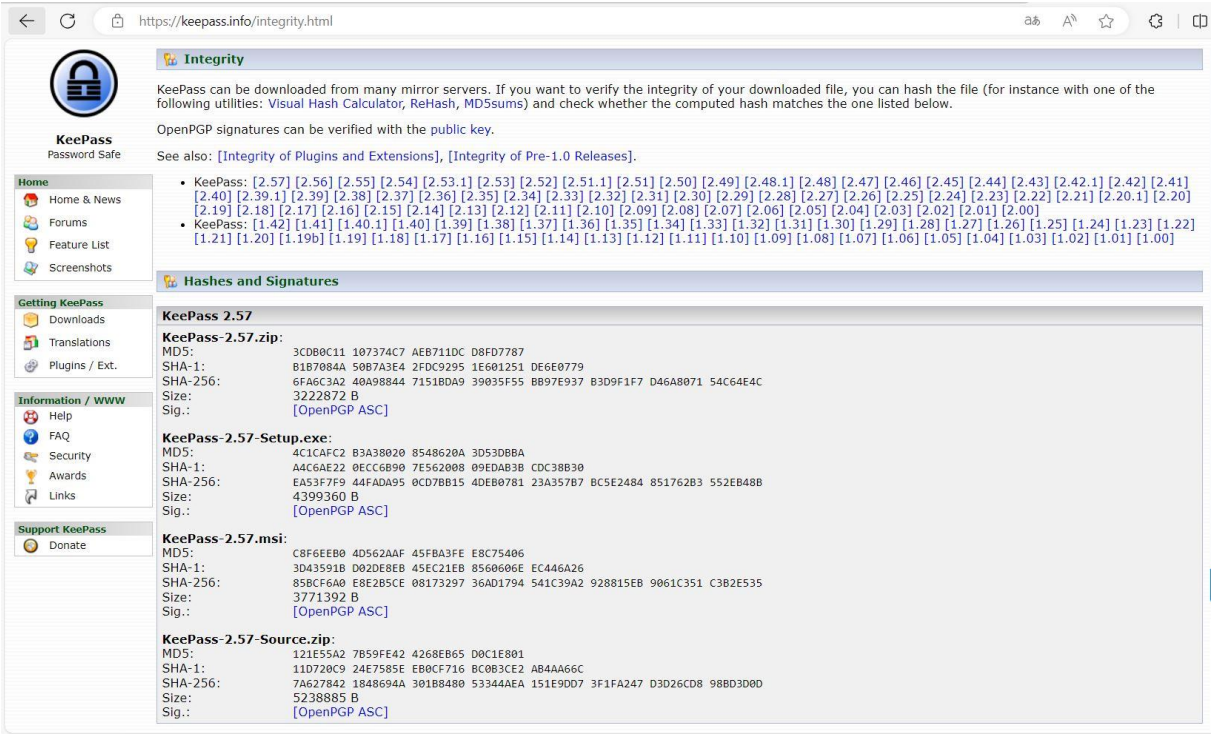
KeePass installieren

Die Kontrolle von Sicherheitssoftware ist elementar wichtig, denn ein manipulierter Passwortmanager mit einer Hintertür für Cyberkriminelle ist sehr gefährlich. Aus diesem Grund wird von Ihrer IT-Abteilung eine sichere Version auf einem internen File Server bereitgestellt.

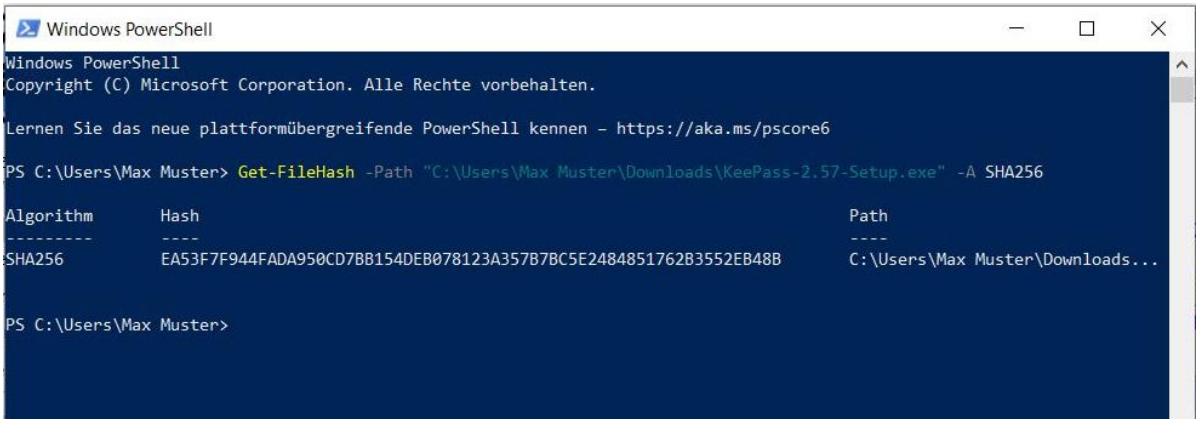
Speicherort:

Sicherheitsüberprüfung nur für private Nutzung

Falls Sie auch privat Ihre Passwörter sicher verwalten wollen, beziehen Sie bitte den Passwortmanager nur von der offiziellen Quelle. https://keepass.info/ Bitte überprüfen Sie anschließend die Echtheit der Software mit diesen Daten. https://keepass.info/integrity.html



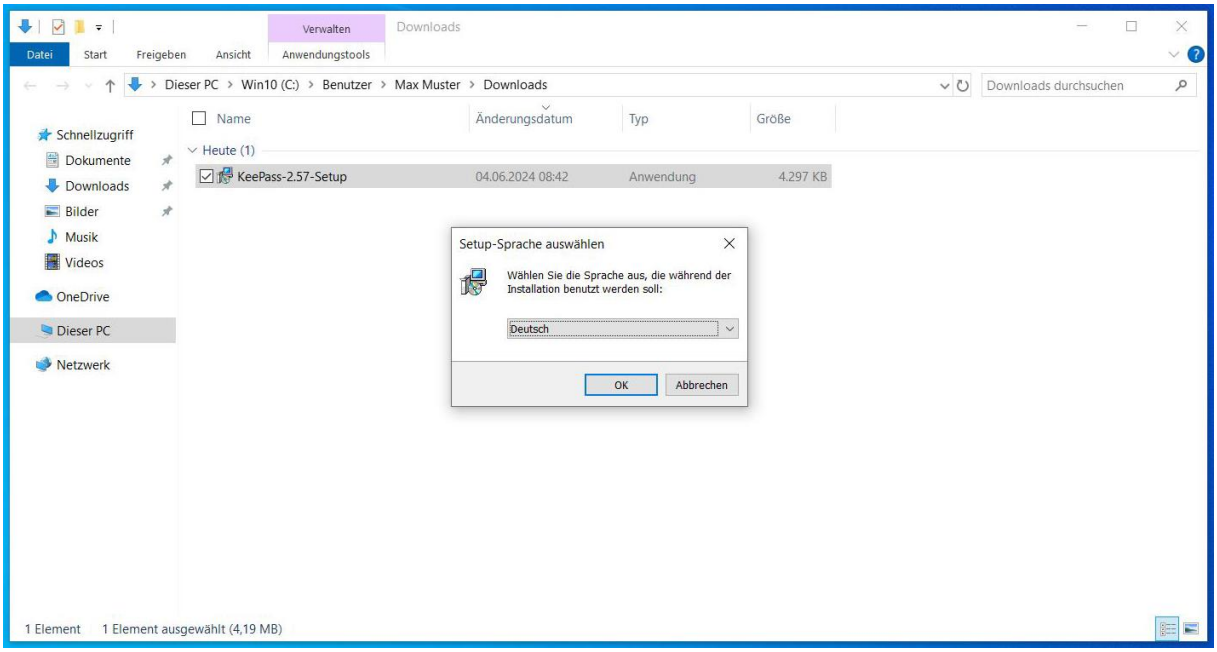
Bei Windows Systemen können Sie die Echtheit der Software mit der im Betriebssystem integrierten PowerShell überprüfen. Hier ein Screenshot:

