Le gestionnaire de mots de passe

KeePass XC

Rodrigue GALANI

Pôle usagers et qualité
Direction du numérique
Université de Strasbourg

2025-2026

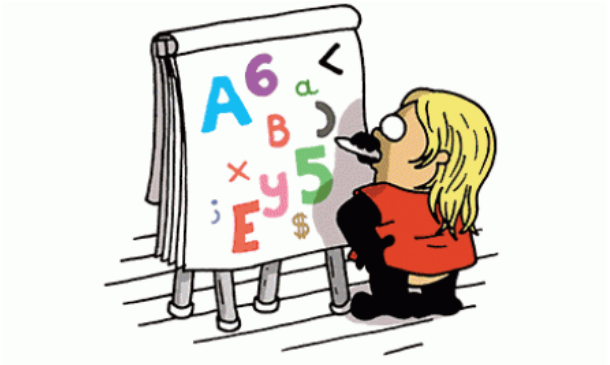
Centre
de culture numérique
Université de Strasbourg

Risques actuels

- Les menaces de type cyber se multiplient pour les particuliers comme pour les organisations.

  À l'université par exemple, chaque année, des centaines de comptes d'usagers doivent être fermés suite à une intrusion liée à un vol de mot de passe.

- Les mots de passe peuvent être vulnérables dans différents cas : trop faible, stocké sur un support mal protégé ou dans le navigateur …



Risques actuels

Qu'est-ce qu'un mot de passe faible?

- La faiblesse est dans son manque de complexité : mot de passe trop court, mot du dictionnaire, lié à une donnée personnelle, caractères utilisés, …
- La faiblesse est contextuelle. Chaque année les techniques cyber s'améliorent et un mot de passe fort en 2020 peut être faible en 2025.
- La faiblesse est dans son manque de variabilité : même mot de passe pour plusieurs sites ou services ou encore inchangé depuis longtemps.

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

Infographie FRANCENUM.GOUV.FR Source : Hive Systems

Solutions

Comment renforcer ses mots de passe ?

- En les rendant longs et complexes
- En utilisant un mot de passe par compte
- En le modifiant régulièrement
- En utilisant une double authentification (si elle est proposée par le service)

Solutions

Autres précautions

- Ne notez vos mots de passe nulle part, même si le navigateur vous le propose !

- Ne transmettez jamais vos mots de passe.

  Aucun organisme, service ou autre ne vous les demandera jamais. Si c'est le cas, c'est une tentative malveillante.

- Protégez votre ordinateur avec un anti-virus et ne téléchargez rien d'un site dont vous n'êtes pas sûr

Solutions

Mais alors que faire pour créer de nombreux mots de passe forts sans avoir à les mémoriser ou à les noter, tout en y accédant sans efforts ?

La solution conseillée par l'ANSII **:** **le gestionnaire de mots de passe**

La plupart des gestionnaires de mots de passe (ou coffre-fort, vault en anglais) sont des applications qui **stockent en ligne**, dans une base de données**, le triplet « adresse web + identifiant + mot de passe ».**

Ces triplets sont **chiffrées** et le seul moyen de les rendre fonctionnels passe par l'utilisation d'un **mot de passe maître**, le seul que vous devez retenir et ne jamais oublier (il n'est stocké nulle part et il n'existe aucun moyen de le récupérer).

Avantages des gestionnaires de mots de passe

Sécurité

- Vous pouvez stocker de manière sûre tous vos mots de passe
- Vous pouvez créer des mots de passe complexes
- Fermeture automatique (paramétrable) du coffre

Confort

- Un seul mot de passe à retenir
- Remplissage facile des champs d'identification et authentification : il suffit de savoir copier et coller ou d'ajouter une extension à votre navigateur pour un remplissage automatique en un clic.
- Conserve les clés d'accès fournies par certains services en ligne

Vous pouvez également ajouter une double authentification pour l'accès au coffre

Principe de base

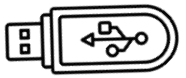
KeePass XC est un gestionnaire de mots passe qui a la particularité de ne pas stocker la base de données sur le serveur du fournisseur du service. **Sa base de données est stockée par vos soins où vous voulez.**

L'application (KeePass XC) ira chercher la base là où vous lui indiquerez et vous demandera le mot de passe maître pour l'ouvrir et vous permettre d'utiliser les mots de passe.

Sur le Web	Sur le PC
Le compte à ouvrir	**L'application KeePass XC** + **Base de données**

ou

Sur le Web	Sur le PC	Support ext. ou « cloud »
Le compte à ouvrir	**L'application KeePass XC**	**Base de données**



Note : Dans tous les cas la base de données doit être accessible dans l'arborescence de l'ordinateur (voir note en fin diaporama)

Avantages supplémentaires de KeePass XC

Sécurité

- Le stockage de vos mots de passe est maîtrisé

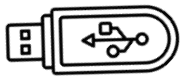
Et plus encore

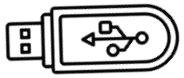
- Possibilité de créer plusieurs coffres (avec des mots de passe différents)
- Fonction TOTP (time based one time password ; double authentification)

Les solutions commerciales sont entièrement en ligne. Vous pouvez y accéder partout et sur n'importe quel PC.

Comme KeePass XC n'est pas une application en ligne il est nécessaire de faire en sorte que l'application soit accessible au PC dont vous vous servez. Pour un usage totalement nomade :

Sur le Web	Support ext	Support ext. ou « cloud »
Le compte à ouvrir	**L'application KeePass XC**	**Base de données**



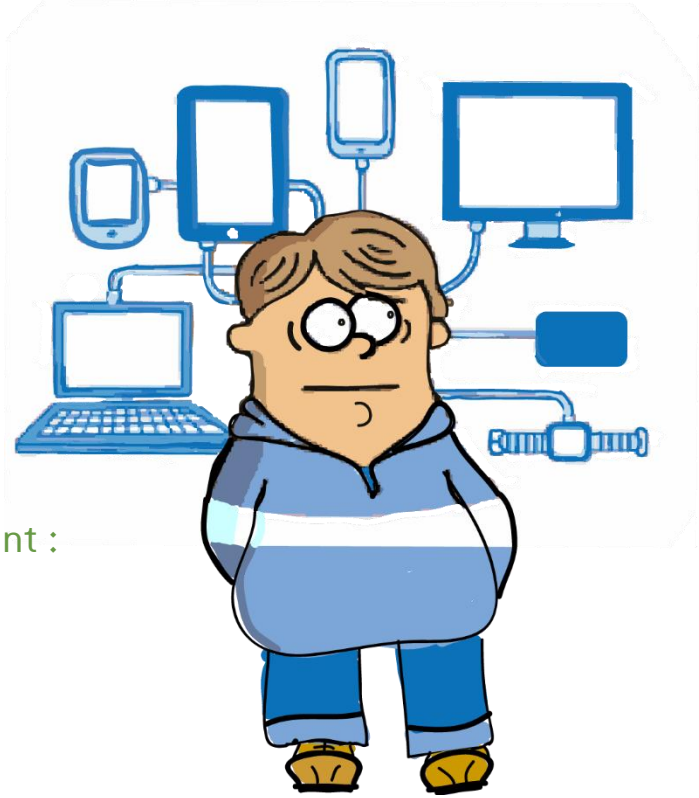


Note : La base de données doit être accessible dans l'arborescence de l'ordinateur (voir note en fin diaporama)

Plateformes pour KeePass XC

À choisir selon vos usages et votre matériel :

- Windows (installateur 64-bit, portable 64-bit, ...)
- MACOS (Apple Silicon, Intel , macOS 11....)
- Linux



KeePass XC ne développe pas de version pour les mobiles mais ils recommandent :

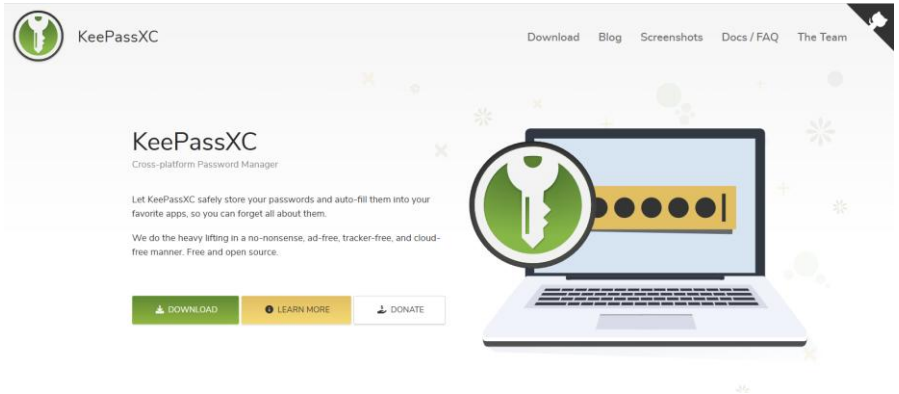
- Pour Android : KeePassDX et KeePass2Android.
- Pour iOS : Strongbox et KeePassium.

