IQ.SH
Institut für Qualitätsentwicklung
an Schulen Schleswig-Holstein
des Ministeriums für Bildung,
Wissenschaft und Kultur
des Landes Schleswig-Holstein

ANLEITUNG –

PASSWORTMANAGER KEEPASSXC AUF LEHRKRÄFTE-ENDGERÄTEN (WINDOWS)

Letzte Änderung: 22.02.2022

IQ.SH
Institut für Qualitätsentwicklung an Schulen Schleswig-Holstein
des Ministeriums für Bildung, Wissenschaft und Kultur des Landes Schleswig-Holstein

1 Einleitung

Auf den Lehrkräfte-Endgeräten ist die Speicherung von Passwörtern direkt im Browser nicht möglich. Daher wird der Passwortmanager KeepassXC für die Verwaltung Ihrer Zugangsdaten zur Verfügung gestellt. Diese werden dann in einer verschlüsselten Datenbank gespeichert.

Die Software kann über den internen Appstore (Hub) installiert werden. Eine Anleitung für die Softwareinstallation über den Appstore ist im Handbuch - Endgeräte für Lehrkräfte (Windows) enthalten.

1.1 Vorteile von KeePassXC als Passwortmanager

- Sie müssen sich nur noch ein einziges Passwort merken, nämlich das zum Entschlüsseln der Datenbank.
- Sie können die verschlüsselte Datenbank (*.kdbx-Datei) einfach und ohne Bedenken auf ein externes Backup-Medium kopieren.
- Das Browser-Plugin (s. Kapitel 6) liefert eine ähnliche Funktionalität wie die im Browser verfügbare Passwortverwaltung, ohne dass die Passwörter direkt im Browser gespeichert werden. Dies erhöht die IT-Sicherheit, bei vergleichbarem Komfort.

1.2 Risiken bei der Nutzung

- Wenn Sie das Passwort zur Datenbank vergessen und die in der Datenbank hinterlegten Passwörter nicht auswendig wissen, können Sie je nach Account nur über das Zurücksetzen des Passworts (solange Sie noch Zugriff auf Ihre Emails haben), den entsprechenden IT-Support oder gar nicht mehr auf Ihre Accounts zugreifen.
- Bei der Nutzung eines Passwortmanagers ist zu beachten, dass dieser niemals auf einem unbeaufsichtigten, entsperrten Computer z. B. im Klassenraum geöffnet sein darf. In diesem Fall wären alle Ihre Passwörter für die Personen im Raum einseh-, kopier- und veränderbar. Um dieses Risiko zu senken, gibt es einen automatischen Sperrmechanismus, dessen Aktivierung in Kapitel 2 beschrieben wird.

1.3 Exkurs: Sichere, merkbare Passwörter

Detaillierte Informationen zum Thema „Sichere Passwörter erstellen“ liefert das Bundesamt für Sicherheit in der Informationstechnik (BSI). Im Kern geht aus diesen Informationen hervor, dass sichere Passwörter entweder komplex oder lang sind und in keinem (Wörter-)Buch vorkommen. Um diese Eigenschaften zu erreichen gibt es verschiedene Methoden.

Beispielmethode (Komplexität, mind. 8 Zeichen):

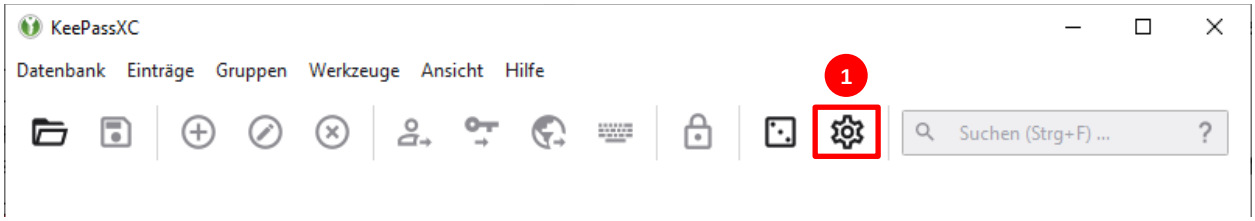
1. Wählen Sie einen Satz, z. B.: Ich esse jeden Tag eine warme Mahlzeit und am Sonntag zwei.
2. Ersetzen Sie einige Wörter durch Zahlen und Sonderzeichen: Ich esse jeden Tag 1 warme Mahlzeit + am Sonntag 2.
3. Reduzieren Sie den Satz auf die Anfangsbuchstaben, Zahlen und Sonderzeichen: IejT1wM+aS2.

Beispielmethode (Länge mind. 20 Zeichen):

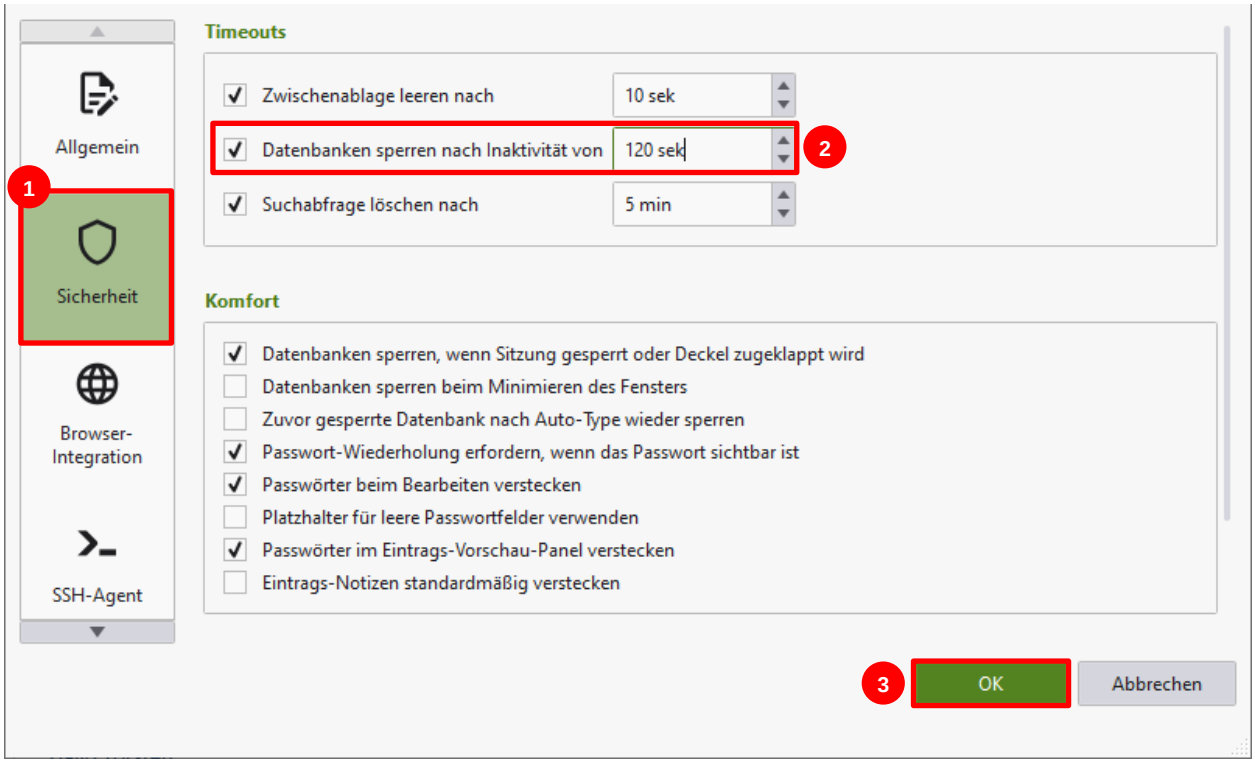
- Bilden Sie einen „Blödsinn-Satz“, den Sie sich gut merken können z. B.: Magier trinken Bromthymolblau huepfend in Clausthal.
- Fügen Sie dem Satz entsprechend der ggf. vorhandenen Passwortregeln z. B. noch Zahlen hinzu. Leerzeichen werden i. d. R. als Sonderzeichen akzeptiert. Sollte dies nicht der Fall sein, können die Leerzeichen durch andere Sonderzeichen ersetzt werden: Magi3r+trink3n+Bromthymolblau+hu3pf3nd+in+Clausthal.
- Um den Satz im Notfall zu rekonstruieren, kann auch eine durch Angreifer/innen nur schwer simulierbare Methodik für das Finden der Wörter gewählt werden. Z. B. können Sie aus ihren 6 Lieblingsbüchern das jeweils 15. Wort auf der 15. Seite wählen.

