Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

IT Services Support

Werftestrasse 4, Postfach 2969, CH-6002 Luzern
T +41 41 228 21 11
www.hslu.ch

KeePass

Kurzbeschrieb:	Installationsanleitung & Beschreibung der Grundfunktionen von KeePass inkl. Browser Erweiterung für Google Chrome und Mozilla Firefox. (Windows)	
Klassifikation:	☒ IT intern ☐ Andere	☒ Public
Kundengruppe:	☒ HSLU ☐ Andere	☒ PHLU
Rolle:	☒ Mitarbeitende/Doz. ☐ Andere	☒ Studierende
Geräteverwaltungstyp:	☒ HSLU/PHLU-Geräte ☐ Andere	☒ Private Geräte
Betriebssystem:	☒ Windows ☐ Andere	☐ Mac
Publikation:	☒ hslu.ch/helpdesk ☐ Andere	☒ Intranet
Support:	Web: hslu.ch/helpdesk E-Mail: informatikhotline@hslu.ch Tel: 041 / 228 21 21 Portal: helpdesk.hslu.ch	

Änderungsverzeichnis

Version	Datum	Status	Änderungen und Bemerkungen	Bearbeitet von
Nr. 0.1	19.07.2017		Erstellung	scc
Nr. 0.2	04.08.2017		Überarbeitet	scc
Nr. 1.0	10.08.2017		Fertigstellung	Scc
Nr. 2.0	17.03.2020		Ergänzung Browser Extension	kju

Inhaltsverzeichnis

1. Über KeePass

KeePass ist ein Passwortverwaltungstool. Mit KeePass können Login Daten geschützt abgespeichert werden. Die gesamte Datenbank in welcher die Passwörter gespeichert werden ist verschlüsselt. Nur mit einem Hauptschlüssel, welcher bei der Eröffnung einer neuen Datenbank definiert wird, ist diese zugänglich.

Für Google Chrome und Mozilla Firefox gibt es ein Browser Add-On, welches dem Benutzer ermöglicht, die KeePass Datenbank mit dem Browser zu verknüpfen.

2. Download und Installation

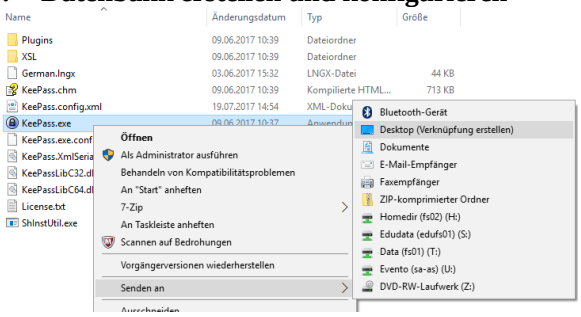
KeePass Professional Edition unter http://keepass.info/download.html herunterladen.

Damit keine Installation durchgeführt werden muss, sollte die portable Version (ZIP-Datei) ausgewählt werden.

Zusätzlich zur KeePass Professional Edition kann noch das deutsche (oder ein anderes) Sprachpaket heruntergeladen werden (http://keepass.info/translations.html).
Speichern Sie beide ZIP-Dateien an einem lokalen Speicherort auf Ihrem Computer.

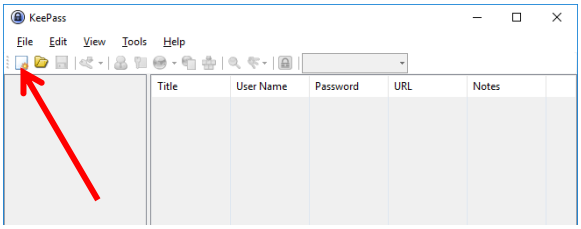
Entpacken Sie die beiden heruntergeladenen ZIP-Dateien. Legen Sie danach das deutsche Sprachpaket *German.lngx* in den entpackten KeePass-Ordner.

3. Datenbank erstellen und konfigurieren

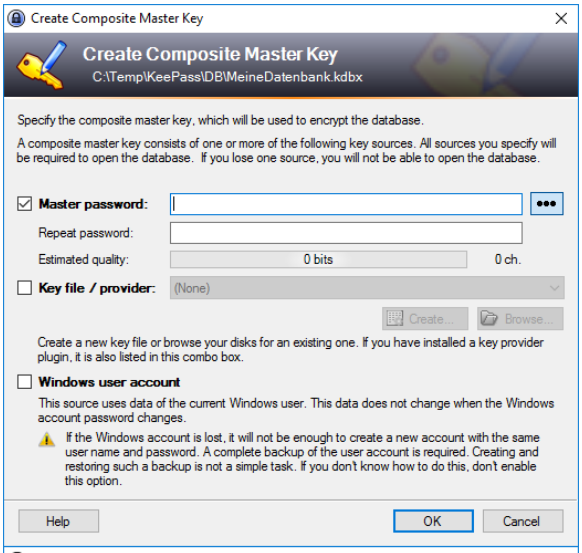


Um beim Starten von KeePass nicht ständig den *Programme*-Ordner öffnen zu müssen, kann eine Desktopverknüpfung erstellt werden: Klicken Sie dafür mit der rechten Maustaste auf die EXE-Datei und wählen Sie im Kontextmenü *Senden an / Desktop (Verknüpfung erstellen)*.

Anschliessend lässt sich KeePass mittels Doppelklick auf die neu erstellte Desktop-Verknüpfung starten. Es wird empfohlen, automatisch nach Updates zu suchen.

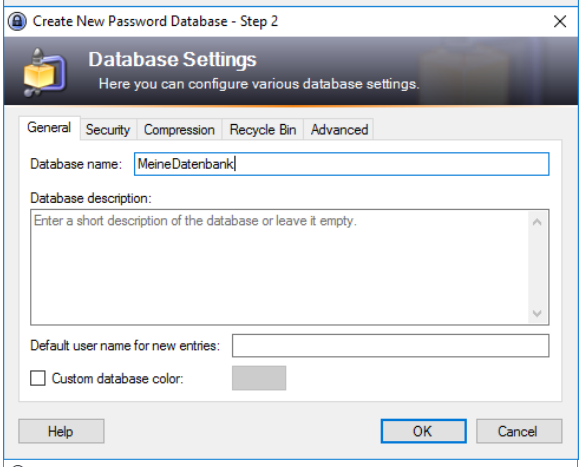


Da noch keine Datenbank existiert, muss nach dem ersten Programmstart eine solche erstellt werden.
Dies geschieht entweder durch Klicken auf das entsprechende Symbol aus dem Menüband oder über *File / New*.

