Démarrer et utiliser les principales fonctions

Le gestionnaire de mots de passe KeePass XC

Version 2.7.6

2024

Pôle Usagers et Qualité

Direction du numérique

Table des matières

Démarrer avec KeePassXC 3

Lancer KeePassXC 3

Créer votre base de données 3

Déposer vos identifiants 6

Utiliser KeePassXC pour une connexion 7

Méthode basique 7

Méthode automatique 8

Méthode utilisant une extension du navigateur 8

Les fonctions utiles 12

L'onglet « Base de données » 12

L'onglet « Affichage » 14

À propos de paramètres 16

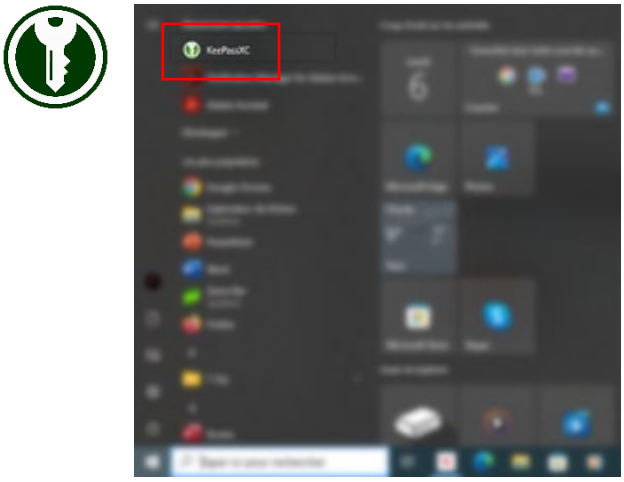
KeePass sur mobile 17

Démarrer avec KeePassXC

KeePass XC est un gestionnaire de mots passe sécurisé. L'application va stocker et chiffrer les adresses des sites et autres plateformes en ligne ainsi que les identifiants nécessaires pour y accéder. Cette base de données est verrouillée par un « mot de passe maître », le seul mot de passe qu'il sera nécessaire de retenir.
L'application est disponible pour toutes les plateformes : Windows, MacOS ou Linux et téléchargeable depuis le site https://keepassxc.org/ .
Une fois installée il faut créer, à partir de l'application, la base de données et à paramétrer l'application.

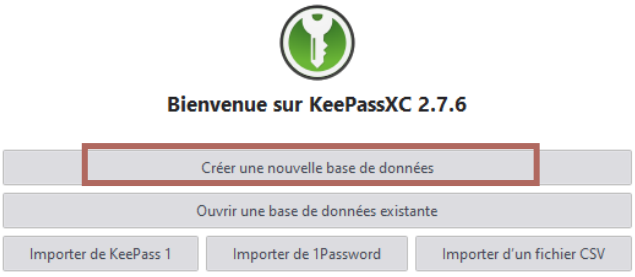
① Lancer KeePassXC

Démarrez KeePassXC comme n'importe quelle autre application que vous utilisez.



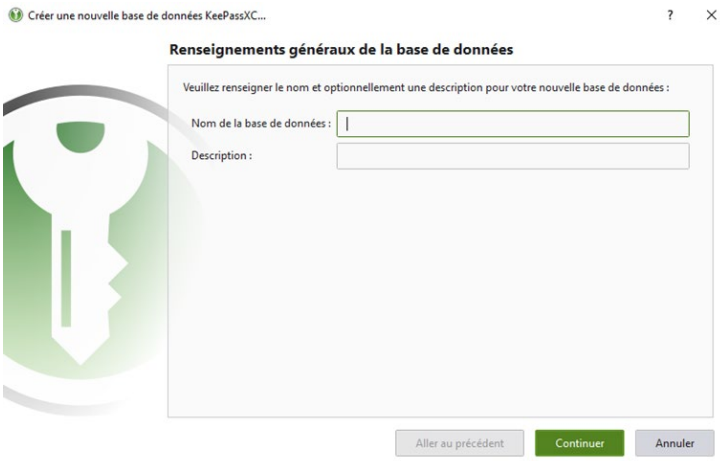
② Créer votre base de données

Il s'agit de créer le fichier qui contiendra les identifiants associés à chaque compte en ligne qui y sera stockée. Il est possible de créer plusieurs bases de données selon les besoins.



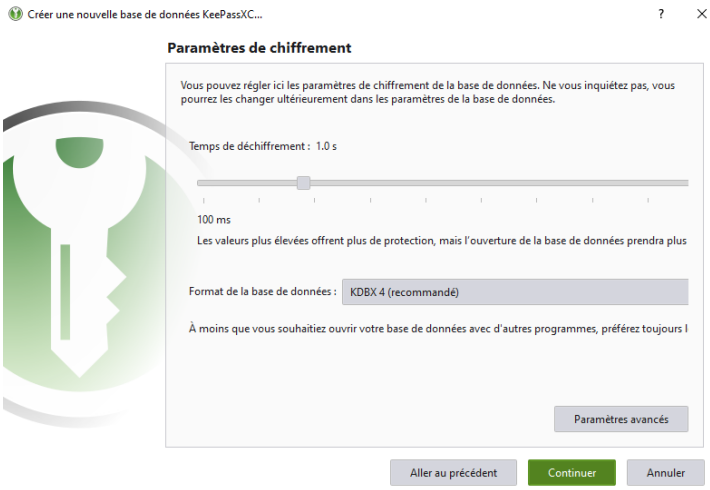
→ Donnez un nom explicite au coffre

Si vous êtes amené à créer plusieurs bases de données, il sera plus facile de retrouver des identifiants si chacune d'elles porte un nom et une description en relation avec son contenu.