2 Grundeinstellungen anpassen

Noch bevor die erste Passwortdatenbank erzeugt wird, empfiehlt es sich die Sicherheitseinstellungen auf den Einsatz in Schule zu optimieren. Hierfür wird innerhalb der Software KeePassXC das Zahnradsymbol (1) gewählt.



Daraufhin öffnen sich die Einstellungen in der Ansicht „Allgemein“. Durch die Wahl der Kachel „Sicherheit“ (1) wird die Ansicht gewechselt.

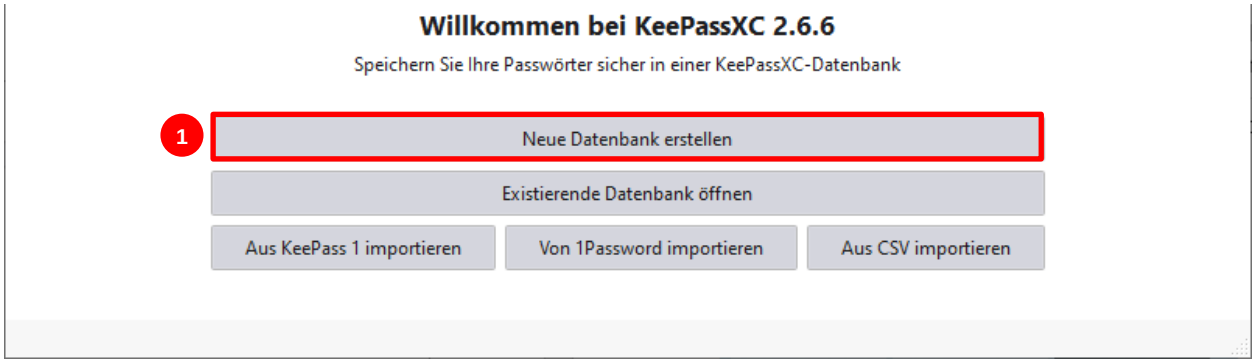


Nun muss das Häkchen (2) bei „Datenbanken sperren nach Inaktivität von“ gesetzt und eine sinnvolle Sekundenzahl (z. B. 240 Sekunden) eingetragen werden. Dies sorgt dafür, dass die Datenbank nach Ablauf der definierten Sekundenzahl ab dem Zeitpunkt der letzten Nutzung automatisch wieder verschlüsselt wird. Bestätigen Sie die Einstellung mit „OK“ (3).

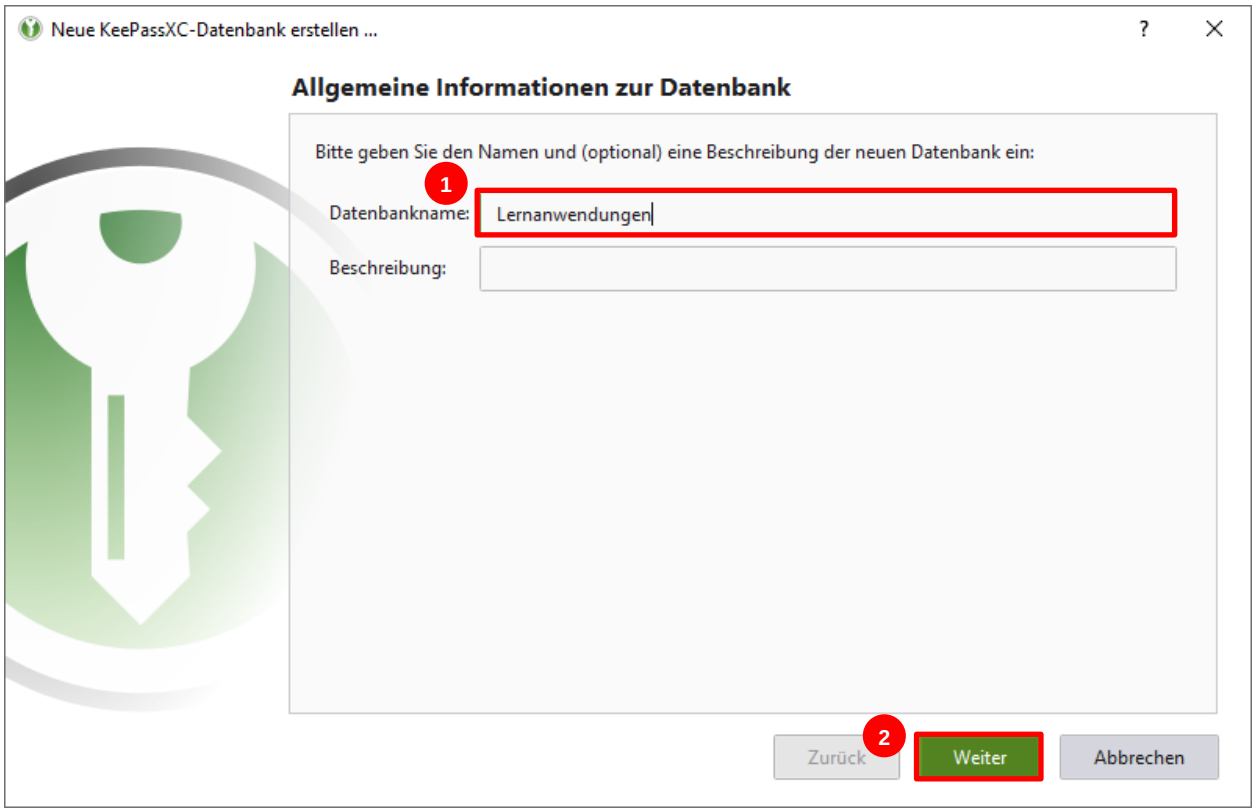
Hinweis: Das Setzen des Häkchens (2) ist eine Zusatzsicherung, für den Fall, dass Sie den Passwort-Manager in einem Raum nutzen, in dem sich auch andere Personen befinden (Klassenraum, Lehrerzimmer), Sie den Raum spontan ohne ihr Endgerät verlassen und dabei vergessen den Bildschirm mit „Windows-Taste + L“ zu sperren (vgl. 1.2).