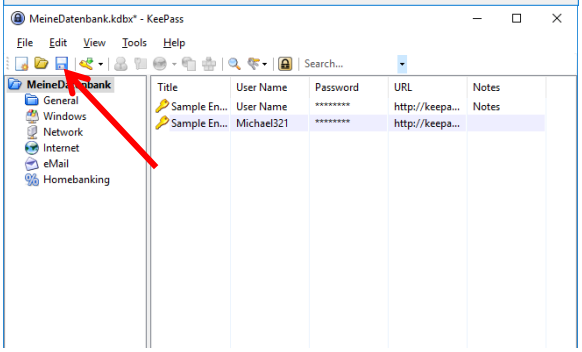


Die Passwort-Datenbank wird verschlüsselt auf dem Computer gespeichert; aus diesem Grund muss ein Masterpasswort eingegeben und wiederholt werden.

Es ist wichtig, dass mit dem Masterpasswort und nicht mit einem Key File oder dem Benutzer-Konto von Windows gearbeitet wird.

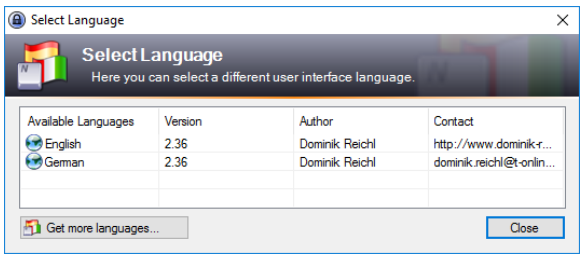


Wenn das Masterpasswort zweimal fehlerfrei eingetippt wurde, können Einstellungen und Zusatzinformationen für die Datenbank hinterlegt werden.
Wichtig ist sicherlich ein aussagekräftiger Datenbankname in der Registerkarte *General*.



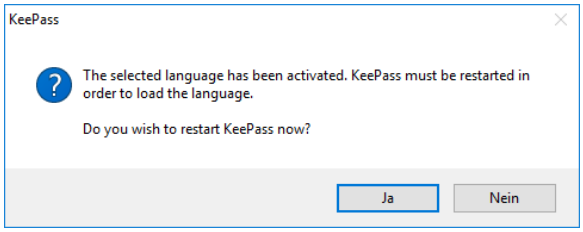
Nachdem alle Angaben getätigt und der Prozess mit *OK* abgeschlossen wurde, wird die Struktur der neu erstellten Datenbank im linken Navigationsbereich ersichtlich.

Sämtliche Manipulationen an und in der Datenbank werden erst durch das Speichern dauerhaft übernommen. Daher ist es wichtig, nach jeglichen Änderungen auf *Speichern* zu klicken.



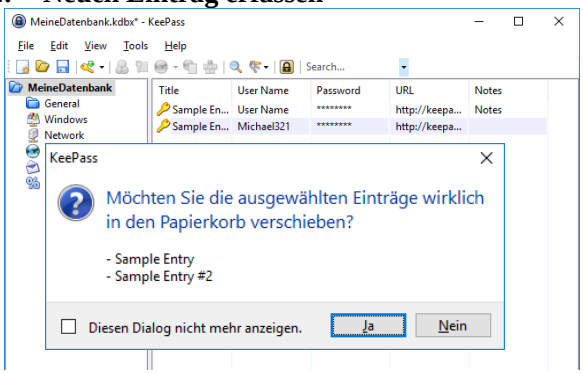
Sollte die englische Sprache störend sein, kann durch das zusätzlich heruntergeladene, entpackte und installierte Sprachpaket auf Deutsch gewechselt werden.

Dazu über den Menüpunkt *View / Change Language…* die zusätzlich aufgelistete Sprache *German* auswählen.



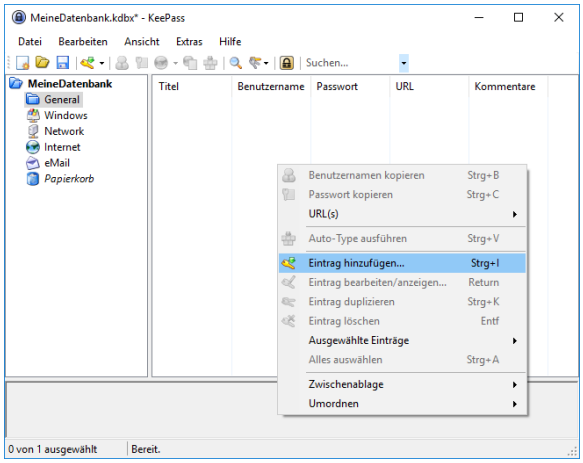
Nachdem die Auswahl getroffen wurde, sollte KeePass neu gestartet werden, damit die Änderungen übernommen werden.

4. Neuen Eintrag erfassen



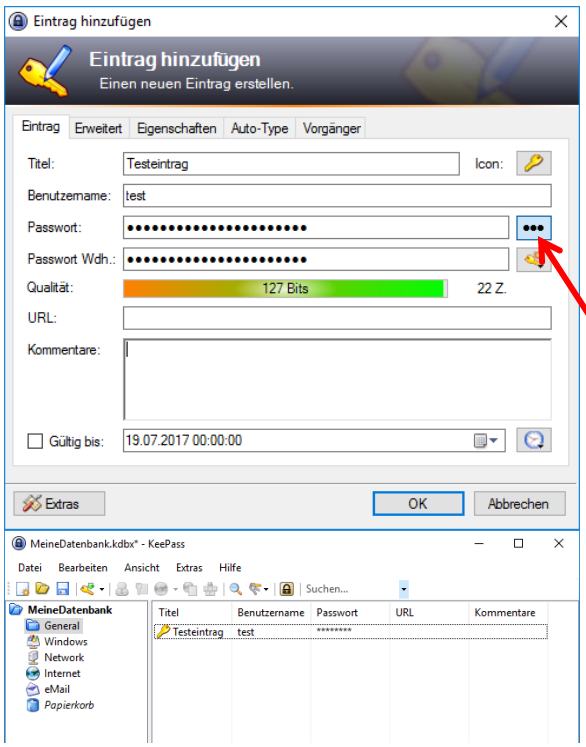
Als erster Schritt sollten die beiden Beispieldateien *Sample Entry* und *Sample Entry #2* gelöscht werden.

