

# **Tuto d'usage KEEPASS**

## **Prise en main en 5 minutes**

**L'utilisation d'un gestionnaire de mots de passe permet d'avoir des mots de passe robustes et différents pour chaque outil, limitant fortement les risques de piratage en cas de fuite d'identifiants.**

**KeePass ne stocke pas vos mots de passe en ligne. L'accès à votre base dépend uniquement du fichier enregistré sur votre appareil et de votre mot de passe maître. Ce mot de passe ne peut pas être récupéré : en cas de perte, l'ensemble des données devient définitivement inaccessible.**

*Ce tutoriel propose une prise en main simple de l'outil KeePass, solution gratuite.*

### **Contexte et objectif**

La sécurisation des accès numériques constitue une obligation au titre de l'article 32 du Règlement Général sur la Protection des Données, qui impose la mise en œuvre de mesures techniques et organisationnelles appropriées pour protéger les données personnelles.

L'utilisation d'un gestionnaire de mots de passe tel que KeePass est recommandée par la CNIL dans ses conseils relatifs à la sécurisation des mots de passe et reconnue comme solution pertinente par l'ANSSI dans ses recommandations de cybersécurité.

*Les principales failles de sécurité sont liées à l'utilisation de mots de passe faibles, la réutilisation du même mot de passe sur plusieurs outils, l'enregistrement automatique des mots de passe dans les navigateurs, le partage non sécurisé d'identifiants.*

*L'utilisation d'un gestionnaire de mots de passe permet de générer des mots de passe robustes, éviter leur réutilisation, sécuriser leur stockage, ne pas enregistrer ses mots de passe sur le navigateur, faciliter la gestion des accès aux outils utilisés par la CPTS.*

### **Accès et fonctionnement de la base KeePass**

La base de données KeePass est un fichier chiffré enregistré sur votre ordinateur (ou tablette).

Cela signifie que :

- vos mots de passe ne sont pas stockés en ligne ;
- ils restent uniquement accessibles sur l'appareil où la base est enregistrée.

Si vous souhaitez utiliser votre base sur plusieurs appareils, vous devrez copier le fichier de la base de données (.kdbx) vers un autre appareil (clé USB sécurisée, espace de stockage sécurisé, etc.).

**⚠ Important : sans ce fichier, vous ne pourrez pas accéder à vos mots de passe.**

## Attention au mot de passe maître

Lors de la création de votre base KeePass, vous définissez un mot de passe maître.

Ce mot de passe est la clé permettant d'accéder à tous vos mots de passe enregistrés.

Points essentiels :

- il doit être robuste et mémorisable ;
- **il ne peut pas être récupéré si vous l'oubliez ;**
- ni KeePass, ni un administrateur informatique ne peuvent le restaurer.

⚠ Si le mot de passe maître est perdu, la base de données devient définitivement inaccessible.

Il est donc recommandé de :

- choisir un mot de passe que vous pouvez mémoriser ;
- conserver une copie sécurisée dans un lieu sûr (export de fichier CSV).

## Les 5 étapes pour sécuriser ses mots de passe

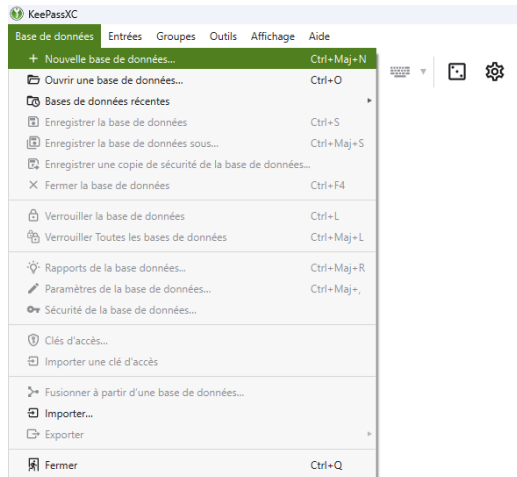
1. Installer KeePass
2. Créer sa base de données sécurisée
3. Enregistrer un mot de passe
4. Paramétrage pour un remplissage des mots de passe lors de connexion internet
5. Remplissage du mot de passe lors de la connexion internet
6. Exporter ses mots de passe (CSV / Excel)

## 1) Installer KeePass

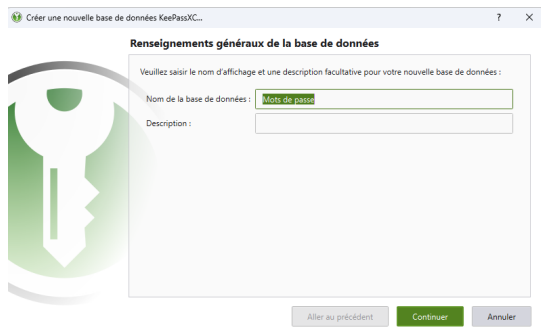
- a) Installer KeePassXC depuis le site officiel : [KeePassXC Password Manager](#)