3 Neue Passwortdatenbank erzeugen

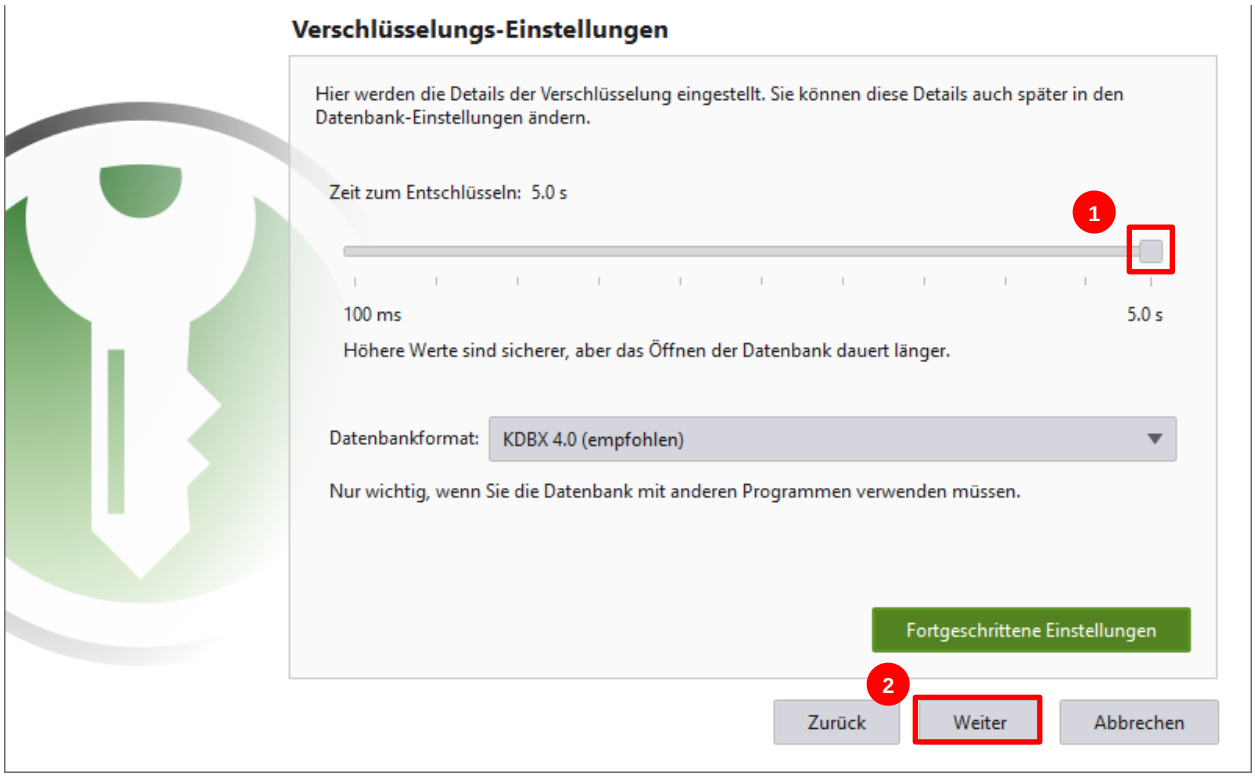
Wählen Sie die Option „Neue Datenbank erstellen“ (1):



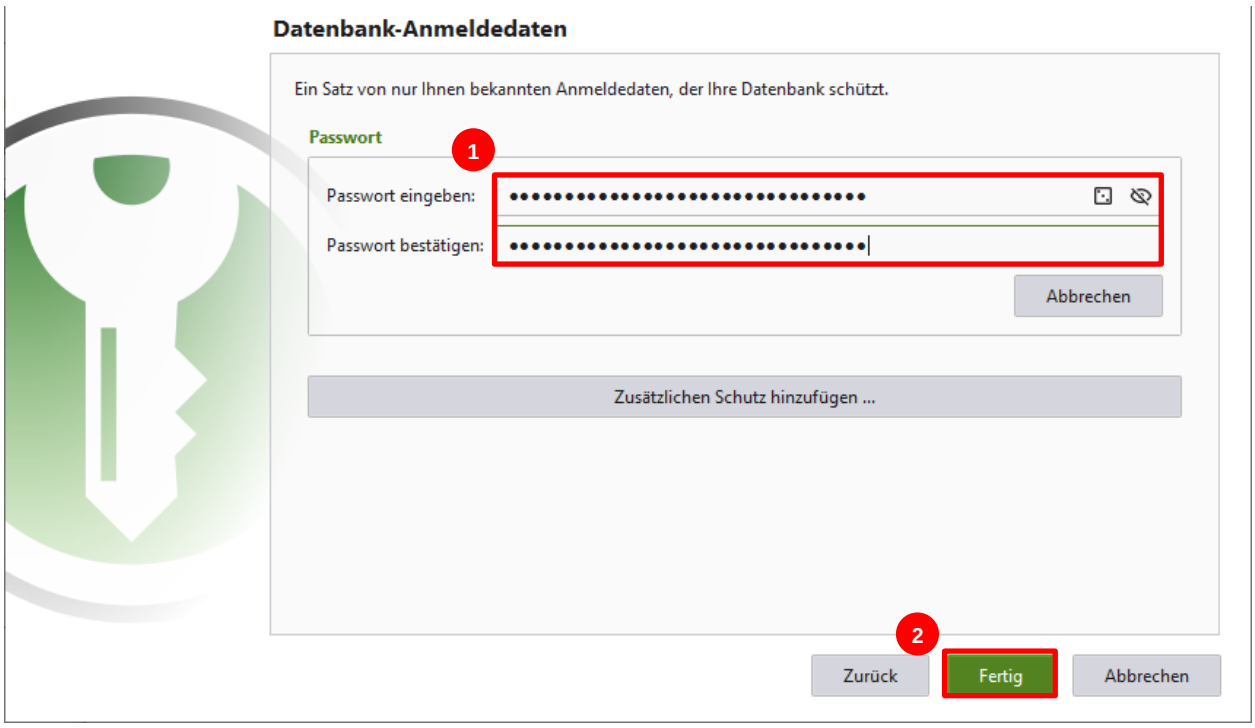
Wählen Sie einen sinnvollen Datenbanknamen (1) und bestätigen mit „Weiter“ (2):



Im nächsten Schritt muss die Sicherheit der Verschlüsselung eingestellt werden. Es wird die maximale Sicherheit empfohlen (1). Bestätigen Sie mit „Weiter“ (2):