Hinweis:
Daten werden erst nach dem Leeren des Papierkorbs endgültig aus der Datenbank entfernt.



Um übersichtlicher durch die Passwörter navigieren zu können, ist es wichtig, eine gute Ordnerstruktur zu erstellen oder mit der durch den Hersteller bereits vorgegebenen Struktur zu arbeiten.

Neue Einträge lassen sich im gewünschten Ordner (bspw. *General*) durch Rechtsklick und der Kontextauswahl *Eintrag hinzufügen…* erstellen.



Alle notwendigen Angaben zu einem Passwort können dem betr. Eintrag hinzugefügt werden.

Zumindest sollte ein aussagekräftiger Titel gewählt und der Benutzername und das Passwort selbst eingetragen werden.

Zusätzlich können auch noch URL, Kommentare und weitere Informationen hinterlegt werden.

Hinweis:
Über den Knopf neben dem Passwort-Feld kann die Sichtbarkeit der getätigten Eingabe ein- resp. wieder ausgeschaltet werden.

Über den *OK*-Knopf kann der betr. Eintrag vorgenommen werden, dieser wird dann im gewünschten Ordner gelistet.
Wird nun ein bestimmtes Passwort benötigt, kann der betr. Eintrag konsultiert werden.

Hinweis:
Speichern nicht vergessen!

5. Onlinespeicher (SWITCHdrive)

Um Passwörter aus dem KeePass Passwort Safe mit mehreren Geräten zu verwenden, kann die KeePass-Datenbankdatei mit einem Onlinespeicher synchronisiert werden.

Mitarbeitende, Dozierende und Studierende der Hochschule Luzern können den Cloud-Service *SWITCHdrive* geschäftlich sowie privat kostenlos nutzen.

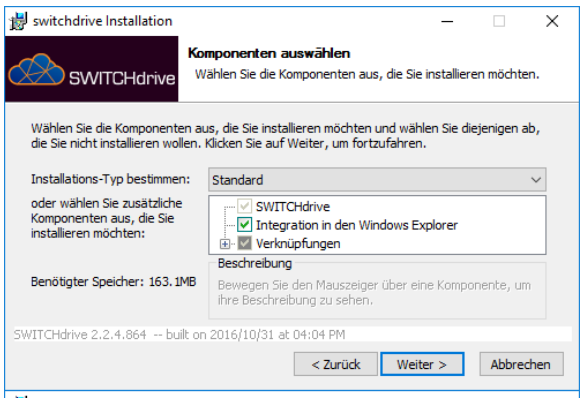
IT Services empfiehlt ausdrücklich die Verwendung von SWITCHdrive; von anderen Cloud-Diensten wird aus sicherheitstechnischen Gründen abgeraten.

Um lokale Dateien mit der SWITCHdrive-Plattform synchronisieren zu können, kann der SWITCHdrive-Client installiert werden. Da es sich hierbei um eine Installation (Ausführung einer EXE-Datei) handelt, werden lokale Administratorenrechte benötigt.

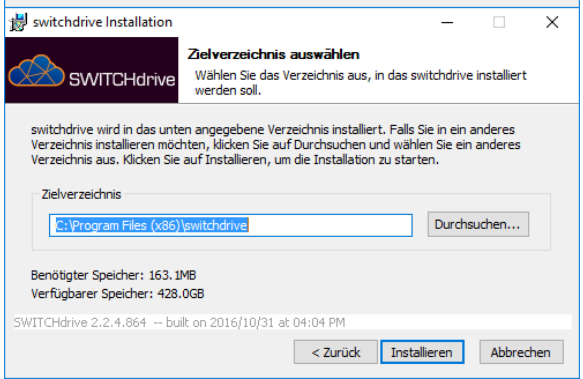
Der SWITCHdrive-Client kann unter https://help.switch.ch/drive/downloads/ heruntergeladen werden.

Nach der Ausführung der EXE-Datei startet der Installationsassistent.

Hinweis: Auf gemangten HSLU/PHLU-Geräten kann SWITCHdrive über den Softwarekiosk (https://softwarekiosk.hslu.ch) bezogen werden.

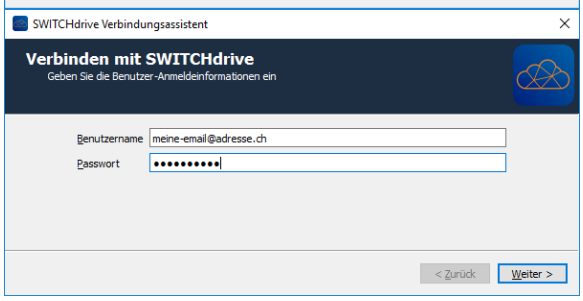


Installations-Typ *Standard* auswählen. Eine manuelle Anpassung ist nicht erforderlich.



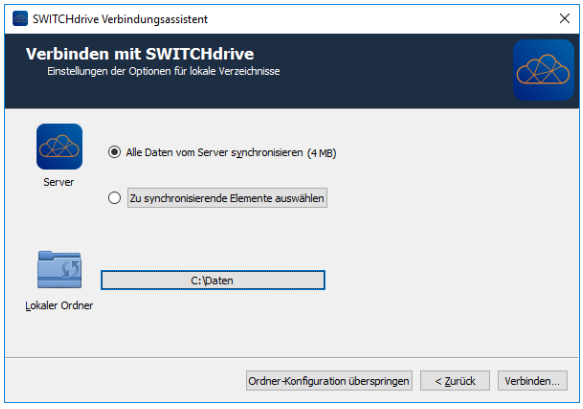
Zielort für die Installationsdateien auswählen und über *Installieren* die Installation starten.

