

---

# KeePass Tutorial

---

**Installation und Nutzung des Passwort-Managers KeePass**  
IT Sicherheit der TU Darmstadt



TECHNISCHE  
UNIVERSITÄT  
DARMSTADT

**IT-Sicherheit!**  
Informationssicherheit | TU Darmstadt

---

## Zusammenfassung

---

Dieses Tutorial erklärt die Installation und Nutzung des Passwort-Managers KeePass.

---

## Inhaltsverzeichnis

---

<b>1</b>	<b>Wichtiger Hinweis</b>	<b>3</b>
<b>2</b>	<b>KeePass Installieren</b>	<b>3</b>
2.1	Durch das HRZ gemangte PCs . . . . .	3
2.2	Alle anderen PCs . . . . .	3
<b>3</b>	<b>Einrichten der portablen KeePass Version (ohne Installation)</b>	<b>6</b>
<b>4</b>	<b>KeePass das erste Mal starten</b>	<b>6</b>
<b>5</b>	<b>Nutzung des Passwortmanagers</b>	<b>9</b>
5.1	Einen neuen Passwort-Eintrag erzeugen . . . . .	10
5.2	Konfigurieren des Password Generators und Erzeugen von Passwörtern . . . . .	11
5.3	Nutzen der Einträge (um sich bei Services einzuloggen) . . . . .	11
<b>6</b>	<b>Synchronisation mit anderen Geräten mittels Hessenbox</b>	<b>12</b>
6.1	Synchronisieren mit dem Hessenbox Client . . . . .	12
6.2	Synchronisieren ohne Hessenbox Client mittels WebDAV . . . . .	12
<b>7</b>	<b>Weiterführende Informationen</b>	<b>13</b>

---

## 1 Wichtiger Hinweis

---

Passwortmanager machen das Leben leichter und Sie werden diese nicht mehr missen wollen. Aber: Sie müssen sich im Klaren sein, dass der Verlust der Passwortdatenbank auch den Verlust all Ihrer Passwörter bedeutet. Das heißt:

- Das Masterpasswort, das Sie für den Schutz der Passwortdatenbank verwenden, dürfen Sie auf keinen Fall vergessen.
- Stellen Sie sicher, dass Sie ein regelmäßiges Backup Ihrer Passwortdatenbank machen, sodass Sie diese im Falle eines Geräteverlusts oder Defekts wiederherstellen können.

---

## 2 KeePass Installieren

---

### 2.1 Durch das HRZ gemangte PCs

---

Wenn Sie einen vom HRZ gemangten Rechner verwenden, können sie KeePass ganz einfach aus dem Softwaredepo installieren. In diesem Fall können Sie die Abschnitte 2.2 und 3 überspringen und einfach mit Abschnitt 4 fortfahren.



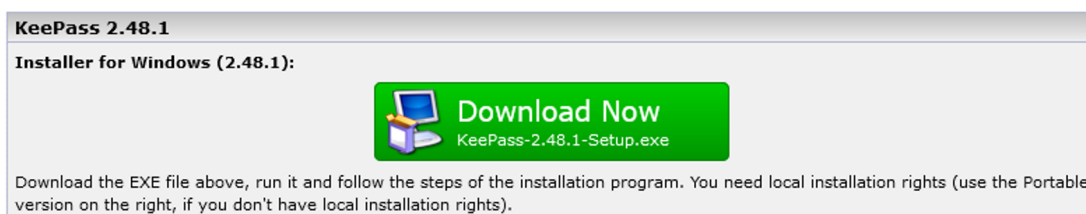
---

### 2.2 Alle anderen PCs

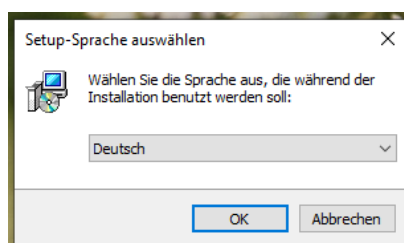
---

Auf allen anderen PCs (ausreichende Berechtigungen vorausgesetzt) können Sie KeePass folgendermaßen installieren. Sollten Sie nicht über die Berechtigung zum Installieren von Software verfügen, können Sie die Portable Version nutzen (siehe Abschnitt 3).