Pour démarrer (exemple sur PC)

L'application est disponible pour toutes les plateformes : Windows, MacOS et Linux.

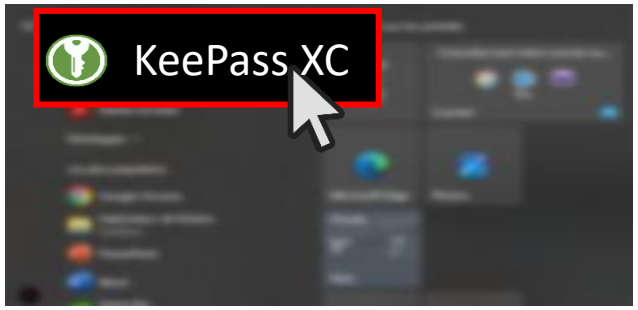
Si les services de l'université administrent votre ordinateur vous pouvez demander son installation.

Si votre ordinateur est géré par vos soins, elle est téléchargeable depuis le site https://keepassxc.org/ .



Après installation…

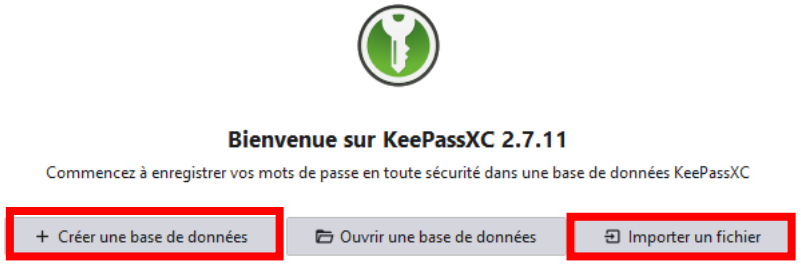
① Ouvrez l'application



Pour démarrer

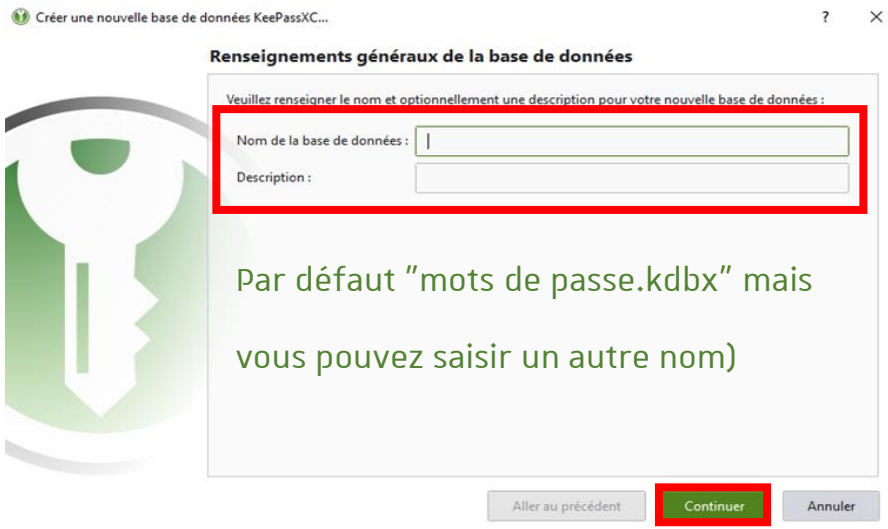
② À l'invite, créez votre base de données (ou importez-la)

2.1 Il s'agit de créer le fichier qui contiendra les identifiants de chaque compte en ligne. Si vous disposez déjà d'un stockage de vos identifiants, vous pouvez également l'importer (voir note en fin de diaporama)



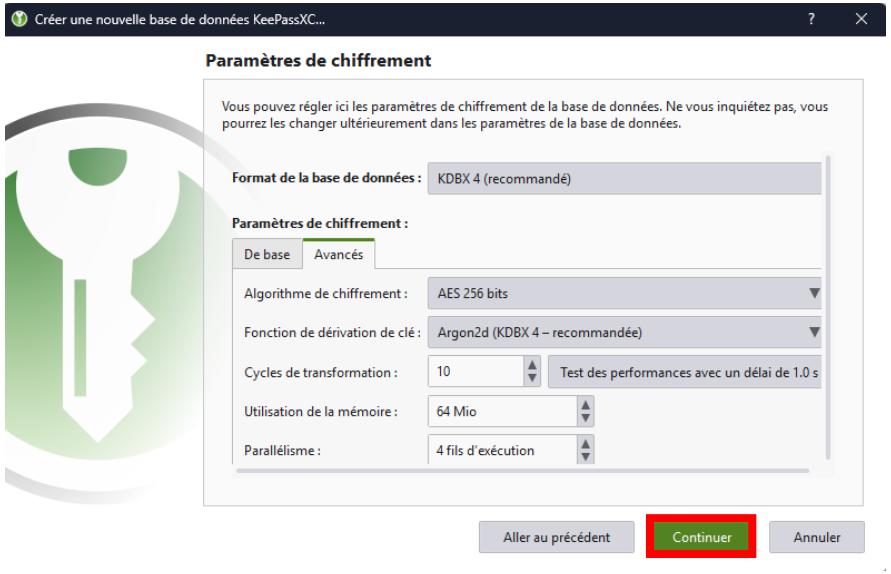
Pour démarrer

2.2 Nommez votre base de données de sorte à la retrouver facilement, notamment si vous en créez d'autres par la suite. Vous pouvez également en faire une brève description.



2.3 Ne rien faire

Ici vous pouvez paramétrer le chiffrement. Cette partie est plutôt réservée à des usagers avancés. Le chiffrement proposé est excellent.

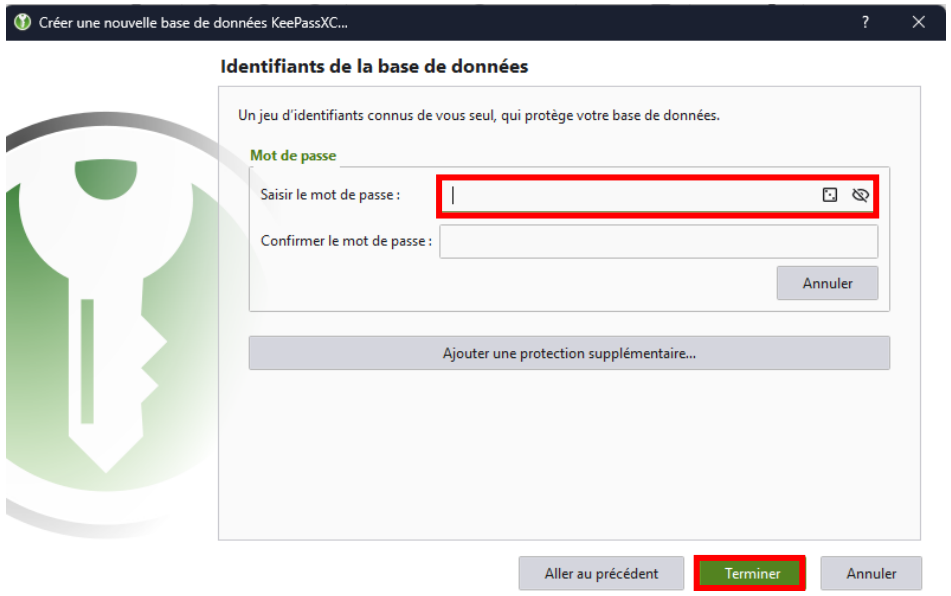


Pour démarrer

③ Créez un 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.



