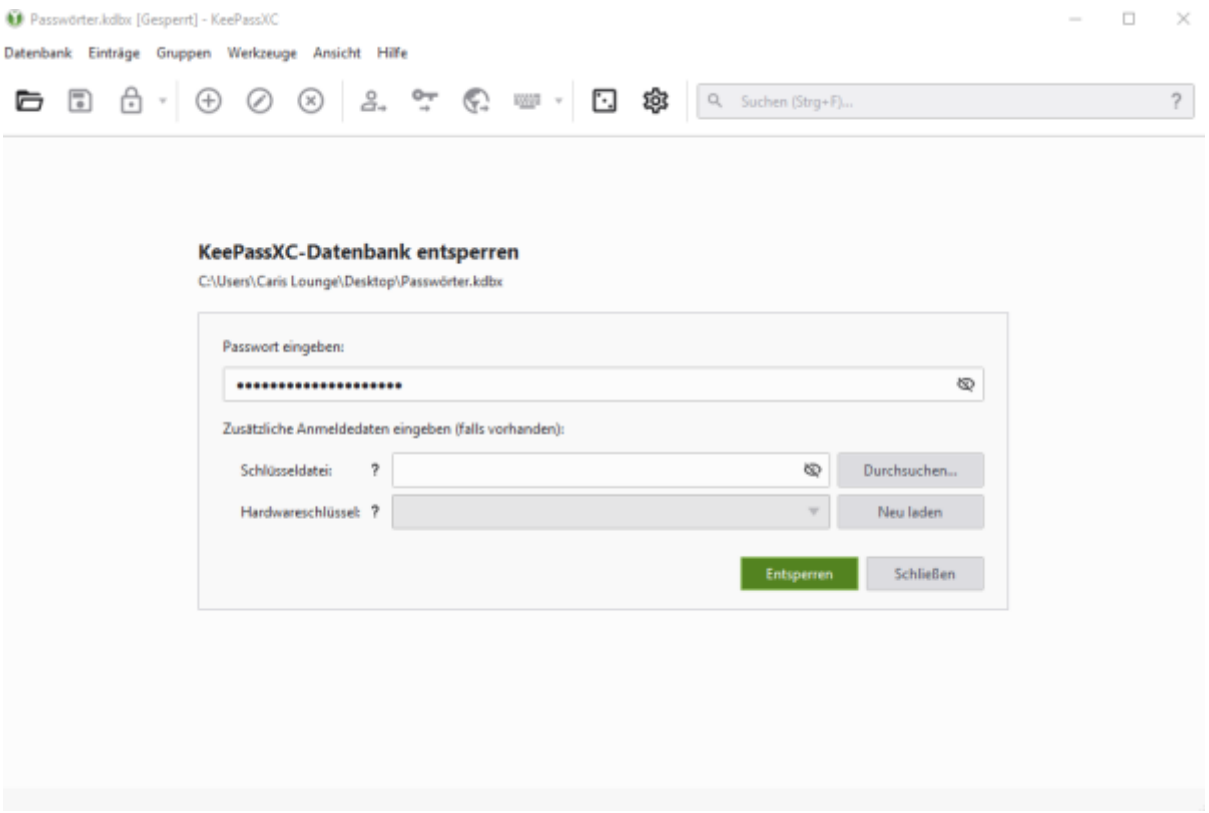
Wenn Sie auf mehreren Geräten arbeiten, können Sie in KeePassXC auf eine existierende Datenbank zugreifen. Ebenso in Abteilungen, wo allgemeine Zugangsdaten für mehrere Mitarbeiter*innen zur Verfügung gestellt werden, können die betreffenden Personen dieselbe Datenbank verwenden.

Eine Datenbank für KeePassXC wird im kdbx-Format abgelegt.

Öffnen Sie die KeepassXC-Anwendung. Klicken Sie auf die Schaltfläche „Existierende Datenbank öffnen“. Sie werden gebeten den Speicherort für die Datenbank (im kdbx.Format) herauszusuchen und zu öffnen.



Anschließend werden Sie gebeten, das Passwort der Datenbank einzugeben. Je nachdem, ob eine Schlüsseldatei als zusätzlicher Schutz hinzugefügt wurde, muss Diese ebenfalls geladen werden. Klicken Sie auf „Entsperren“ und die Datenbank ist nun verfügbar.