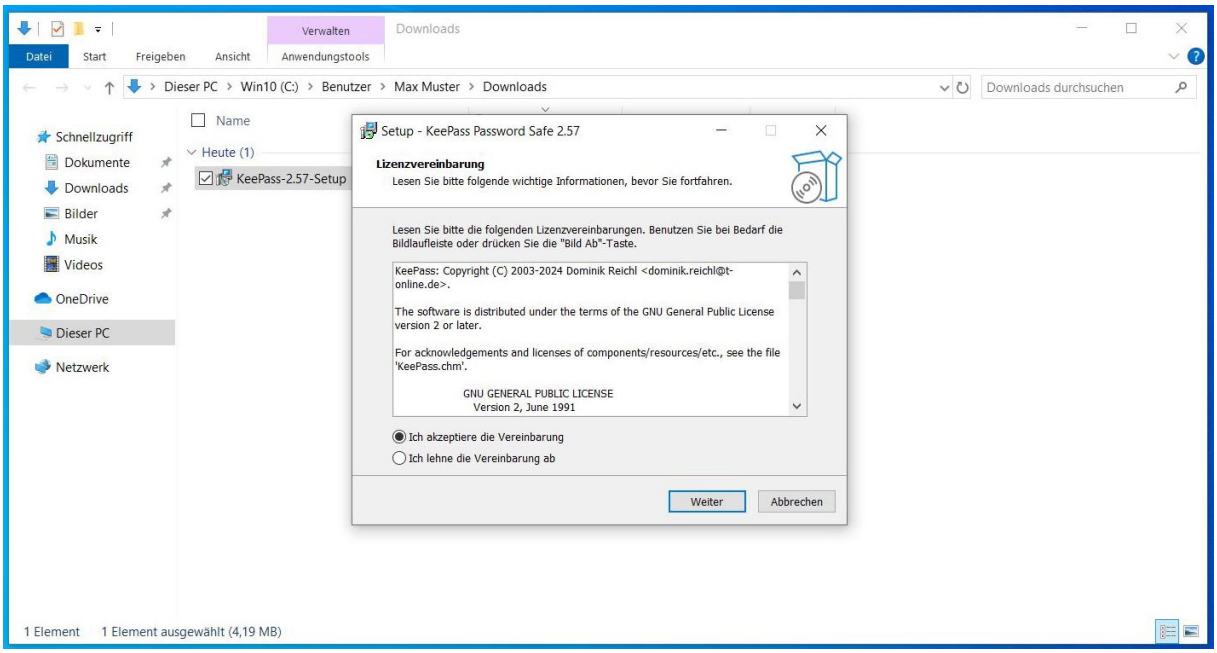


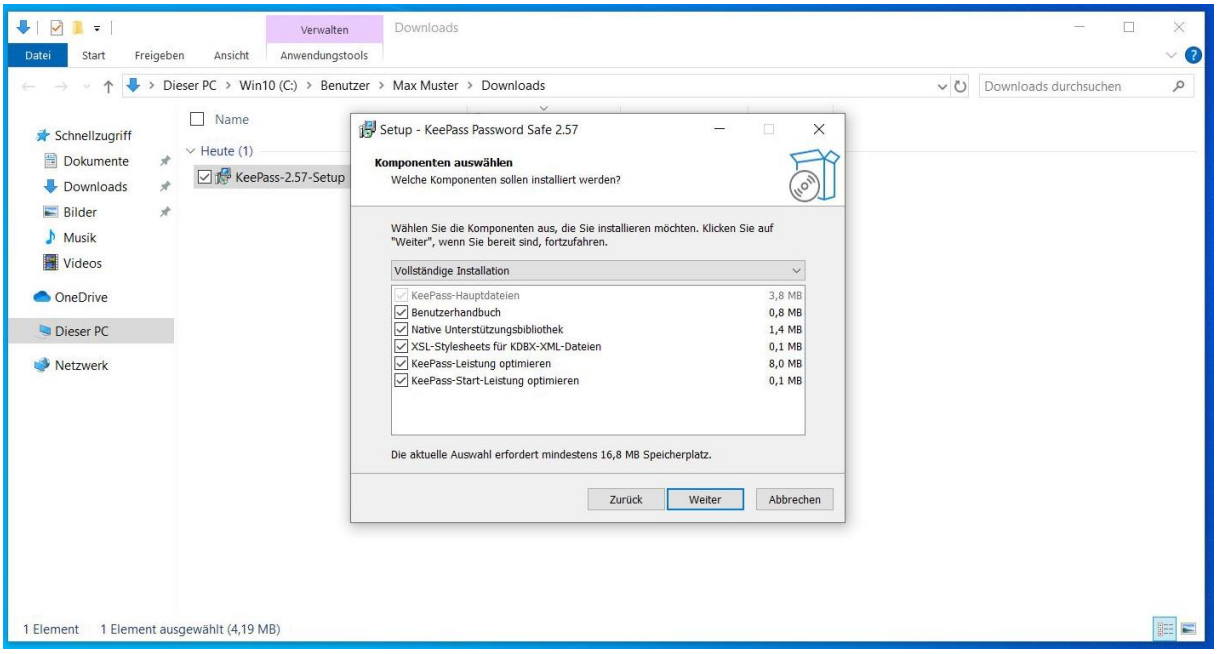
Den errechneten HASH-Wert können Sie dann mit dem Wert auf der Internetseite vergleichen. Falls dieser nicht übereinstimmt, wurde die Datei manipuliert und Sie sollten Sie keinesfalls verwenden. Diese Überprüfung muss auch bei jedem Update durchgeführt werden.

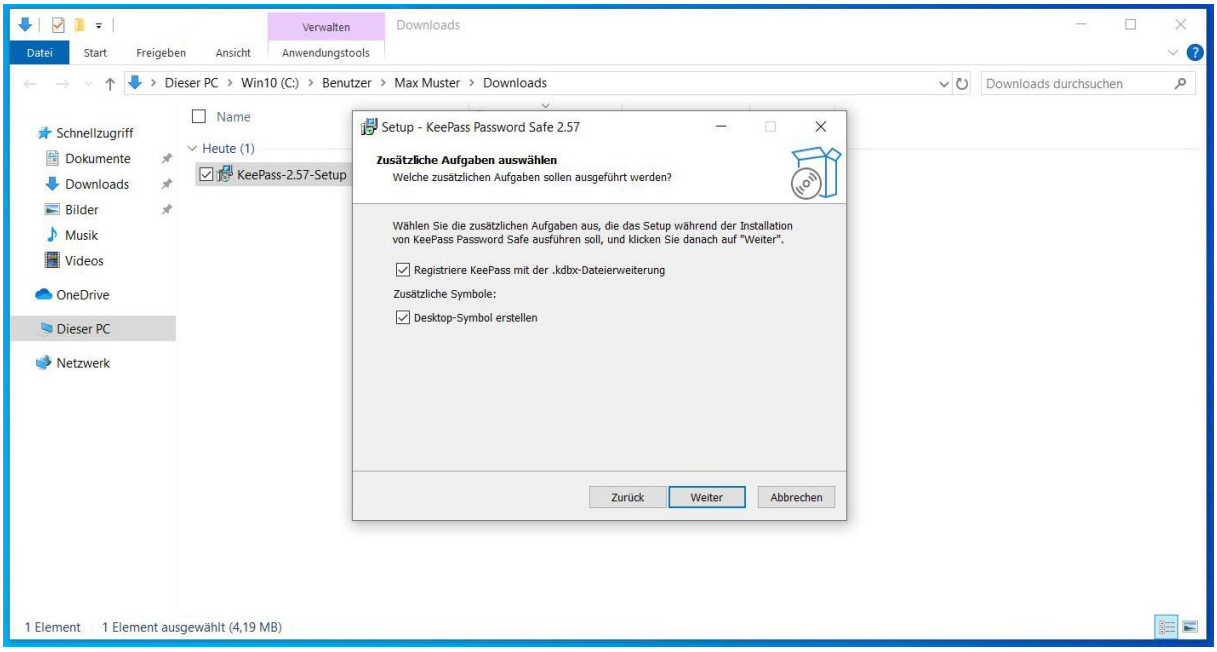
Installation starten

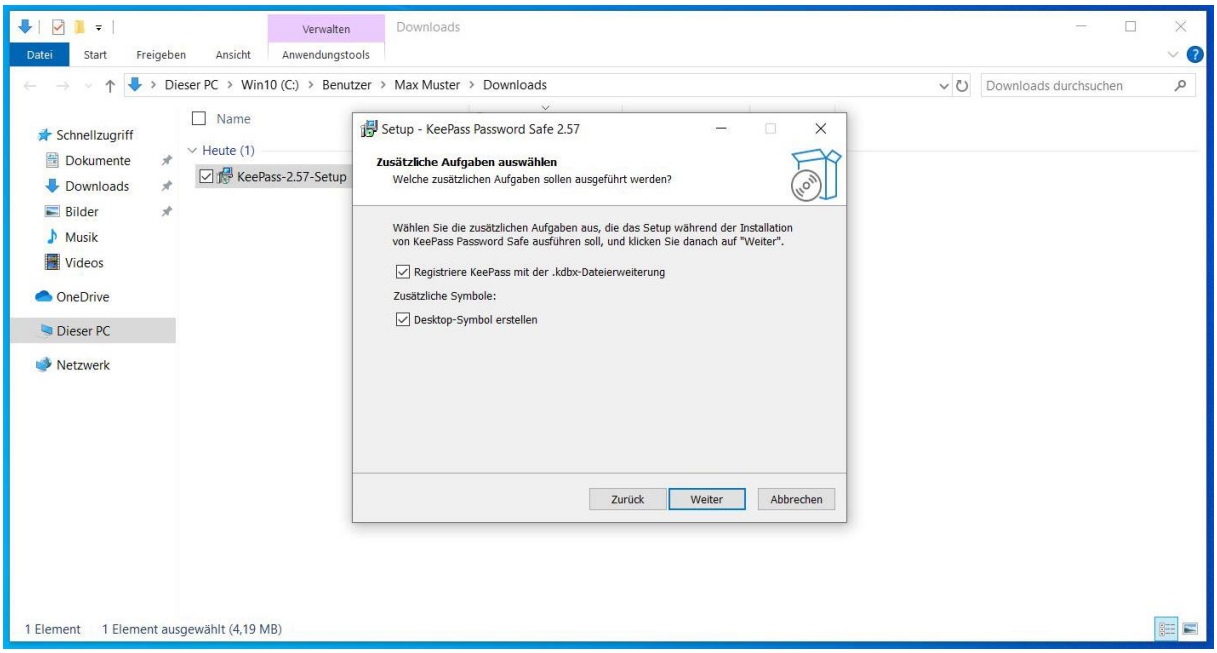
Schritt 1: Führen Sie die Datei – KeePassX-XX-Setup.exe aus.