C'est le seul mot de passe que vous devrez connaître par la suite alors retenez que :

- Un bon mot de passe doit être long : **au minimum 12 caractères**, mais 15, 20 ou plus est encore meilleur.
- Un bon mot de passe doit être **complexe** : il ne doit figurer dans aucun dictionnaire ou livre et ne doit pas se déduire facilement d'un titre, d'un proverbe, etc.
- Il ne doit contenir **aucun élément permettant de vous identifier** (domicile, nom, prénom, surnom, date de naissance, etc.).

En cas de perte, il est impossible à récupérer ou réinitialiser.

Pour démarrer

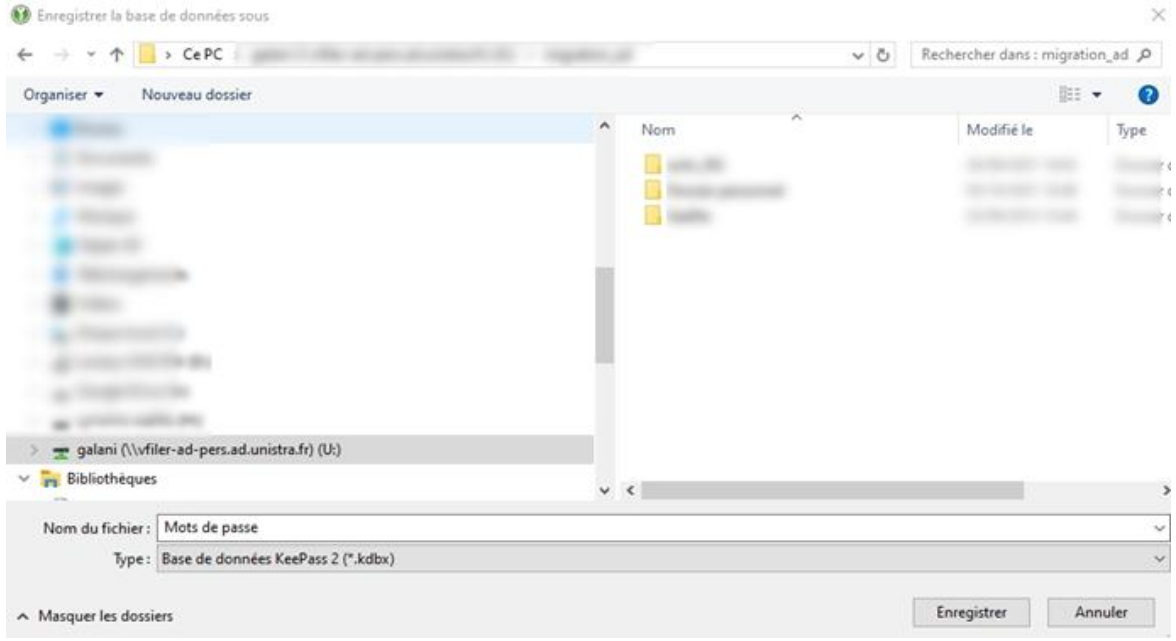
④ Définissez la localisation du stockage de la base de données

Lorsque l'interface vous invite à désigner un emplacement de la base de données, vous pouvez choisir celle qui vous convient le plus, du moment qu'elle vous est accessible (par exemple dans un répertoire placé dans "Mes documents«).

Vous pouvez en faire une copie (qu'il faudra mettre à jour en cas de modification)

La base se présente alors sous la forme d'un fichier du type : nom_du_fichier.kdbx

(par défaut "mots de passe.kdbx" mais vous pouvez saisir un autre nom)

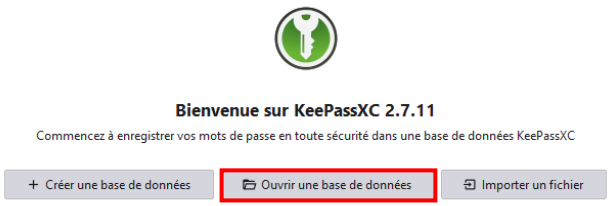


Note: Vous pouvez installer la base de données dans Seafile (Université) mais pour ouvrir Seafile il vous faudra le mots de passe Unistra...

Dépôt des identifiants dans la base

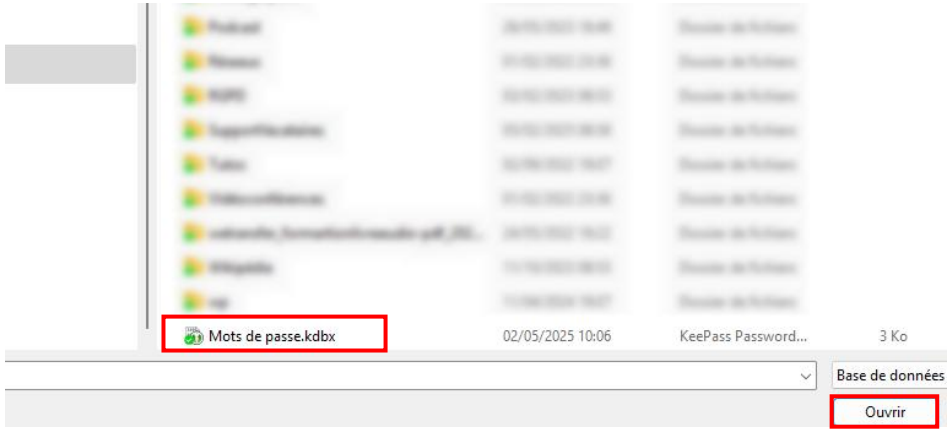
Pour alimenter la base de données il faudra d'abord se rendre dans l'application et ouvrir la base de données soit depuis la fenêtre d'accueil, soit via le menu « Base de données ».

① Lors du lancement de l'application

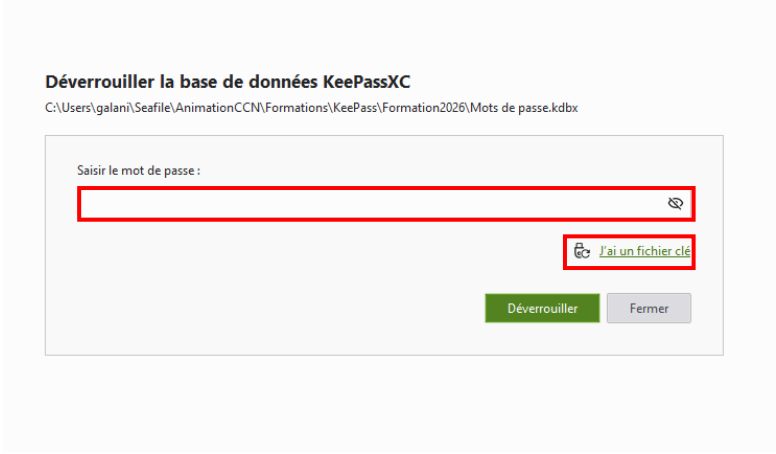


Ou depuis l'onglet "Base de données" :
"Ouvrir une base de données"