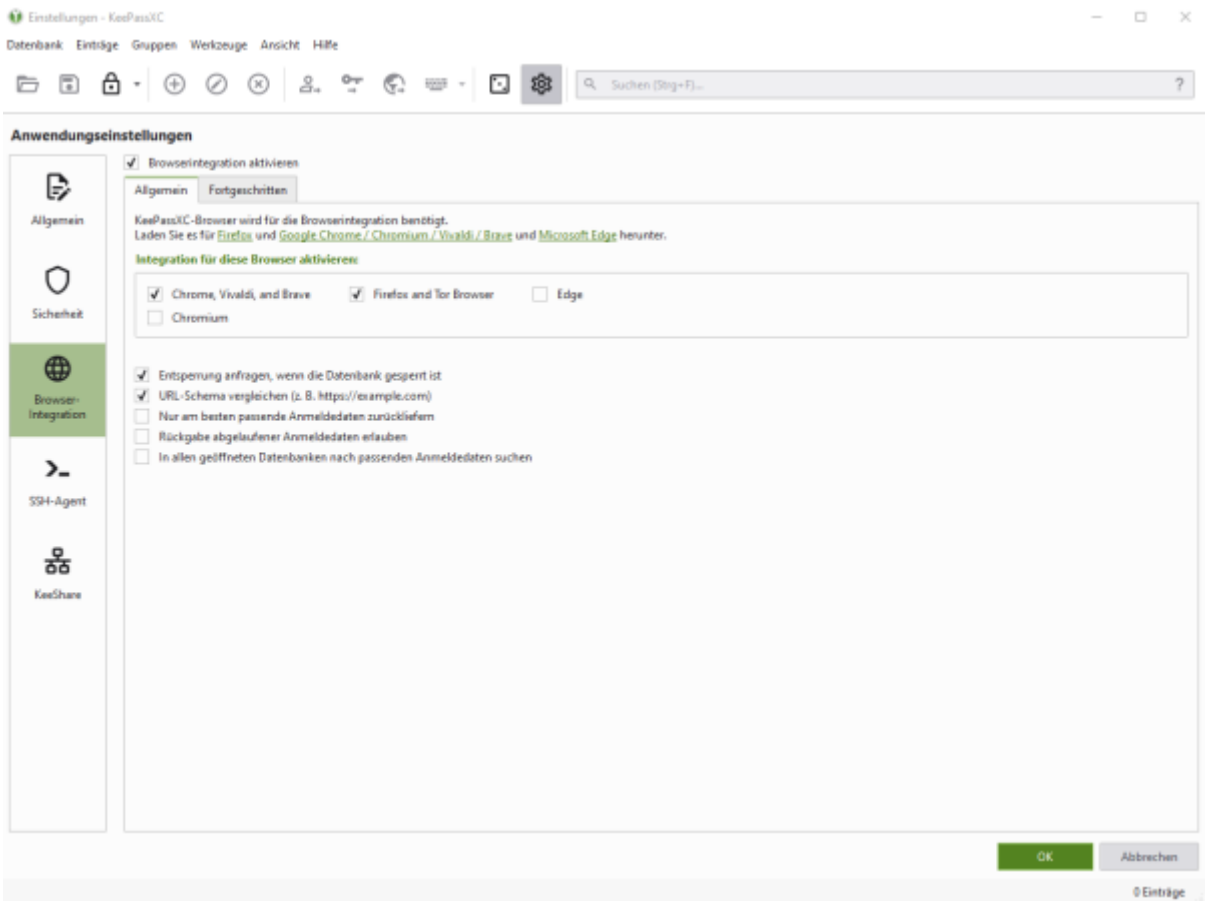
Browser-Integration

Durch die KeePassXC-Browser-Integration können die Benutzer automatisch Benutzernamen und Passwörter aus KeePassXC abrufen und direkt in die Anmeldefelder der Webseiten einfügen. Die Daten müssen nicht manuell aus der KeePassXC-Datenbank kopieren werden.

Um die Browser-Integration nutzen zu können, muss zum einen im KeePassXC die Funktion aktiviert werden und zum anderen das Plugin bzw. Add-on für den jeweiligen Browser installiert werden.

Browser-Integration im KeePassXC

Klicken Sie im KeePassXC auf das Zahnrad-Symbol und wählen „Browser-Integration“ aus. Dort setzen Sie den Haken bei „KeePassXC-Browser-Integration aktivieren“. Anschließend wählen Sie die Browser aus, mit denen Sie die KeePass-Erweiterung nutzen möchten und bestätigen mit „OK“.



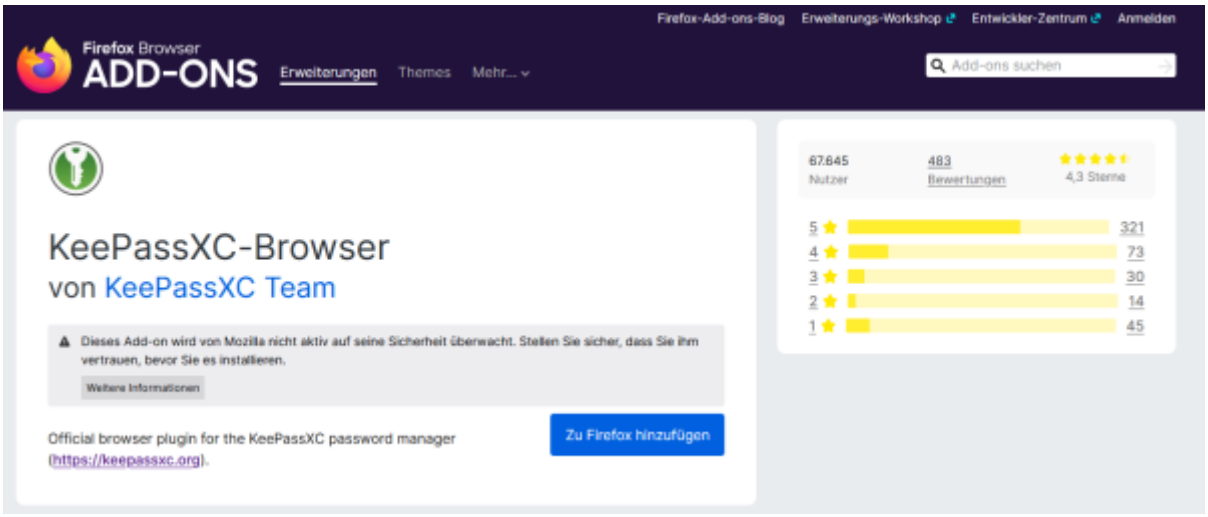
KeePassXC-Browser Erweiterung für Firefox

Die Browser-Erweiterung (auch Add-on genannt) muss für den jeweiligen Browser ebenfalls installiert werden, um die Funktionen von KeePassXC verwenden zu können.