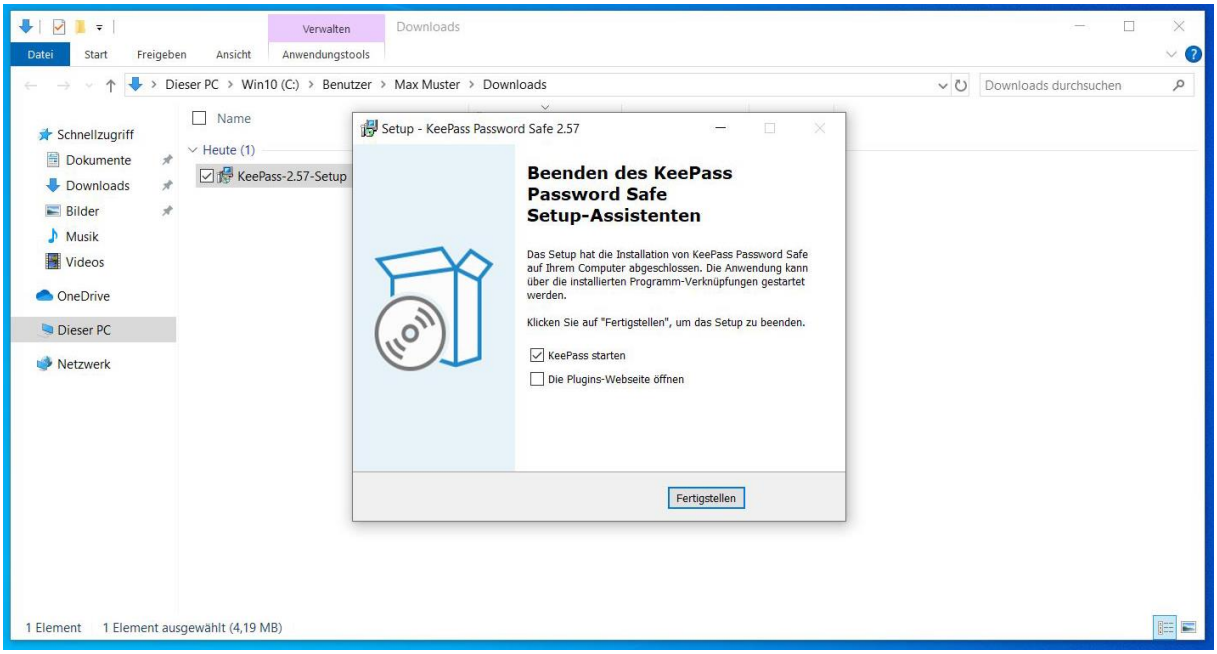


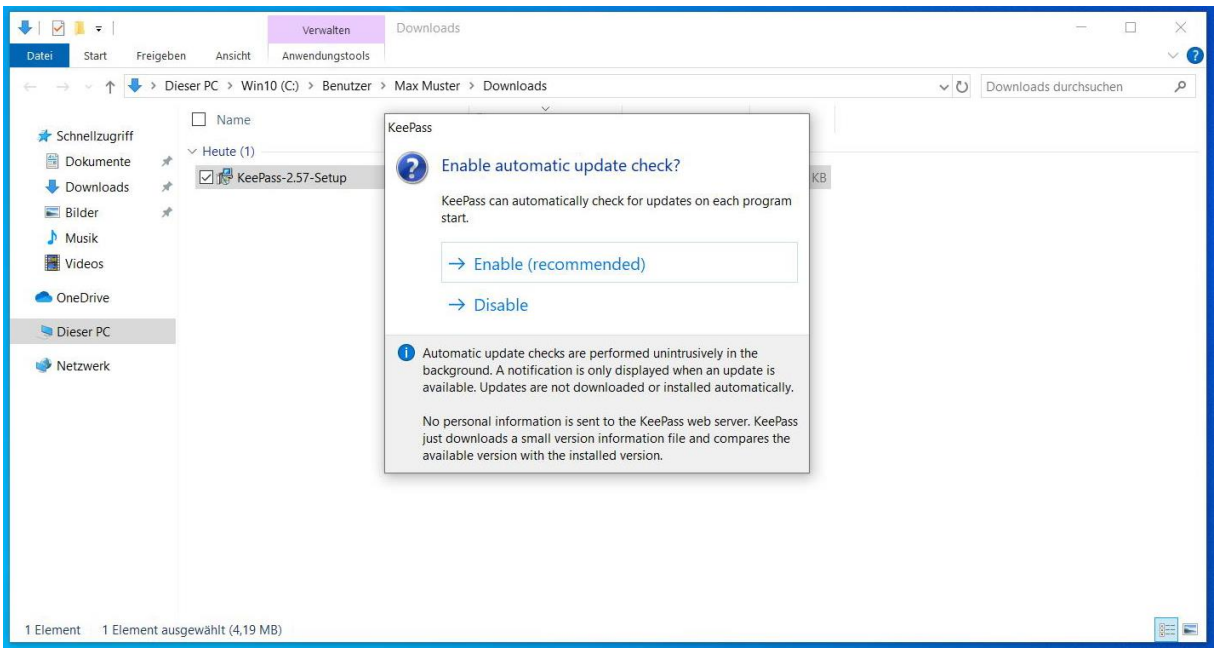



Verwalten
Downloads
Datei
Start
Freigeben
Ansicht
Anwendungstools
Dieser PC › Win10 (C:) › Benutzer › Max Muster › Downloads
Downloads durchsuchen
Schnellzugriff
Dokumente
Downloads
Bilder
Musik
Videos
OneDrive
Dieser PC
Netzwerk
Name
Heute (1)
KeePass-2.57-Setup
Setup - KeePass Password Safe 2.57
Komponenten auswählen
Welche Komponenten sollen installiert werden?
Wählen Sie die Komponenten aus, die Sie installieren möchten. Klicken Sie auf "Weiter", wenn Sie bereit sind, fortzufahren.
Vollständige Installation
KeePass-Hauptdateien 3,8 MB
Benutzerhandbuch 0,8 MB
Native Unterstützungsbibliothek 1,4 MB
XSL-Stylesheets für KDBX-XML-Dateien 0,1 MB
KeePass-Leistung optimieren 8,0 MB
KeePass-Start-Leistung optimieren 0,1 MB
Die aktuelle Auswahl erfordert mindestens 16,8 MB Speicherplatz.
Zurück
Weiter
Abbrechen
1 Element
1 Element ausgewählt (4,19 MB)


Verwalten
Downloads
Datei
Start
Freigeben
Ansicht
Anwendungstools
Dieser PC › Win10 (C:) › Benutzer › Max Muster › Downloads
Downloads durchsuchen
Schnellzugriff
Dokumente
Downloads
Bilder
Musik
Videos
OneDrive
Dieser PC
Netzwerk
Name
Heute (1)
KeePass-2.57-Setup
Setup - KeePass Password Safe 2.57
Zusätzliche Aufgaben auswählen
Welche zusätzlichen Aufgaben sollen ausgeführt werden?
Wählen Sie die zusätzlichen Aufgaben aus, die das Setup während der Installation von KeePass Password Safe ausführen soll, und klicken Sie danach auf "Weiter".
Registriere KeePass mit der .kdbx-Dateierweiterung
Zusätzliche Symbole:
Desktop-Symbol erstellen
Zurück
Weiter
Abbrechen
1 Element
1 Element ausgewählt (4,19 MB)


Verwalten
Downloads
Datei
Start
Freigeben
Ansicht
Anwendungstools
Dieser PC › Win10 (C:) › Benutzer › Max Muster › Downloads
Downloads durchsuchen
Schnellzugriff
Dokumente
Downloads
Bilder
Musik
Videos
OneDrive
Dieser PC
Netzwerk
Name
Heute (1)
KeePass-2.57-Setup
Setup - KeePass Password Safe 2.57
Zusätzliche Aufgaben auswählen
Welche zusätzlichen Aufgaben sollen ausgeführt werden?
Wählen Sie die zusätzlichen Aufgaben aus, die das Setup während der Installation von KeePass Password Safe ausführen soll, und klicken Sie danach auf "Weiter".
Registriere KeePass mit der .kdbx-Dateierweiterung
Zusätzliche Symbole:
Desktop-Symbol erstellen
Zurück
Weiter
Abbrechen
1 Element
1 Element ausgewählt (4,19 MB)