② Rendez vous sur le lieu de stockage de la base



③ Saisir le mot de passe maître



Note : si votre ordinateur est équipé d'un dispositif biométrique (Windows Hello ou Touch ID), il sera utilisé par défaut par KeePass XC.
Vous pouvez le désactiver dans « Paramètres > Sécurité »

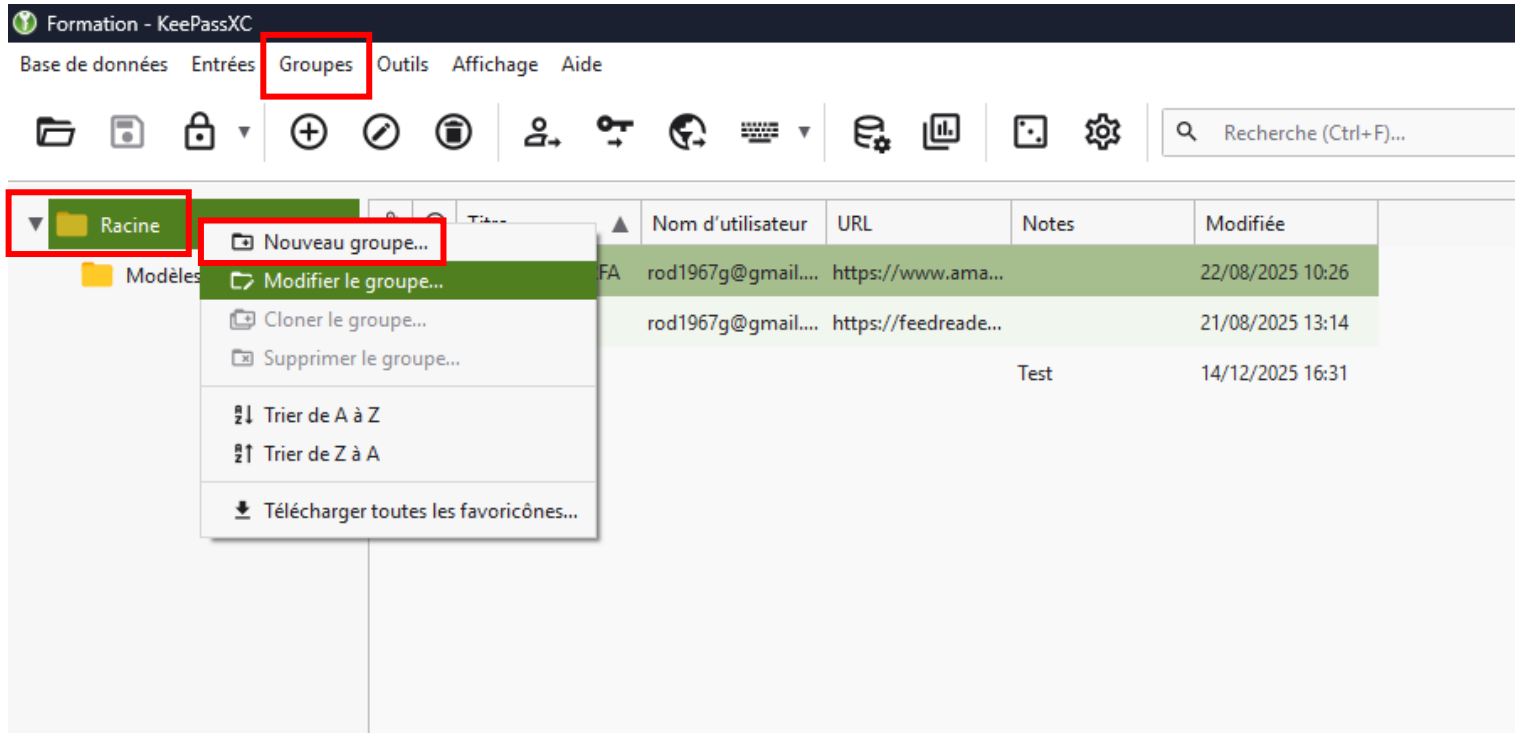
Dépôt des identifiants dans la base

Si vos mots de passe sont nombreux et que vous voulez les catégoriser, il est recommandé de regrouper les triplets « adresse web+identifiant+mot de passe » par thème ou sujet. Pour cela il suffit de créer des « groupes » qui correspondent à des dossiers dans ce qui ressemble à un explorateur de fichiers.

Vous pouvez créer ces groupes à partir de l'onglet dédié

ou

À partir de la racine de la base de données, en utilisant le clic droit de la souris



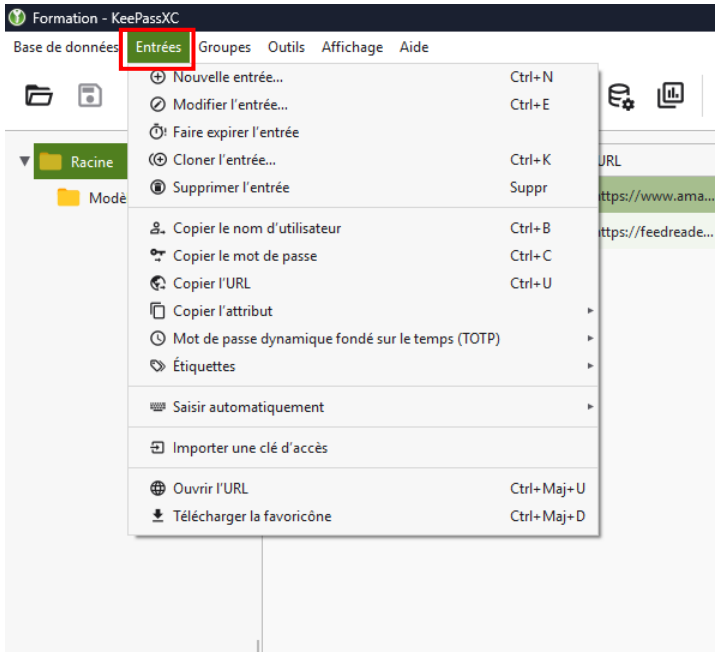
S'ils ne sont pas nombreux vous pouvez enregistrer les « triplets » directement à la racine.

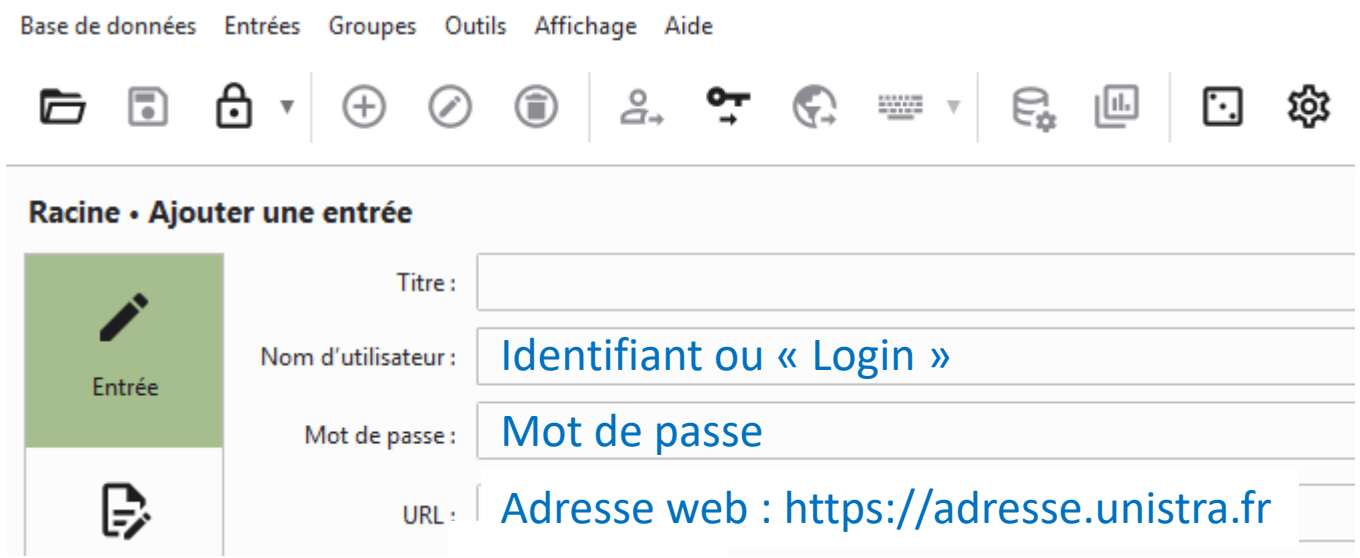
Dépôt des identifiants dans la base

Les « triplets » adresse web+identifiant+mot de passe sont nommés **« Entrées »** dans KeePass XC.