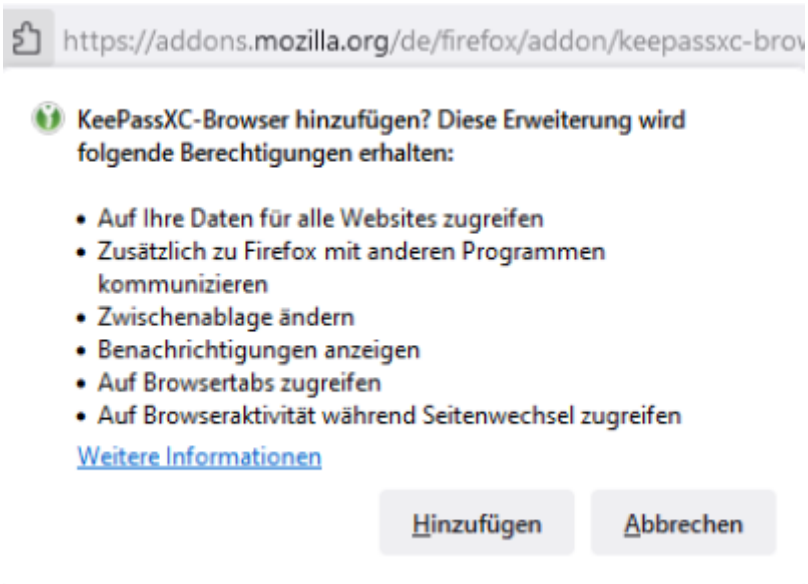
Die Geräte, welche vom Rechenzentrum betreut werden, sollten in der Regel mit den Add-ons für Firefox und Chrome automatisch installiert sein, sofern KeePassXC

eingerichtet ist.

Unter folgendem Link können Sie das Plugin installieren:
https://addons.mozilla.org/de/firefox/addon/keepassxc-browser/



Nachdem Sie „Zu Firefox hinzufügen“ angeklickt haben, taucht eine Meldung auf, in der die Berechtigungen für die Erweiterung aufgelistet werden. Wählen Sie „hinzufügen“ aus. Das Plugin ist installiert.



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

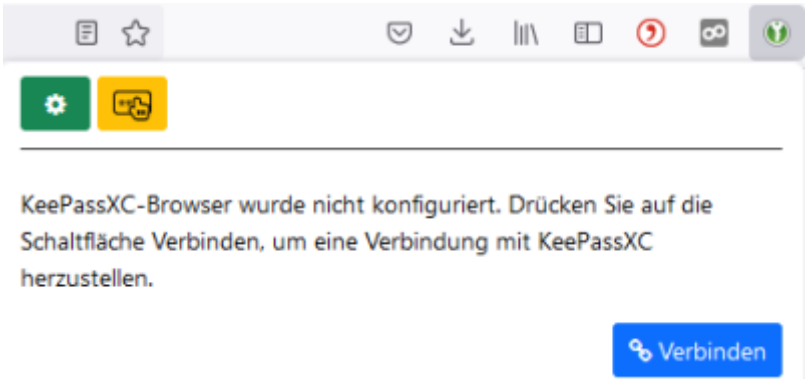
KeePassXC läuft nicht oder ist nicht verbunden.

Mit KeePassXC verbunden, aber die Datenbank ist gesperrt.

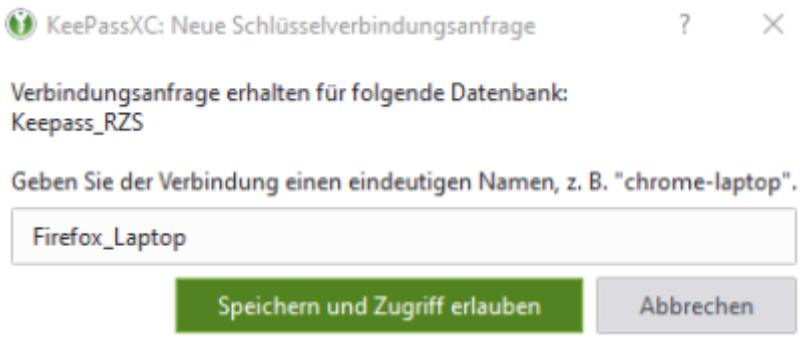
Verbunden mit KeePassXC und bereit zur Verwendung

Klicken Sie auf das Symbol und überprüfen den Status. Erscheint eine Fehlermeldung, überprüfen Sie, ob KeePassXC läuft und die Datenbank entsperrt ist. Nur dann funktioniert die Verbindung.

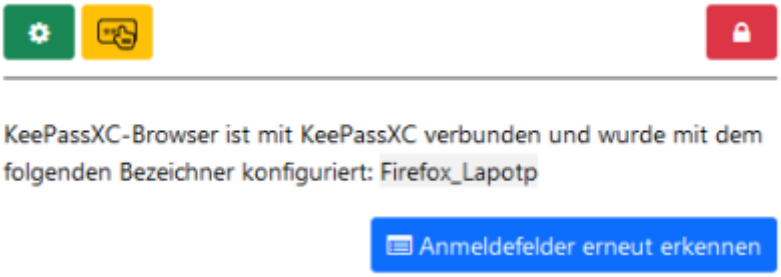
Wenn die Verbindung möglich ist erscheint eine Meldung, dass diese noch eingerichtet werden muss. Klicken Sie auf „Verbinden“.



KeePassXC meldet sich und fragt, ob Sie die „Neue Schlüsselverbindungsanfrage“ zulassen wollen. Wählen Sie einen eindeutigen Namen für diese Verbindung, z.B. „Firefox_Laptop“ und klicken Sie dann auf „Speichern und Zugriff erlauben“.