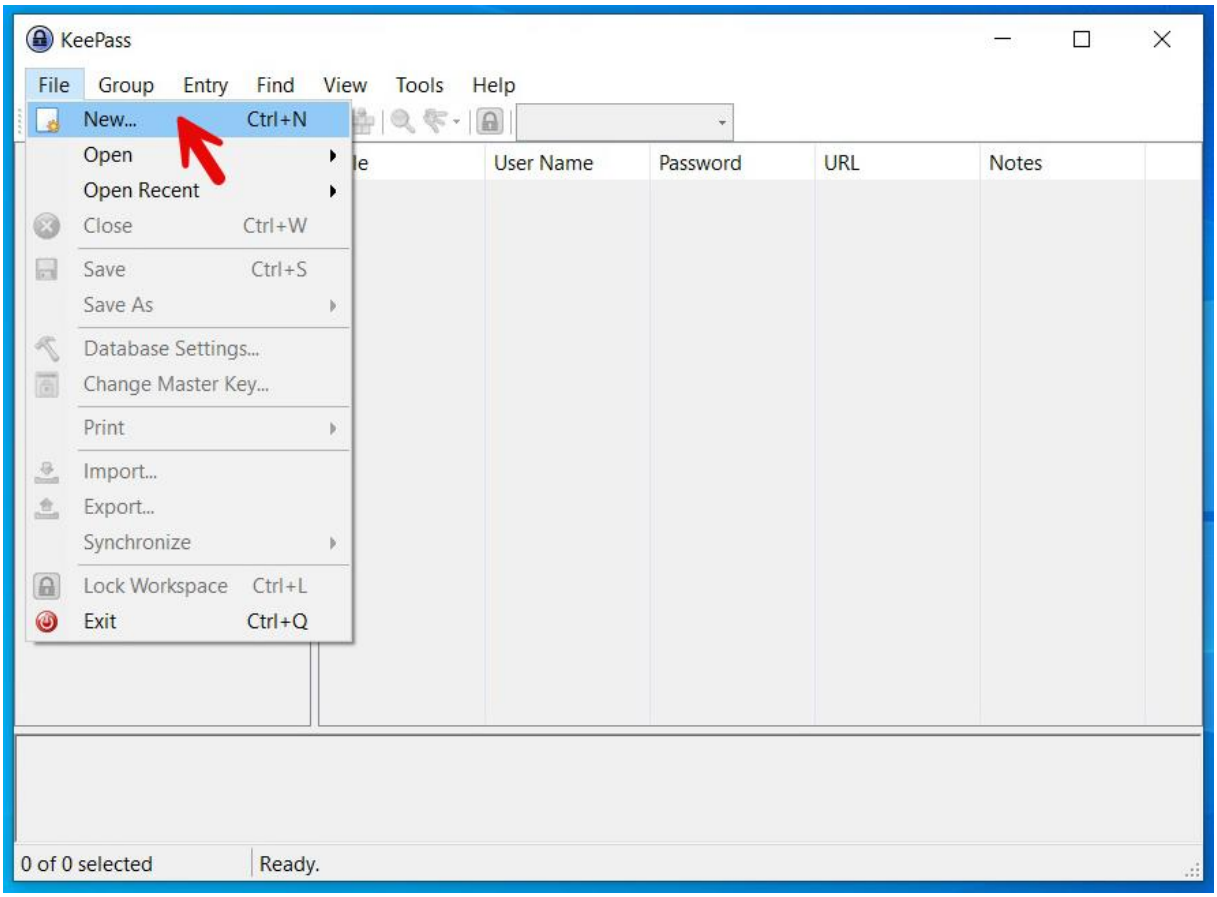




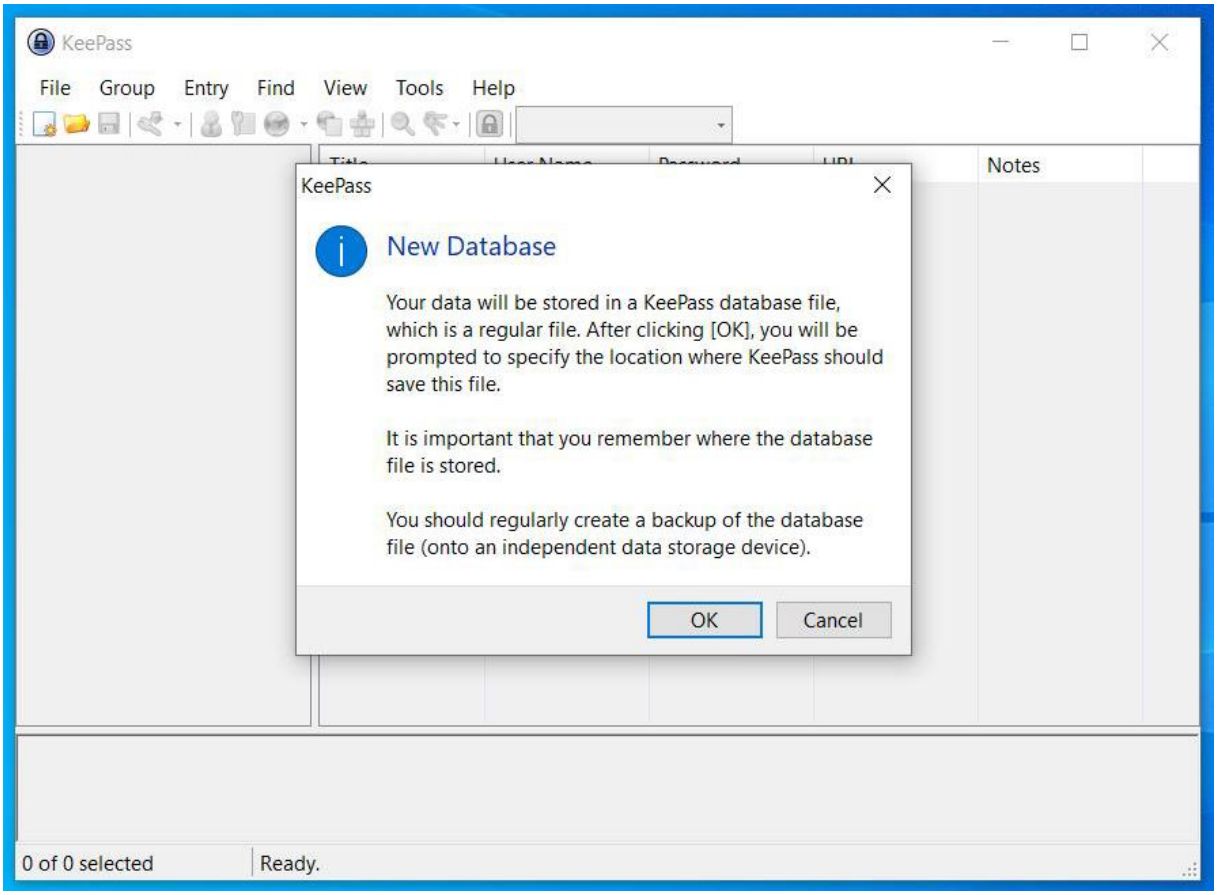
Um regelmäßig über Updates informiert zu werden, wählen Sie bitte „Enable (recommended)“ aus.

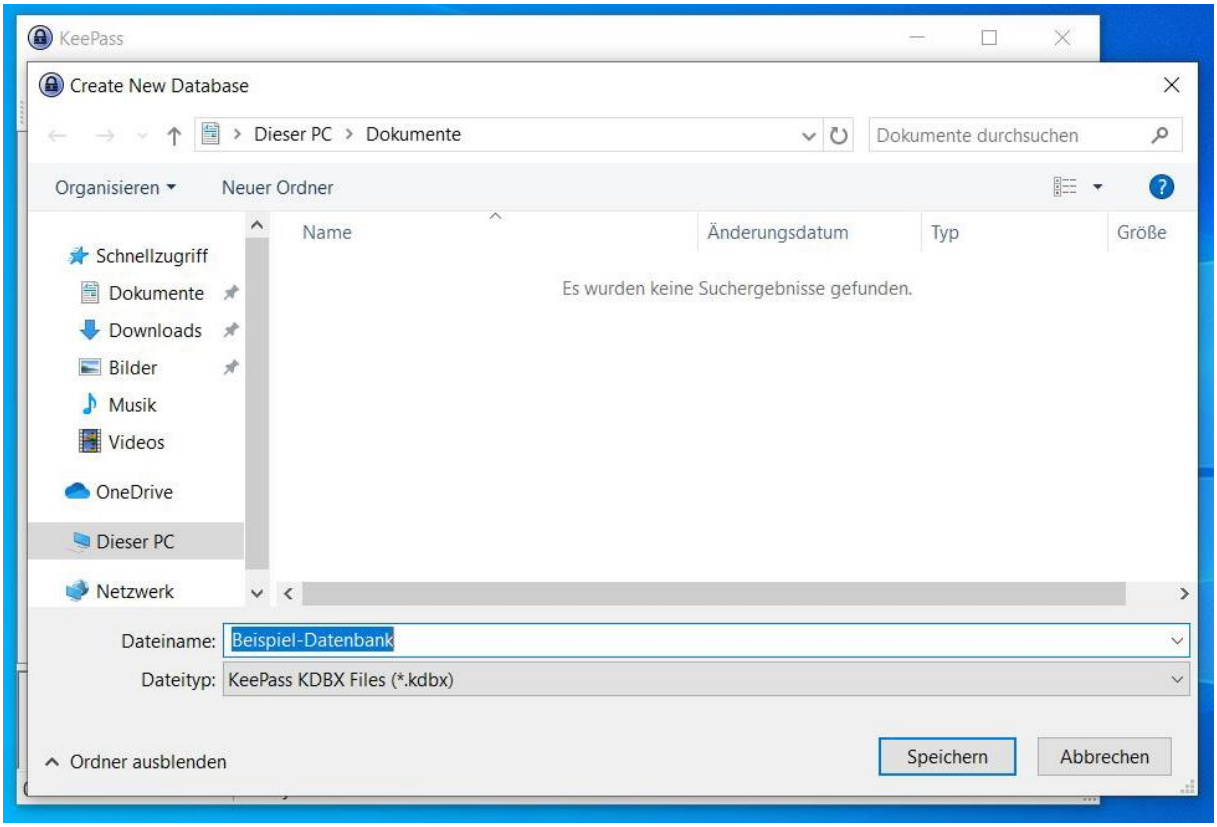
Konfiguration - KeePass Datenbank für Ihre Passwörter anlegen

Bevor Sie erste Passwörter in KeePass abspeichern können, müssen Sie sich zuerst über „File“ -> „New“ eine neue Datenbank anlegen.