→ Chiffrement

Vous pouvez laisser les paramètres par défaut.



→ Choisissez le mot de passe maître

C'est une phase **essentielle** dans la création de votre base de données.

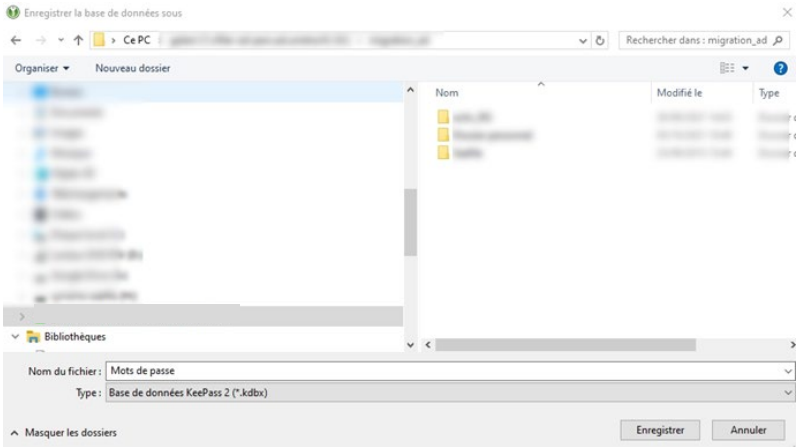
Ce mot de passe unique, appelé « mot de passe maître », est celui qui donnera accès à tous les autres mots de passe enregistrés dans la base de données.

Personne ne pourra retrouver un mot de passe maître perdu.

Il n'y a aucune copie enregistrée accessible.

→ Stockage de la base de données

Lorsque l'interface vous invite à désigner un emplacement de la base de données, vous pouvez choisir n'importe quel support de stockage qu'il soit interne, externe ou distant.



Par la suite, vous pourrez en faire une copie sur un autre support (par exemple une clé USB).

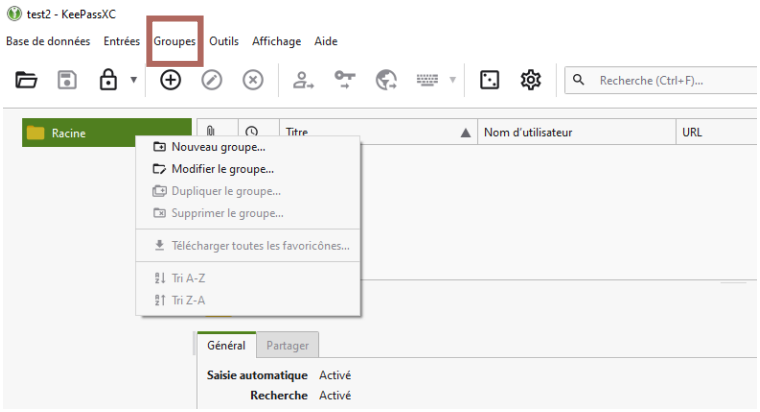
Notez que pour utiliser cette base de données sur un autre ordinateur il faudra installer KeePass XC sur l'appareil concerné.

3 Déposer vos identifiants

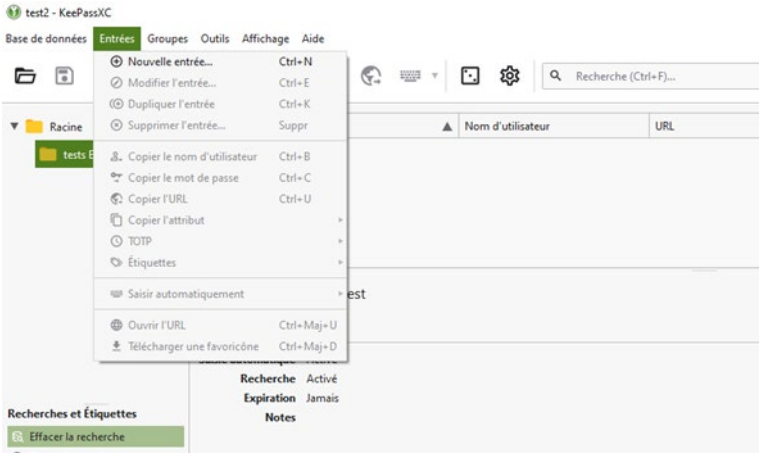
Les triplets « nom utilisateur + mot de passe + adresse de la page », appelés « Entrées » dans l'application, peuvent être conservés dans des dossiers appelés « Groupes ». On peut les voir comme des dossiers de votre explorateur de fichiers.

Un premier groupe est créé par défaut : « Racine ».