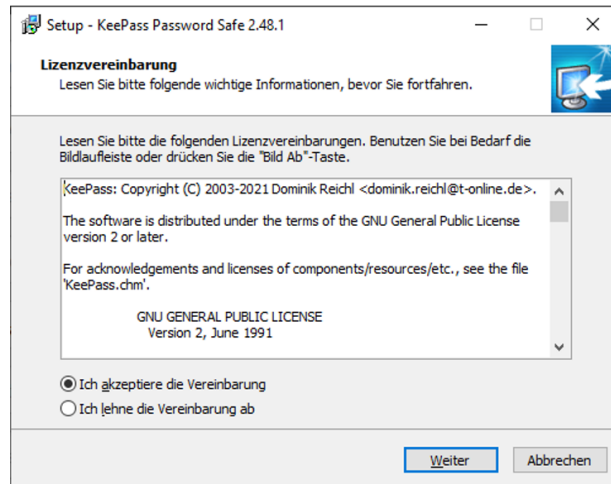
1. Herunterladen von: <https://keepass.info/download.html>



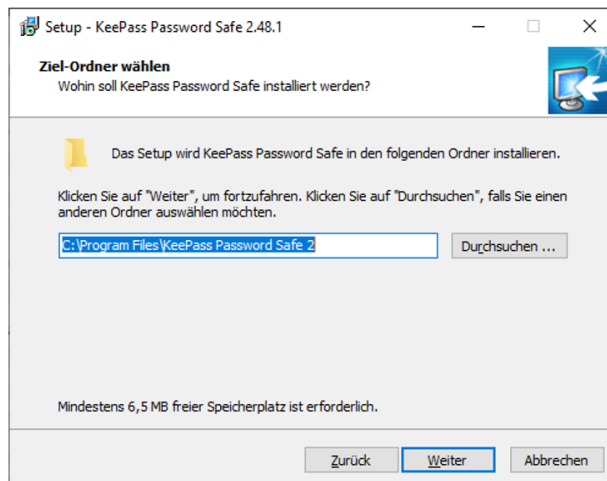
2. Starten Sie den heruntergeladenen Installer. In der Regel bekommen Sie eine Warnung von Windows und werden gefragt, ob Sie die Installation zulassen wollen / Eingabe des Administrator-Kennworts: Bestätigen Sie diese Abfrage bzw. geben sie das Kennwort ein.
3. Wählen Sie die Sprache aus.



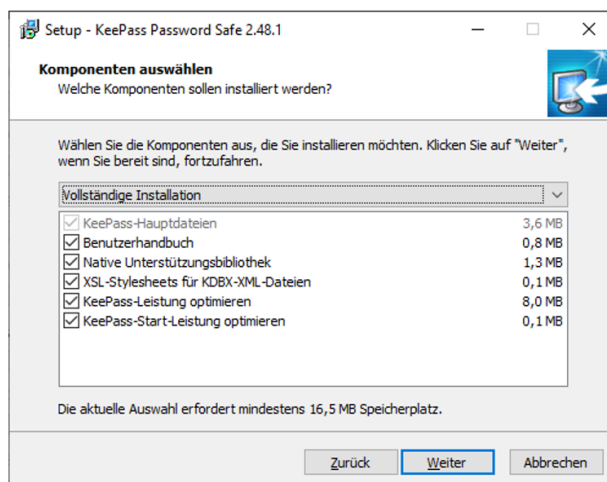
4. Akzeptieren sie die Lizenzvereinbarung.



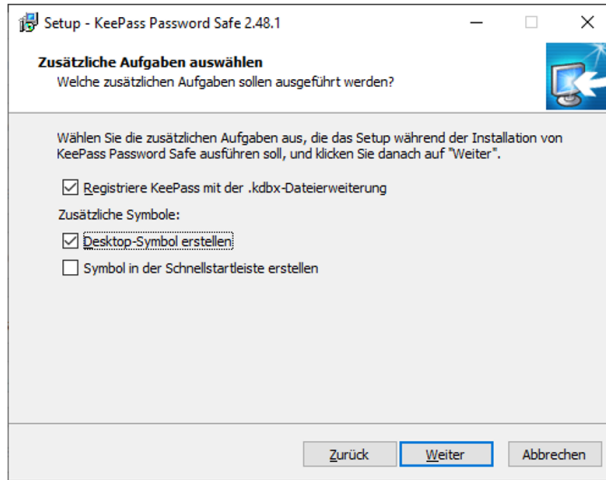
5. Wählen Sie aus wohin KeePass installiert werden soll. Belassen Sie die Standardeinstellungen und bestätigen mit weiter.



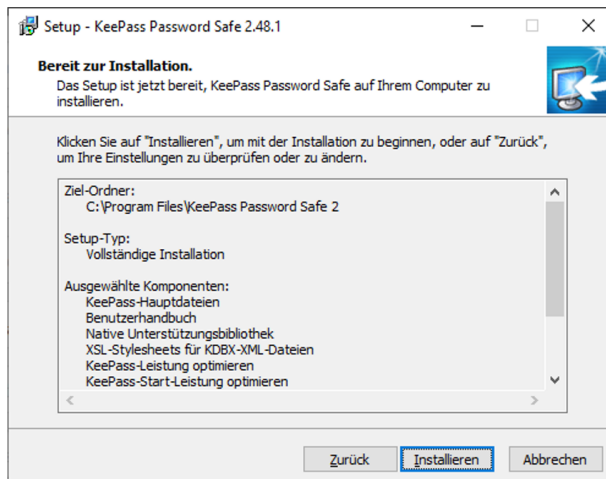
6. Sie werden aufgefordert die Komponenten auszuwählen. Das können Sie lassen wie es voreingestellt ist. Bestätigen mit Weiter.