Der Assistent zeigt anschliessend über einen grünen Balken wie weit die Installation fortgeschritten ist. Nach dessen Abschluss kann SWITCHdrive direkt ausgeführt werden.



Wird der SWITCHdrive-Client ausgeführt, muss eine Verbindung mittels E-Mail-Adresse und dazugehörigem Passwort aufgebaut werden.

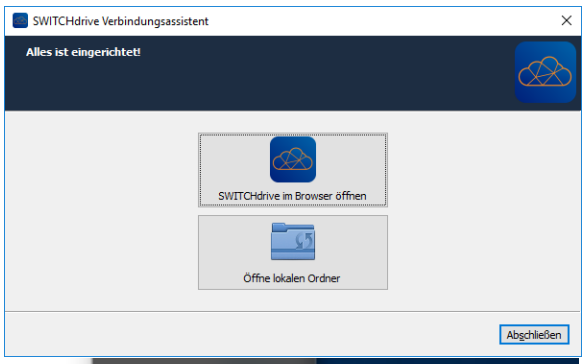
Hinweis:
Vorgängige Registrierung bei https://drive.switch.ch/ wird vorausgesetzt; d.h. ein entspr. Konto muss bereits vorhanden sein.



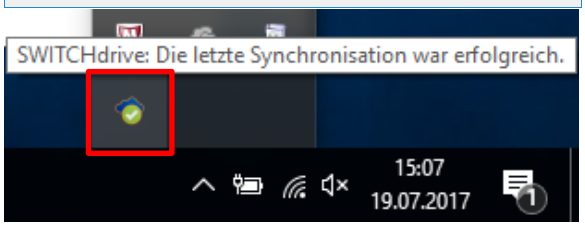
Synchronisationseinstellungen vornehmen:

- Vom SWITCH-Server können entweder alle Daten synchronisiert oder einzelne Elemente ausgewählt werden
- Den lokalen Ordner für die Synchronisation auswählen.

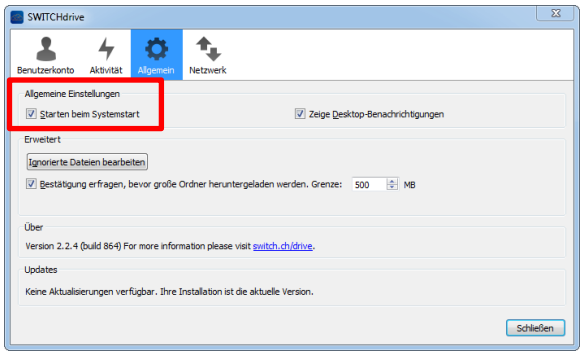
Hinweis:
Falls der ausgewählte lokale Ordner nicht leer ist, können die lokalen Daten behalten oder mit einer sauberen Synchronisation begonnen werden, wobei die vorhandenen lokalen Daten entfernt werden.



Nach der Konfiguration wird durch einen Klick auf *Abschliessen* der Verbindungsassistent beendet und die Synchronisation gestartet.



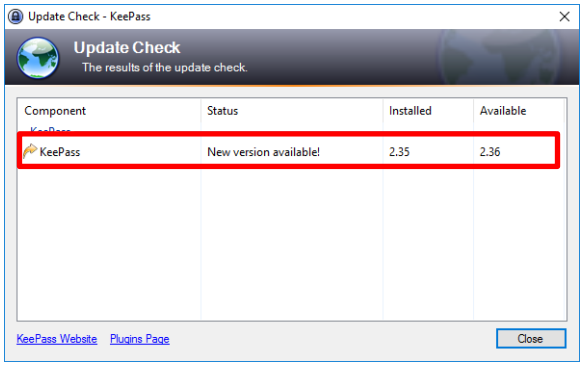
Der aktive Client wird als Symbol in der Taskleiste (unten rechts neben der Uhr) angezeigt.
Über das Taskleisten-Symbol können die Benutzeroberfläche, Einstellungen usw. aufgerufen werden.



Damit der SWITCHdrive-Client bei jedem Systemstart automatisch geöffnet wird, kann im Register *Allgemein* die dafür vorgesehene Checkbox aktiviert werden.

6. Updates

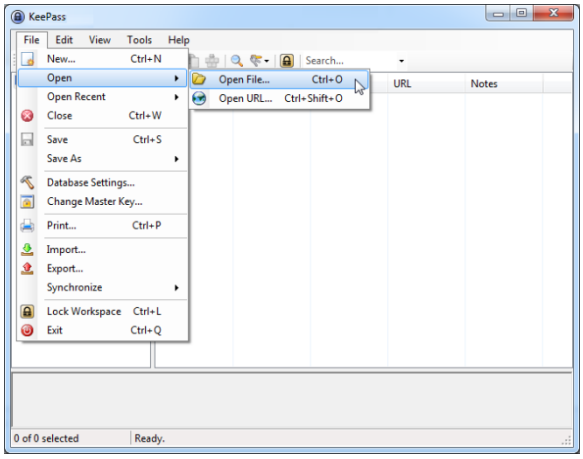
Wie vorgängig in Kapitel 2 erwähnt und empfohlen, bietet KeePass die Möglichkeit, automatisch beim Programmstart nach Updates zu suchen. Sollte eine neue Version verfügbar sein, wird ein entsprechender Hinweis angezeigt.



Wie aus dem automatisch ausgeführten *Update Check* hervorgeht, ist eine neue Version von KeePass verfügbar. Durch einen Doppelklick auf den entsprechenden Hinweis wird die KeePass-Website geöffnet.

Das Vorgehen zum Herunterladen und Entpacken der neuen KeePass-Version bleibt gleich wie bei der Erstinstallation.

Hinweis:
Bevor Dateien gelöscht oder überschrieben werden, vergewissern Sie sich, dass Ihre persönlich erstellte Passwort-Datenbankdatei nicht verloren geht. Sichern Sie diese Datei, sofern sich diese im Programmverzeichnis befindet.

