Comp-Sys Informatik AG
Glutz-Blotzheim-Strasse 1
4500 Solothurn
032 653 70 77

KeePass
Benutzerhandbuch

COMP-SYS
0 Probleme. 1 Lösung.

Inhalt

Was ist KeePass?

Die Software dient dem sicheren und einfachen Umgang mit Passwörtern.
KeePass selbst übernimmt dabei die Rolle eines digitalen Safes auf ihrem PC. Zum Öffnen dieses Safes wird ein Masterkennwort benötigt, dieses sollte für kein anderes Login verwendet werden. Ausschliesslich für den Passwort Safe.
Im KeePass Safe können Passwörter, Benutzernamen, Links zu zugehörigen Websites und auch Notizen erfasst werden. All diese Daten sind lokal auf Ihrem PC gespeichert und verschlüsselt. Selbst bei Entwendung des Safes sind die Daten nicht zu entschlüsseln und dem Dieb somit nutzlos. Die Anmeldeinformationen bleiben sicher.

Installation und Einrichtung

Download

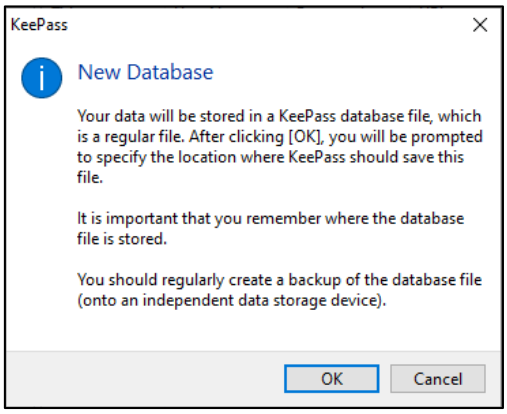
KeePass ist unter der offiziell zugehörigen Website zum Download verfügbar.
https://keepass.info/download.html

Neben der meist gebrauchten und standardmässig installierten englischen Version, wird die Software auch in anderen Sprachen angeboten. Die Übersetzungen sind nicht immer fehlerfrei, da diese durch freiwillige Mitarbeit von Laienübersetzern stammen. Aufgrund dieser Übersetzer ist die neuste Version von KeePass nicht immer in allen angebotenen Sprachen verfügbar.
Die deutsche Übersetzung ist meist sehr aktuell, da der Anbieter Dominik Reichl selbst aus Deutschland stammt und diese Aufgabe übernimmt.
Der Download in der deutschen und auch weiteren Sprachen ist unter folgendem Link verfügbar:
https://keepass.info/translations.html

Die Installation von KeePass ist bei einer Comp-Sys Standard-Eichrichtung dabei. Beziehen Sie also einen PC oder einen Laptop über uns, oder bringen Sie uns ein Gerät zum Aufsetzen, dann wird diese Software auch installiert.

Einrichtung

Wird KeePass zum ersten Mal geöffnet, wird eine mehrheitlich leere Oberfläche angezeigt. 
Im Menüband oben links ist das Symbol zum Erstellen einer neuen, verschlüsselten Datenbank gelistet.
Wird diese Datenbank angelegt, muss zuerst eine Meldung mit "OK" bestätigt werden.



Daraufhin wird der Benutzer von KeePass nach dem gewünschten Speicherort der Datenbankdatei gefragt.
Geben Sie diesen wie gewünscht an. Sind Sie sich nicht sicher, wählen Sie wie folgend:
"Dieser PC" → "System (C:)" → "Benutzer" → Ihren Benutzername
Wählen Sie nun "Speichern".
Lesen Sie weiteres zum Speicherort unter «Synchronisation»

Nun geht es mit dem Masterschlüssel des Passwort-Safes weiter. Zum Öffnen der Datenbank muss ein Passwort definiert werden. Werden alle anderen Passwörter in diesem Safe gespeichert, ist dies das einzige Passwort, welches sich der Benutzer merken muss. Alle anderen Passwörter sind dann sicher im Safe dokumentiert.