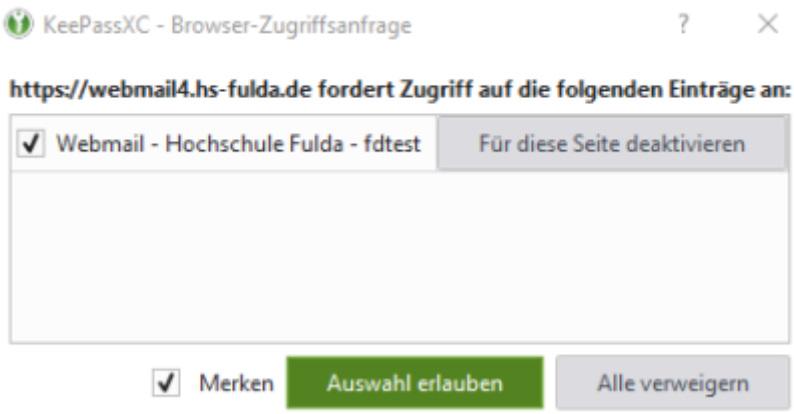
Damit ist die Verbindung hergestellt. Firefox kann jetzt auf die Passwörter zugreifen, die Sie in KeePassXC gespeichert haben.



Verwenden der Browser-Erweiterung

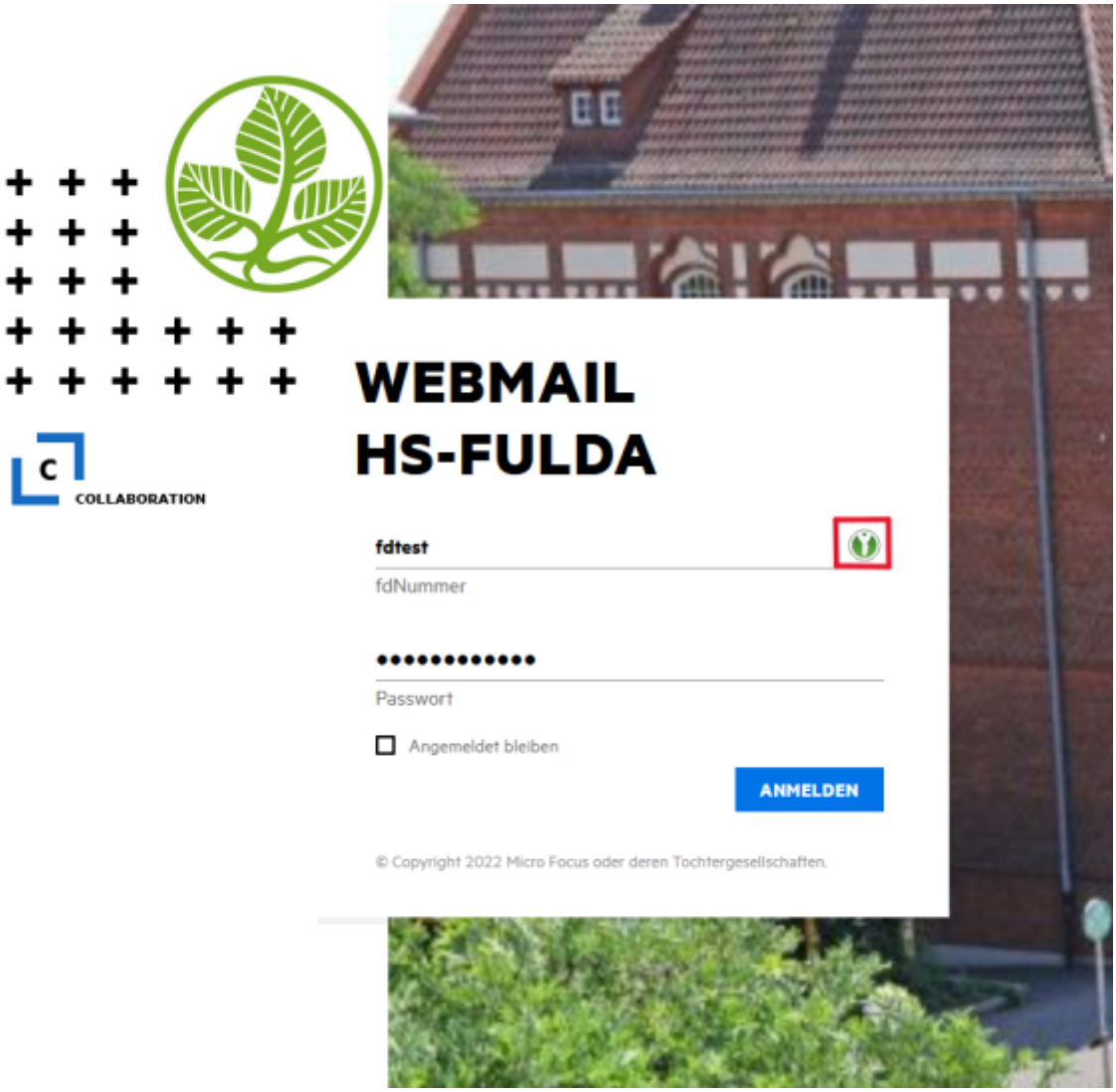
Um die Browser-Integration zu nutzen, starten Sie die Anwendung KeepassXC und entsperren Sie Ihre Datenbank. Im Webbrowser öffnen Sie die URL, die Sie mit Ihrer Datenbank verwenden möchten. Im Eingabefeld für den Benutzernamen ist das grüne KeepassXC-Symbol zu sehen. Wenn ein passender Eintrag in der Datenbank vorhanden ist, klicken Sie auf das grüne Schlüsselsymbol.

Es erscheint eine KeePassXC Browser-Zugriffsanfrage. Dort wird der passende Eintrag aufgelistet, das automatische Ausfüllen müssen Sie mit „Auswahl erlauben“ bestätigen. Ein Klick auf „Merken“ speichert diesen Zugriff für weitere Besuche auf dieser Seite. Die Anmeldefelder werden dann künftig automatisch ausgefüllt bei Betätigen des grünen Schlüsselsymbols.