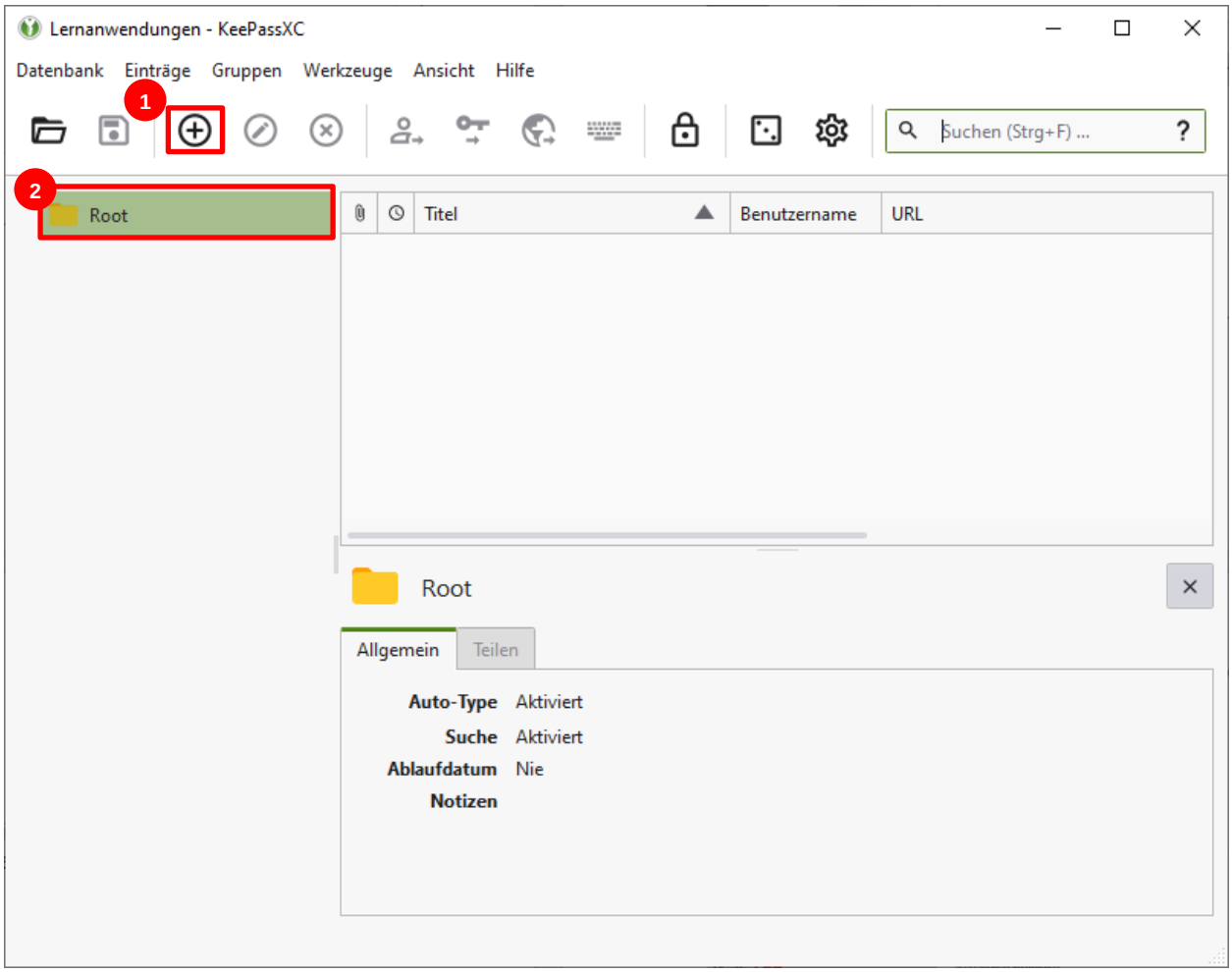
Wählen Sie jetzt ein sicheres, gut merkbares Passwort (1) zum Verschlüsseln/Entschlüsseln der Datenbank. Orientieren Sie sich hierfür an den Methoden aus 1.3.



Nach dem Bestätigen durch „Fertig“ (2) öffnet sich ein Fenster, über welches der Speicherort und der Dateiname festgelegt werden muss. Als Speicherort sollte der vorgeschlagene Ordner „Dokumente“ verwendet werden. Als Dateiname sollte derselbe Name gewählt werden, der für die Datenbank benutzt wurde (siehe oben). Nach dem Speichern der Datei, wird die neu erzeugte Datenbank angezeigt. Diese beinhaltet standardmäßig eine leere Gruppe „Root“.

4 Neuen Datenbankeintrag anlegen

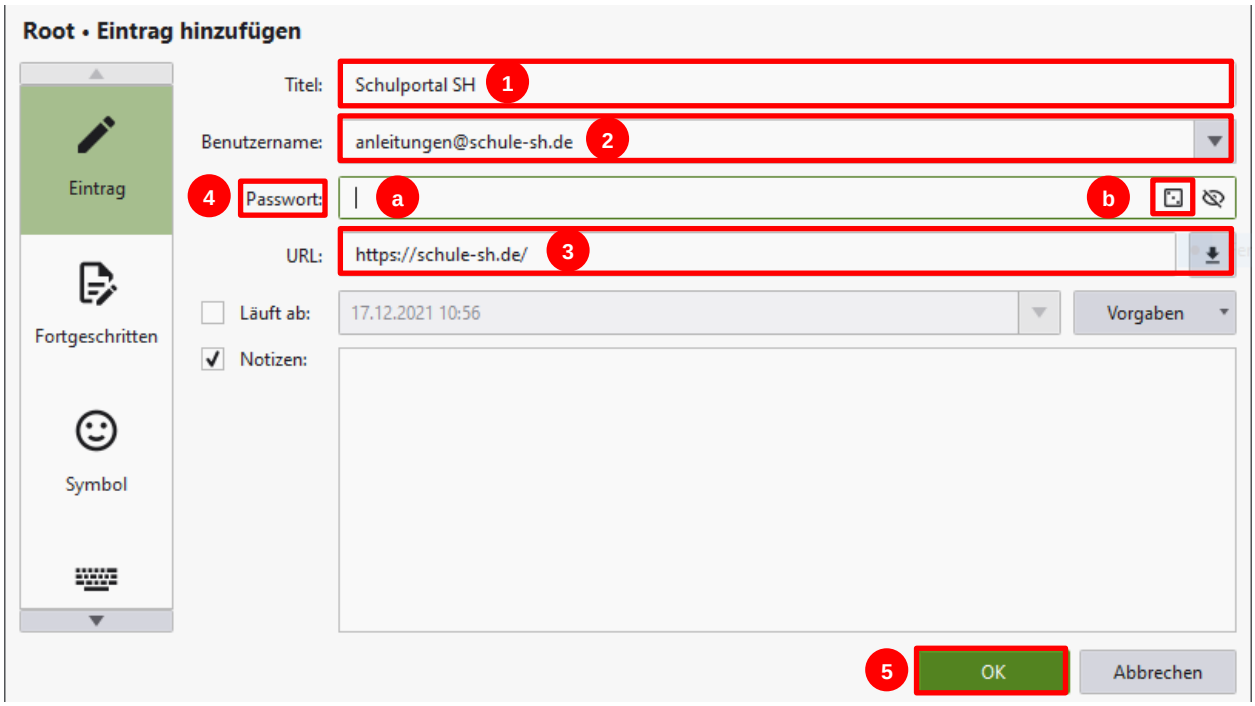
Drücken Sie das Plus-Symbol (1), um der Datenbank einen neuen Satz Zugangsdaten hinzuzufügen. Der Eintrag wird in der Gruppe „Root“ (2) erzeugt.



Hinweis: Durch Rechtsklick auf die Gruppe „Root“ (2) können Sie Untergruppen erzeugen oder die Gruppe umbenennen.

Wählen Sie einen Anzeigenamen bzw. „Titel“ (1) für den neuen Eintrag in der Datenbank. Hinterlegen Sie den „Benutzernamen“ (2). Je nach Account kann es sich hierbei z.B. auch um Ihre Emailadresse handeln. Wenn es sich bei dem Account, um ein Web-Konto handelt, können Sie die entsprechende „URL“ (3) hinzufügen. Beim Passworteintrag haben Sie zwei Optionen: Entweder Sie tragen ein existierendes Passwort händisch (a) in das Feld „Passwort“ (4) ein

oder Sie lassen sich ein sicheres Passwort erzeugen, indem Sie das Würfel-Symbol (b) drücken. Um den Datenbankeintrag anzulegen, abschließend mit „OK“ (5) bestätigen.