Que vous ayez sélectionné la racine ou un groupe, pour saisir les triplets il suffit de cliquer sur l'onglet « Entrée » et de choisir « Nouvelle entrée » ou cliquez sur l'icône ⊕

Si vous devez créer un mot de passe, vous pouvez utiliser la fonction « dé » ⚄





N'oubliez pas de cliquer sur OK

Utiliser Keepass XC au quotidien

KeePass XC a démarré et vous avez ouvert votre base de données à l'aide du mot de passe-maître.
Depuis votre poste de travail rendez vous sur le site ou la plateforme à laquelle vous voulez accéder.

Il est possible d'utiliser trois méthodes différentes pour compléter les champs d'identification : **manuelle, automatique ou depuis le navigateur**

Saisie « manuelle »

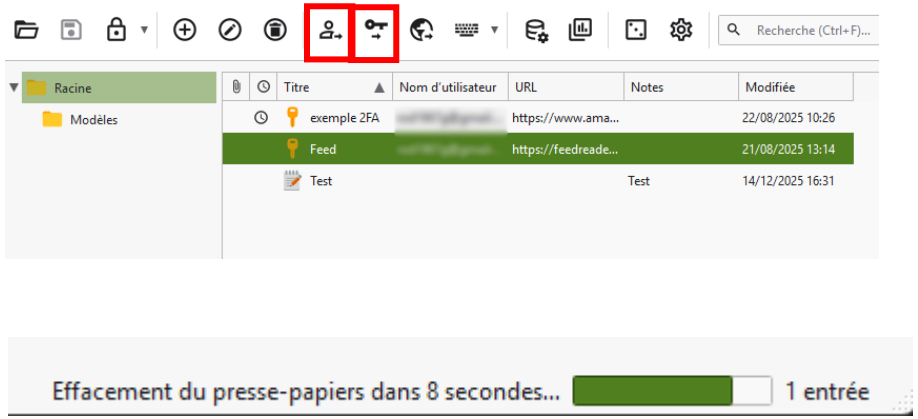
Sélectionnez l'entrée puis :

Copiez l'identifiant en cliquant sur

Collez-le dans le champ ①

Copiez le mot de passe en cliquant sur

Collez-le dans le champ ②

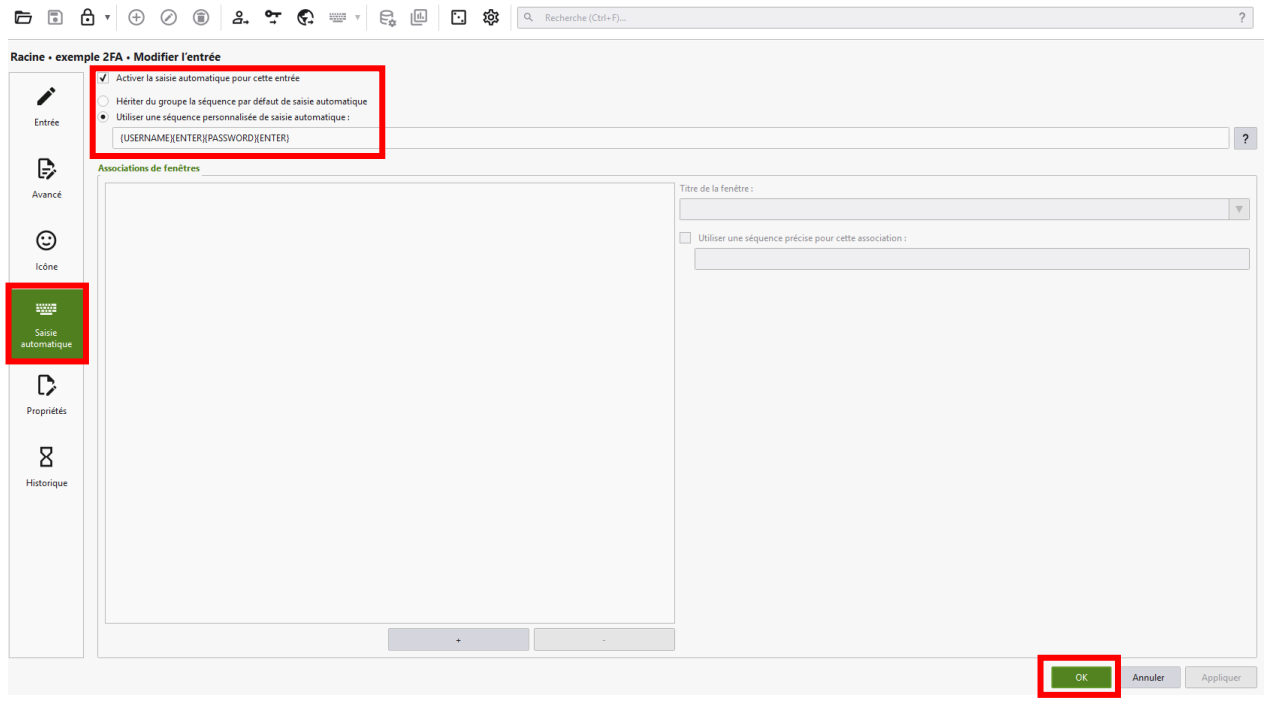


Note : Par sécurité, la copie reste dans le presse-papier pendant 10s (par défaut)

Utiliser Keepass XC au quotidien

Saisie « automatique » : paramétrage

La saisie automatique doit être paramétrée pour chaque entrée. De fait, il faut préciser l'ordre de présentation des champs sur le site pour lequel vous cherchez à vous identifier.



Lors de la création de l'entrée, ou par la suite en la modifiant, rendez-vous dans la section **« Saisie automatique »** et activez la saisie automatique.

Le modèle de saisie automatique par défaut correspond aux champs et à la séquence la plus courante :

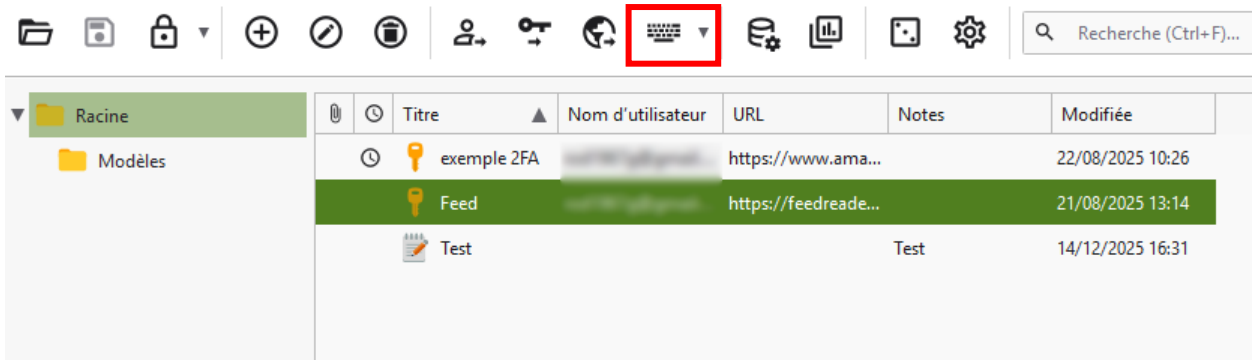
Identifiant > passage au champ suivant > mot de passe > touche entrée. Il est noté {USERNAME}{TAB}{PASSWORD}{ENTER}

Dans l'exemple ci-dessus la séquence a été personnalisée car le site correspondant propose, sur une première page, la saisie de l'identifiant qu'il faut valider avant de passer à une seconde page demandant la saisie du mot de passe (à valider également). Cela donne : {USERNAME}{ENTER}{PASSWORD}{ENTER}.