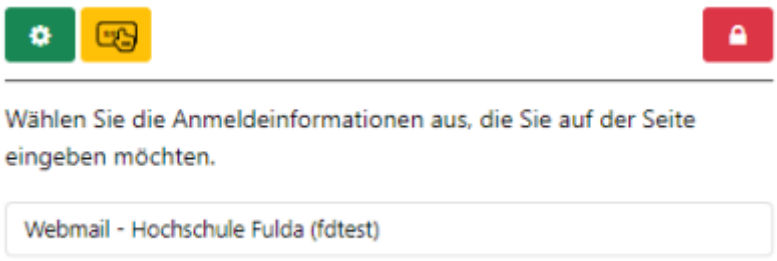


Das automatische Ausfüllen kann auf zwei Arten ausgeführt werden.

- Zum Einen können Sie neben dem Anmeldefenster von „Benutzername“ auf das grüne Schlüsselsymbol klicken. Ist die Berechtigung dauerhaft gespeichert, werden die Felder „Benutzername“ und „Passwort“ automatisch ausgefüllt.



- Zum Anderen können Sie in der rechten oberen Ecke auf das grüne Schlüsselsymbol klicken, dieses zeigt als Zusatz ein rotes Fragezeichen. Es öffnet sich ein Feld, wo passende Anmeldedaten für diese Webseite aufgelistet werden. Klicken Sie auf Ihre Anmeldedaten und die Zugangsdaten werden automatisch ausgefüllt.

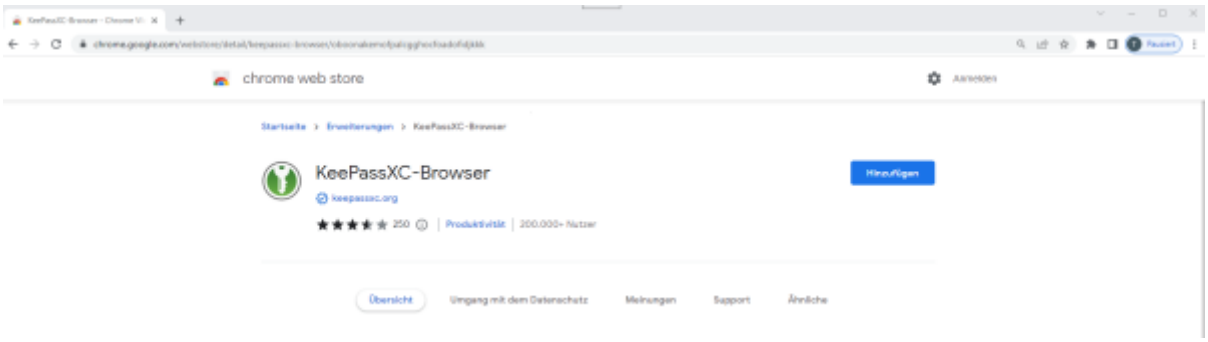


KeePassXC-Browser Erweiterung für Chrome

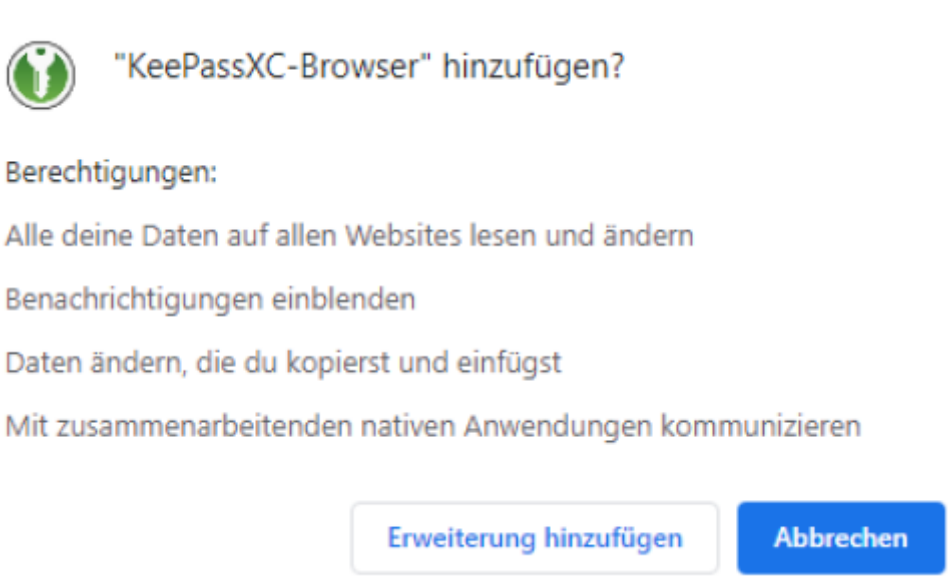
Die Browser-Erweiterung (auch Add-on genannt) muss für den jeweiligen Browser ebenfalls installiert werden, um die Funktionen von KeePassXC verwenden zu können.

Die Geräte, welche vom Rechenzentrum betreut werden, sollten in der Regel mit den Add-ons für Firefox und Chrome automatisch installiert sein, sofern KeePassXC eingerichtet ist.

Unter folgendem Link können Sie das Plugin installieren:
https://chrome.google.com/webstore/detail/keepassxc-browser/oboonakemofpalcgghocfoadofidjkkk



Nachdem Sie „Hinzufügen“ angeklickt haben, taucht eine Meldung auf, in der die Berechtigungen für die Erweiterung aufgelistet werden. Wählen Sie „Erweiterung hinzufügen“ aus. Das Plugin ist installiert.