Nun den Masterschlüssel doppelt im Fenster eingeben und mit «OK» bestätigen.
Der farbige Balken unterhalb der Eingabefelder zeigt wie sicher das angegebene Passwort ist.
Sehen Sie hierzu im Abschnitt "Passwort Qualität".
Mit folgendem Symbol kann das eingegebene Passwort angezeigt werden. 

Im letzten Fenster kann optional, wenn gewünscht, ein Name oder eine Beschreibung angegeben werden.
Mit "OK" wird die Einrichtung abgeschlossen.

Möchten Sie sichergehen, oder befürchten Sie den Masterschlüssel zu vergessen, so können Sie im geöffneten Fenster mit "Print" ein Notfallblatt ausdrucken. Bewahren Sie dieses Dokument an einem sicheren und für unbefugte unzugänglichen Ort auf.
Möchten Sie auf dieses Blatt verzichten, wählen Sie "Skip".

Die Einrichtung ist nun abgeschlossen.

Synchronisation

Sämtliche in KeePass erfassten Einträge werden in Form einer Datei im Tresor gespeichert.
Diese Datei sollte nicht entwendet werden. Um diesen vor einer solchen Entwendung zu schützen, ist ein gut überlegter Speicherort von Wichtigkeit. Aber auch für gemeinsame Safes oder Safes mit Zugriff von verschiedenen Geräten ist dieser gut zu durchdenken.

Um dieser Aufgabe möglichst gerecht zu werden, empfiehlt die Comp-Sys einen Cloudspeicher oder einen Netzwerkspeicher.
Bevor Sie ihre Daten aber mit einem Dienst wie OneDrive oder Dropbox auf einen Cloudspeicher in Amerika oder einem unbekannten Standort auslagern, denken Sie über eine lokale Lösung nach. Wir bieten Ihnen mit Nextcloud eine sichere Lösung in der Schweiz gelegen.
Weiteres unter: https://www.comp-sys.ch/nextcloud/

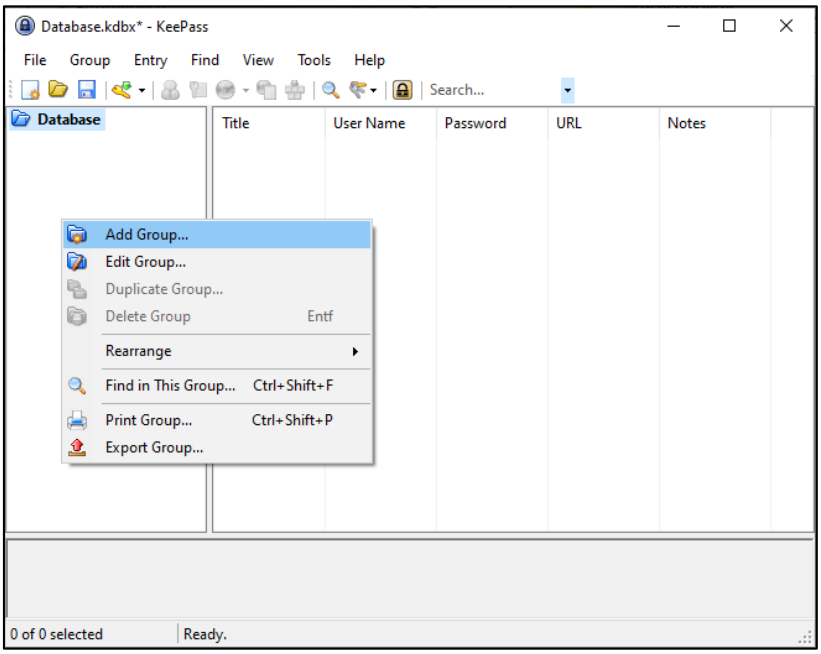
Die Speicherung auf einem Cloudspeicher oder Netzwerkspeicher ermöglicht es Ihnen ihre Datenbank synchronisiert vom Handy, PC, Tablet oder anderen möglichen Geräten zu öffnen.
Teilt eine Firma bestimmte Passwörter intern aus und würde diese gerne gemeinsam speichern, so ist mit dieser Variante auch hierfür gesorgt.