Speicherort wählen

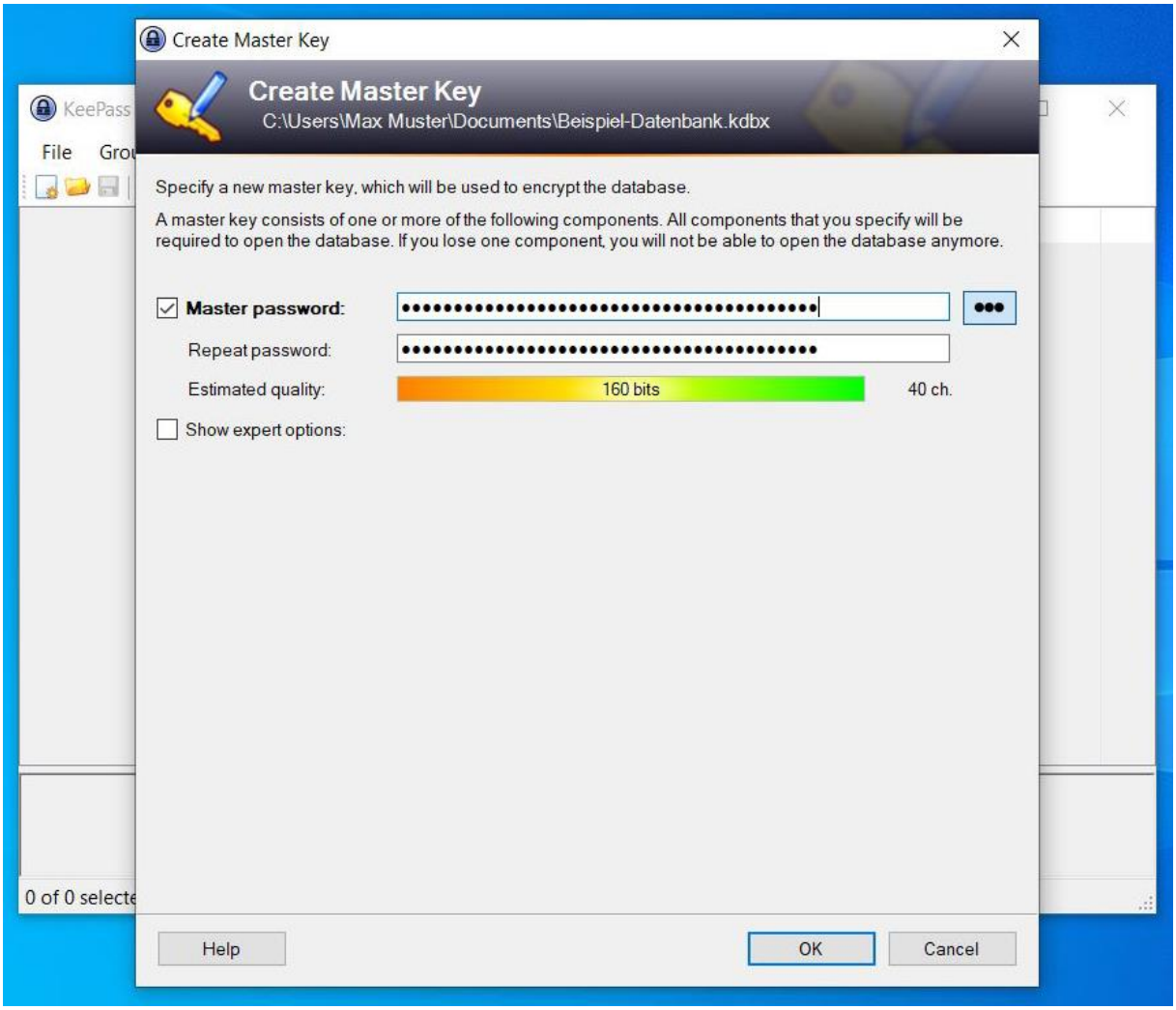




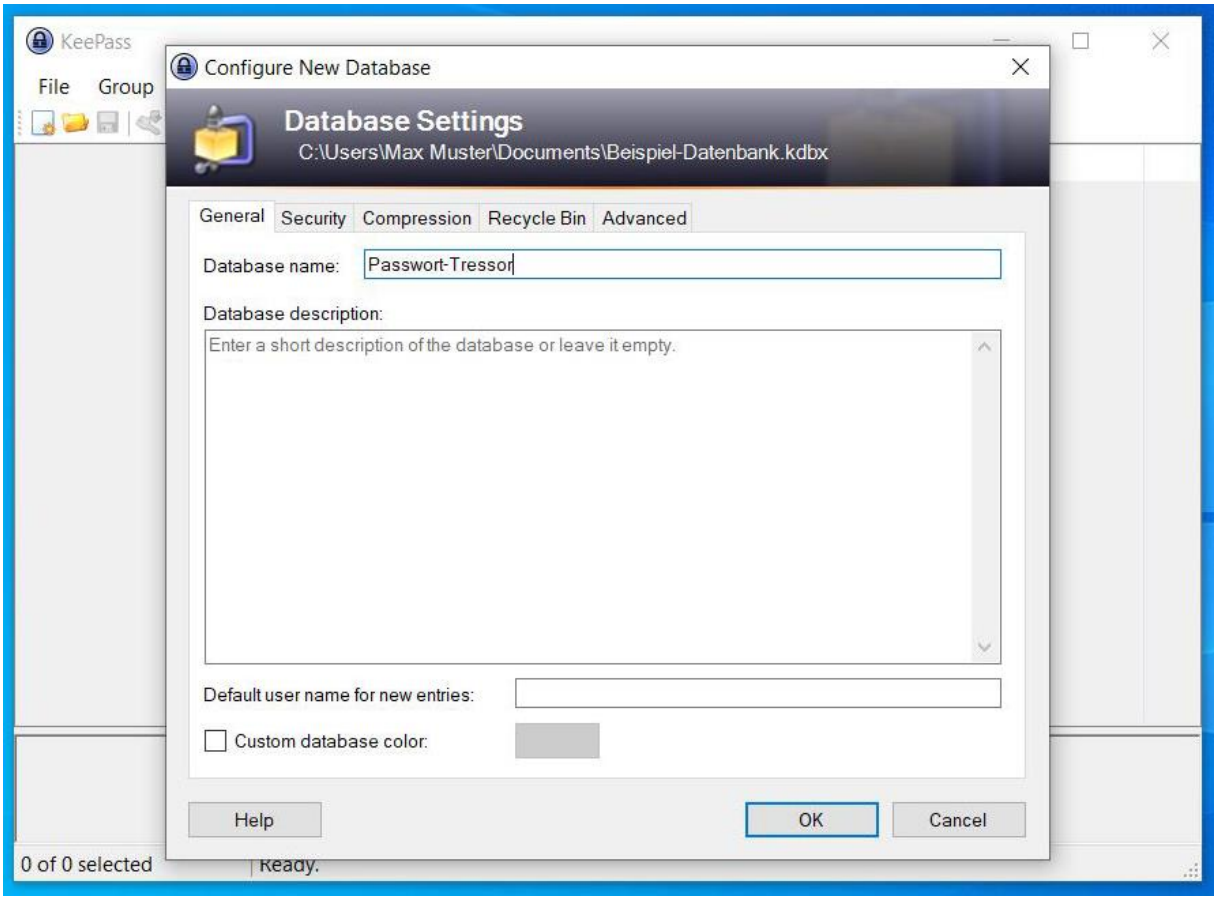
Wichtig: Bitte bedenken Sie bei der Auswahl des Speicherorts, dass nur Sie selbst Zugriff auf die Datenbank haben dürfen! Die Ablage sollte zudem nicht im KeePass Ordner erfolgen. So verhindern Sie, dass bei Löschung einer älteren KeePass Version die Datenbank mit gelöscht wird. Bitte beachten Sie, dass Sie die Datenbank regelmäßig sichern.

Schritt 3: Hauptschlüssel eingeben

Immer wenn Sie Ihren Passwortmanager öffnen müssen Sie dieses Kennwort eingeben.



Wichtig: Bitte beachten Sie hierbei, dass dieses Passwort alle Ihre anderen Passwörter schützt! Es sollte daher sehr komplex und lang sein. Mindestens sollte es jedoch 12 Zeichen lang sein, Groß- & Kleinbuchstaben, Sonderzeichen und Zahlen enthalten. Bitte beachten Sie dabei die Anforderungen aus der Passwortrichtlinie.