## 2) Créer sa base de données sécurisée

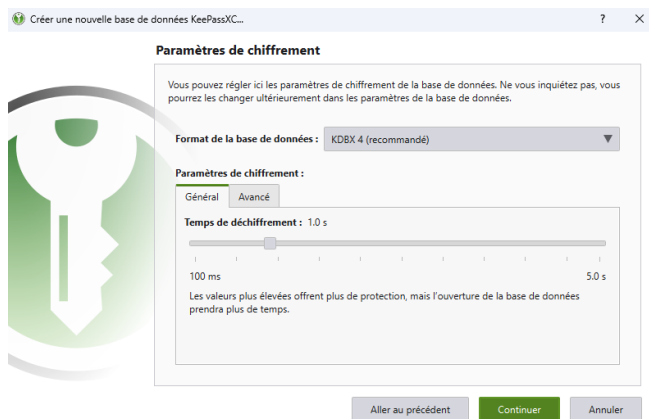
- a) Ouvrez KeePassXC.  
b) Cliquez sur Base de données en haut à gauche puis sur « Nouvelle base de données ».



- c) Choisissez le « Nom de la base de données ». La « Description » est optionnelle.  
Cliquez sur « Continuer ».



- d) Sur la fenêtre « Paramètres de chiffrement », rien à faire, cliquez sur « Continuer ».

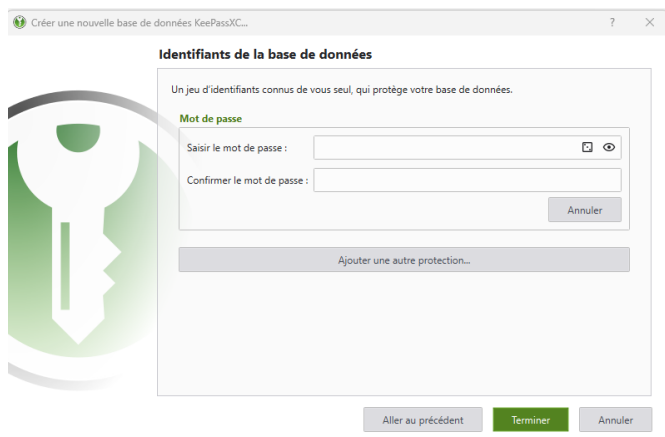


e) Vous arrivez sur la fenêtre « Identifiants de la base de données ».

f) **Choisir un mot de passe robuste que vous retiendrez.**

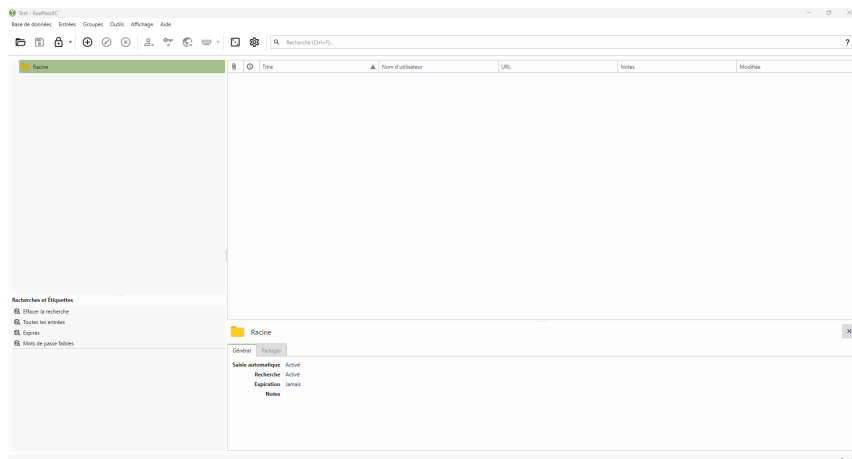
*Vous pouvez utiliser l'option de génération automatique de mot de passe (icône en forme de dé à droite du champ). Attention : ce mot de passe maître doit impérativement être mémorisé ou conservé dans un endroit sécurisé. Il est indispensable pour accéder à votre base de données et ne pourra pas être récupéré en cas de perte.*

Confirmez-le. Cliquer sur Terminer.