Anwendung

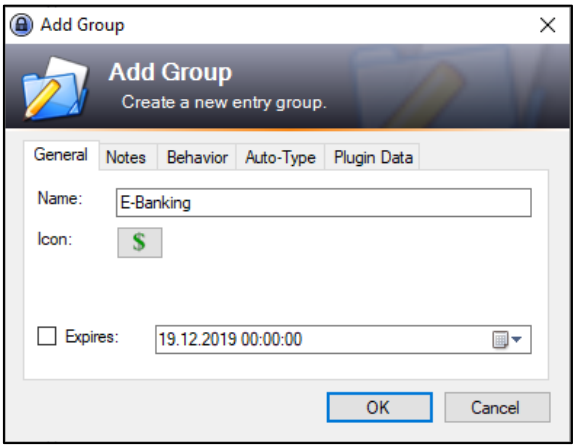
Gruppe anlegen

Um dem Safe eine übersichtliche Struktur zu geben und die erfassten Einträge auffindbar zu ordnen, sollten Gruppen angelegt werden. Dies wird wie folgt getan:

- Rechtsklick im linken Bereich des Fensters.
- "Add Group…" wählen.



- Gruppenname angeben und Symbol auswählen.



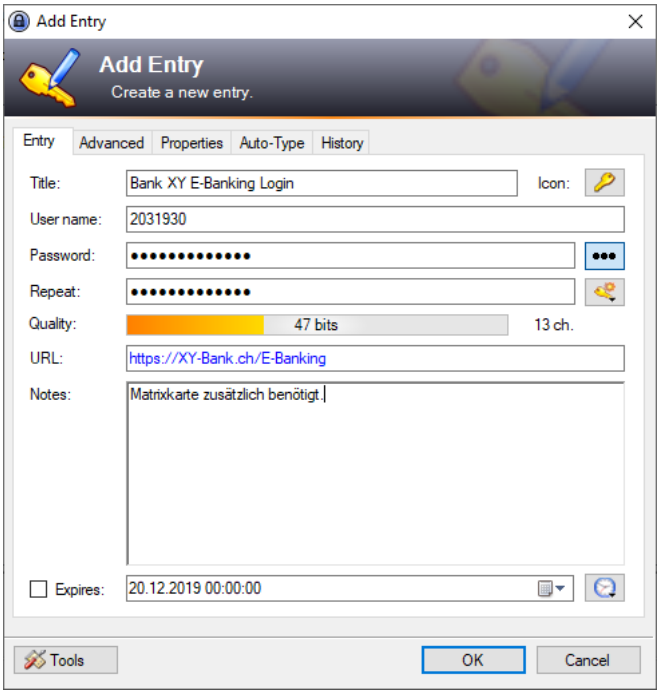
- "OK" wählen.
- Im linken Bereich wird nun die erstellte Gruppe gelistet. In dieser Gruppe können jetzt neue Einträge erfasst werden.

Eintrag erfassen

Um einen Eintrag zu erfassen, wird in der Funktionsliste am oberen Fensterrand folgendes Symbol angewählt:

Bevor jedoch ein Eintrag angelegt wird, sollte geprüft werden welche Gruppe im linken Seitenbereich ausgewählt ist. Der Eintrag wird dann der entsprechenden Gruppe zugeordnet.

Im neu geöffneten Fenster werden nun Informationen angegeben. Dabei sind die Feldbezeichnungen selbsterklärend: Überschrift, Benutzername, Passwort, Passwort Wiederholung, Qualität (Mehr Infos hier), Webadresse und zuletzt die Notizen.