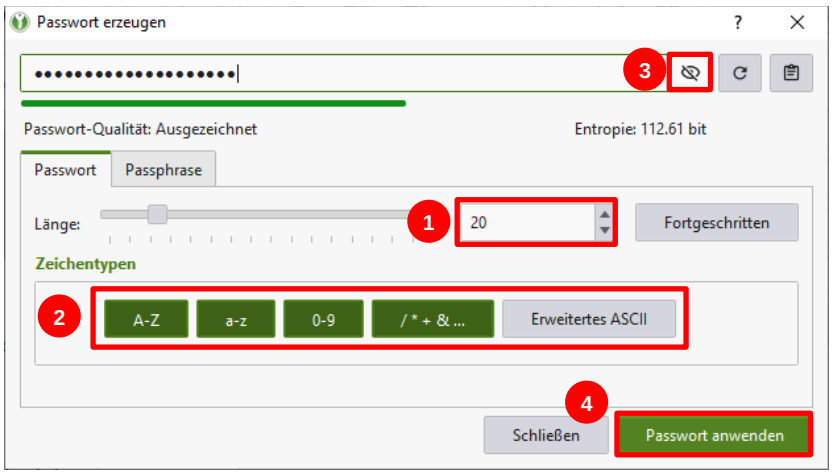


Hinweis: Möchten Sie die Browsererweiterung (s. Kapitel 6) nutzen, tragen Sie bei „URL“ (3) den direkten Link zur Login-Seite und nicht den Link zur Startseite des Dienstes ein.

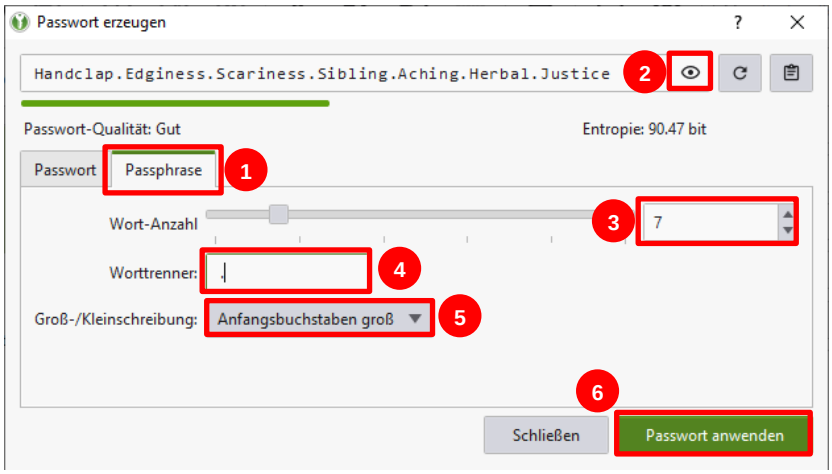
4.1 Erzeugung eines Passworts in einem Datenbankeintrag (4)(b)

KeepassXC bietet zwei Möglichkeiten der Passworterzeugung: Passwörter und Passphrasen.

Bei der Erzeugung eines Passworts, muss die Anzahl der Zeichen - „Länge“ (1) - festgelegt werden. Außerdem können verschiedene „Zeichentypen“ (2) an- bzw. abgewählt werden. Je mehr Zeichentypen verwendet werden, desto höher wird die Komplexität des Passworts. Sie können sich das erzeugte Passwort anzeigen lassen, indem Sie das Augensymbol (3) klicken. Wählen Sie „Passwort anwenden“ (4), um das Passwort dem Datenbankeintrag hinzuzufügen.



Wechseln Sie in den Reiter „Passphrase“ (1), um ein Passwort aus Zufallswörtern statt Zufallszeichen zu erzeugen. Sie können die Zufallswörter sehen, wenn Sie das Augensymbol (2) anwählen. Über den Schieberegler oder das Eingabefeld „Wort-Anzahl“ (3) können Sie die Anzahl der Wörter in der Passphrase definieren. Zwischen den Wörtern werden die unter „Worttrenner“ (4) eingetragenen Zeichen eingefügt. Über das Drop-Down-Menü „Groß-/Kleinschreibung“ (5) können Sie festlegen, ob die Wörter vollständig klein, vollständig groß oder mit großen Anfangsbuchstaben geschrieben werden sollen. Wählen Sie „Passwort anwenden“ (6), um dem Datenbankeintrag die erzeugte Passphrase hinzuzufügen.

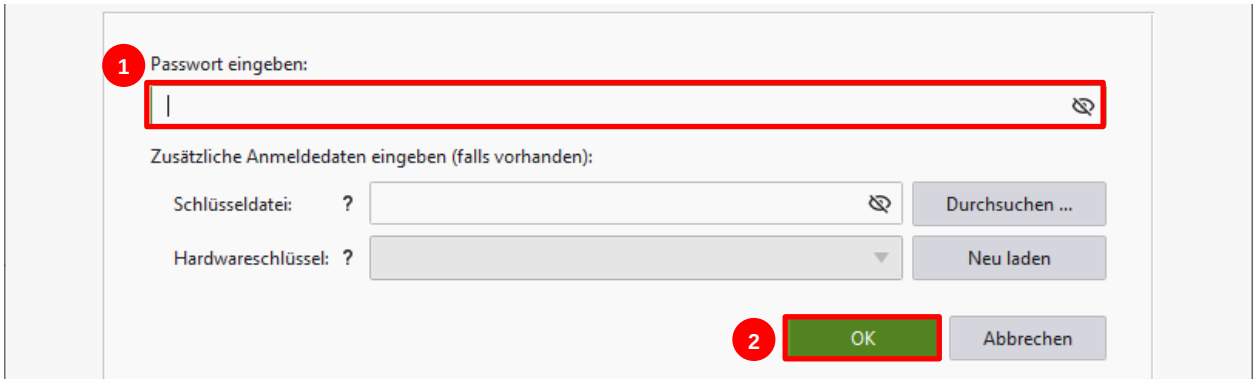


Hinweis: Erzeugen Sie ein neues Passwort für einen vorhandenen Account, muss das bisherige Passwort natürlich ausgetauscht werden. Dies ist in der Regel über die Account-(Sicherheits-)Einstellungen möglich.

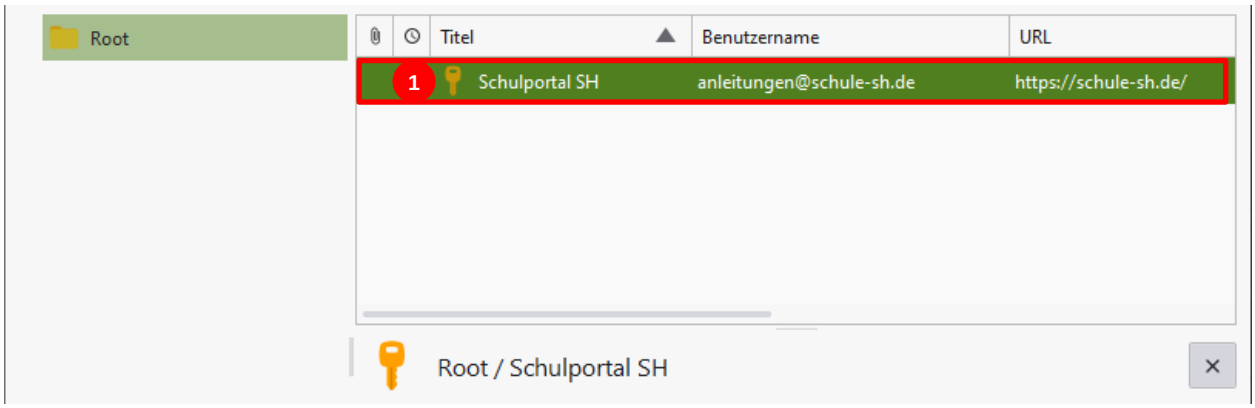
Hinweis: Alle Accounts, welche Zugriff auf sensible Daten haben, sollten mit einem Passwort versehen sein, welches mind. den Anforderungen aus 1.3 genügt. Das Füllen der Passwortdatenbank ist ein guter Zeitpunkt, um ggf. unsichere Passwörter auszutauschen.