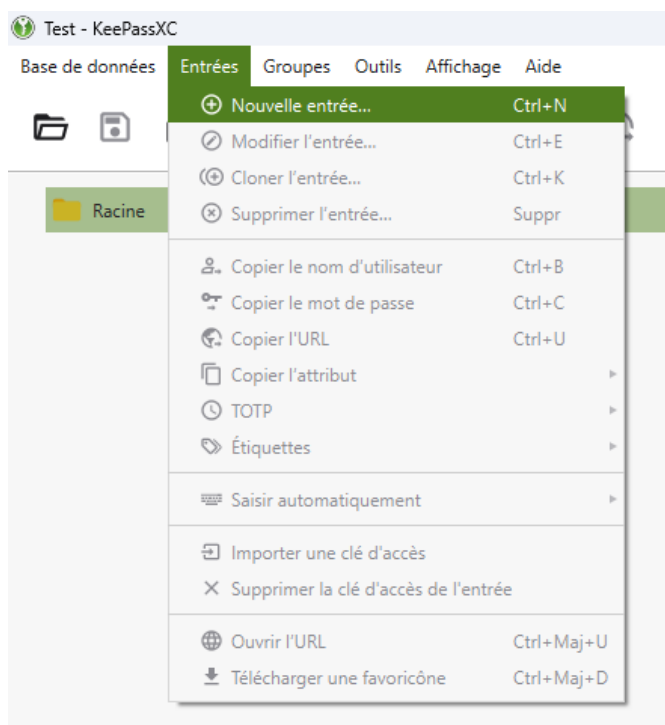
g) Enregistrer votre base de données.

h) Vous devez arriver sur cet affichage.

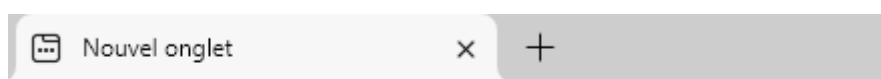


### 3) Enregistrer un mot de passe

- a) Dans Entrées > Nouvelle entrée (CTL+N) (une nouvelle entrée correspond à un nouveau mot de passe à enregistrer).



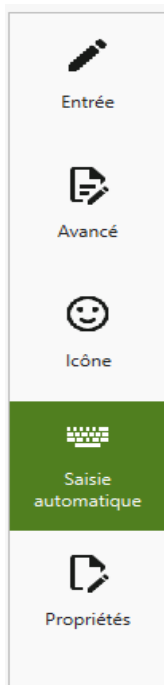
- b) Dans Titre > Nom de l'onglet qui s'affiche lorsque vous ouvrez une page « Nouvel onglet » dans la capture ci-dessous par exemple)



- c) Nom d'utilisateur > E-mail = Identifiant = Login (celui correspondant au site que vous êtes en train d'enregistrer).

- d) Mot de passe > Insérer le mot de passe correspondant au login. Si c'est la première utilisation, vous pouvez en créer un à l'aide du petit dé sur la droite.

Mot de passe : |



- e) URL > adresse qui s'affiche dans la barre de recherche du navigateur quand vous ouvrez une page (page d'accueil, celle où on vous demande vos identifiants).

*Même si elle n'est pas indispensable pour la saisie automatique avec raccourci clavier, l'URL permet de sécuriser l'utilisation (vérification du site) et d'organiser votre base de mots de passe. L'URL peut également permettre une reconnaissance automatique du site dans certains usages avancés.*

- f) Sur la gauche descendre vers « Saisie Automatique ».  
g) Cocher « Activer la saisie automatique pour cette entrée ».  
h) Cliquez sur « Appliquer » (en bas à droite).  
i) Cliquez sur « OK ».

*Option : Certains sites, comme Gmail, demandent d'abord l'identifiant puis le mot de passe sur deux écrans distincts. Dans ce cas, la saisie automatique doit être utilisée en deux étapes.*

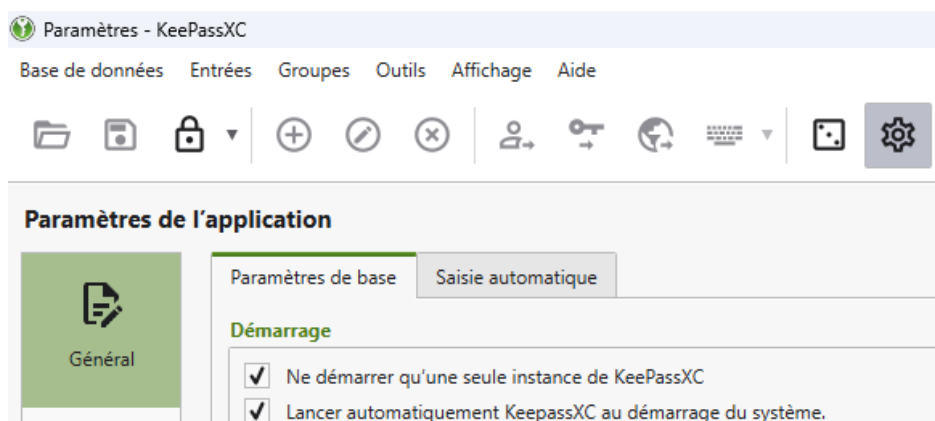
*Cette option permet de définir l'ordre de remplissage des champs (identifiant, mot de passe). En exemple, dans la barre de saisie, pour :*