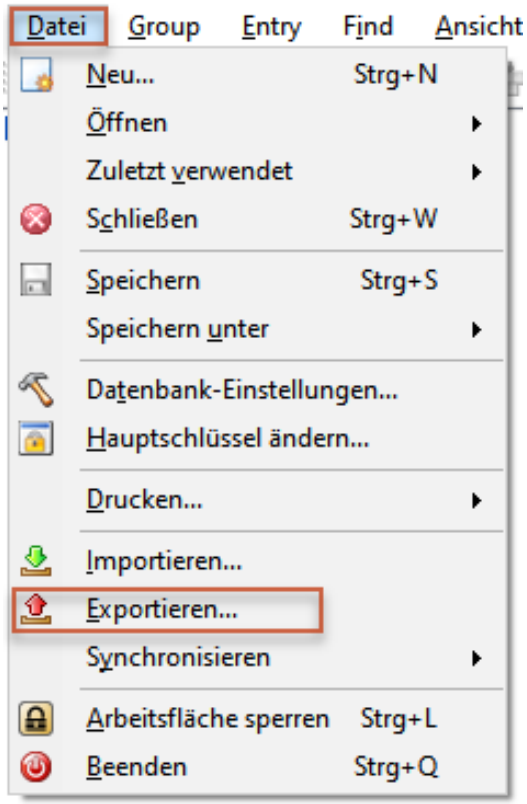


Nach der Installation der aktuellsten Version kann KeePass gestartet werden. Über den Menüpunkt *Datei / Öffnen / Datei öffnen…* kann die alte Passwort-Datenbankdatei ausgewählt und verwendet werden.

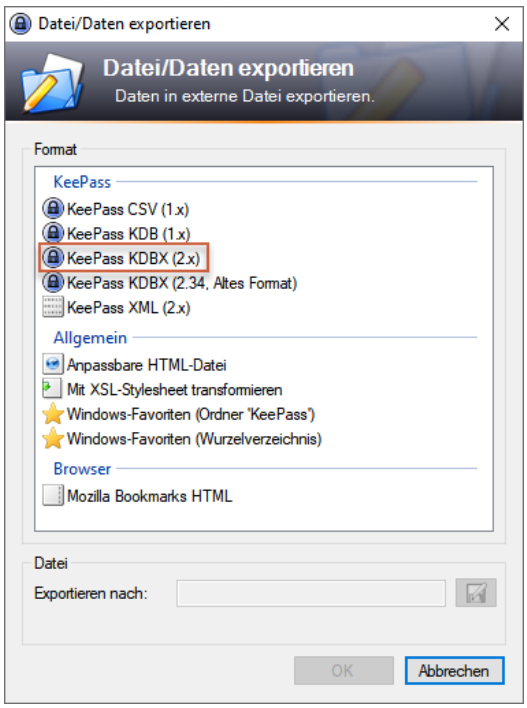
Hinweis:
Falls gewünscht, muss auch das deutsche Sprachpaket erneut heruntergeladen und installiert werden.

7. Datenbank exportieren

Die KeePass Datenbank kann exportiert werden und z.B. auf einem neuen Computer wieder importiert werden.



In der KeePass Applikation unter *Datei* und anschliessend auf *Exportieren* klicken.

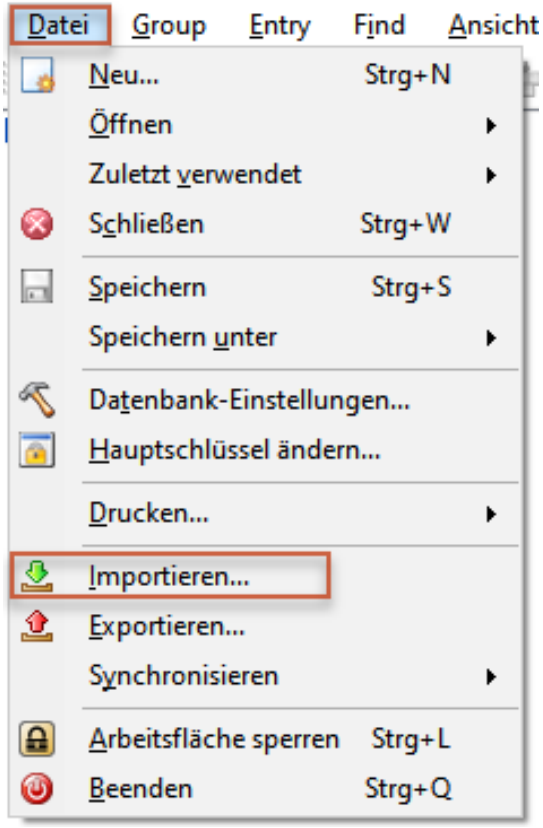


Wählen Sie das Format *KeePass KDBX (2.x)*.

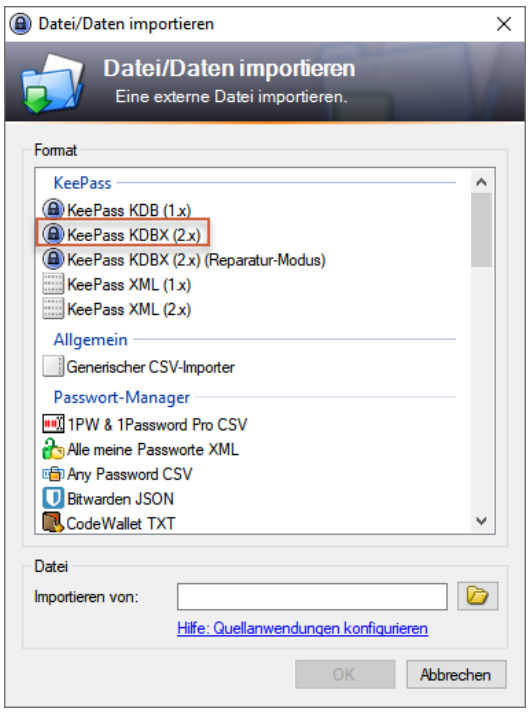
Wählen Sie einen Speicherort für die exportiere Datenbank.

Bestätigen Sie mit *OK*.

7.1. Datenbank importieren



In der KeePass Applikation unter *Datei* und anschliessend auf *Importieren* klicken.



Wählen Sie das Format *KeePass KDBX (2.x)*.

Wählen Sie die Datei aus, welche Sie importieren wollen.