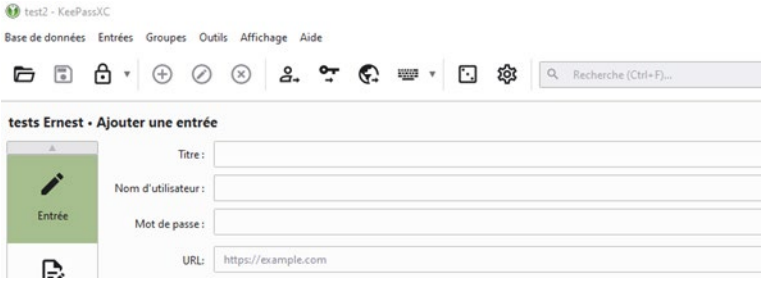
Pour un créer un groupe, utilisez l'onglet « Groupes » ou faites un clic droit sur « Racine ».



Pour créer une entrée, sélectionnez un groupe et rendez-vous dans l'onglet « Entrées ».



Saisissez un nom (titre) pour le compte puis les identifiants associés à l'adresse web (URL).

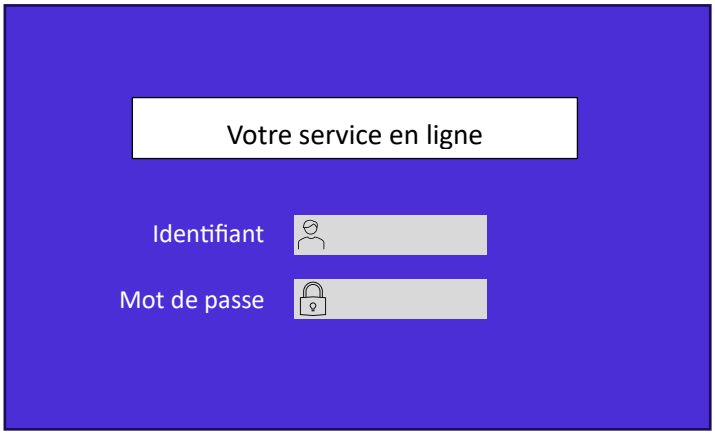


Utiliser KeePassXC pour une connexion

Avant de commencer, rendez-vous dans les paramètres de Firefox (ou tout autre navigateur), puis dans « Vie privée et sécurité » pour décocher la case "Proposer d'enregistrer des mots de passe". Enregistrer les identifiants dans le navigateur est fortement déconseillé.

① Méthode basique

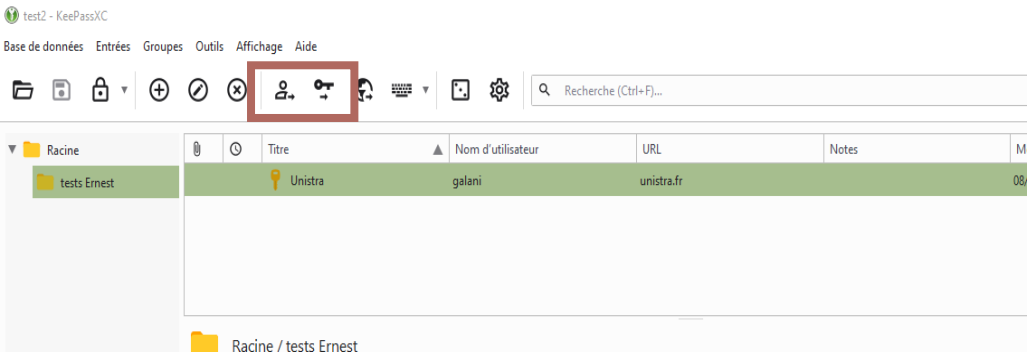
→ Ouvrez le navigateur à la page de connexion d'un de vos comptes.



→ Ouvrez KeePassXC et déverrouillez la base de données avec votre mot de passe maître

→ Copiez le nom d'utilisateur en cliquant sur et collez-le dans le champ identifiant de la page web.

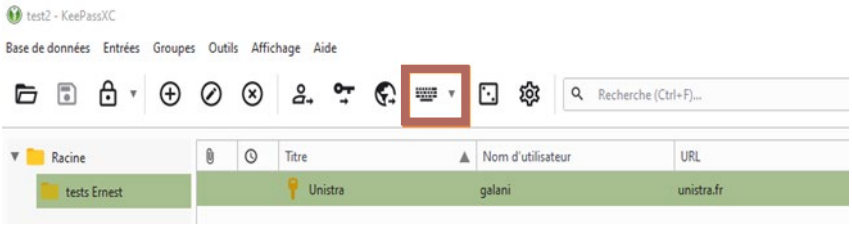
Copiez le mot de passe en cliquant sur et collez-le dans le champ correspondant de la page web.



Lorsque vous copiez un identifiant ou un mot de passe, vous disposez d'un temps limité pour le coller dans le navigateur (par défaut 10 s).

② Méthode automatique

Le menu  permet un remplissage automatique des identifiants. Notez que cette méthode ne fonctionne que sur les sites dont les champs sont normalisés.



Dans tous les cas d'utilisation, il faut que le coffre soit ouvert pour accéder aux mots de passe.