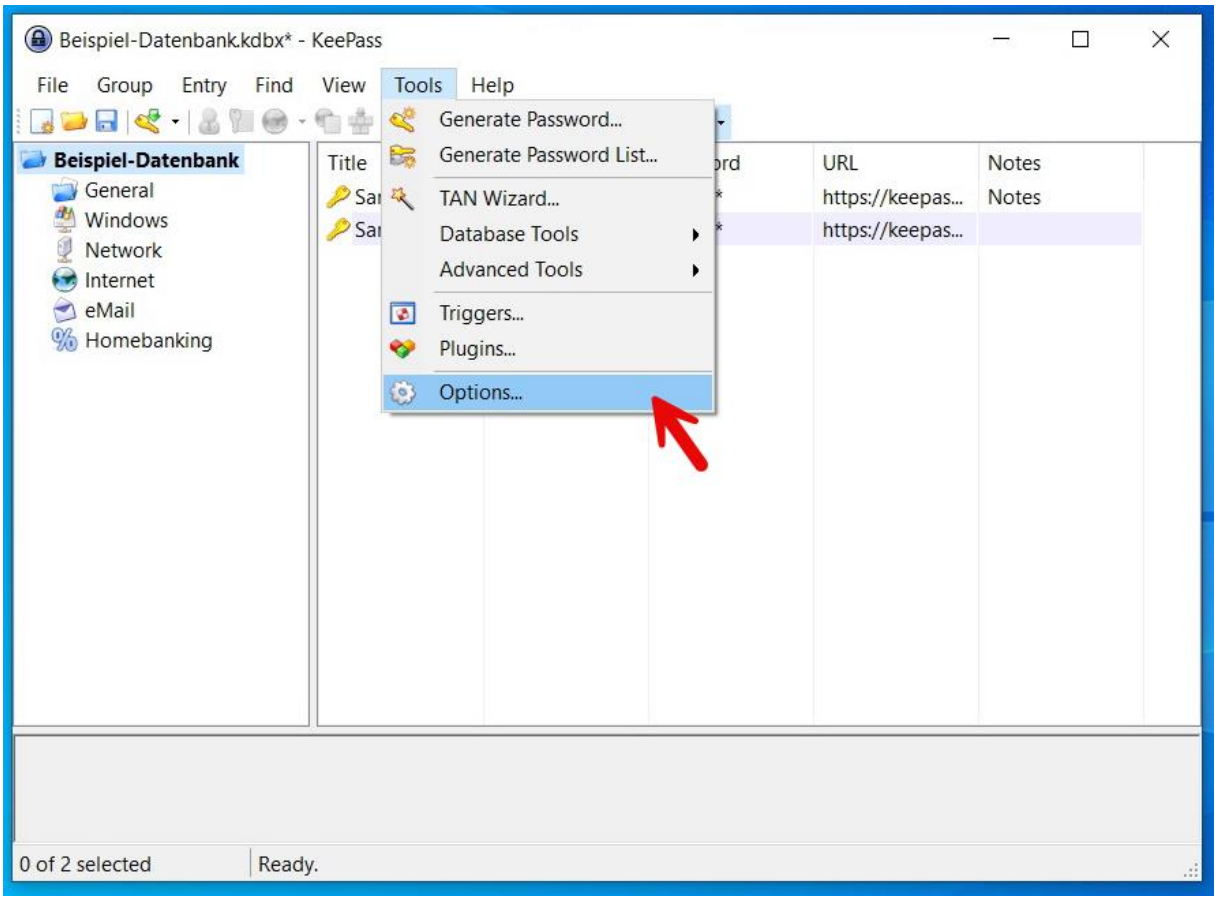


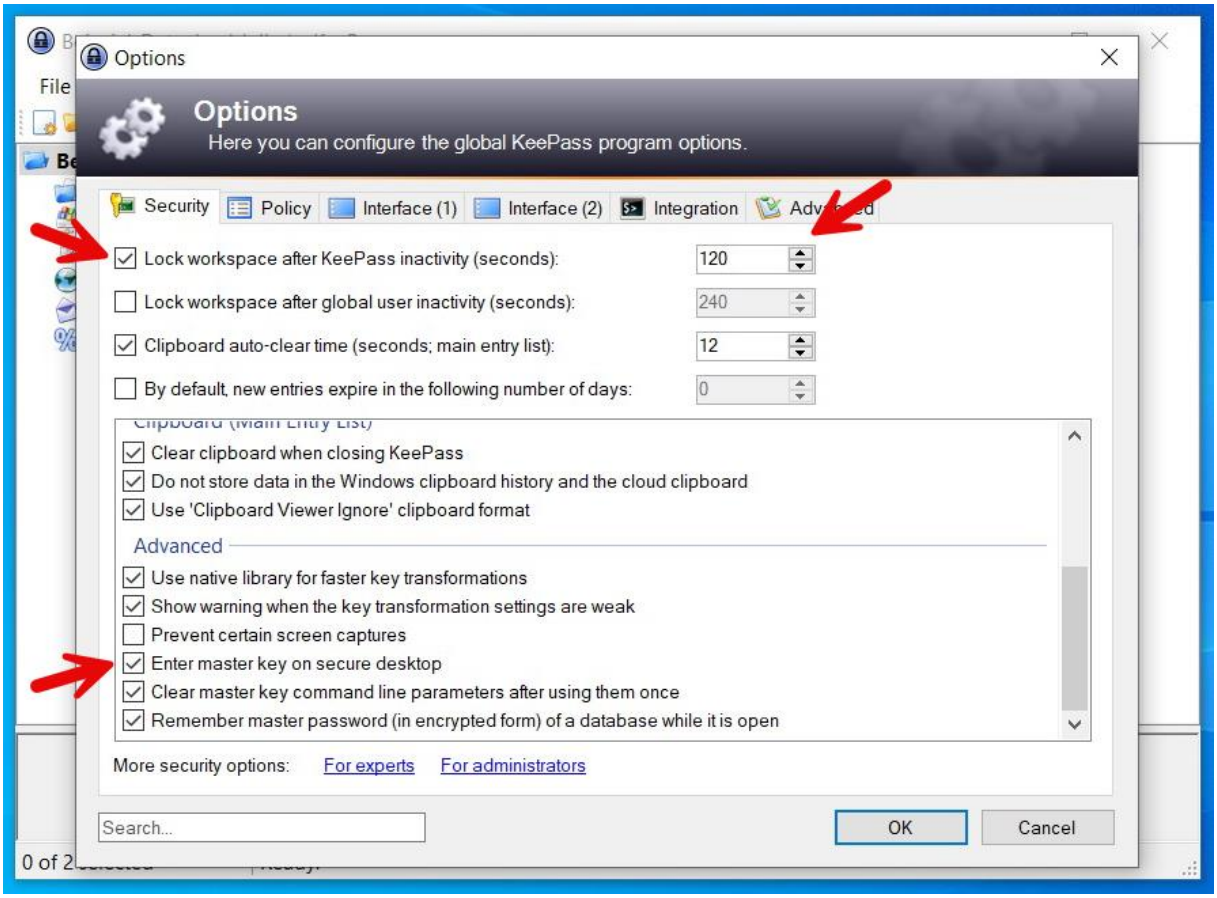
Notfallblatt erstellen

Drucken Sie sich Ihr Notfallblatt aus und verwahren Sie es an einem sicheren Ort. Es kann Ihnen helfen, wenn Sie nach einem schönen Urlaub Ihr Passwort vergessen haben sollten.

Sicherheitseinstellungen

Nachdem Ihre Datenbank angelegt wurde, sollten Sie über „Tools“ -> „Options“ ein paar Sicherheitseinstellungen anpassen





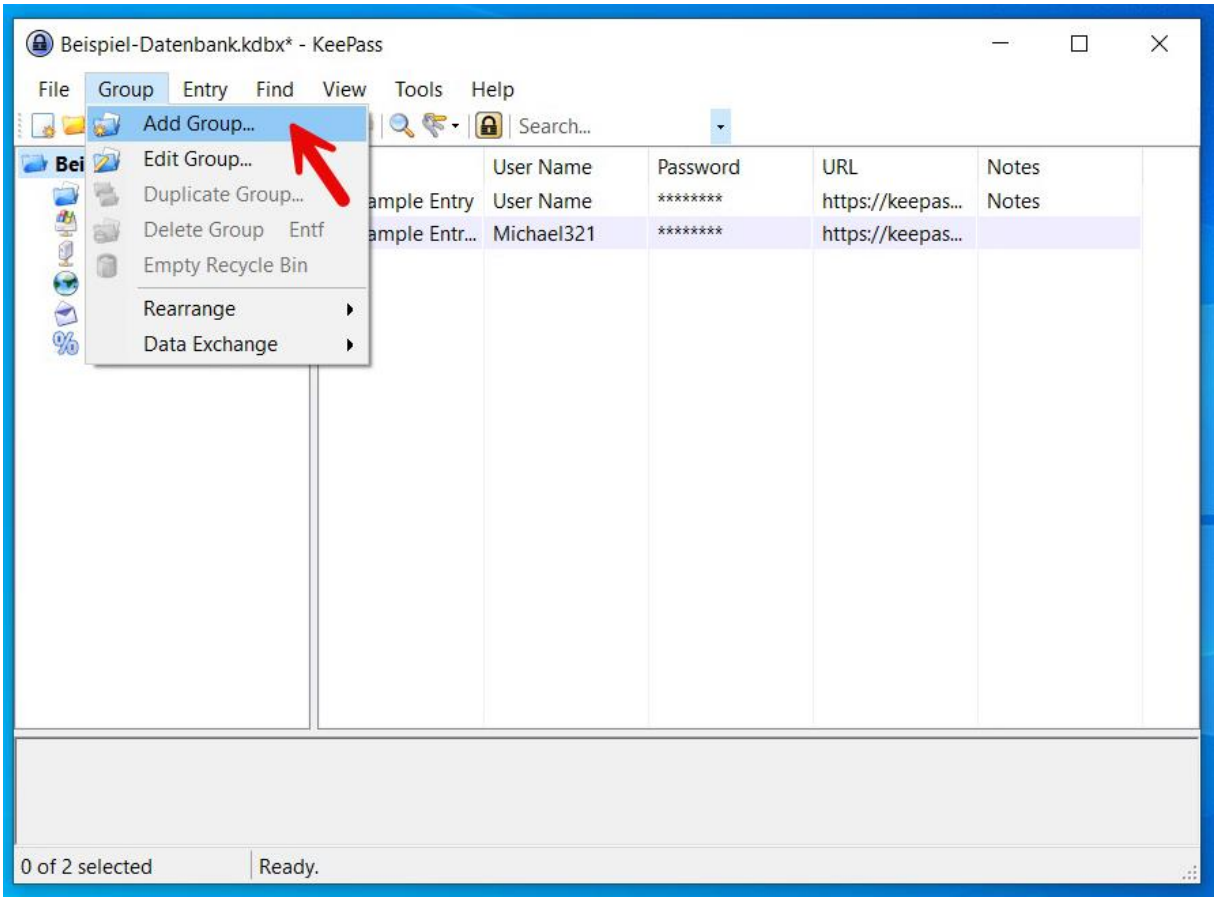
Um KeePass bei Nicht-Benutzung automatisch zu sperren, setzen Sie unter dem Reiter „Security“ den Haken bei „Lock workspace after KeePass inactivity (seconds).“ und geben den Wert 120 an.

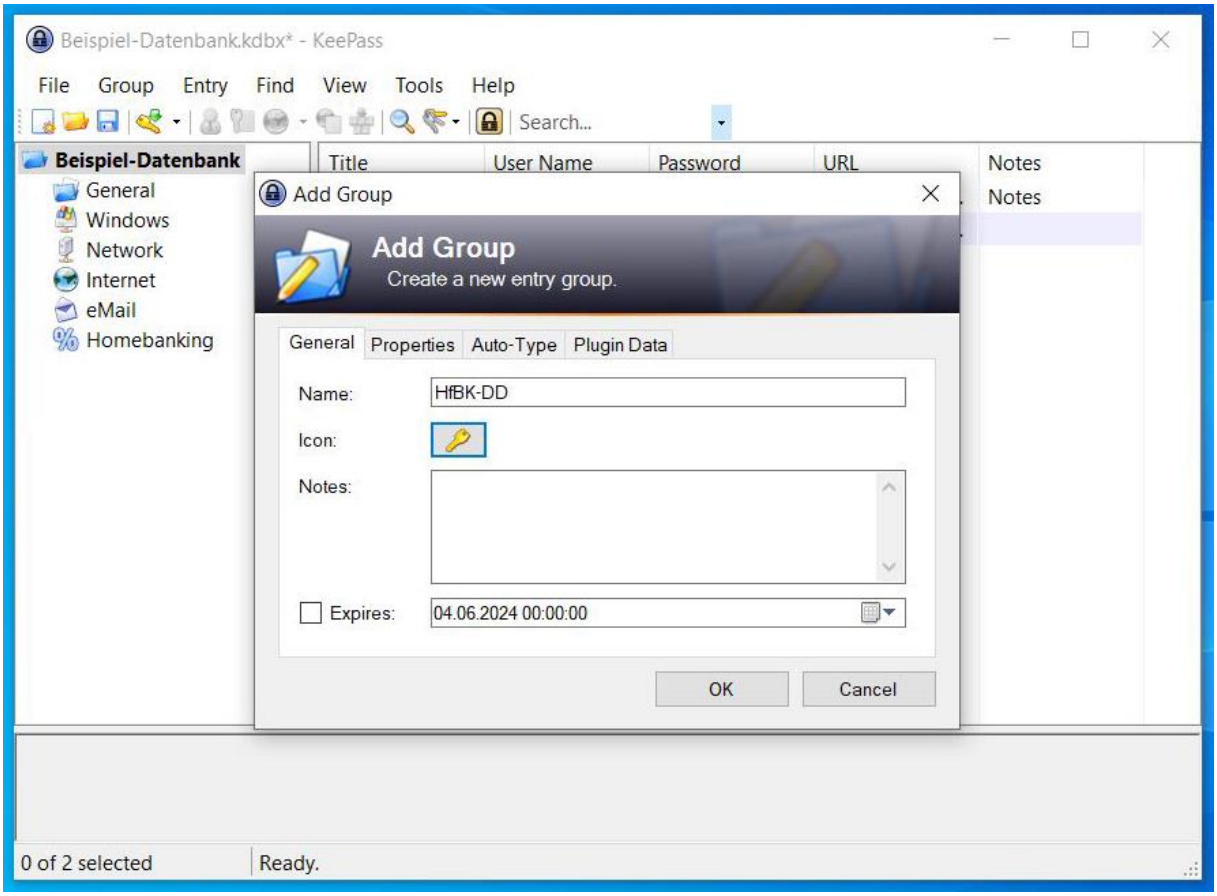
Zusätzlich sollten Sie im Scrollfeld ganz unten den Haken bei „Enter master key on secure desktop“ setzen. In diesem Zustand pausiert Windows alle Hintergrundprozesse. Auch mögliche Schadprogramme, wie beispielsweise Keylogger, die Ihre Tastatureingabe mitlesen könnten, werden so bei der Eingabe des Hauptschlüssels blockiert.

Gruppen / Ordner

Gruppen haben in Ihrem Passwortmanager eine ähnliche Funktion wie Ordner in Ihrem Dateisystem. Damit Sie auch bei vielen Passwörtern den Überblick behalten können Sie diese in einer Gruppe ablegen. Sie können direkt in der vordefinierten Gruppe Ihre Passworteinträge abspeichern.