7. Im nächsten Schritt bietet es sich an ein Desktop Symbol zu erstellen. Weiter.



8. Es wird Ihnen eine Zusammenfassung angezeigt. Wählen Sie Installieren..



9. Beenden Sie den Installer und starten Sie KeePass.



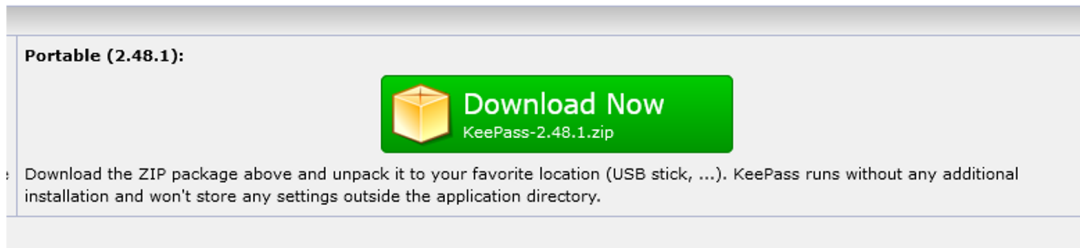
---

## 3 Einrichten der portablen KeePass Version (ohne Installation)

---

Wenn Sie nicht über die Berechtigung zum Installieren von Software verfügen, oder Sie KeePass auf einem portablen Medium wie einem USB Stick installieren wollen, können Sie die Portable Version nutzen.

1. Herunterladen von: <https://keepass.info/download.html>



2. Entpacken sie die heruntergeladene Zip Datei (Rechtsklick → Alle extrahieren...) in einen beliebigen Ordner, beispielsweise in einen neu angelegten Ordner „KeePass“ auf Ihrem Desktop. Wichtig ist, dass Sie sich den Speicherort gut merken. Der Ordner hat nach dem Entpacken folgenden Inhalt:

📁 Languages	10.05.2021 10:28	Dateiordner	
📁 Plugins	10.05.2021 10:28	Dateiordner	
📁 XSL	23.08.2021 11:20	Dateiordner	
📄 KeePass.chm	23.08.2021 11:20	Kompilierte HTML...	747 KB
📄 KeePass.exe	23.08.2021 11:20	Anwendung	3.087 KB
📄 KeePass.exe.config	23.08.2021 11:20	XML Configuratio...	1 KB
📄 KeePass.XmlSerializers.dll	23.08.2021 11:20	Anwendungserwe...	424 KB
📄 KeePassLibC32.dll	23.08.2021 11:20	Anwendungserwe...	561 KB
📄 KeePassLibC64.dll	23.08.2021 11:20	Anwendungserwe...	728 KB
📄 License.txt	23.08.2021 11:20	Textdokument	19 KB
📄 ShInstUtil.exe	23.08.2021 11:20	Anwendung	86 KB

3. Jetzt kann es losgehen. Starten Sie KeePass.exe.

Anmerkung: Im Falle, dass Sie den KeePass Ordner nicht direkt auf Ihrem Desktop abgelegt haben, bietet es sich an ein Verknüpfung zu KeePass.exe auf dem Desktop anzulegen.

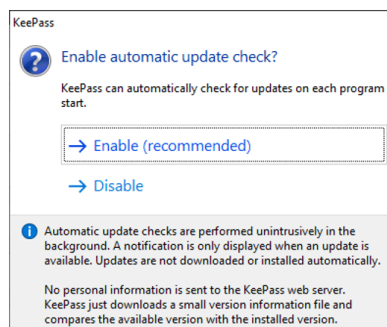
---

## 4 KeePass das erste Mal starten

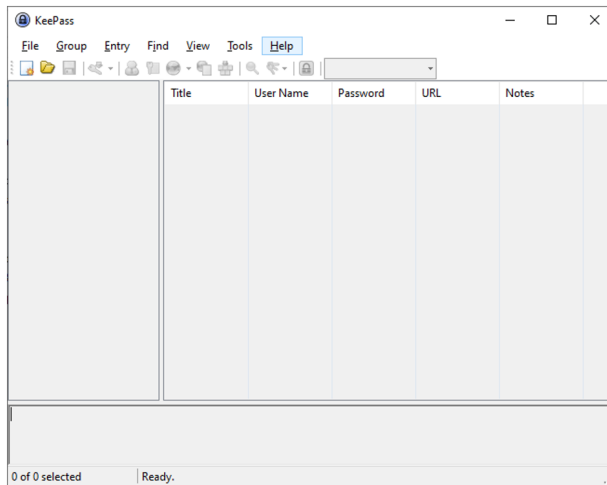
---

Dieser Abschnitt beschreibt die einmalig durchzuführenden Schritte beim ersten Start von KeePass. Wenn Sie KeePass nicht direkt nach der Installation gestartet haben, tun Sie dies jetzt (Windows-Startmenü oder Doppelklick auf KeePass.exe oder die entsprechende Verknüpfung).

