Nutzung von KeePassXC im TightGate-Pro

Das Programm **KeePassXC** ist ein lokal arbeitender Passwortmanager zur sicheren Speicherung und Verwaltung von Zugangsdaten in einer verschlüsselten Datenbank. Die Datenbank ist Datei-basiert und liegt lokal auf TightGate-Pro, es ist daher keine Cloud-Anbindung erforderlich.

Installation

Damit KeePassXC auf TightGate-Pro läuft ist das Programm zusätzlich zu installieren. Bitte beachten Sie, dass das Programm bei TightGate-Pro Clustern vorab auf jedem Node einzeln zu installieren ist. Die Installation erfolgt so:

- Anmelden als Administrator ***update*** und Auswahl des Menüpunkts **Optionale Pakete hinzufügen**.
- Es ist das optionale Paket **webext-keepassxc-browser** und **mprivacy-custom-XXXXX** auszuwählen und zu installieren. (Das Paket beinhaltet sowohl das KeePassXC-Programm, wie auch das keepassxc Browser-Add-on für Firefox. Die KeePassXC-Erweiterung für Google-Chrome muss manuell hinzugefügt werden.)

Hinweis

Damit ein für Sie angepasstes Custom-Profil (**mprivacy-custom-XXXXX**) bereit gestellt wird, wenden Sie sich bitte an den technischen Support der m-privacy GmbH.

Start und Benutzeroberfläche

Nach der Installation startet beim Aufruf des TightGate-Viewers automatisch das KeePassXC im minimierten Modus. Wird das KeePassXC zum ersten mal gestartet, muss eine neue Datenbank angelegt werden oder einen bestehende Datenbank verknüpft werden.

Erstellen einer neuen Datenbank

- **Datenbank > Neue Datenbank**
- Name und Beschreibung vergeben
- Verschlüsselungseinstellungen wählen (Standard empfohlen)
- Hauptschlüssel definieren: (**Master-Passwort)**
  Best Practices:
    - Mind. 12-16 Zeichen
    - Mischung aus Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen
    - Kein Wiederverwenden von Passwörtern
- Die Datei wird als .kdbx-Datei im Ordner **transfer** gespeichert: Beispiel: internet-pw.kdbx

Verwenden einer bestehenden Datenbank

Soll eine bestehende Datenbank verwendet werden, so ist diese vorab über die TightGate-Schleuse in das Transfer-Verzeichnis des Benutzers zu legen.

Die Übertragung der DB kann entweder durch den Admin **transfer** erfolgen oder durch die Nutzer selbst. Im Fall dass Nutzer die Datenbank selbstständig übertragen sollen, ist darauf zu achten, dass in der Upload-Berechtigung für den Nutzer der MIME-Typ **application/octet-stream** freigegeben ist.

Eine bestehende Datenbank wird im KeePassXC wie folgt verwendet:

- **Datenbank > Öffnen**
- Datenbank (.kdbx-Datei) auswählen
- Master-Passwort eingeben

KeePassXC konfigurieren

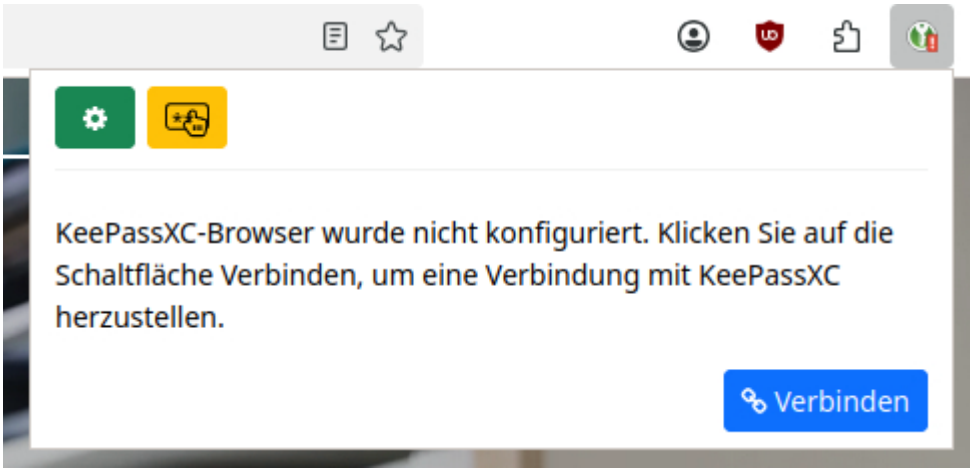
Folgende Werte sollten abweichend von der Standardeinstellung im KeePassXC unter **Werkzeuge > Einstellungen** konfiguriert werden:

In der Kategorie **Allgemein > Programmstart**	
Menüpunkt	**Empfohlener Wert**
KeePassXC beim Systemstart automatisch starten	Ja
Bei Programmstart Fenster minimieren	ja
Fenster nach Entsperren der Datenbank minimieren	ja
In der Kategorie **Allgemein > Benutzeroberfläche**	
Menüpunkt	**Empfohlener Wert**
Minimieren, statt Programm zu beenden	ja
Taskleistensymbol anzeigen	ja
Taskleistensymbol	Bunt

Browser-Integration

Damit der Firefox / Chrome-Browser die Passwortdatenbank von KeePassXC direkt nutzen kann, ist diese im jeweiligen Browser zu aktivieren. So erfolgt die Aktivierung:

- **Werkzeuge > Einstellungen > Browser-Integration**
- Menüpunkt **Browserintegration aktivieren** auswählen
- Im Menüpunkt **Integration für diese Browser aktivieren** die folgenden Browser aktivieren: **Firefox** und bei Bedarf **Google-Chrome**.
- Mit **OK** bestätigen.
- Im Firefox / Chrome-Browser die keepassxc-Erweiterung öffnen und dort die Schaltfläche **Verbinden** auswählen.



- In der KeePassXC-Erweiterung der Verbindung einen eindeutigen Namen vergeben und über die Schaltfläche **Speichern und Zugriff erlauben** die Verbindung zur KeePassXC-Datenbank bestätigen.