Gruppe hinzufügen

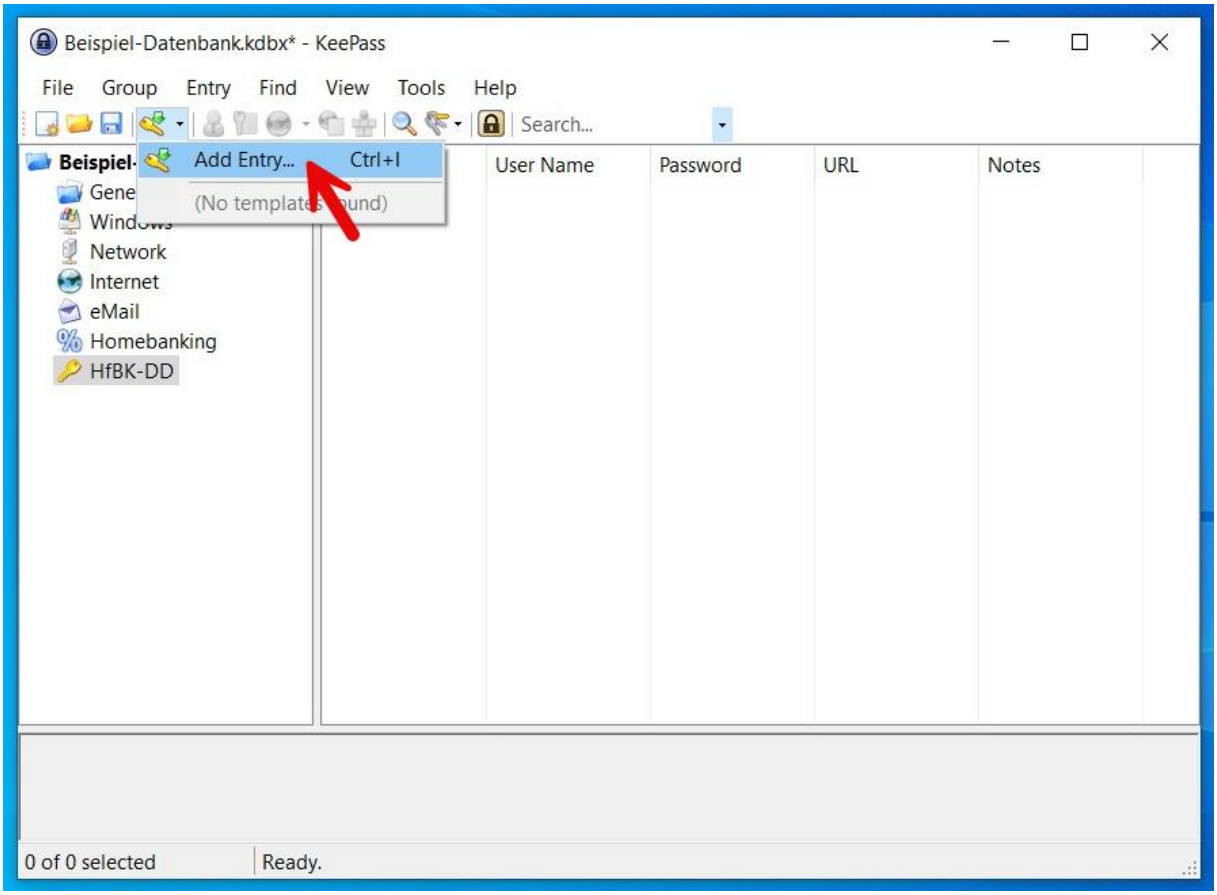


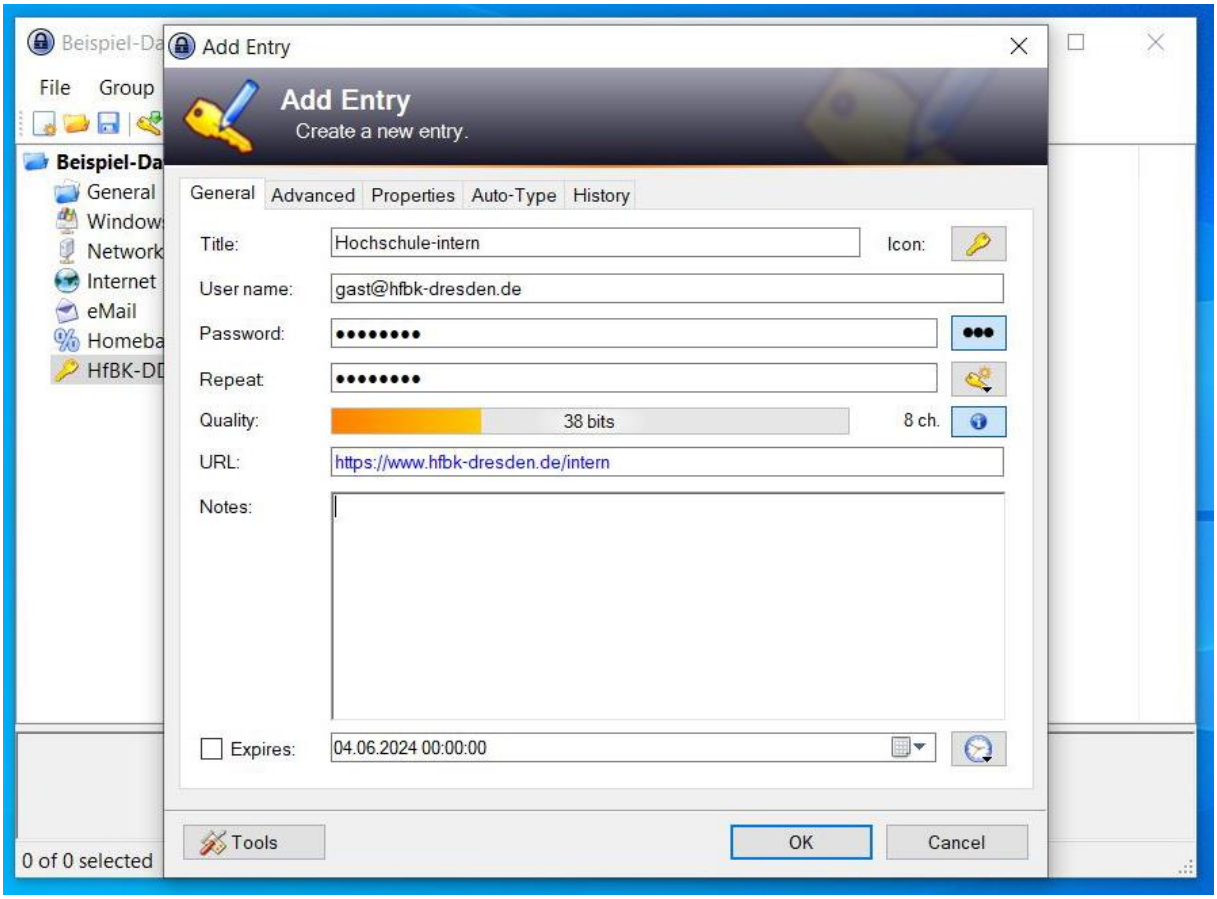


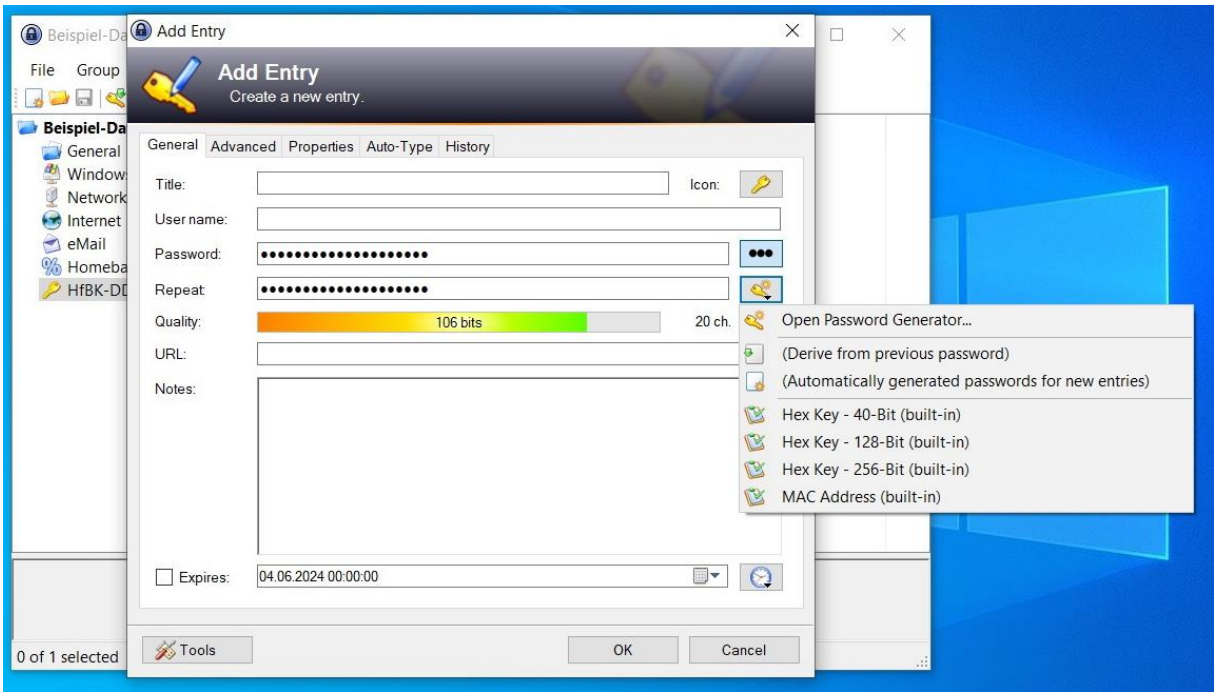
Geben Sie der Gruppe nun noch einen Namen. Zusätzlich haben Sie die Möglichkeit, durch Klick auf das Icon der Gruppe dieses zu ändern.

Passwort speichern

Um einen neuen Eintrag zu erstellen, müssen Sie zuerst die Gruppe auswählen, unter welchem Sie den Eintrag hinzufügen möchten.