*Outlook : {USERNAME}{ENTER}{PASSWORD}{ENTER}*

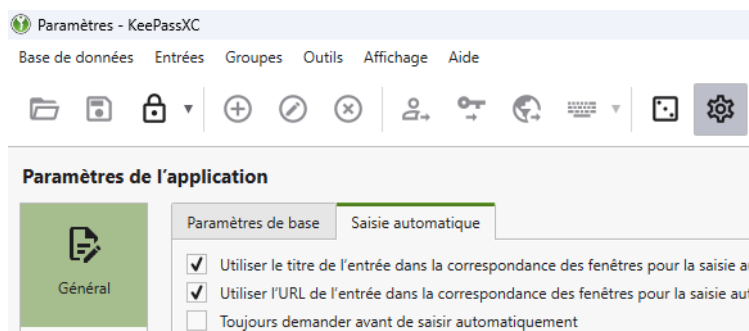
*Le bon coin : {USERNAME}{TAB}{PASSWORD}{ENTER}*

#### 4) Paramétrage pour un remplissage des mots de passe lors de connexion internet

- a) Dans Paramètres (pictogramme rouage) > Paramètres de base > Cochez « Lancer automatiquement KeePassXC au démarrage du système »



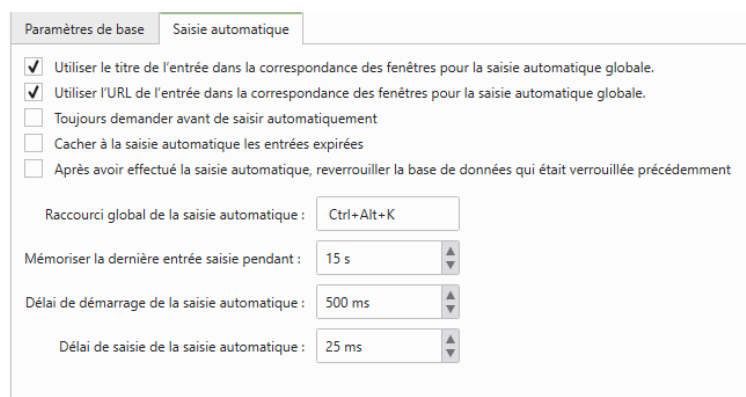
- b) Passez ensuite sur « Saisie automatique » > Décochez « Toujours demander avant de saisir automatiquement ».



## Méthode 1 – Raccourci clavier

- a) Dans « Raccourci global de la saisie automatique », saisissez le raccourci que vous souhaitez utiliser (ex : Ctrl + Alt + K)

*Ce raccourci permet de remplir automatiquement vos identifiants et mots de passe dans un site ou une application, sans avoir à les copier-coller manuellement.*



- b) Cliquez sur « OK » en vert en bas à droite.

## Méthode 2 –Remplissage automatique - Extension navigateur

- a) . Installer une extension navigateur (optionnel).

*KeePassXC peut être utilisé avec une extension navigateur permettant de remplir automatiquement les identifiants et mots de passe sans utiliser de raccourci clavier.*

*Cette fonctionnalité permet une reconnaissance automatique du site et un remplissage automatique des champs de connexion. Son utilisation nécessite une configuration préalable et une vigilance particulière en matière de sécurité (vérification du site, gestion des accès).*

Pour aller plus loin, vous pouvez télécharger l'extension : [KeePassXC-Browser - Chrome Web Store](#) ; et ; consulter la notice d'extension du navigateur : [KeePassXC : Guide de démarrage](#).

## **5) Remplissage du mot de passe lors de la connexion internet**

- a) Lorsque vous ouvrez une page, cliquez sur l'espace de saisie au niveau de l'identifiant.

b) Valider la séquence.

➔ **Bravo vous êtes connectés**

**6) Exporter ses mots de passe (CSV / Excel)**

a) En haut à gauche, cliquer sur « Base de données »

b) Sélectionner « Exporter »

c) Choisir le format « CSV »

d) Enregistrer le fichier sur votre ordinateur ou disque dur externe

**Attention : Le fichier exporté n'est pas chiffré.**