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

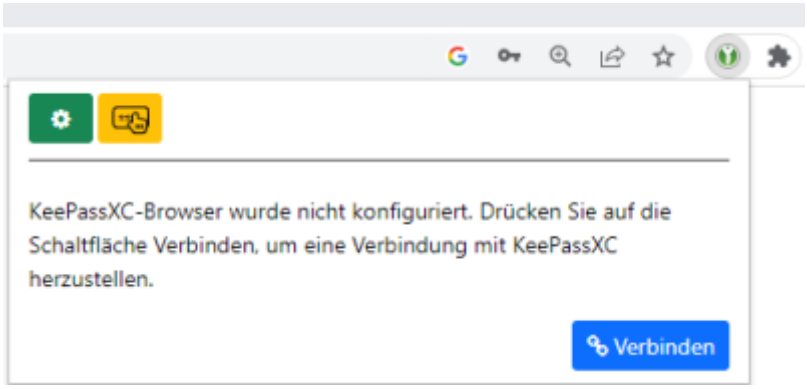
KeePassXC läuft nicht oder ist nicht verbunden.

Mit KeePassXC verbunden, aber die Datenbank ist gesperrt.

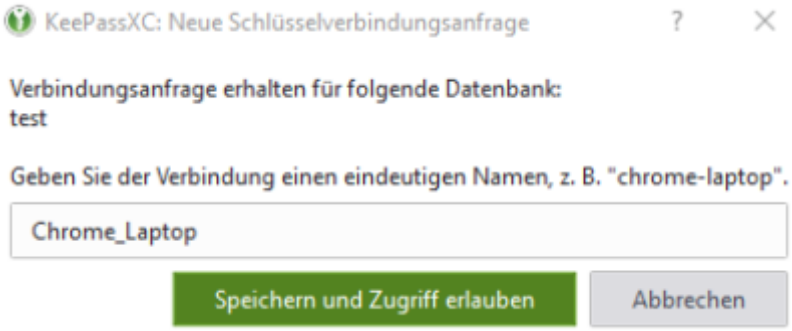
Verbunden mit KeePassXC und bereit zur Verwendung

Klicken Sie auf das Symbol und überprüfen den Status. Erscheint eine Fehlermeldung, überprüfen Sie, ob KeePassXC läuft und die Datenbank entsperrt ist. Nur dann funktioniert die Verbindung.

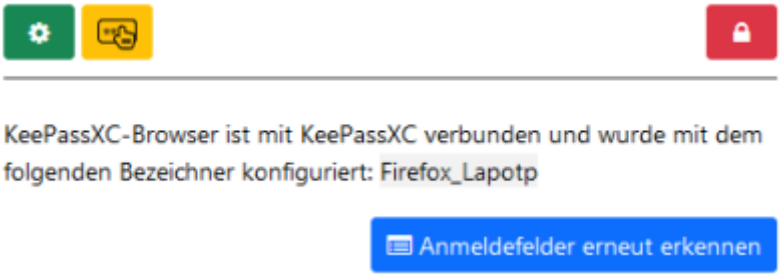
Wenn die Verbindung möglich ist erscheint eine Meldung, dass diese noch eingerichtet werden muss. Klicken Sie auf „Verbinden“.



KeePassXC meldet sich und fragt, ob Sie die „Neue Schlüsselverbindungsanfrage“ zulassen wollen. Wählen Sie einen eindeutigen Namen für diese Verbindung, z.B. „Chrome_Laptop“ 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.