1. „Enable automatic update check?“ mit „→ Enable (recommended)“ bestätigen



Sie sehen jetzt das Startfenster des Passwort Managers:



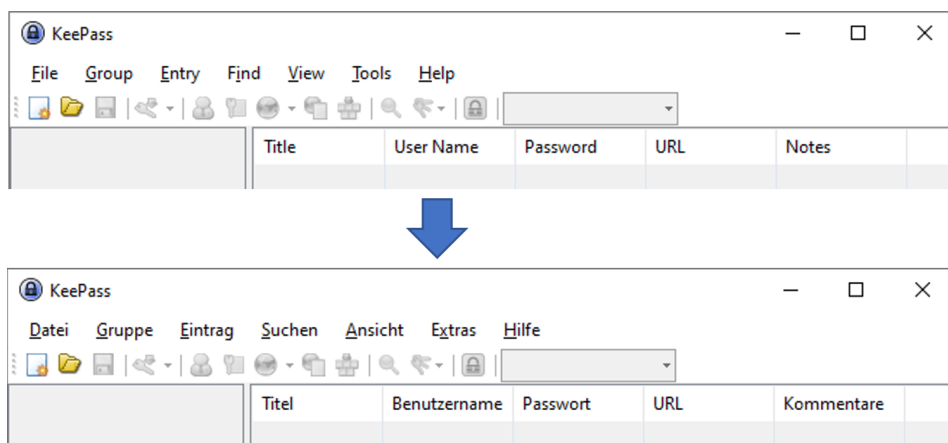
2. KeePass ist zunächst auf Englisch. Falls Sie die englische Version nutzen wollen, können Sie diesen und den nächsten Punkt überspringen.

Es gibt Übersetzungen in eine Vielzahl von Sprachen. Diese finden Sie hier: <https://keepass.info/translations.html>

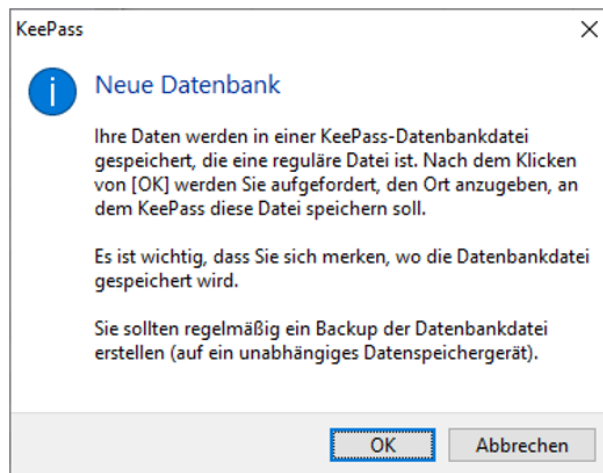
Wollen Sie den Passwortmanager beispielsweise auf Deutsch nutzen, laden Sie sich das deutsche Sprachpaket (wichtig, Version [2.48+]) herunter.

- a) Die heruntergeladene zip Datei entpacken.
- b) Die Datei „German.lngx“ kopieren.
- c) Rufen Sie mit dem Dateimanager den Ordner auf, in den Sie KeePass installiert haben (bei Installation im Standardverzeichnis ist das C:\Program files\KeePass Passwort Safe 2 bzw. C:\Programme\KeePass Passwort Safe 2), oder in den Sie die portable Version gespeichert haben (in unserem Beispiel der KeePass Ordner auf dem Desktop).
- d) Dort finden Sie einen Ordner „Languages“. Öffnen Sie diesen und fügen Sie die „German.lngx“ Datei hier ein.

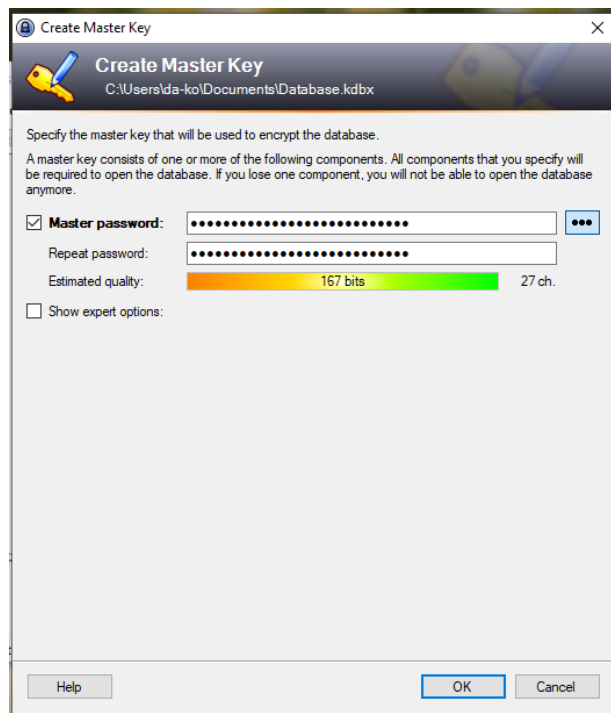
3. Als nächstes wählen Sie in KeePass *View* → *Change language* und wählen dann die gewünschte Sprache, bspw. „German“. KeePass wird neugestartet und erscheint jetzt auf Deutsch.