Bestätigen Sie mit *OK*.

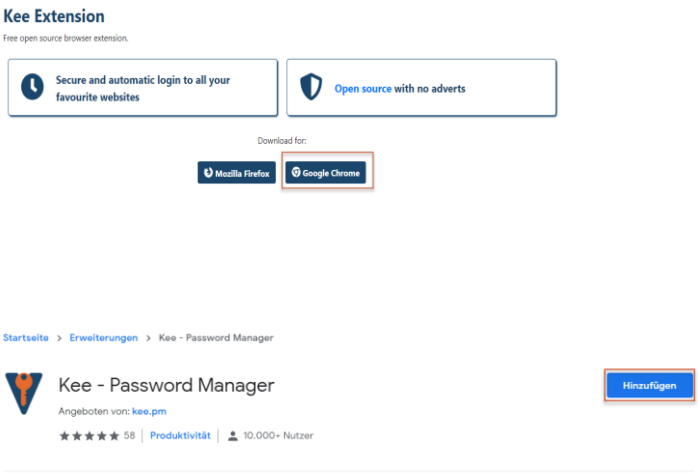
8. Browser Erweiterung

8.1. Voraussetzungen

- KeePass 2 Passwort Safe muss installiert sein
- KeePass 2 Passwort Safe muss durchgehend offen sein bei der Benutzung von der Browser Erweiterung

8.2. Installation Google Chrome

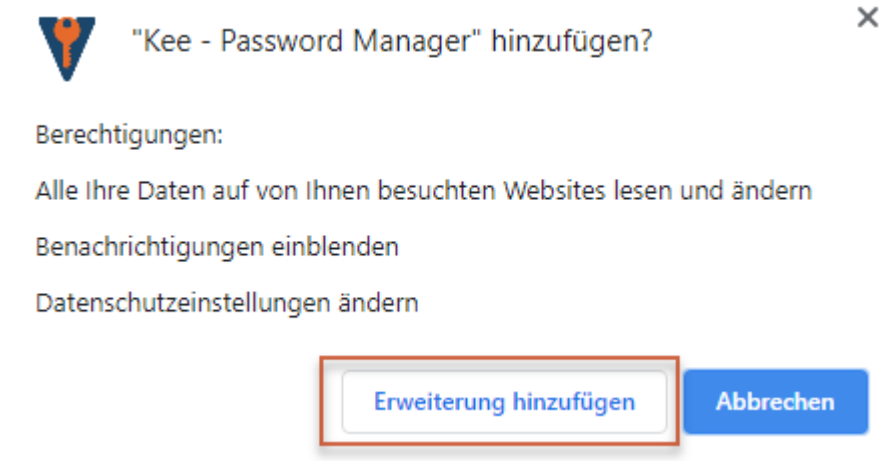
Stellen Sie sicher, dass Sie KeePass auf ihrem Computer gestartet haben, bevor Sie mit der Installation des Add-Ons beginnen.



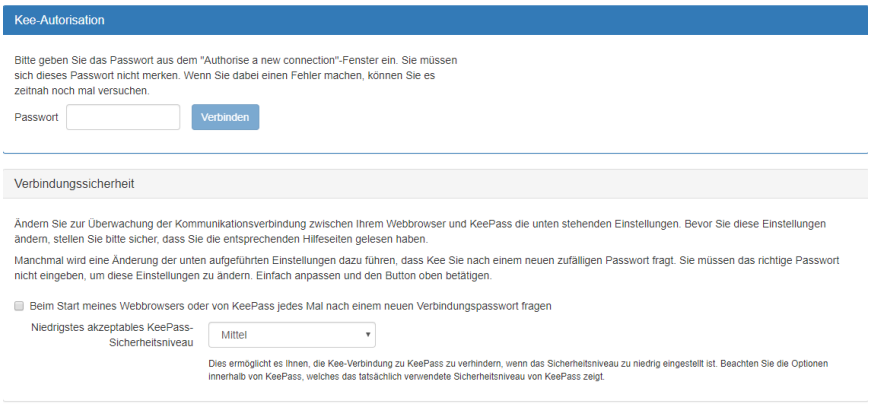
Gehen Sie auf folgende Webseite in Ihrem Google Chrome: https://www.kee.pm

Unter *Kee Extension* klicken Sie *Download for Google Chrome*.

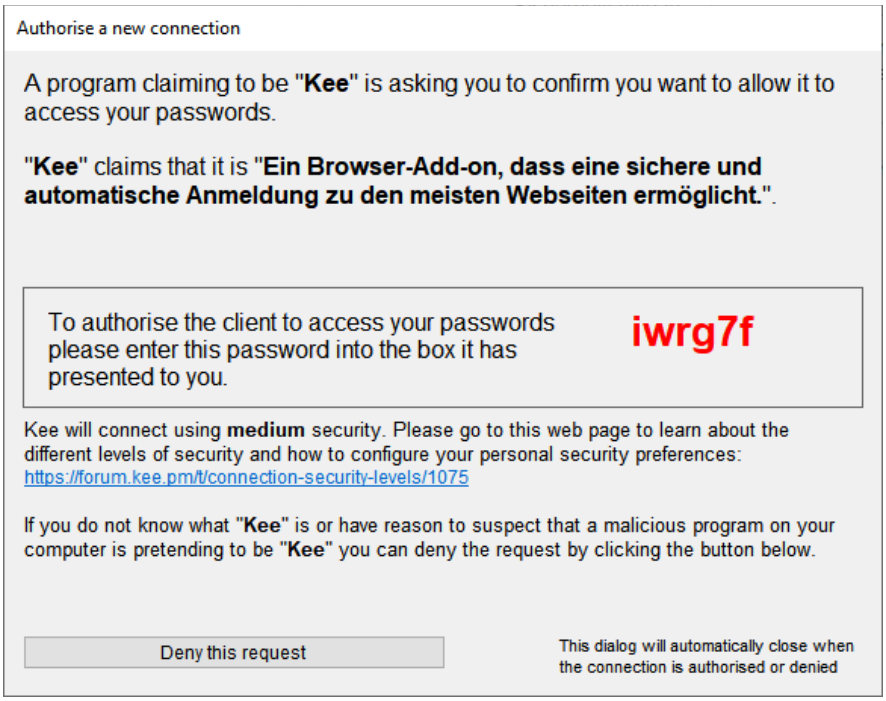
Klicken Sie auf *Hinzufügen*.