Utiliser Keepass XC au quotidien

Saisie "automatique" : utilisation

Après la sélection de l'entrée concernée il suffit de cliquer sur ⌨▾
Après une demande confirmation, les champs de la fenêtre active seront automatiquement saisis



Note : la saisie se fera sur la dernière fenêtre active dans le navigateur. Soyez prudents quant aux fenêtres et onglets que vous avez ouvert en dernier.

Utiliser Keepass XC au quotidien

Saisie depuis le navigateur

Il est possible de **déporter les fonctions principales de KeePass XC dans le navigateur** (mais il faudra tout de même ouvrir la base de données depuis l'application).

L'application peut alors rester ouverte en arrière-plan et vous pourrez compléter les champs directement depuis le navigateur.

Note : Si vous utilisez peu de mots de passe au cours de votre session, cette fonction n'est peut-être pas utile.

Cette connexion entre le navigateur et l'application se fait grâce à une extension**, KeePass XC Browser**, qu'on ajoute au navigateur.

Sur les ordinateurs administrés par la Dnum l'extension est déjà installée dans Firefox.

Pour les autres ordinateurs, il suffit de l'installer depuis le catalogue de votre navigateur comme suit :

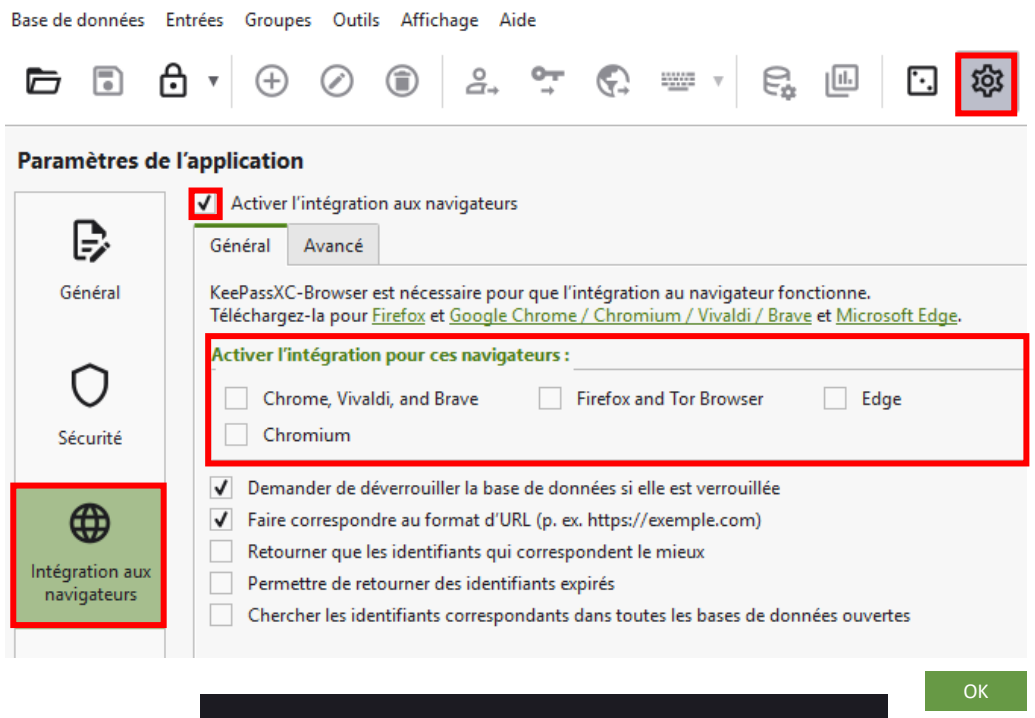
Depuis l'icône  qui se trouve sur la barre de votre navigateur, cliquez sur gérer les extensions et cherchez **KeePass XC-Browser** et cliquez sur Ajouter à Firefox.

Note: Pour les navigateurs Chrome, après « Gérer les extensions », cliquez sur le lien Chrome Web Store

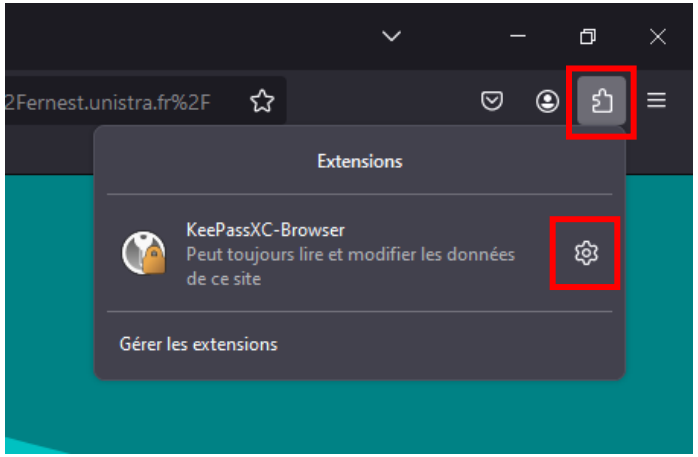
Utiliser Keepass XC au quotidien

Connexion entre KeePass XC Browser et KeePass XC

① **Dans KeePass XC**
cliquez sur l'icône des paramètres et choisissez l'onglet "Intégration aux navigateurs".
Définissez votre navigateur

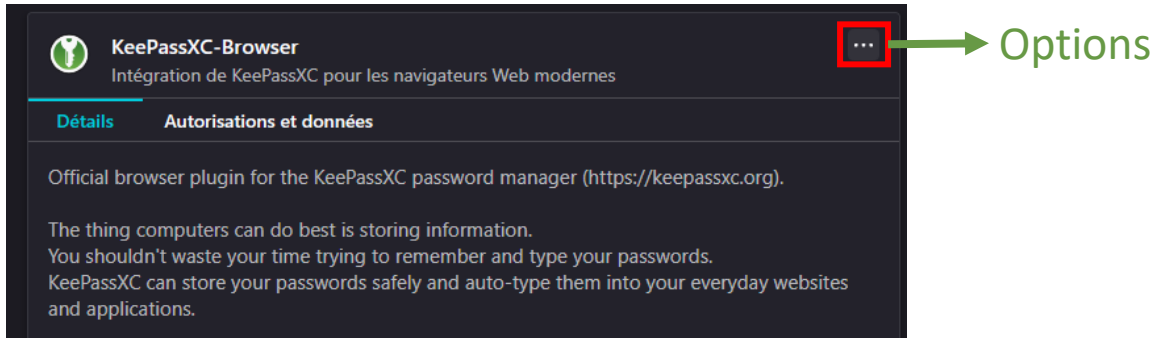


② **Dans le navigateur**
Cliquez sur l'icône des extensions et, pour KeePass XC Browser, cliquez sur l'icône des paramètres

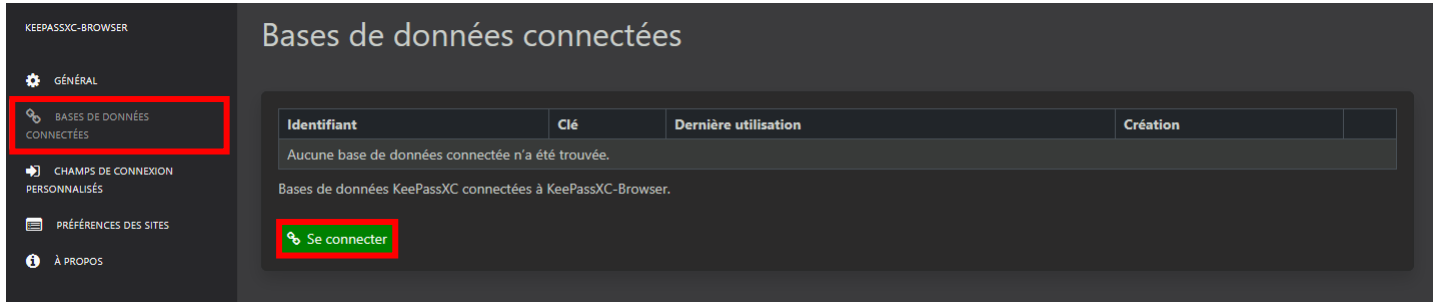


Utiliser Keepass XC au quotidien

Dans la fenêtre des paramètres, cliquez sur l'accès aux options.