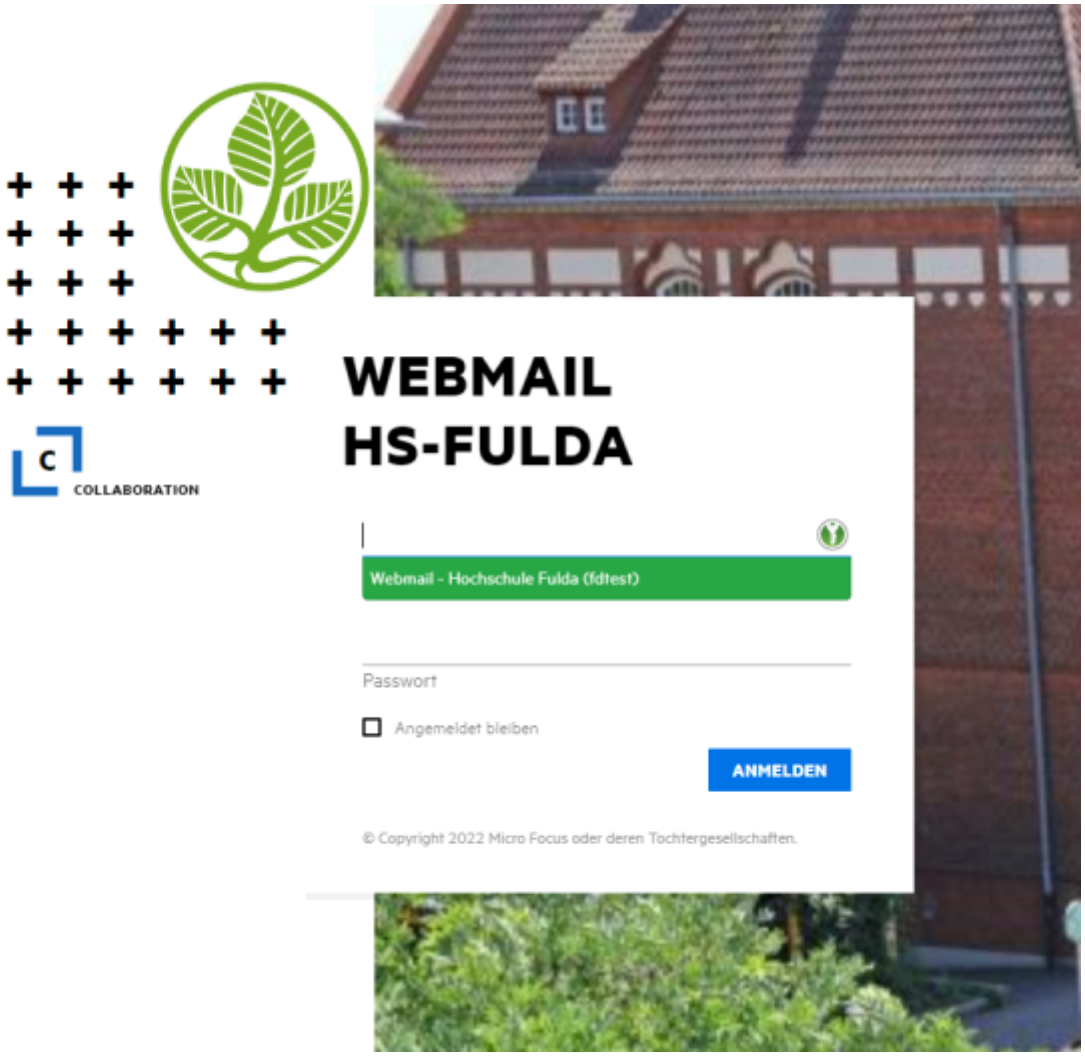


Verwenden der Browser-Erweiterung

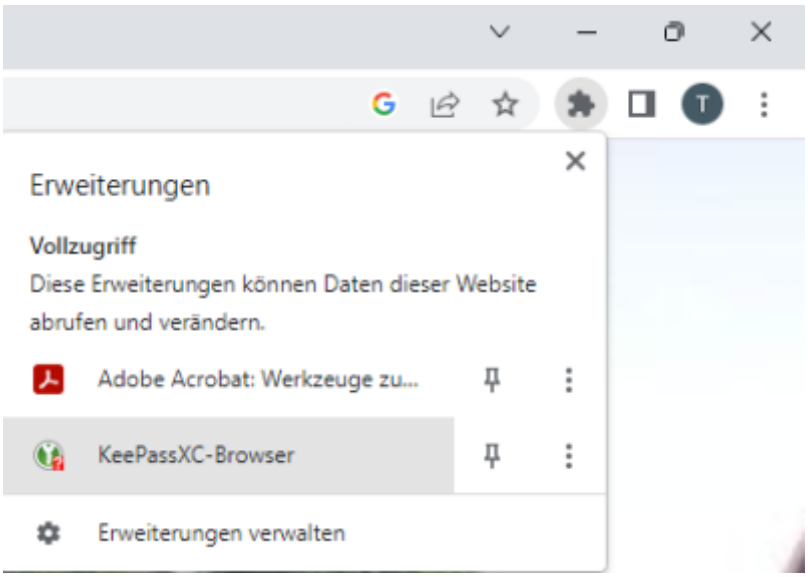
Um die Browser-Integration zu nutzen, starten Sie die Anwendung KeepassXC und entsperren Sie Ihre Datenbank. Im Webbrowser öffnen Sie die URL, die Sie mit Ihrer Datenbank verwenden möchten. Im Eingabefeld für den Benutzernamen ist das grüne KeepassXC-Symbol zu sehen.

Das automatische Ausfüllen kann auf zwei Arten ausgeführt werden.

- Zum Einen bekommen Sie mit Klick auf den Benutzernamen ein Feld angezeigt, wenn ein passender Eintrag für diese Webseite vorhanden ist. Mit Klick darauf, werden die Anmeldedaten für „Benutzername“ und „Passwort“ automatisch ausgefüllt.

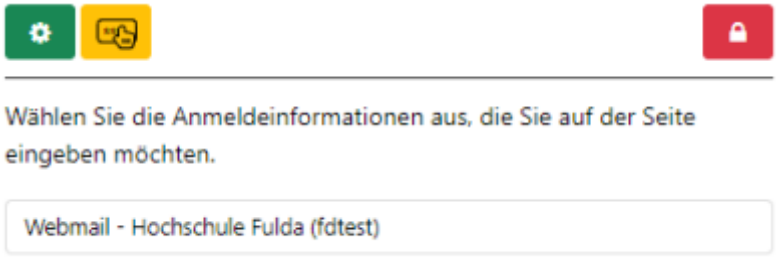


- Zum Anderen können Sie in der rechten oberen Ecke auf das „Puzzle-Symbol“ klicken. Dort öffnen Sich Ihre installierten Erweiterungen. Wählen Sie „KeePassXC-Browser“ aus.



Es öffnet sich ein Feld, wo passende Anmeldedaten für diese Webseite aufgelistet werden. Klicken Sie