Bestätigen Sie die Installation im neuen Fenster indem Sie auf *Erweiterung hinzufügen* klicken.



Es wird ein Fenster mit einer Passwortabfrage geöffnet, dieses Passwort ist in der KeePass Applikation ersichtlich.

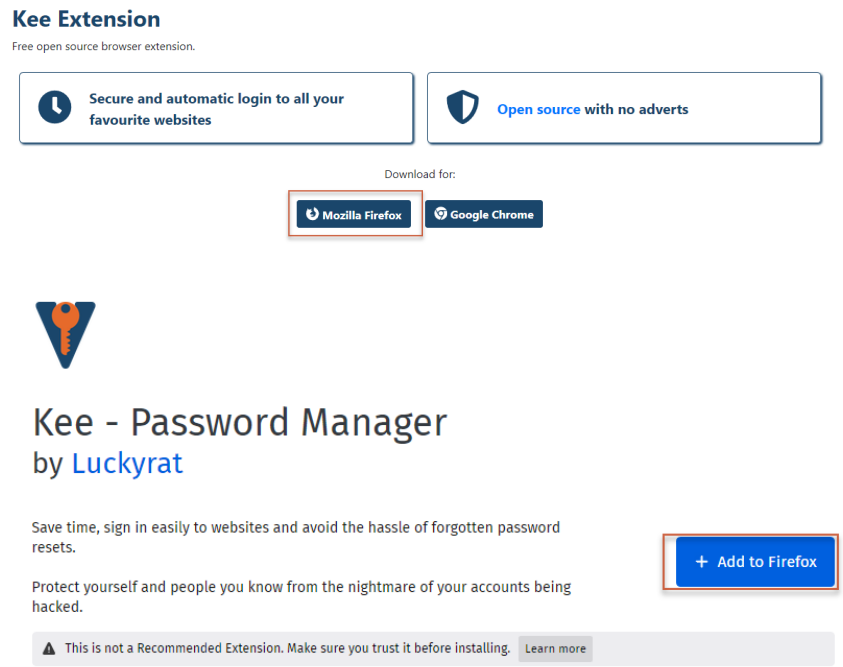


Kopieren Sie das rote Passwort und geben Sie dieses im geöffneten Browserfenster unter Passwort ein.

Anschliessend ist das Add-On installiert.

Nun ist oben rechts in Browser das Symbol vom Kee-Add-On ersichtlich.

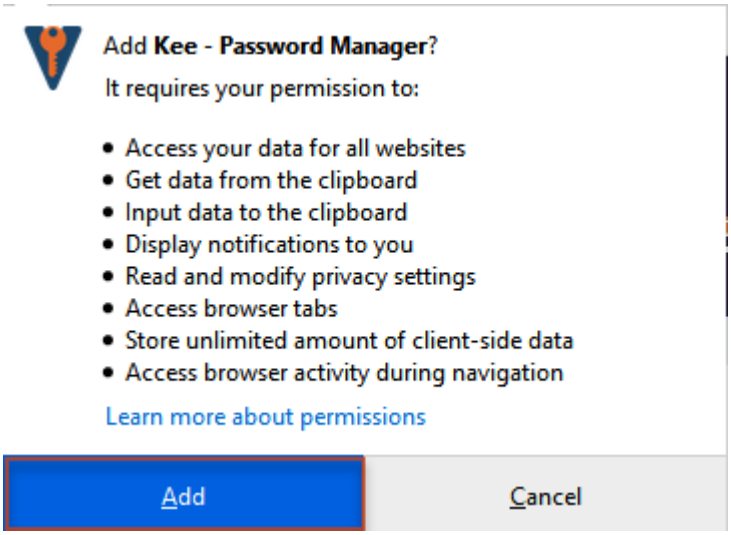
8.3. Installation Firefox



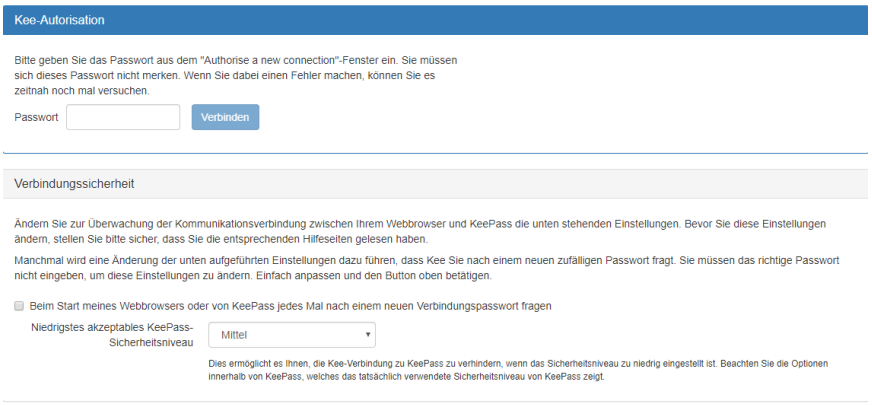
Gehen Sie auf folgende Webseite in Ihrem Firefox: https://www.kee.pm

Unter *Kee Extension* klicken Sie *Download for Mozilla Firefox*.