5 Nutzung des Passwortmanagers

Öffnen Sie KeePassXC. Geben Sie das in Kapitel 3 gewählte Passwort ein (1) und bestätigen Sie die Eingabe mit „OK“ (2), um die Datenbank zu entsperren und auf die Einträge zugreifen zu können.



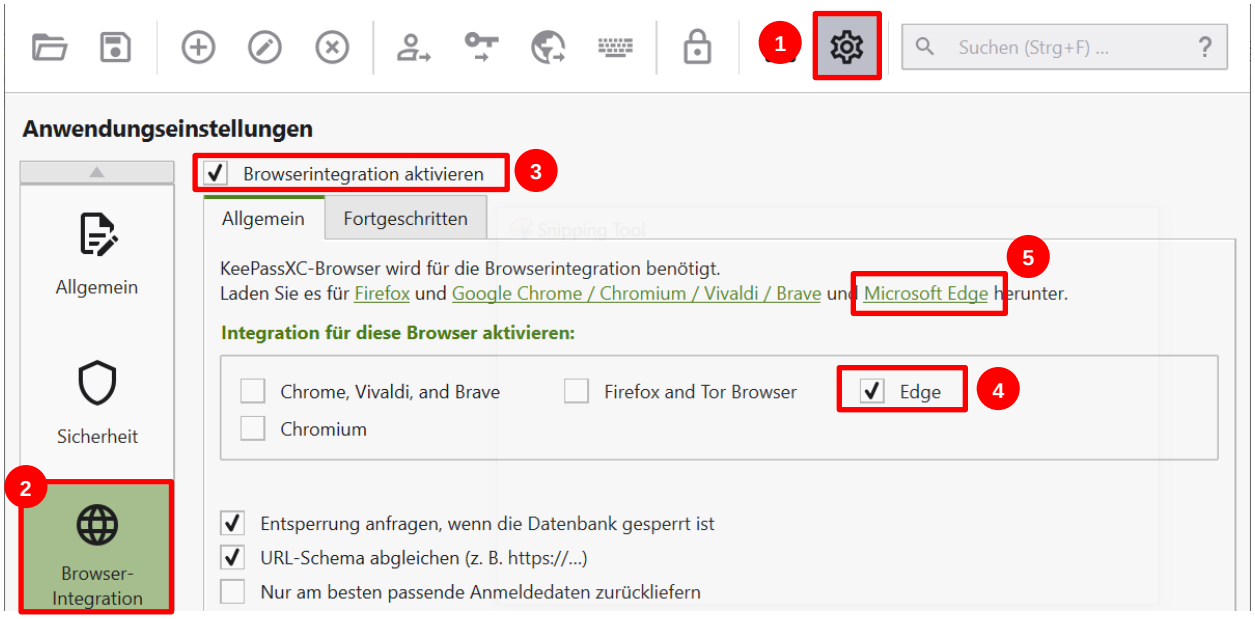
Möchten Sie den Benutzernamen eines Datenbankeintrags kopieren, können Sie dies per Rechtsklick auf den entsprechenden Eintrag (1) tun. In diesem Fall öffnet sich ein Kontextmenü mit der Option „Benutzername kopieren“. Alternativ können Sie den Eintrag (1) anwählen und die Tastenkombination „Strg + B“ drücken. Der Benutzername wird daraufhin in die Zwischenablage ihres Computers kopiert. Dasselbe gilt für das im Eintrag hinterlegte Passwort. Dieses können Sie per Rechtsklick und wählen der Option „Passwort kopieren“ oder durch das Drücken von „Strg + C“ in Ihre Zwischenablage kopieren. Aus Sicherheitsgründen wird der jeweils kopierte Eintrag nach 10 Sekunden wieder aus Ihrer Zwischenablage entfernt.



6 Nutzung des KeePassXC Browserplugins (vgl. 1.1)

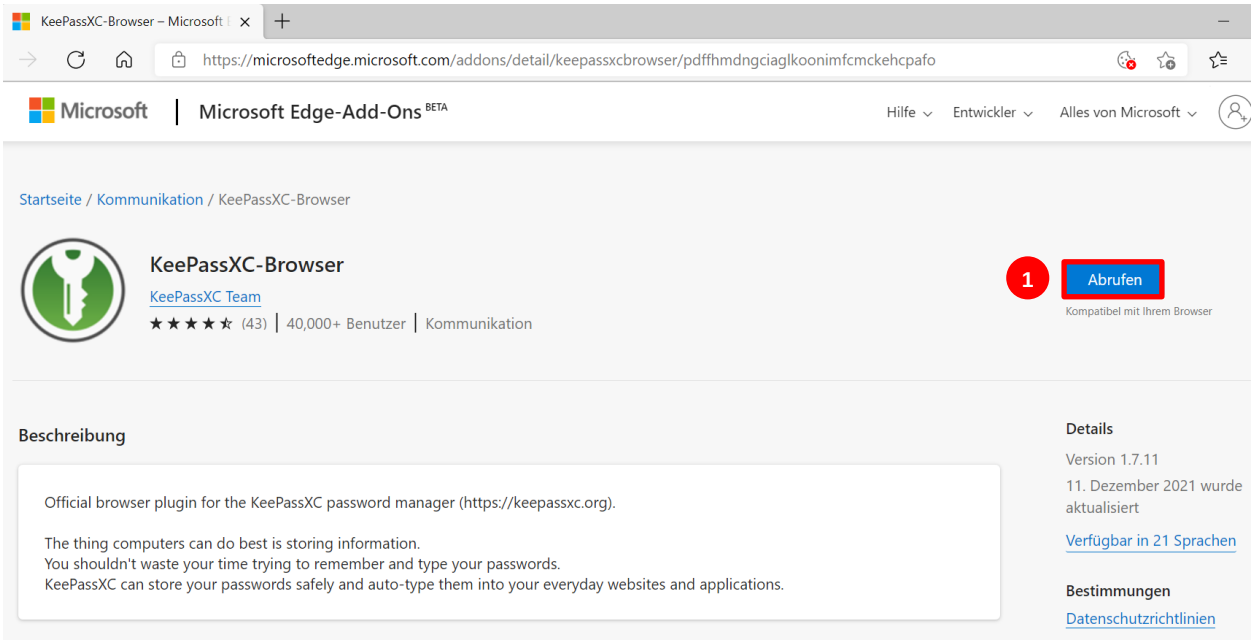
Hinweis: In dieser Anleitung wird beispielhaft das Browserplugin für den Edge-Browser eingerichtet. Der Ablauf ist auch auf den Browser Mozilla Firefox übertragbar.

Wählen Sie innerhalb der Software KeePassXC das Zahnradsymbol (1). Daraufhin öffnen sich die Einstellungen in der Ansicht „Allgemein“. Wählen Sie die Kachel „Browserintegration“ (2) und setzen Sie das Häkchen „Browserintegration aktivieren“ (3). Wählen Sie nun das Häkchen „Edge“ (4) und rufen den Download-Link „Microsoft-Edge“ (5) mit dem Edge-Browser auf.