4. Jetzt muss zunächst eine neue Passwortdatenbank angelegt werden. Wählen Sie *Datei* → *Neu...* Sie bekommen einige Hinweise, die Sie lesen sollten und dann mit OK bestätigen.

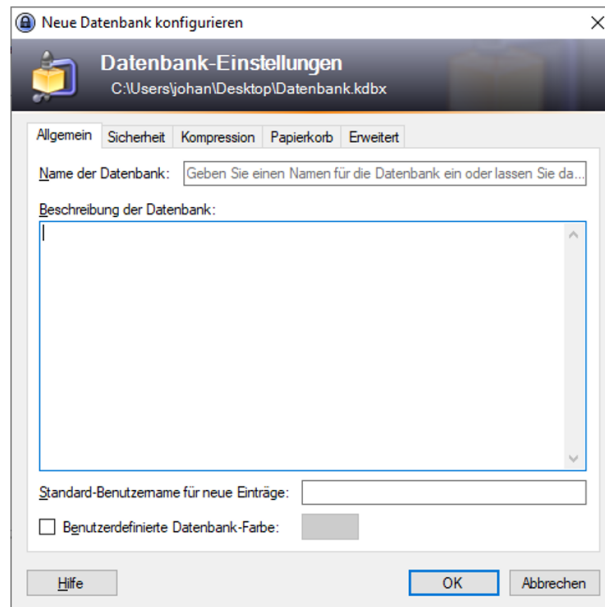


- a) Sie müssen nun einen Speicherort wählen. Das kann ein lokaler Ordner, ein Netzlaufwerk oder ein Ordner der mit Ihrer Hessenbox synchronisiert wird sein (zu Synchronisierung siehe Abschnitt 6). Wenn Sie ihre Passwörter nur auf diesem einen PC nutzen wollen, wählen Sie beispielsweise erneut ihren Desktop. Wichtig ist, dass Sie sich diesen Ort merken.
- b) Geben Sie nun noch einen beliebigen Dateinamen ein. Achten sie darauf die Dateiendung „.kdbx“ nicht zu löschen.
- c) Fahren Sie fort mit „Speichern“.
- d) Nun werden Sie aufgefordert ein Hauptpasswort einzugeben. Das ist das Passwort zum Schutz der Datenbank. This is the password that protects your database and all the contained passwords. **Geben Sie ein möglichst langes Passwort ein (20 Zeichen oder länger – die geschätzte Qualität sollte mindestens ins grün übergehen), dieses müssen Sie sich unbedingt gut merken. Sie benötigen es bei jedem Öffnen der Datenbank.** (Und keine Sorge, Sie müssen die Datenbank nicht bei jeder Verwendung eines Passwortes erneut öffnen, dazu später mehr)





- e) Nach Bestätigung können Sie noch weitere Datenbankeinstellungen tätigen. Hier kann alles auf den Standardeinstellungen belassen werden. Bestätigen Sie einfach mit OK.



- f) Im Anschluss werden Sie gefragt, ob Sie ein Notfallblatt drucken wollen. Dort können Sie das Hauptpasswort vermerken (müssen das Notfallblatt aber unbedingt an einem sicheren Ort aufbewahren). Falls Sie das nicht benötigen, einfach überspringen.

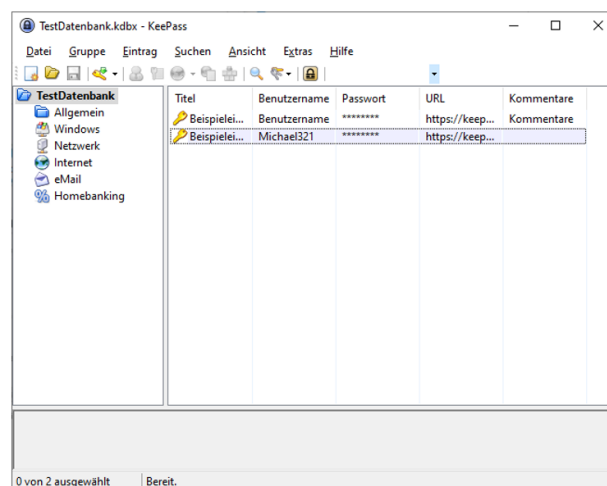
5. Fertig, Sie können jetzt Passworteinträge anlegen.