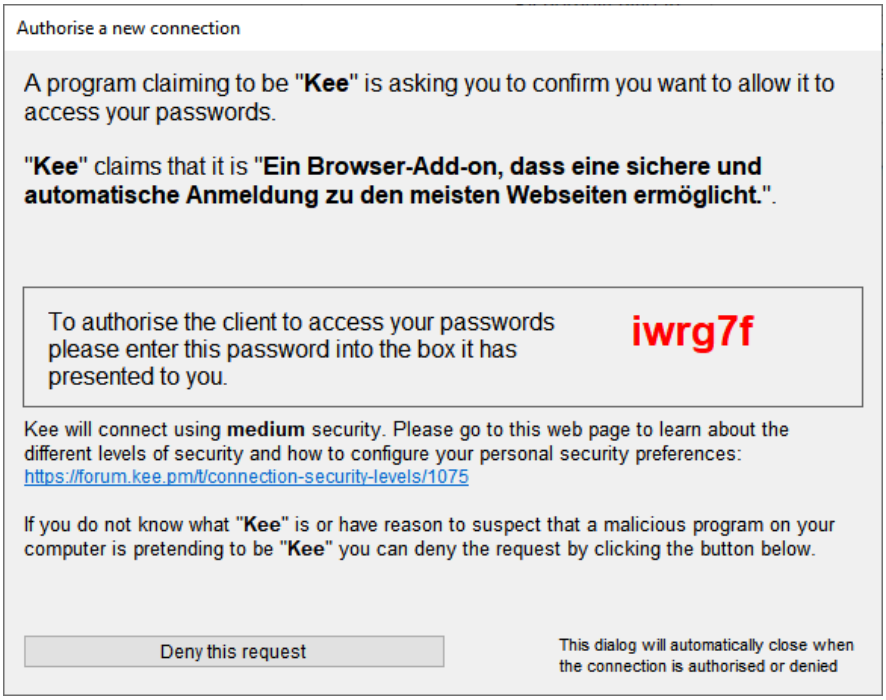
Klicken Sie *Add to Firefox*.



Bestätigen Sie die Installation im neuen Fenster indem Sie auf *Add* klicken.



Es wird ein Fenster mit einer Passwortabfrage geöffnet, dieses Passwort ist in der KeePass Applikation ersichtlich.



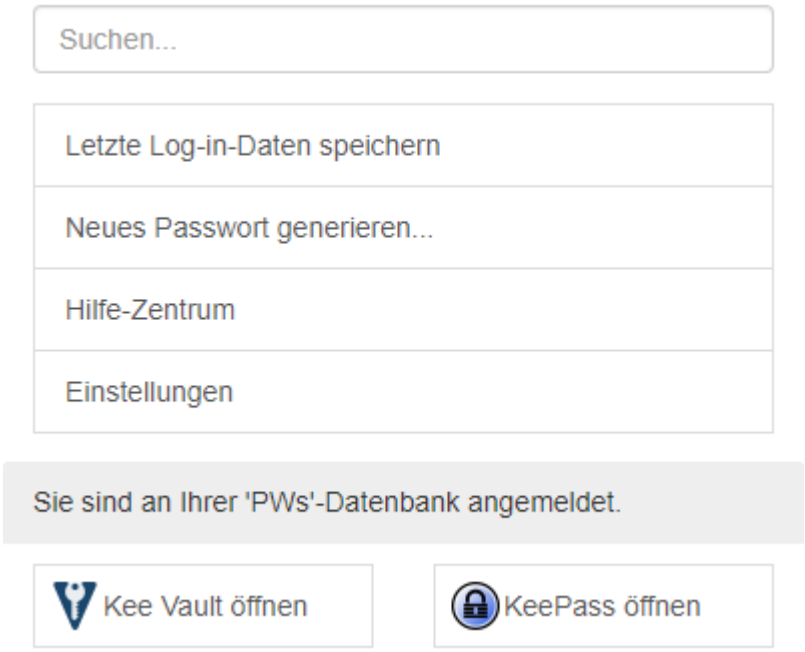
Kopieren Sie das rote Passwort und geben Sie dieses im geöffneten Browserfenster unter Passwort ein.

Anschliessend ist das Add-On installiert.

Nun ist oben rechts in Browser das Symbol vom Kee-Add-On ersichtlich.

9. Grundfunktionen der Browser Erweitung

9.1. Login Daten nach Login speichern

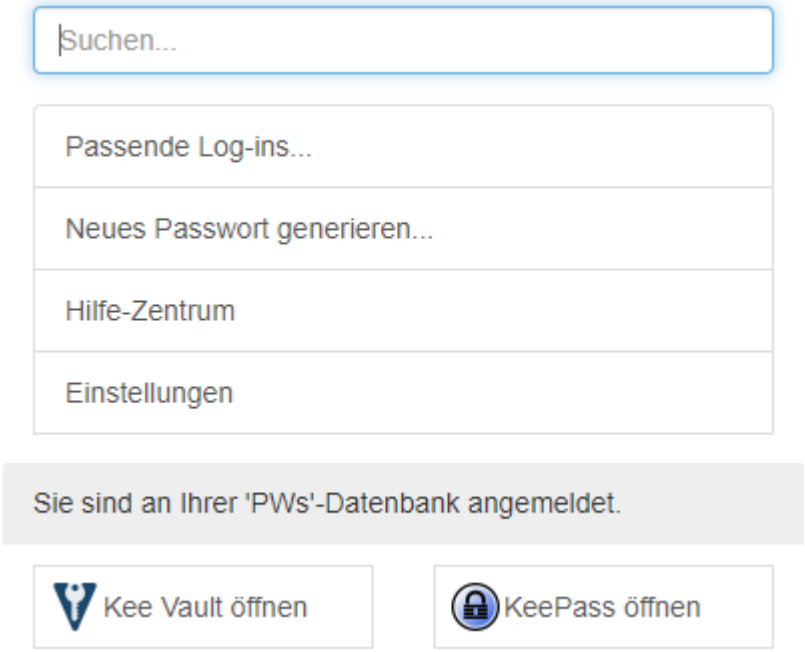


Nach einem Login, kann das Passwort gespeichert werden mit einem Datenbankeintrag.

Dafür klicken Sie nach einem Login, direkt auf das Kee-Add-On Symbol oben rechts. Anschliessend klicken Sie auf Letzte Log-in-Daten speichern.

In Zukunft ist Benutzername und Passwort direkt ausgefüllt bei dieser Webseite.

9.2. Passwörter automatisch einfüllen



Klicken Sie oben rechts auf das Kee Symbol.

Sie können nun nach Passwörtern suchen im Suchfeld, oder auf *passende Log-ins* klicken.

Passende Log-ins sind nur verfügbar, wenn im KeePass ein Eintrag mit der richtigen URL vorhanden ist. Diese Einträge werden durch das Speichern der letzten Log-in-Daten erstellt (beschrieben bei Punkt 4.1)