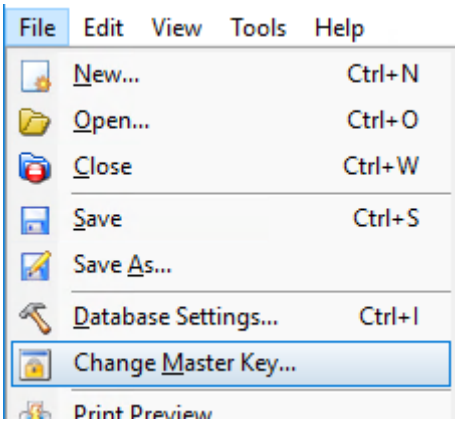


Mit folgendem Symbol kann das eingegebene Passwort angezeigt werden.

Mit "OK" wird der Eintrag gespeichert.

Masterkennwort ändern

Natürlich bleibt auch der Masterschlüssel nicht ewig derselbe. Darum ist es wichtig den Masterschlüssel für bestehende KeePass Datenbanken anpassen zu können. Dies ist unter dem Reiter «File» mit der Funktion «Change Master Key…» möglich.



Es ist wichtig, sicherzugehen, dass der Tresor vor der Änderung kopiert wird. Sollte beim Eingeben des neuen Kennworts ein Tippfehler passieren, sind alle gespeicherten Einträge verloren, da der Safe nicht mehr geöffnet werden kann.

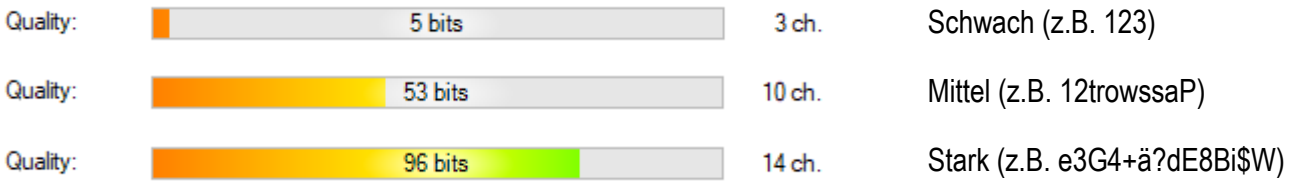
Nun kann ein neues Masterkennwort definiert werden.
Dieses muss folgend mit einer zweiten Eingabe bestätigt werden.

Es gilt nun den Safe mit einem Testversuch zu öffnen. Ist dieser erfolgreich, so kann und sollte die Kopie wieder gelöscht werden.

Passwort Qualität

Beim Erfassen eines Eintrages wird, gefolgt von den Spalten zur Angabe des Passworts, ein Balken angezeigt. Dieser Balken zeigt dem Benutzer, wie stark sein Passwort ist, sprich wie gut dieses Passwort möglichen Angriffen standhält.

Je weiter sicher der Balken in den grünen Bereich bewegt, desto sicherer ist das gewählte Passwort.



Was macht ein gutes Passwort aus?

Wird ein Angriff gegen ein Konto versucht, kann dieser sehr simpel aufgebaut sein. Es werden einfach alle möglichen Kombinationen versucht. Folglich müsste für ein Passwort mit den zehn Zahlen (0-9) und einer Länge von 3 Zeichen nur 1'000 Versuche gemacht werden. (10^3, Alle Zahlen von 000-999)
Anhand dieses kurzen Beispiels merken wir bereits, dass ein optimales Passwort möglichst viele verschiedene und eine möglichst grosse Anzahl an Zeichen verwendet.
Aber was genau macht ein gutes Passwort aus? Hier einige Punkte:

- Anzahl an Zeichen (möglichst grosse Anzahl)
- Verschiedene Zeichen (z.B. Sonderzeichen, Klein-, Grossbuchstaben und Zahlen verwenden)
- Keine Wörter oder Namen benutzen.
- Keine logischen Muster oder bekannte Systeme (z.B. abcdefg… , 1234567…, a1b2c3…)
- Nicht mehrfach vorhanden.
  (Im optimalen Fall verwenden Sie für jedes Log-In ein unterschiedliches Passwort.)