## 5 Nutzung des Passwortmanagers

Den Passwortmanager müssen Sie zunächst starten. Das machen Sie beispielsweise, wenn Sie beginnen zu arbeiten. Beim Start geben Sie einmal das lange Hauptpasswort ein, und können dann all Ihre Passwörter nach Belieben ohne weitere Passworteingabe nutzen, bis Sie den PW Manager beenden und später neu starten.

Der PW Manager kann dann im Hintergrund laufen. Wichtig ist aber, dass sie den PW Manager niemals unbeaufsichtigt geöffnet lassen (jeder mit Zugriff auf ihren PC hätte dann Zugriff auf all Ihre Passwörter). Sie sollten ihn beenden, wenn Sie aufhören zu arbeiten.


Wenn Sie KeePass erneut starten, wird automatisch die letzte zuvor geöffnete Datenbank geladen und Sie werden aufgefordert das Hauptpasswort einzugeben. Falls Sie eine bestimmte Passwort Datenbank laden wollen, können Sie das bei gestartetem KeePass über *Datei* → *öffnen*.



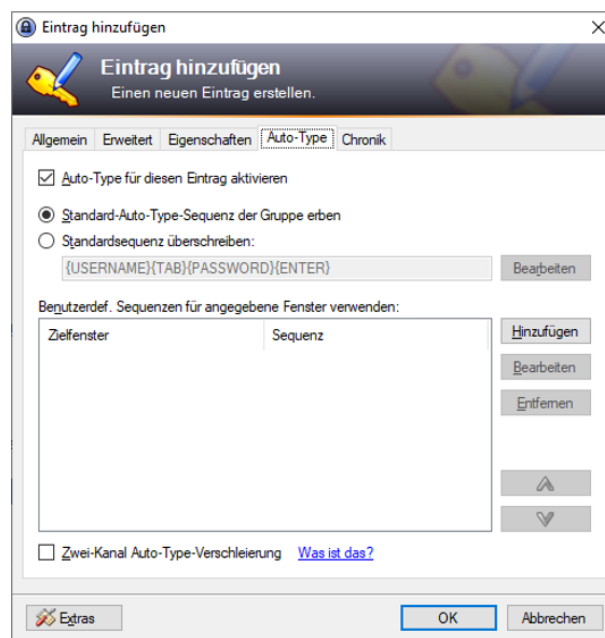
Die zuvor neu angelegte Datenbank enthält bereits zwei Beispieleinträge. Diese können Sie nutzen um auszuprobieren was mit dem PW Manager möglich ist. Wählen Sie einen der Einträge durch Anklicken aus. Wenn sie die Maus über die Icons in der Menüleiste bewegen wird Ihnen angezeigt was die Icons bedeuten.

Links sehen Sie verschiedene vordefinierte Passwortgruppen. Diese können Sie nutzen, um Ihre Passwörter zu kategorisieren. Mit Rechtsklick können Sie weitere Gruppen anlegen, bearbeiten, löschen...

## 5.1 Einen neuen Passwort-Eintrag erzeugen

Einen neuen Passwort-Eintrag erzeugen Sie mit Klick auf . Der neue Eintrag wird in der ausgewählten Gruppe erstellt.

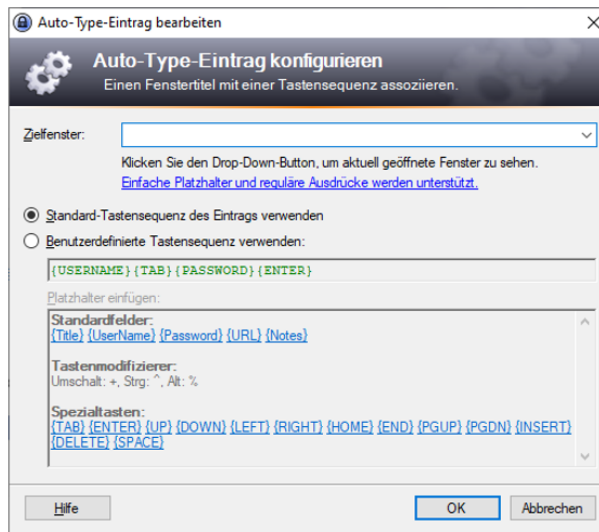
1. Geben Sie einen eindeutigen Titel, Benutzername und Passwort ein. Das Passwortfeld ist bereits mit einem zufällig generierten Passwort vorausgefüllt.
  - I1. Für neu angelegte Accounts können Sie dieses Passwort idR. einfach übernehmen (sollte das Passwort nicht den Richtlinien entsprechen, siehe Abschnitt 5.2).
  - Wenn Sie einen Eintrag zu einem bereits bestehenden Account anlegen, können Sie hier das bestehende Passwort hinterlegen.
  - Das Anlegen von Einträgen für bestehende Accounts ist eine gute Gelegenheit deren Passwörter zu aktualisieren und mit stärkeren Passwörtern zu versehen. Dafür müssen Sie die Passwort-ändern Funktion des jeweiligen Service nutzen, und das bestehende Passwort durch das im Passwortmanager erzeugte ersetzen.
2. Bei URL geben sie die Web Adresse des Service ein. Am besten öffnen Sie die Login Seite in ihrem Browser und kopieren die URL aus der Adresszeile.
3. Um sicherzustellen, dass die automatisierte Eingabe später korrekt funktioniert, gehen Sie jetzt noch zum Reiter „Auto-Type“.