③ Méthode utilisant une extension du navigateur

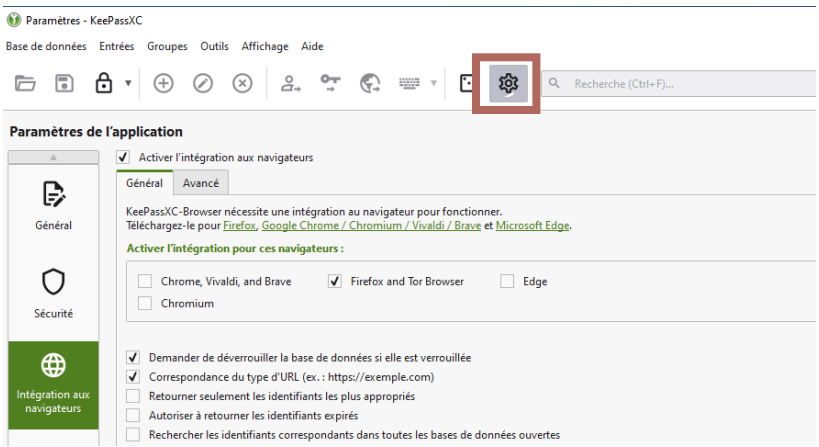
Une extension est un module additionnel qui permet d'ajouter des fonctions au navigateur. Recherchez l'extension KeePass-browser (KeePass pour navigateur) dans le catalogue désigné par le symbole d'une pièce de puzzle (en haut à droite dans la barre d'outils du navigateur).

En couplant l'extension à l'application KeePassXC, vous pourrez réaliser les opérations courantes depuis le navigateur sans faire appel à l'application.

→ Activez l'intégration de l'extension dans KeePassXC

Dans les paramètres de KepassXC, rendez-vous dans l'onglet « Intégration aux navigateurs ».

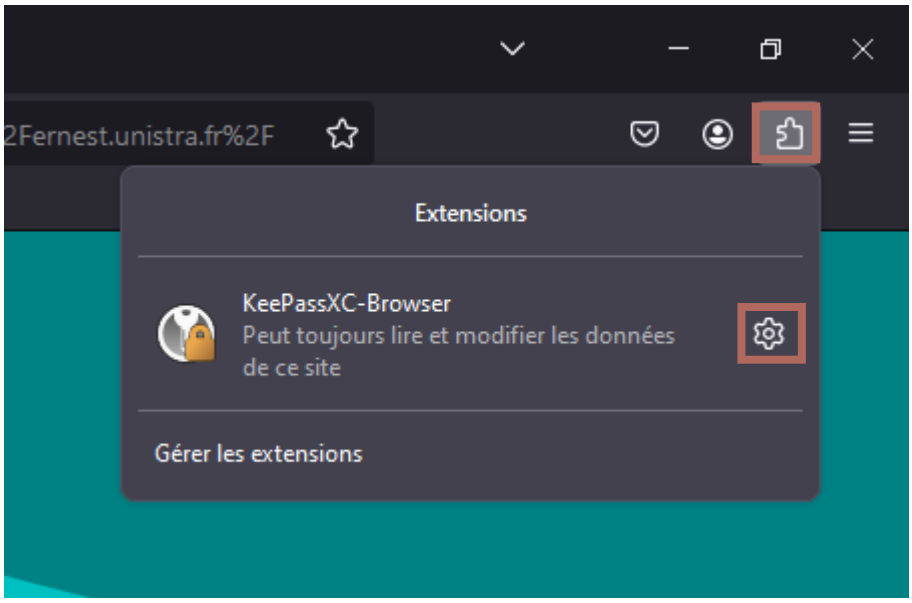
Sélectionnez « Firefox » (ou le navigateur que vous utilisez habituellement).



→ Coupler l'extension avec la base de données

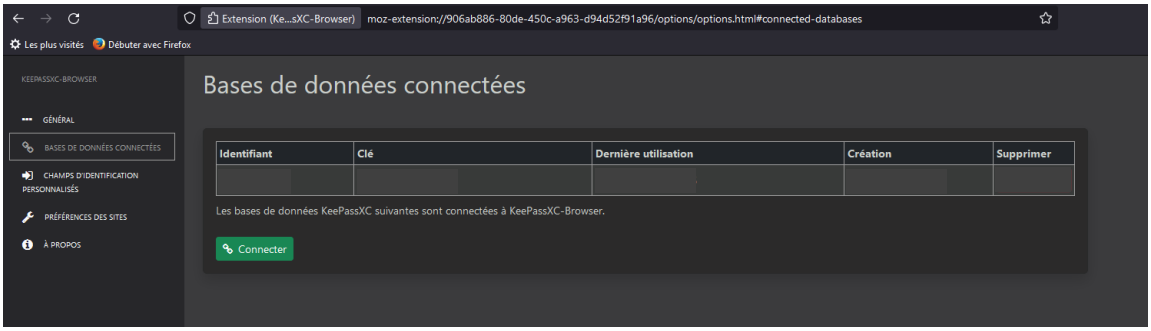
Dans le coin supérieur droit du navigateur, repérez et cliquez sur le symbole

Cliquez sur la roue dentée de la fenêtre de l'extension KeePass-browser

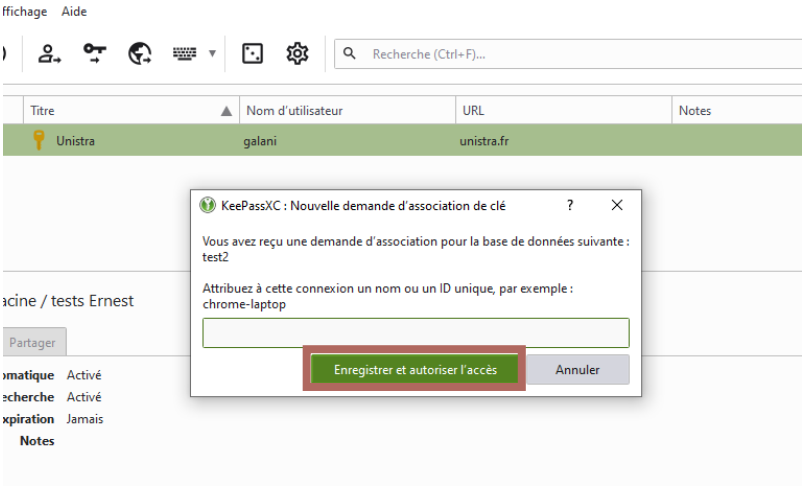


Le coffre-fort doit être déverrouillé pour la suite des opérations.