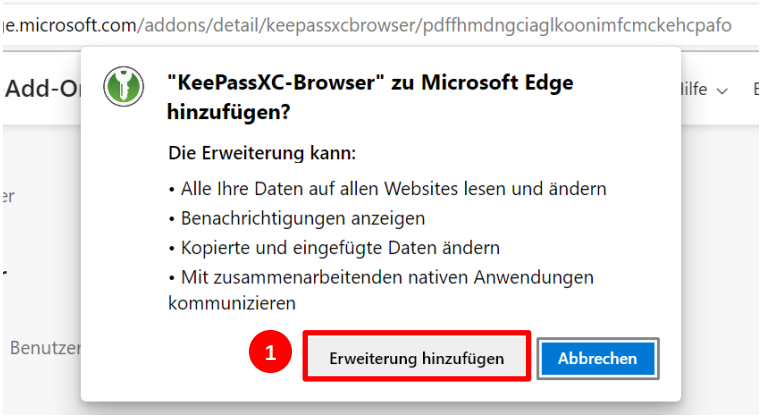


Hinweis: Durch das Klicken des Links (5) öffnet sich Ihr Standardbrowser. Dies ist nicht zwangsläufig MS Edge. Klicken Sie daher ggf. mit der rechten Maustaste auf den Link (5), wählen Sie „Link-Adresse kopieren“, öffnen Sie MS Edge und fügen Sie den Link mit der Tastenkombination Strg+C in die Adresszeile des Browsers. Dadurch rufen Sie die Seite des KeePassXC-Browser AddOns für MS Edge auf.

Wählen Sie auf Seite des KeePassXC-Browser AddOns den Button „Abrufen“ (1) um das AddOn in ihrem Browser zu installieren.

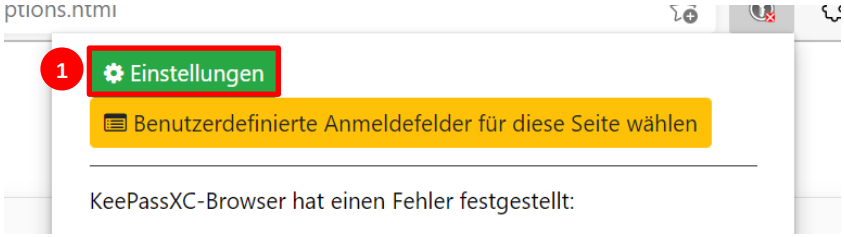


Daraufhin öffnet sich ein Pop-Up-Fenster. Wählen Sie in diesem „Erweiterung hinzufügen“ (1).

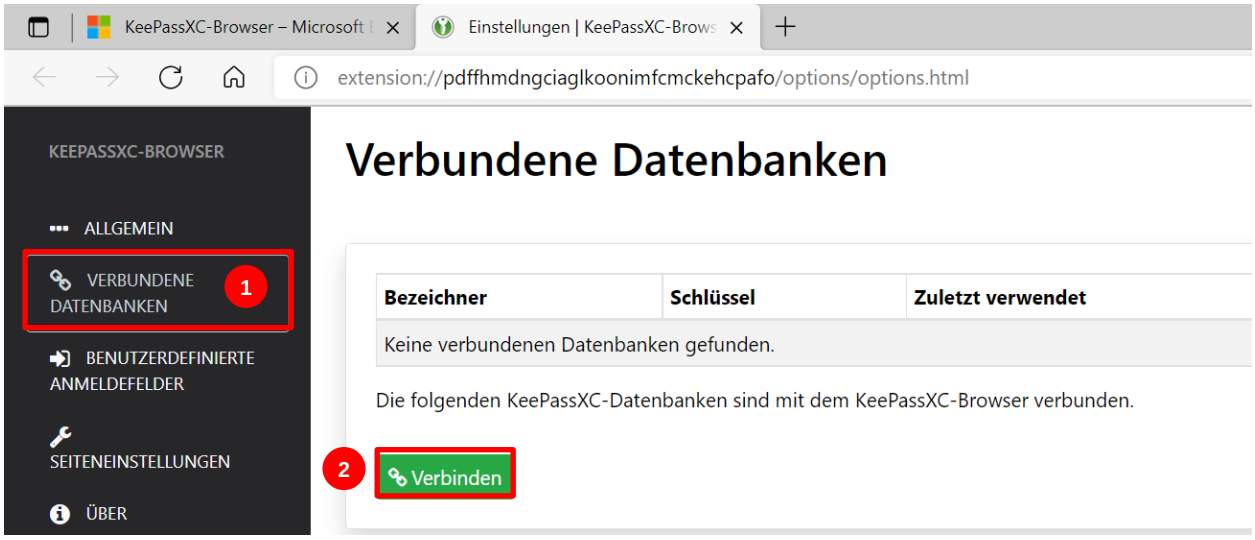


In Ihrem Browser existiert nun neben der Eingabeleiste ein neues Symbol (1) für die KeePassXC-Integration. Klicken Sie auf dieses.

Es öffnet sich ein neues Pop-Up-Fenster. Wählen Sie in diesem Fenster die „Einstellungen“ (1).

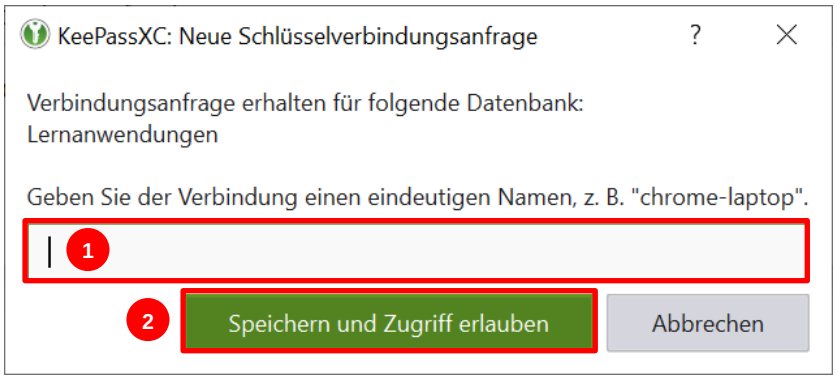


Die Einstellungen öffnen sich in einem neuen Tab. Wechseln sie in die Ansicht „Verbundene Datenbanken“ (1) und klicken Sie den Button „Verbinden“ (2)



Hinweis: Damit eine Verbindung zwischen Browser-Integration und Passwortmanager hergestellt werden kann, muss die Datenbank entschlüsselt sein. Hierfür müssen Sie, aufgrund der automatischen Sperre bei Inaktivität (vgl. Kapitel 2), zu diesem Zeitpunkt ggf. noch einmal den Manager aufrufen und das Datenbankpasswort eingeben (vgl. Kapitel 5).

Durch das Bestätigen des „Verbinden“-Buttons baut die Integration eine Verbindung zum KeePassXC-Passwortmanager auf. Dieser öffnet ein neues Fenster. Legen Sie hier einen Namen für die Verbindung fest (1). Bestätigen Sie die Verbindung durch „Speichern und Zugriff erlauben“ (2).