Dann führen Sie folgende Schritte durch:

- a) Öffnen Sie zunächst mit dem Webbrowser parallel die Login Seite des Service (Logindaten nicht eingeben).

- b) Dann kehren Sie zu Auto-Type zurück und wählen „Hinzufügen“. In der Dropdown Liste bei „Zielfenster“ bekommen Sie nun eine Liste aller geöffneten Programme angezeigt. Dort das Browserfenster wählen und OK klicken.




Anmerkung: Die Passwordeingabe im Browser wurde hier nur als Bsp. verwendet. Sie können die Auto-Type Funktion auch für jedes beliebige Programm auf Ihrem Rechner verwenden, das eine Passwort Eingabe erfordert.

- Den gesamten Eintrag nochmals mit OK bestätigen. Der Passwordeintrag ist jetzt angelegt.
- Mit  speichern sie die Änderung in der Datenbank.  
Wenn Sie KeePass beenden, ohne die Änderungen in der Datenbank zu speichern, werden Sie von KeePass aufgefordert, die Änderungen zu speichern.



## 5.2 Konfigurieren des Password Generators und Erzeugen von Passwörtern

Wie erwähnt wird beim Anlegen eines neuen Eintrages direkt ein neues Passwort generiert. Mit Klick auf  können Sie sich dieses anzeigen lassen.

Da es eine Vielzahl verschiedener Passwortrichtlinien gibt, entspricht diese zunächst generierte Passwort möglicherweise nicht den Richtlinien des Service. In diesem Fall:

- Öffnen Sie mittels des Buttons  den Passwortgenerator.
- Dort geben Sie nun an, welche Zeichen das Passwort enthalten soll – entsprechend der Richtlinie – und die gewünschte Passwortlänge. Durch Klick auf Ok wird ein neues Passwort entsprechend den Vorgaben erzeugt.

## 5.3 Nutzen der Einträge (um sich bei Services einzuloggen)

- Manuell:** Wählen Sie den gewünschten Eintrag aus der PW Datenbank. Mit Doppelklick auf den Nutzernamen oder das (maskierte) Passwort wird das jeweilige in den Zwischenspeicher kopiert. Alternativ können Sie die Icons   dafür nutzen. Sie können Nutzernamen bzw. Passwort dann einfach mit der Tastenkombination STRG + V in das vorgesehene Login Feld einfügen.
- AutoType (empfohlen):** Nutzen der Auto-Type Funktion. Navigieren Sie mit ihrem Browser zur Login Seite. Drücken Sie die Tastenkombination STRG + ALT + A. Benutzername und Passwort werden automatisch eingegeben. KeePass muss dafür im Hintergrund geöffnet sein.

---

## 6 Synchronisation mit anderen Geräten mittels Hessenbox

---

**Achtung:** Die Datenbank wird ausschließlich verschlüsselt in der Hessenbox abgelegt. Das ist gut, denn es schützt Ihre Passwörter. Allerdings können parallele Veränderungen an der Datenbank dadurch nicht abgeglichen werden. Daher sollten Sie darauf achten, die Passwortdatenbank immer nur auf einem Gerät geöffnet zu haben, um sicherzustellen, dass keine Änderungen verloren gehen.

Dieser Abschnitt ist nur relevant für Sie, wenn Sie Ihre Passwörter auf mehreren Geräten benötigen. In dem Fall können Sie die Datenbank ganz einfach über die Hessenbox mit anderen Geräten synchronisieren.