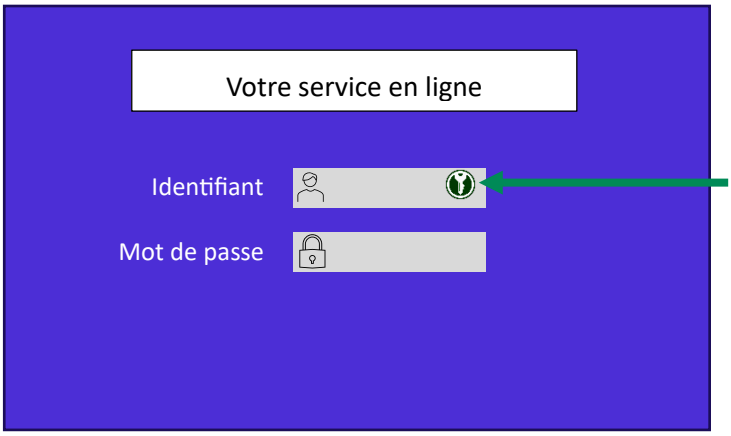
Dans le menu des paramètres, rendez-vous dans « Base de données connectées » et cliquer sur « Connecter ».



→ Dans l'application une fenêtre s'ouvre afin que vous approuviez la connexion entre le navigateur et la base de données. Donnez un nom à cette connexion et cliquez sur « Enregistrer et autoriser l'accès ».



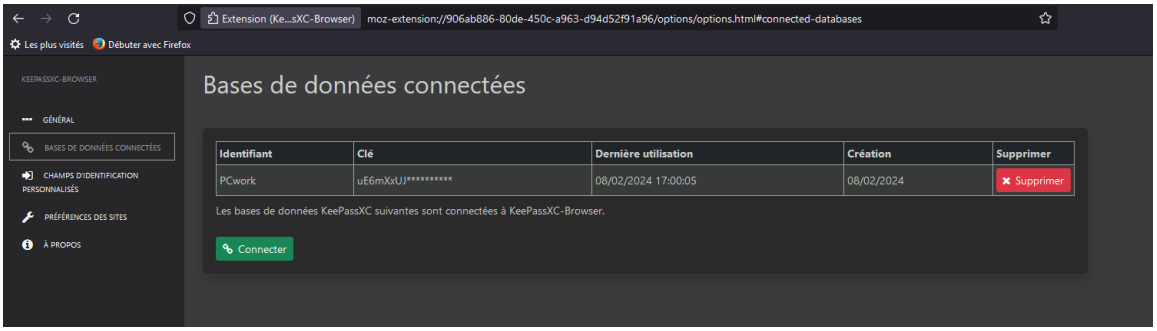
Une fois l'extension connectée, et si la base de données est déverrouillée, les champs se présenteront comme sur cette capture d'écran :



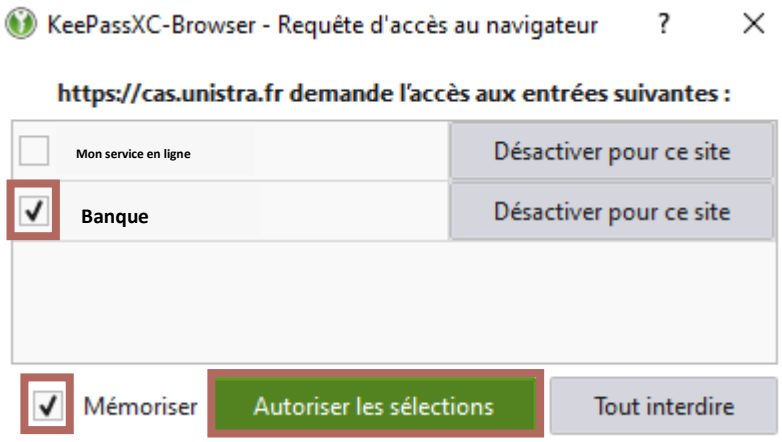
Ici l'icône de KeepassXC est verte indiquant que le coffre-fort est déverrouillé.

Si elle est grise, coffre verrouillé, vous pouvez le déverrouiller en cliquant sur l'icône (le mot de passe maître vous sera demandé)

Vous verrez apparaître cette connexion dans les paramètres de l'extension



Une confirmation est demandée par l'application lors de la première connexion. Il est possible de mémoriser ce choix.