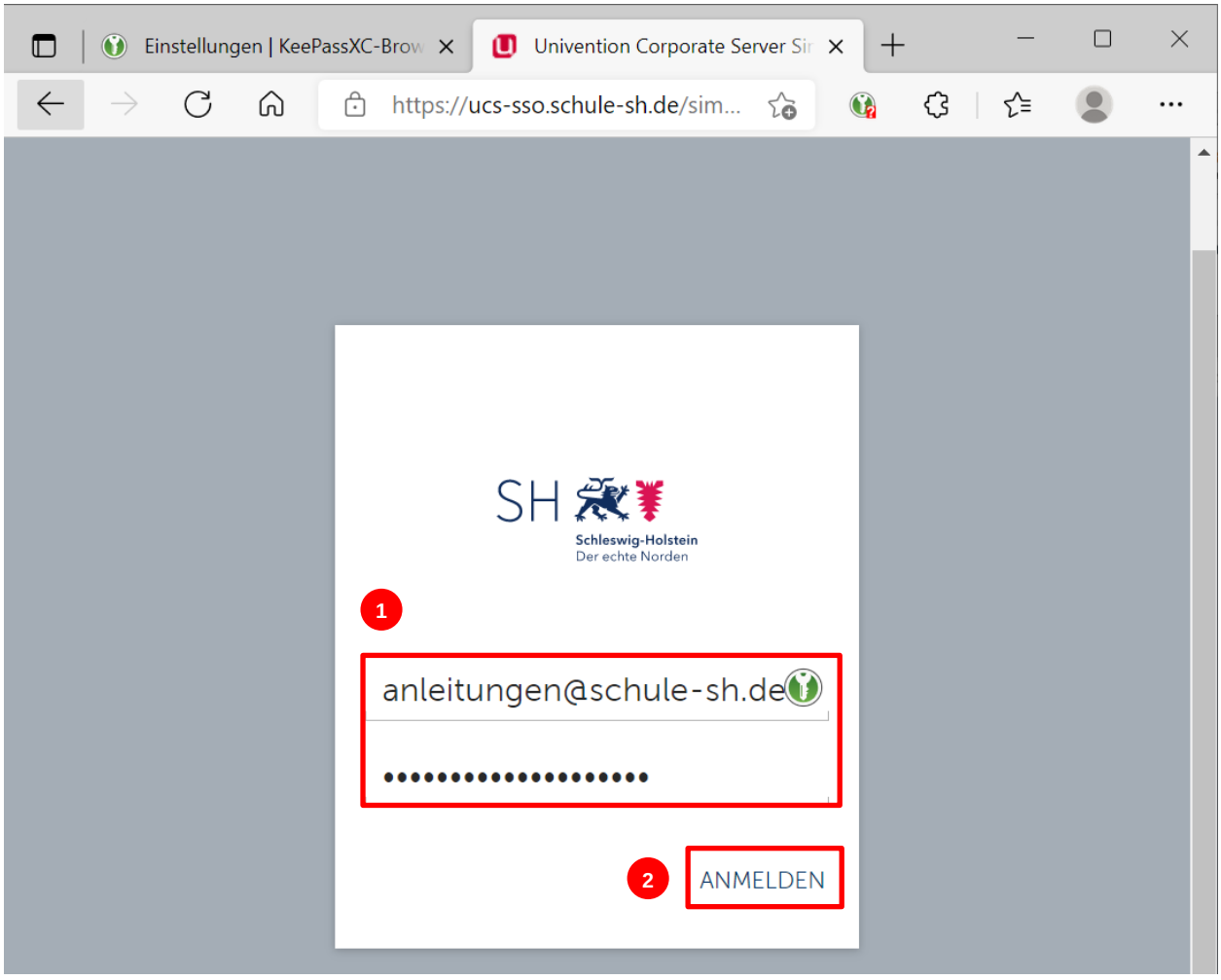


Jetzt können Sie die Browserintegration nutzen. Hier gibt es zwei verschiedene Optionen:

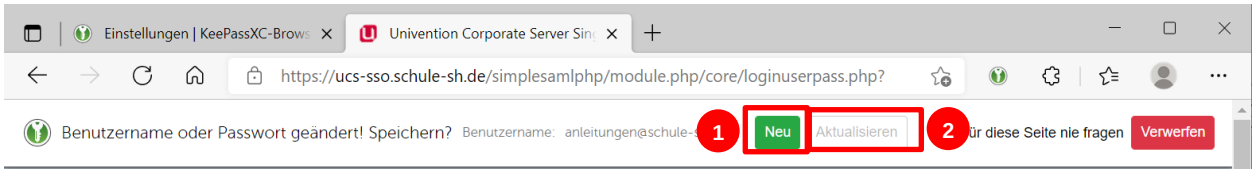
1. Sie loggen sich in einen Account ein, der nicht (vollständig) oder fehlerhaft im Passwortmanager gespeichert ist.
2. Sie haben die Zugangsdaten inklusive Webadresse zur Login-Seite bereits im Passwortmanager hinterlegt.

Rufen Sie in beiden Fällen die Login-Seite des Dienstes auf, in den Sie sich einloggen möchten.

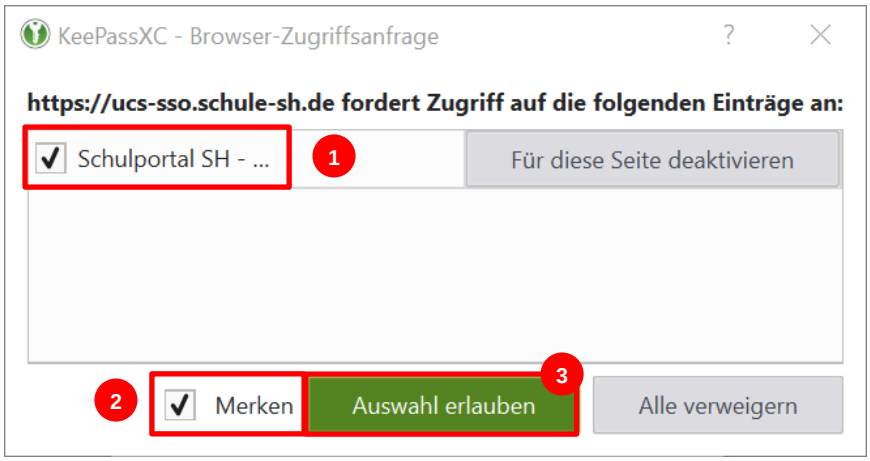
Option 1: Geben Sie ihre Zugangsdaten in die Eingabemaske (1) ein und klicken Sie „ANMELDEN“ (2).



Daraufhin fragt das AddOn, ob Sie den Eintrag Speichern möchten. Beim Speichern haben Sie die Optionen entweder einen neuen Eintrag in der Datenbank anlegen zu lassen (1) oder einen vorhandenen Eintrag zu aktualisieren (2).



Option 2: Hierbei ist es wichtig, dass beim Anlegen des Eintrags im Passwortmanager die URL der Login-Seite des Dienstes angegeben wurde und kein allgemeiner Link zur Startseite. Rufen Sie die URL zur Login-Seite zum ersten Mal nach der Konfiguration der KeePassXC-Browsererweiterung auf, öffnet sich ein Fenster, über welches Sie der Erweiterung Zugriff auf die Datenbank geben können. Setzen Sie das Häkchen „Merken“ (2), damit diese Entscheidung auch für die Zukunft gespeichert wird. Bestätigen Sie durch „Auswahl erlauben“ (3).



Klicken Sie nun auf das Schlüssel-Symbol (1) neben dem Feld für den Benutzernamen. Dadurch werden die Zugangsdaten aus dem Passwortmanager automatisch in die Login-Felder geschrieben. Wählen Sie „ANMELDEN“ (2), um sich einzuloggen.