---

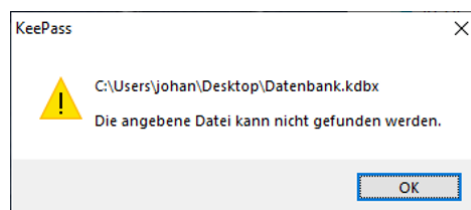
### 6.1 Synchronisieren mit dem Hessenbox Client


---

Hier wird davon ausgegangen, dass Sie den Hessenbox Client bereits eingerichtet haben und bestimmte Ordner automatisch synchronisieren. Eine Anleitung finden Sie hier: [https://www.hrz.tu-darmstadt.de/support\\_und\\_anleitungen/hrz\\_anleitungen/hessenbox\\_anleitungen/index.en.jsp](https://www.hrz.tu-darmstadt.de/support_und_anleitungen/hrz_anleitungen/hessenbox_anleitungen/index.en.jsp)

Um die Synchronisation durchzuführen, muss die Datenbankdatei mit der Endung „.kdbx“, die in obigem Tutorial auf dem Desktop angelegt wurde, lediglich in einem mit der Hessenbox synchronisierten Ordner verschoben werden. Auf diesen Ordner sollten nur Sie Zugriff haben. Am besten legen Sie sich in der Hessenbox einen separaten Ordner „keepass“ an. Dorthin verschieben Sie Ihre Passwortdatenbank. KeePass sollte zuvor geschlossen werden.

Zu beachten: Wenn Sie KeePass nach dem Verschieben erneut öffnen, bekommen Sie eine Fehlermeldung:



Diese mit OK bestätigen. KeePass wird dann ohne Datenbank wie beim ersten Start geöffnet. Über *Datei* → *Öffnen* oder das Icon  können Sie ihre Passwortdatenbank von dem neuen Speicherort öffnen. In Zukunft findet KeePass die Datenbankdatei dann wieder selbst.

Der Hessenbox Client sorgt nun dafür, dass Änderungen direkt in die Hessenbox geladen werden. Auf dem zweiten Gerät richten Sie die Hessenbox Synchronisation gleichermaßen ein und können dort dann die so synchronisierte Passwortdatenbank öffnen und haben direkt Zugriff auf alle Passwörter.

---

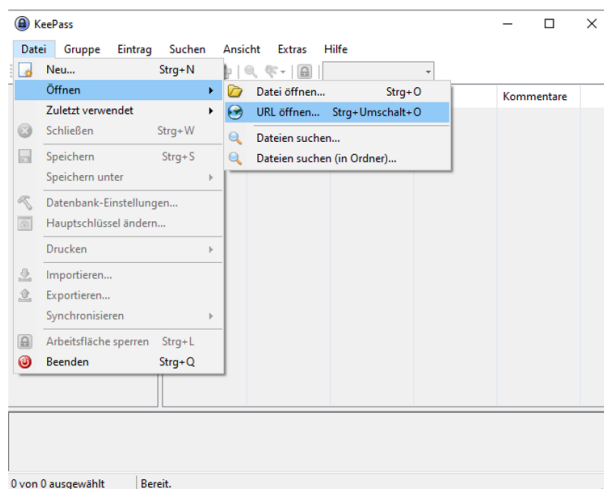
### 6.2 Synchronisieren ohne Hessenbox Client mittels WebDAV

---

**Achtung:** Wenn Sie die Datenbank über WebDAV öffnen, haben Sie nur Zugriff, wenn Sie bereits online sind und die Hessenbox verfügbar ist. Daher sollten Sie die Datenbank auf mindestens einem Gerät lokal gespeichert haben und mittels Hessenbox Client synchronisieren. WebDAV bietet sich beispielsweise bei mobilen Endgeräten an.

Eine Alternative, wie Sie ihre Passwortdatenbank von verschiedenen Geräten aus abrufen können, ohne den Hessenbox Client installieren zu müssen, ist WebDAV. Dies wird von der Hessenbox ebenfalls unterstützt. Nehmen wir an, Sie haben in ihrer Hessenbox einen Ordner „keepass“ angelegt und in diesem die Datenbank „pw.kdbx“ gespeichert.

Dann können Sie diese einfach öffnen, indem Sie im Öffnen Dialog von KeePass „URL öffnen“ wählen: *Datei* → *Öffnen* → *URL öffnen...*



Die WebDAV URL, die Sie eintragen müssen, ist dann <https://hessenbox.tu-darmstadt.de/webdav/keepass/pw.kdbx>. Die Zugangsdaten sind TU-ID und zugehöriges Passwort. Danach werden Sie aufgefordert das Hauptpasswort ihrer Passwortdatenbank einzugeben und die Datenbank wird wie gehabt geöffnet.

Viele andere KeePass kompatible Passwortmanager wie beispielsweise KeePass2Android unterstützen ebenfalls WebDAV. Dort wird das Protokoll direkt explizit als Option im Öffnen Dialog angezeigt.

---

## 7 Weiterführende Informationen

---

- BSI: Passwörter verwalten mit dem Passwort-Manager  
[https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager\\_node.html](https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html)
- Sehr ausführliche Tutorials finden Sie auf den Seiten der TU Braunschweig
  - KeyPassXC <https://doku.rz.tu-bs.de/doku.php?id=software:keepassxc>
  - KeePass2Android <https://doku.rz.tu-bs.de/doku.php?id=software:keepass2android>