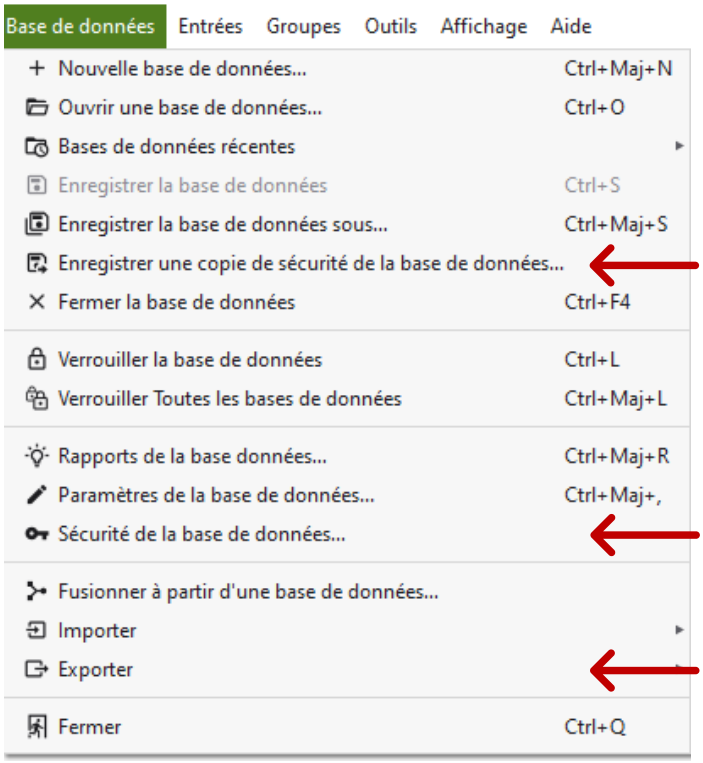
Pensez à épingler l'extension dans la barre d'outils du navigateur pour y accéder plus rapidement (clic droit sur l'icône de l'extension + « épingler à la barre s'outils »). Cela vous évitera de la rechercher dans la liste des vos extensions.

Vous savez désormais l'essentiel pour utiliser votre gestionnaire de mot de passe. Les sections suivantes ne sont pas nécessaires à son bon fonctionnement. Néanmoins elles peuvent vous permettre de l'adapter à vos besoins.

Les fonctions utiles

Cette section du document porte sur des options du gestionnaires de mots de passe qui peuvent s'avérer utiles pour renforcer la sécurité des processus d'authentification. Elle présente également des paramétrages de personnalisation.

① L'onglet « Base de données »



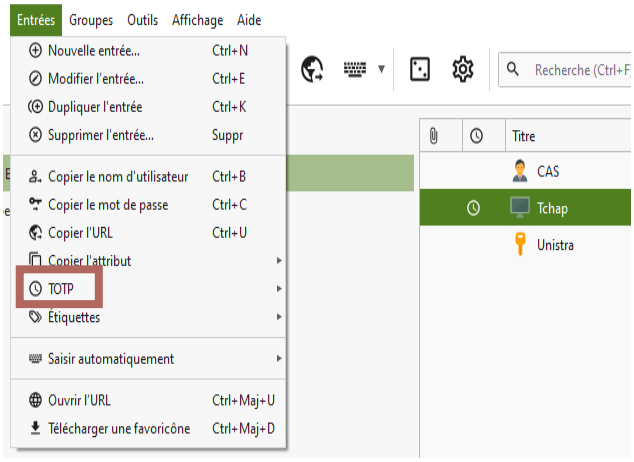
Ici vous pourrez enregistrer une copie de secours de votre base de données (par exemple sur une clé USB). Elle sera chiffrée aussi il n'y pas de risque en cas de perte ou de vol du support.

Dans « Sécurité de la base de données » vous pouvez modifier votre mot de passe ou ajouter un mode de protection supplémentaire comme un fichier clé ou une clé de type YubiKey / OnlyKey.

« Exporter » permet d'obtenir un fichier qui contient toute votre base de données. Il est utile si vous désirez changer de gestionnaire de mot de passe.

⚠ Ne réalisez cet export uniquement lorsque cela s'avère nécessaire et détruisez-le une fois celui-ci enregistré dans le gestionnaire de destination.

② L'onglet « Entrées »

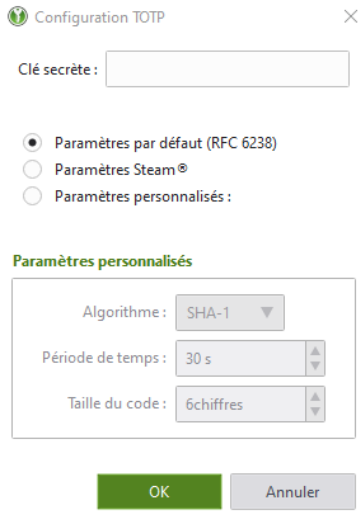


Il faut sélectionner une entrée afin d'accéder à toutes les options de ce menu.

L'option « TOTP[1] », permet d'utiliser une clé de double authentification (2FA) si le site ou la plateforme l'exige (ou si vous avez activé cette fonction sur votre compte sur ce site). Cette fonction vous permet de vous passer d'une application tierce de type « Authenticator »

La double authentification ou authentification à deux facteurs (2FA) est une méthode de renforcement de la sécurité pour un compte en ligne. Habituellement pour accéder à un compte en ligne un identifiant (login) et un mot de passe (authentification) suffisent. Avec la 2FA, une fois le couple de données saisies, et si cette option est disponible et activée sur le site, un code supplémentaire (généralement 4 ou six chiffres) est demandé pour établir la connexion. Cette clé peut être envoyée sur un dispositif individuel (courriel ou SMS) ou récupérée depuis une application tierce qui la génère.