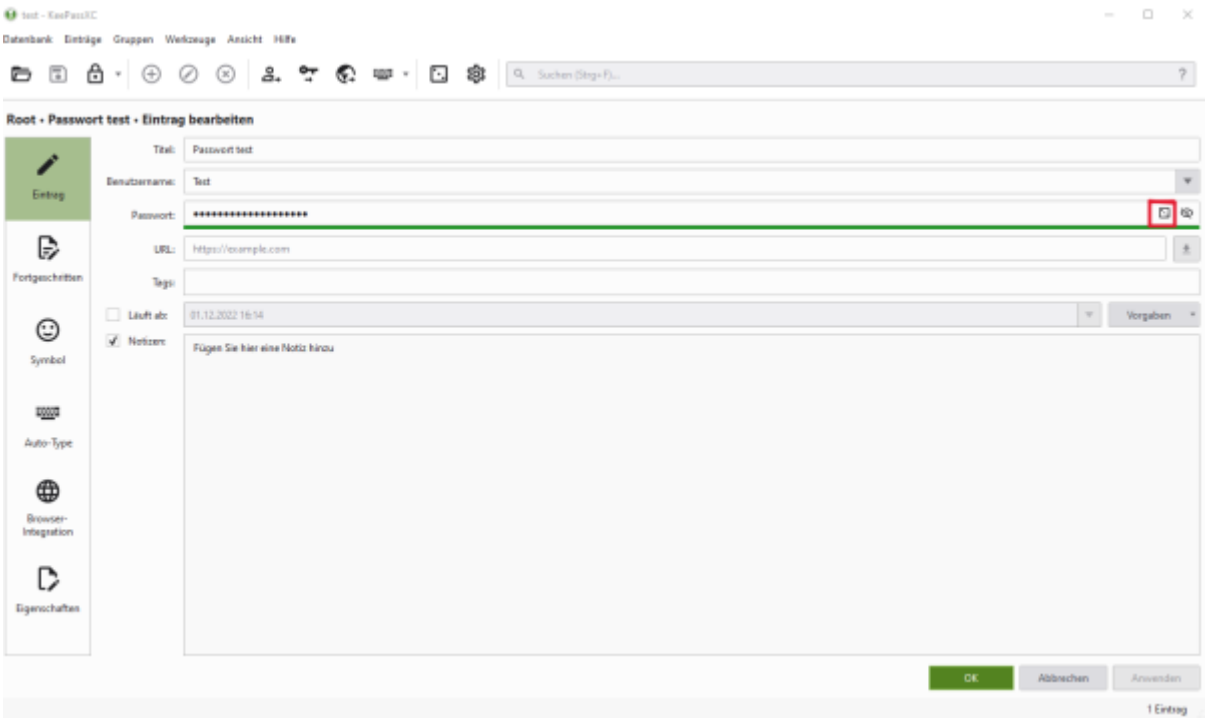
auf Ihre Anmeldedaten und die Zugangsdaten werden automatisch ausgefüllt.



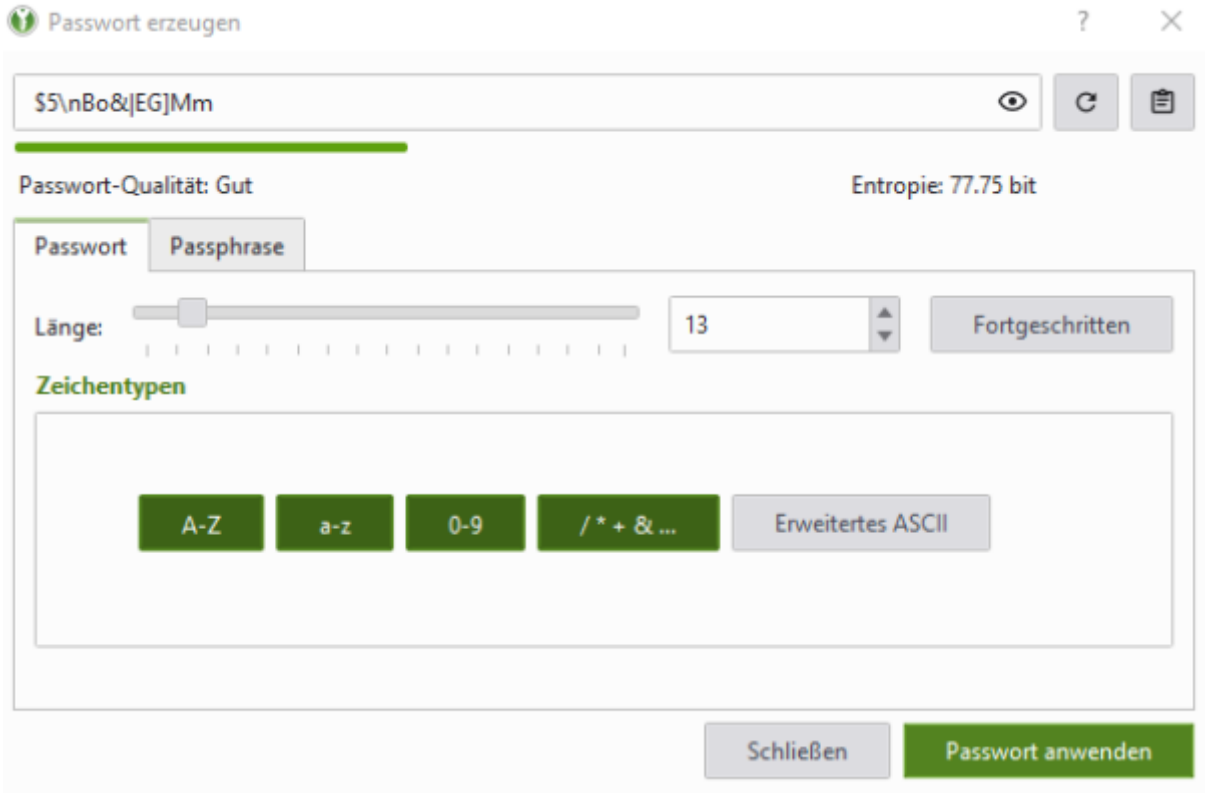
Passwortgenerator

Mit dem Passwortgenerator können Sie zufällige, starke Passwörter oder Passphrasen generieren, die Sie für Ihre Anwendungen und die von Ihnen besuchten Webseiten verwenden können.

Klicken Sie 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.



Abschließend klicken Sie auf „Passwort anwenden“ und das Passwort wird übernommen.