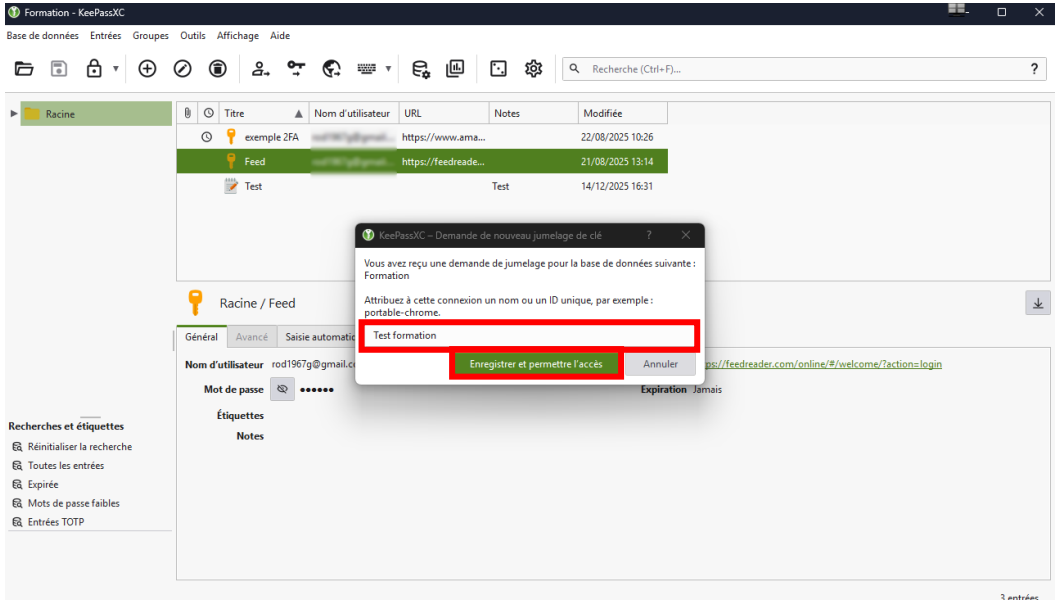
Choisissez « Base de données connectées » puis cliquez sur le bouton « Se connecter »



Utiliser Keepass XC au quotidien

3 **De retour dans KeePass XC**

Suite à la demande connexion, une fenêtre s'ouvre dans l'application pour que vous la validiez. Donnez un nom à cette connexion et cliquer sur « Enregistrer et autoriser l'accès »



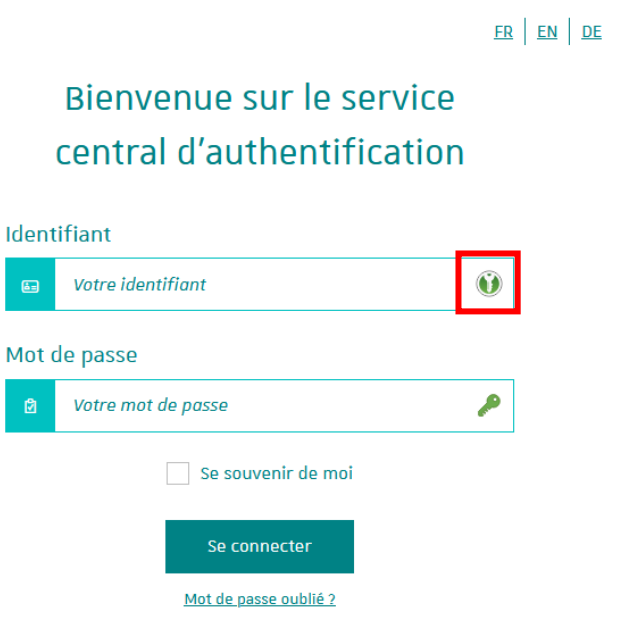
Utiliser Keepass XC au quotidien

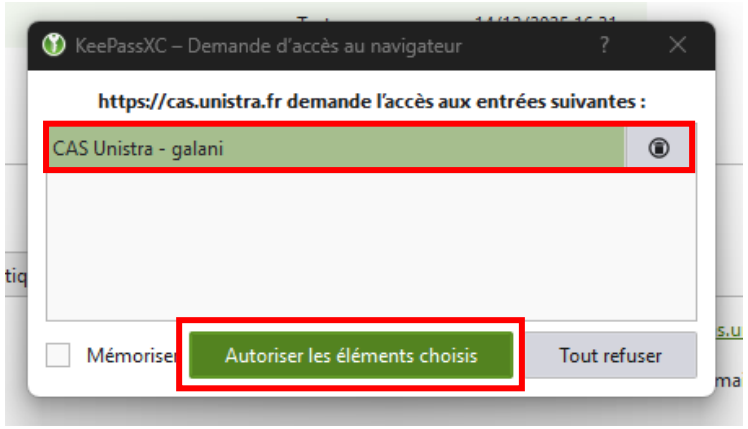
Au quotidien, il suffira de déverrouiller la base de données, et vous verrez apparaître sur les pages de connexion votre navigateur une icône dans les champs à compléter.

Vous indique que la base de données et bien ouverte

Vous indique que la base de données et verrouillée ou que les identifiants pour ce site ne sont pas enregistrés dans KeePass XC

Cliquez sur et les champs seront complétés automatiquement





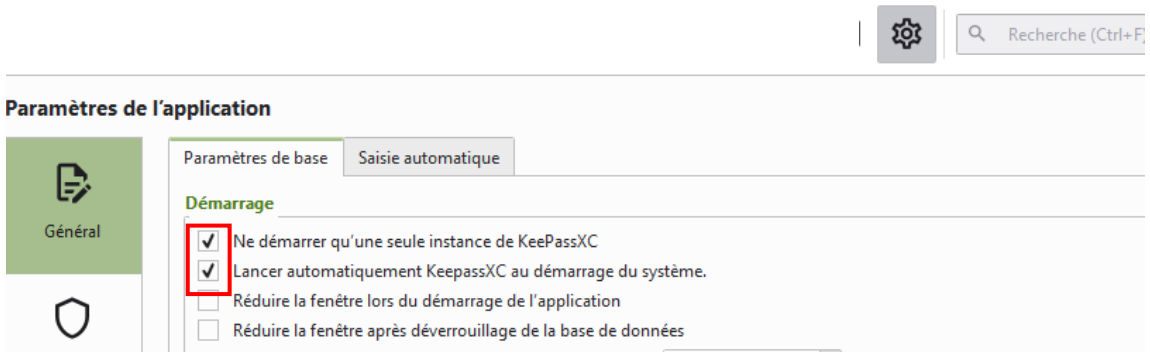
Note : lors de la première utilisation une confirmation vous sera demandée. Pensez à cocher la case « Mémoriser »