Pour commencer rendez vous sur l'option TOTP et choisissez l'option « définir un TOTP… ».

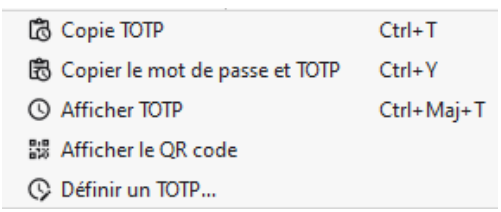


Dans « clé secrète » saisissez la clé unique fournie par le site ou la plateforme lors de l'activation de la 2FA (l'option est généralement activable depuis la section sécurité de votre compte sur le site sélectionné).

Sauf recommandation contraire de la part du site ou de la plateforme, les autres paramètres peuvent être laissés tels quels.

Validez en cliquant sur OK.

Désormais le site de destination de l'entrée reconnaîtra les codes de double authentification fournies par votre gestionnaire de mots de passe.



Par la suite le menu ci-contre sera proposée pour cette entrée.

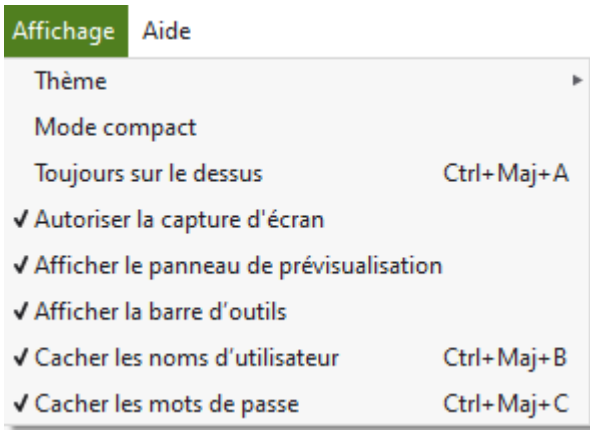
Selon les besoins vous pouvez copier la clé (6chiffres), la clé et le mot de passe, afficher la clé pour l'entrer manuellement sur le site, ou encore afficher un QR code (contenant la clé) pour le scanner à partir d'un autre appareil.

[1] Time based One Time Password

3 L'onglet « Groupes »

Définir un groupe (d'entrées) permet de classer les identifiants par thème ou catégorie. Si plusieurs groupes sont imbriqués les groupes « enfant » héritent des réglages réalisés pour les groupes « parents ».

4 L'onglet « Affichage »



Au bas de ce menu vous trouverez deux options qui vous permettent de rendre invisibles les identifiants associés aux adresses des sites lorsque vous ouvrez le gestionnaire de mots de passe. Il est préférable de les cocher comme dans le panneau ci-contre.

5 La barre d'outils

La barre d'outils reprend certaines fonctions des onglets agissant ainsi comme des raccourcis.

→ Détail des fonction par icône

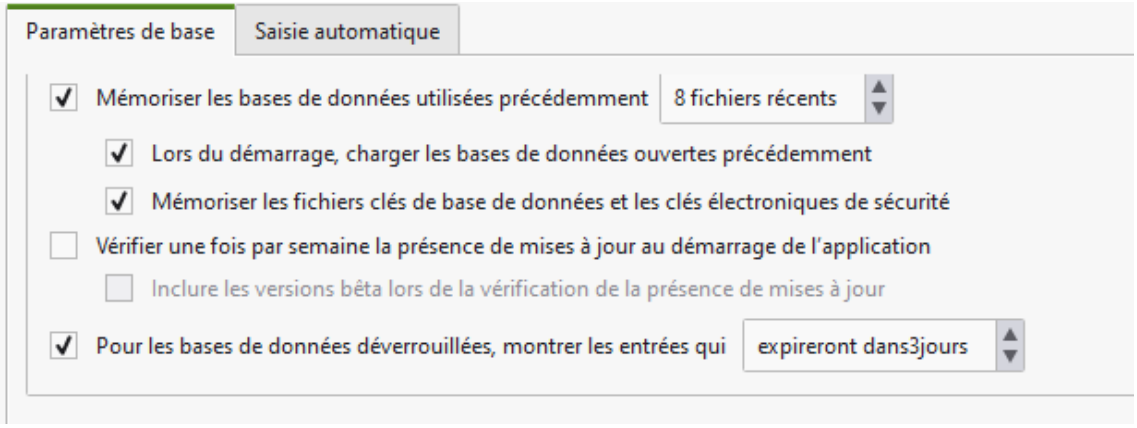
	Ouvre votre explorateur de fichiers pour rechercher votre base de données
	Enregistre la base de données (si elle a été modifiée)
	Verrouille la base de données
	Ajoute une entré dans la base de données
	Modifie une entrée
	Supprime une entrée
	Copie le nom d'utilisateur (identifiant) pour l'entrée sélectionnée. La copie s'efface après 10 s.
	Copie le mot de passe pour l'entrée sélectionnée. La copie s'efface après 10 s.
	Copie l'adresse (url) de l'entrée sélectionnée. La copie s'efface après 10 s.
	Saisie automatique des identifiants
	Générateur de mot de passe. Permet de générer un mot de passe fort selon les critères à définir. Possibilité de le copier pour l'utiliser lors de la création d'un compte en ligne.
	Accès aux paramètres de l'application.