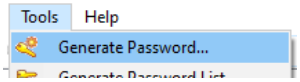
Vermutlich denken Sie sich nun, dass es unmöglich ist all diese Punkte zu beachten und sich solche Passwörter dennoch zu merken. Dies ist auch nicht schlimm.
Mithilfe von KeePass benötigen Sie auch nur noch ein einziges Passwort. Die anderen können Sie sich digital, abgesichert in ihrem Safe abspeichern.

Tipp:
Damit Sie ein sicheres Passwort verwenden und dieses dennoch nicht vergessen, verwenden Sie am besten eine Kombination aus Eselsbrücke und System. Beispiel:

"Erde" + "Mond" + "2107" + "%" = "EMrodned2107%"
Für den Anfang wird von den beiden Worten «Erde» und «Mond» jeweils ein Zeichen abwechselnd geschrieben. (**E**rde+**M**ond+E**r**de+M**o**nd+Er**d**e+Mo**n**d+Erd**e**+Mon**d** = **EMrodned**)
Gefolgt wird die Kombination von den Ziffern für Tag und Monat der ersten Mondlandung. "2107"
Das Ganze wird mit dem gewählten Sonderzeichen "%" vollendet.

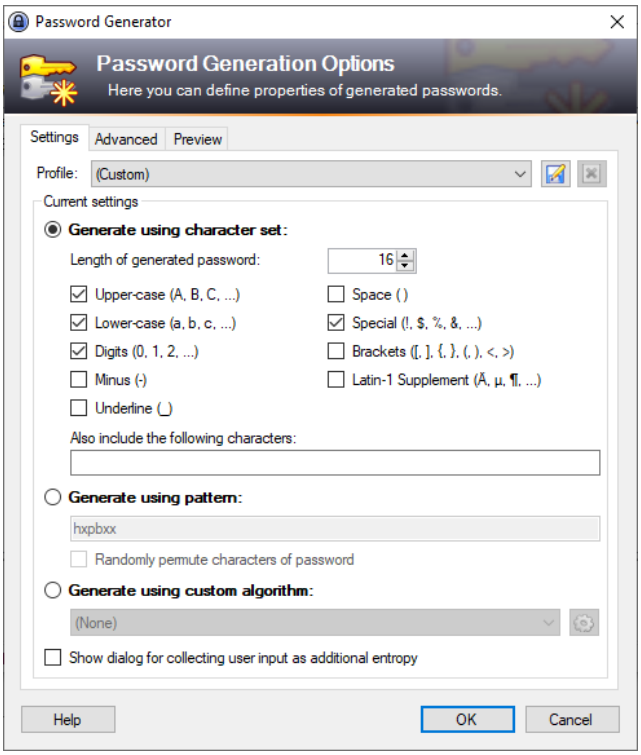
Passwort Generator

Der Passwort Generator kann beim Erfassen eines Eintrags über  dieses Symbol oder im Menüleiste unter "Tools" geöffnet werden.



Zum Erstellen eines Passworts haben Sie drei Möglichkeiten.

- Vorgabe verwendeter Zeichen und Länge des Passworts
- Vorgabe Zeichenmuster (https://keepass.info/help/base/pwgenerator.html)
- Vorgabe Algorithmus (https://keepass.info/help/base/pwgenerator.html)

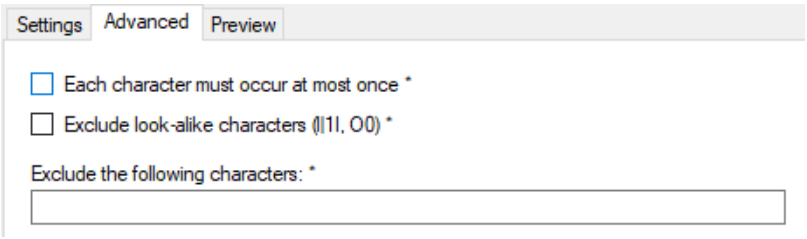


Mit der ersten genannten Methode sind nur wenige Optionen anzugeben.
Mit «Length of generated password» wird die Anzahl verwendeter Zeichen für das Passwort angegeben.
In den darunter folgenden Checkboxen sind die zu verwendenden Zeichentypen anzukreuzen. In der folgenden Klammer sind jeweils Beispiele der Zeichengruppe zu erkennen.