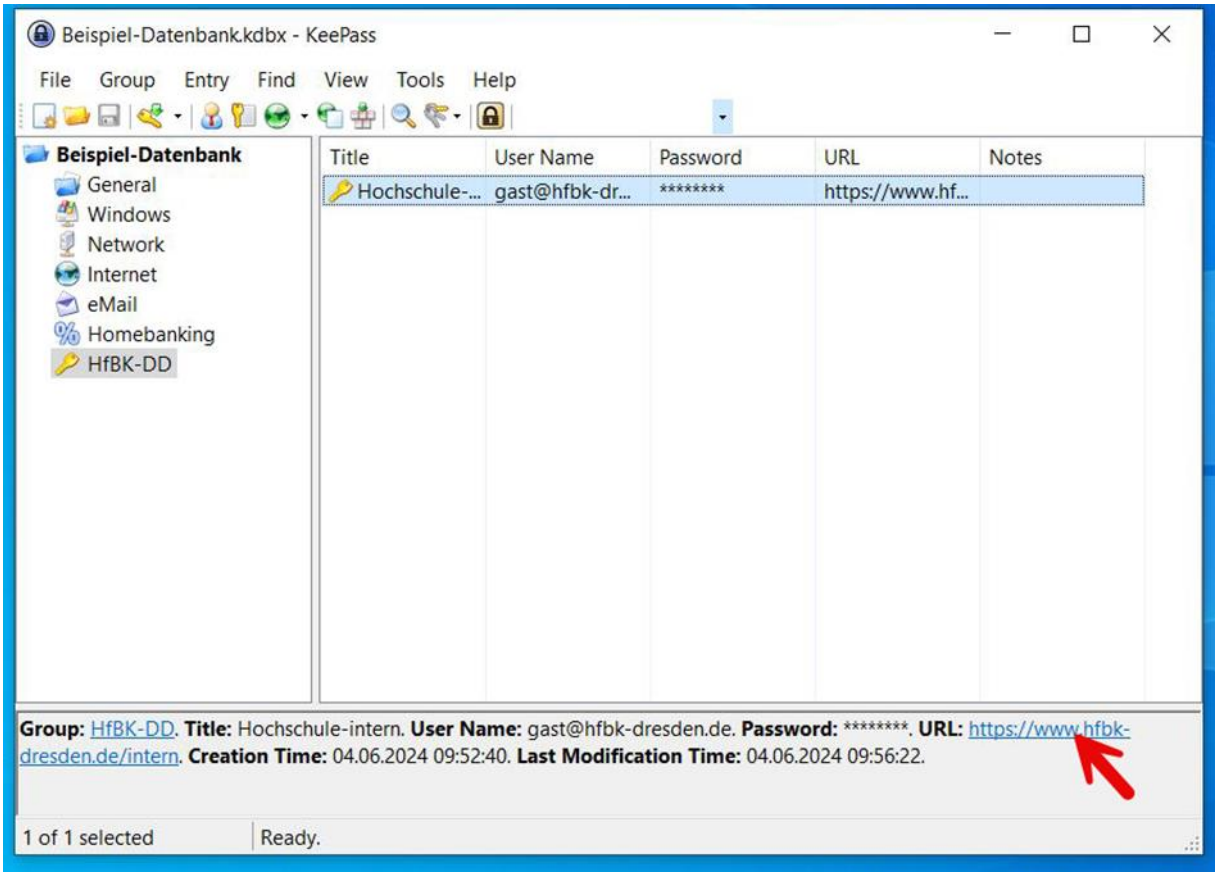


Sie können mit dem Passwortmanager ein sicheres Passwort generieren. Die entsprechenden Optionen werden Ihnen unter dem Schlüssel angezeigt.

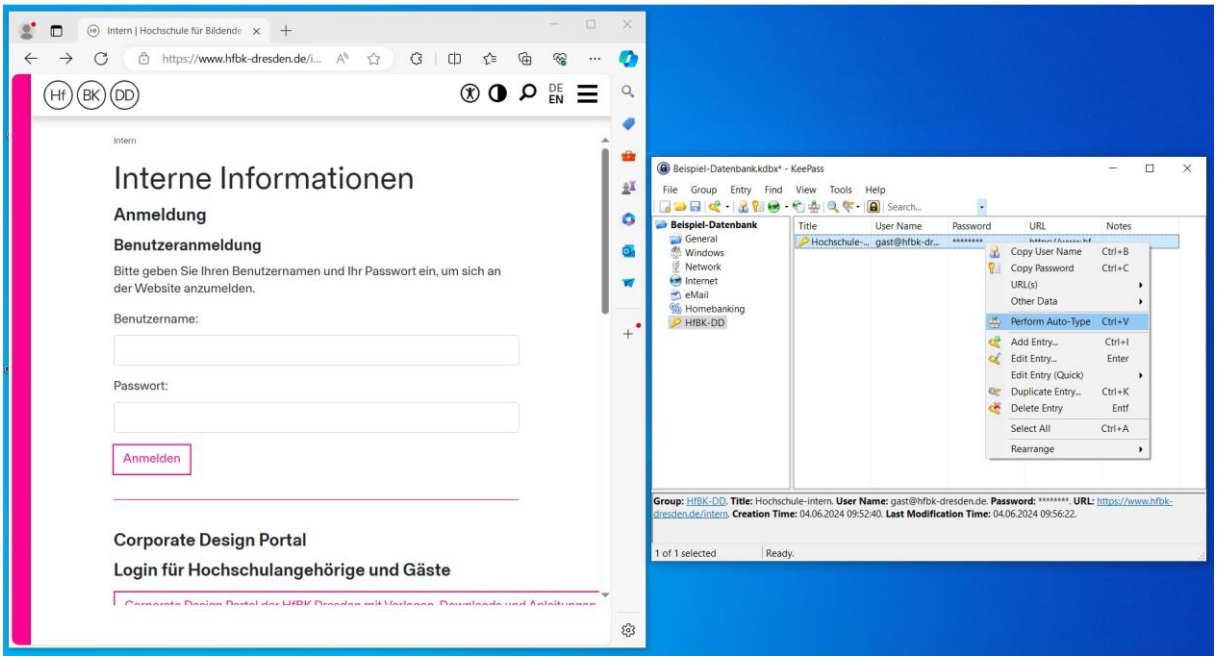
Die Quality: zeigt Ihnen an, wie sicher ihr Passwort ist. Je grüner der Balken ist bzw. je höher die Bit-Anzahl ist, umso sicherer ist Ihr Passwort.

Wenn Sie neben Password: die 3 Punkte aktivieren, wird Ihnen Ihr Passwort angezeigt.

Passwörter komfortabel nutzen:

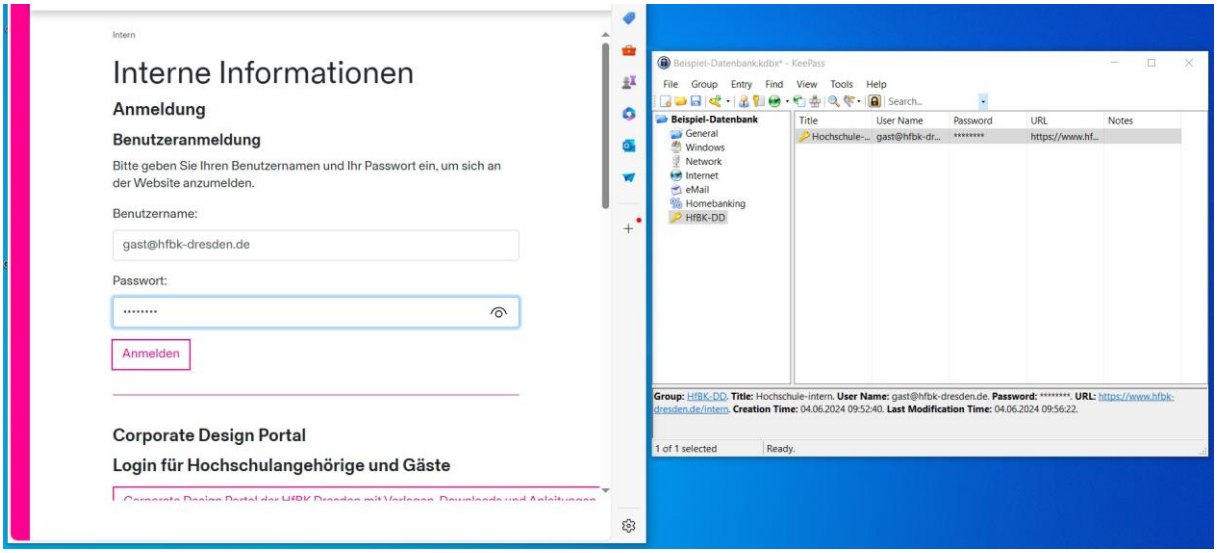


Bei einem gespeicherten Eintrag können Sie mit einem Klick auf den Link ganz einfach die entsprechende Internetseite öffnen.



Jetzt müssen Sie nur den Cursor in den Benutzernahmen navigieren und anschließend im Passwortmanager die Option „Perform Auto-Type“ und schon wird im Browser Ihr Benutzername und Ihr Passwort ausgefüllt. Diese Option funktioniert nur wenn Benutzername und Passwort in der Maske auf einer Seite dargestellt wird.

Sie können alternativ Ihren Benutzernamen und Ihr Passwort einzeln kopieren.


Intern
Interne Informationen
Anmeldung
Benutzeranmeldung
Bitte geben Sie Ihren Benutzernamen und Ihr Passwort ein, um sich an der Website anzumelden.
Benutzername:
gast@hfbk-dresden.de
Passwort:
Anmelden
Corporate Design Portal
Login für Hochschulangehörige und Gäste
Beispiel-Datenbank.kdbx* - KeePass
File Group Entry Find View Tools Help
Search...
Beispiel-Datenbank
General
Windows
Network
Internet
eMail
Homebanking
HfBK-DD
Title User Name Password URL Notes
Hochschule-... gast@hfbk-dr... ******** https://www.hf...
Group: HfBK-DD. Title: Hochschule-intern. User Name: gast@hfbk-dresden.de. Password: ********. URL: https://www.hfbk-dresden.de/intern. Creation Time: 04.06.2024 09:52:40. Last Modification Time: 04.06.2024 09:56:22.
1 of 1 selected
Ready.