6 À propos de paramètres

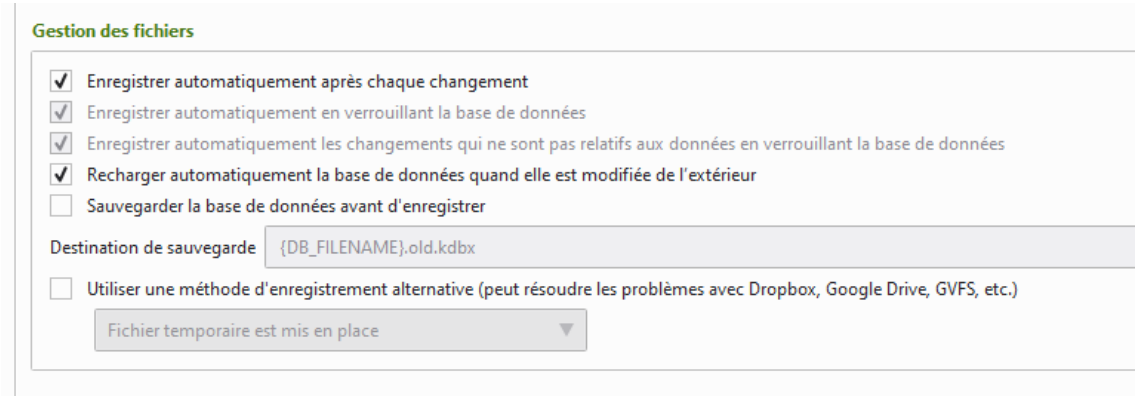
Le détail des trois premières sections de ce menu peut intéresser tout utilisateur de l'application. Les deux dernières sections sont des fonctions avancées dont l'une est vouée à disparaître (Keeshare).

→ Dans la section « Général » on trouve les options de démarrage, d'enregistrement et d'apparence.

Ce panneau vous permet de faire apparaître la ou les base de données que vous avez créées dans l'interface de l'application sans avoir à les rechercher dans votre explorateur de fichiers.

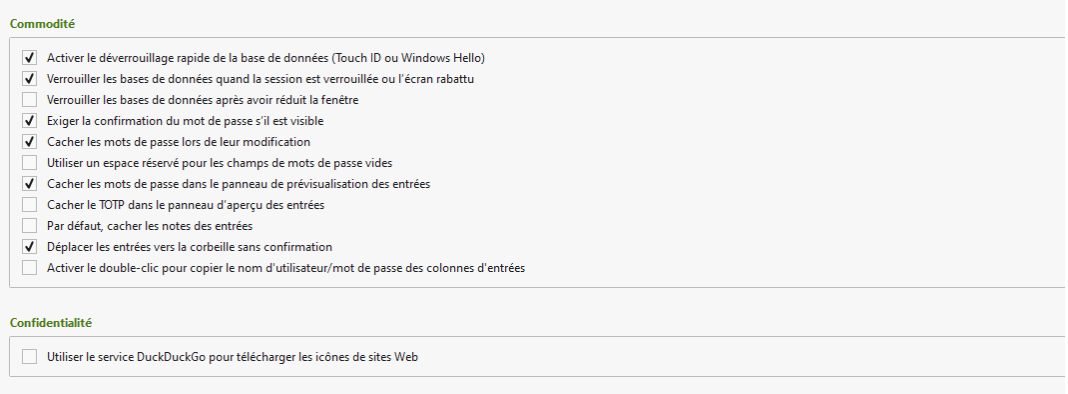


Ce panneau vous permet de gérer les enregistrements de la base de données lors des modifications des entrées.



→ Dans la section « Sécurité » on trouve des réglages que vous pouvez adapter à vos usages.

- « Vider le presse-papier » vous permet de régler le délai pendant laquelle un élément copié (identifiant, mot de passe, code) est gardé dans la mémoire temporaire de votre ordinateur. Après ce délai les éléments sont effacés afin qu'on ne puisse plus les utiliser (ils restent néanmoins stockés dans la base de données).
- « Verrouiller les bases de données après une inactivité de » vous permet de pallier un éventuel oubli de verrouillage de la base de données. Elle se verrouillera automatiquement après le délai que vous avez fixé.



- Dans le même esprit, dans « Commodité » vous pouvez opter pour des réglages de verrouillage/déverrouillage en fonction de votre matériel et de vos besoins.

→ L'intégration aux navigateurs est explicitée dans le point 3 de « Utiliser KeePassXC pour une connexion » de ce document. Cette procédure vous permet d'éviter les navettes entre l'application et le navigateur grâce à l'extension « KeePassXC-Browser »

KeePass sur mobile

L'équipe de KeePass XC n'a pas développée d'application mobile, mais il existe des application tierces recommandées et gratuites :

Pour Androïd : KeePassDX et KeePass2Android

Pour iOS : Strongbox et KeePassium

Dans tous les cas il vous faudra héberger votre base de données dans un serveur distant synchronisé avec votre téléphone (Cloud).

Une documentation (en anglais) très détaillées est disponible sur le site de KeePassXC