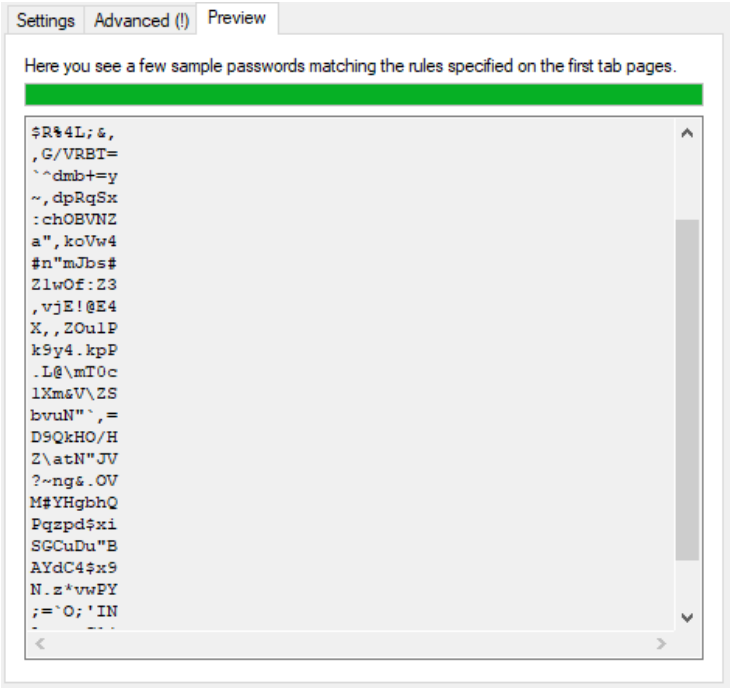
Um das Passwort sicher, aber dennoch möglichst einfach zu halten, sollten nicht zu viele Optionen angewählt werden. Es wird eine Einstellung wie im Bild empfohlen. Bei zu vielen oder speziellen Einstellungen kann es sogar zu Fehlern führen. Beispielsweise die Option «Latin-1 Supplement» gilt es mit Vorsicht zu geniessen, da nicht alle Systeme solche Zeichen unterstützen.

Im Abschnitt "Advanced" gibt es weitere nützliche Optionen.
Es können nicht zu verwendende Zeichen deklariert werden. Dazu können die Zeichen einfach im vorgesehenen Feld angegeben werden. Es ist kein Trennzeichen nötig.

Des Weiteren kann die Wiederholung von Zeichen oder die Verwendung von ähnlichen und schnell verwechselbaren Zeichen wie 0 und O deaktiviert werden.



Der verbleibende Abschnitt "Preview" zeigt eine Vorschau für generierte Passwörter mit den gewählten Einstellungen an. Dazu werden mit den momentan verwendeten Einstellungen einige Beispielpasswörter generiert.
Sind die Einstellungen ungültig, erscheint eine Fehlermeldung.



Um die Sicherheit so weit als möglich sicherzustellen, gehören weitere Faktoren wie z.B. Antivirusprogramme, Verbindungsverschlüsselungen oder eine Firewall dazu.
Haben Sie Fragen zu dieser Anleitung oder wünschen Sie weitere Informationen, melden Sie sich bei uns, wir sind Ihnen gerne behilflich.

E-Mail: *support@comp-sys.ch*
Tel.:*+41 (0)32 653 70 77*