Paramétrages à connaître

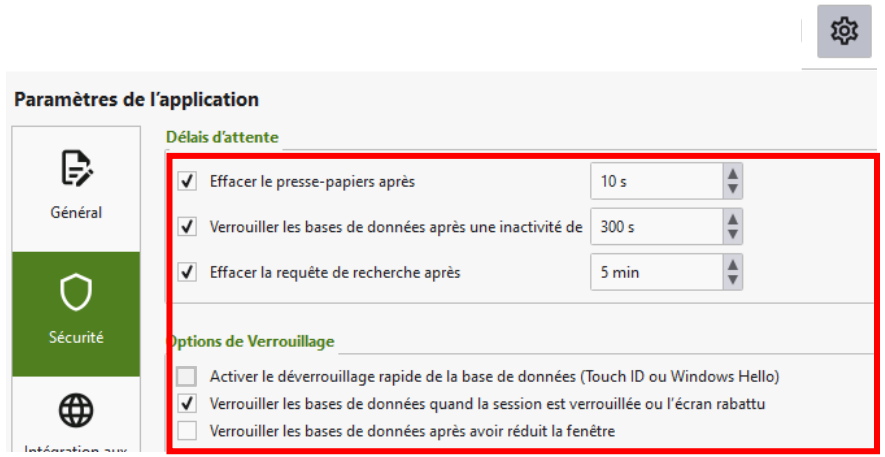
Par défaut un certain nombre de paramètres sont réglés pour une sécurité optimale.

Paramètres

Général



Sécurité



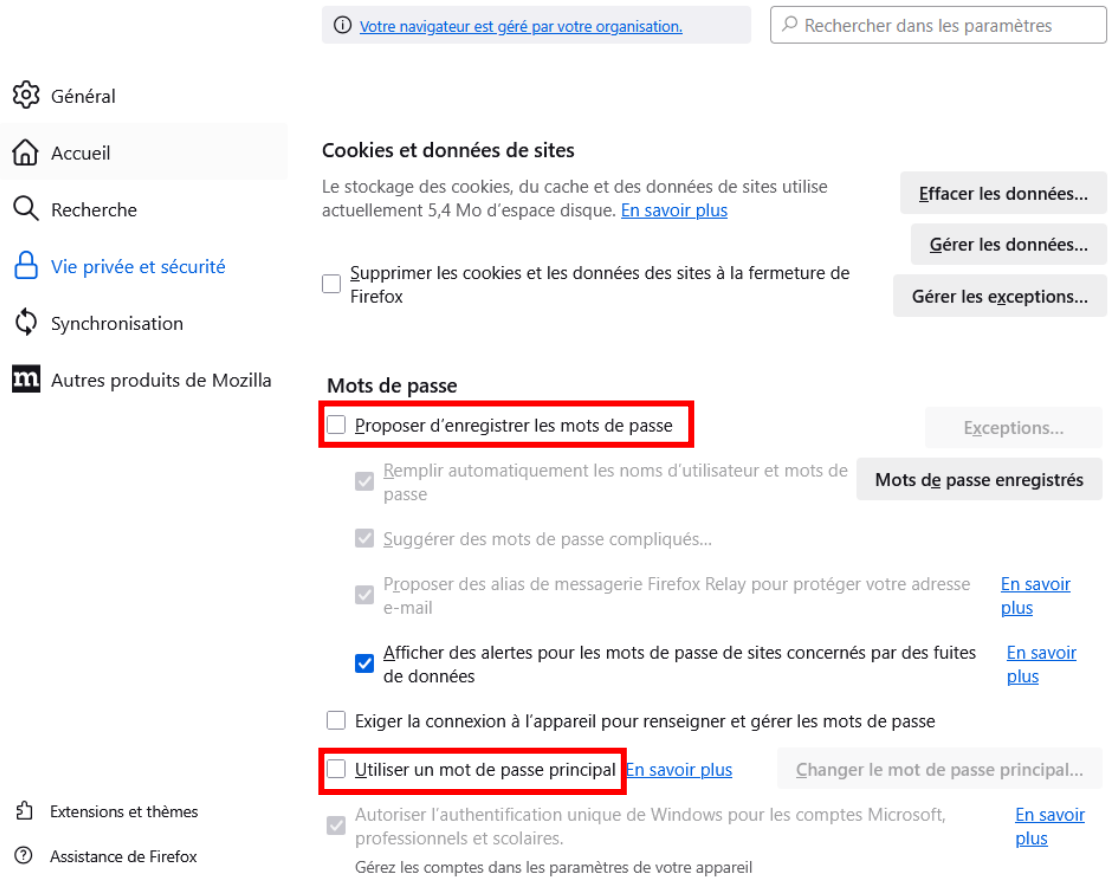
Ces paramètres vous permettent d'automatiser la sécurité : effacement des informations dans le presse-papier, verrouillage de la base...

N’oubliez pas…

Une fois que vous aurez vérifié que tout fonctionne bien, et si vous utilisiez votre navigateur pour sauvegarder vos mots de passe, pensez à :

1. Effacer vos mots de passe du navigateur (menu ⋮ puis « mots de passe »
2. Décocher la case « Proposer d’enregistrer les mots de passe » (menu ⋮ > paramètres > Vie privée et sécurité)
3. Supprimer votre mot de passe principal (si vous en aviez un pour le navigateur)

Exemple de Firefox

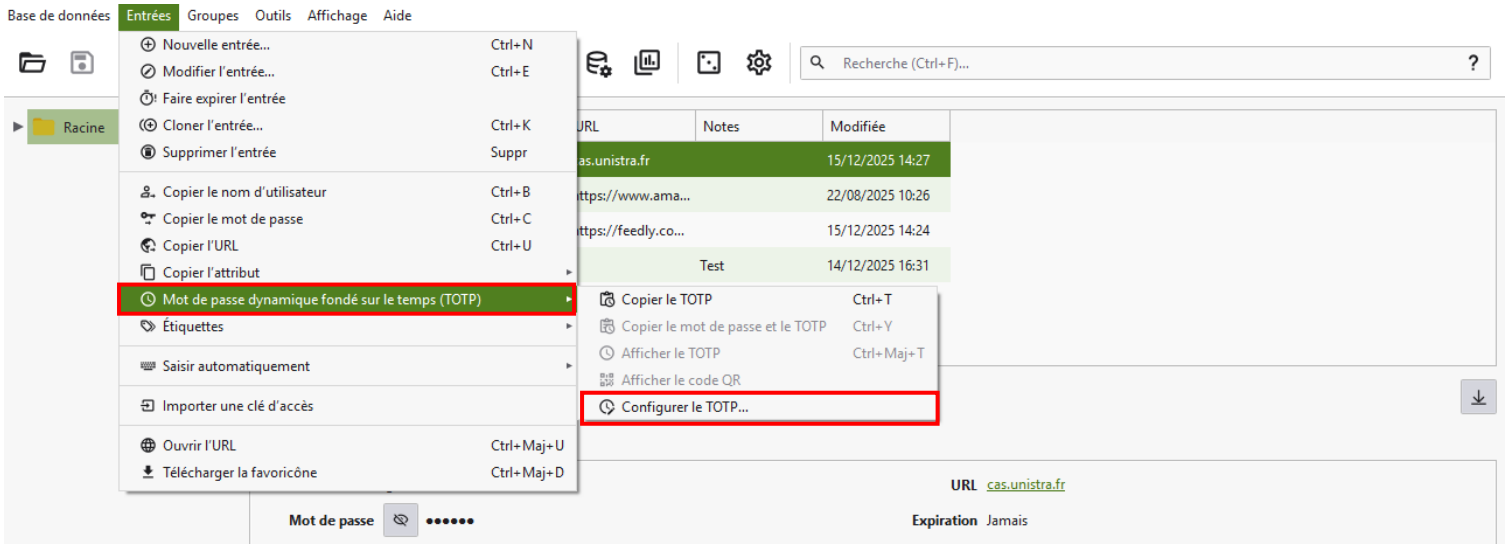


Paramétrage pratique

La double authentification avec la fonction TOTP (time based one time password).

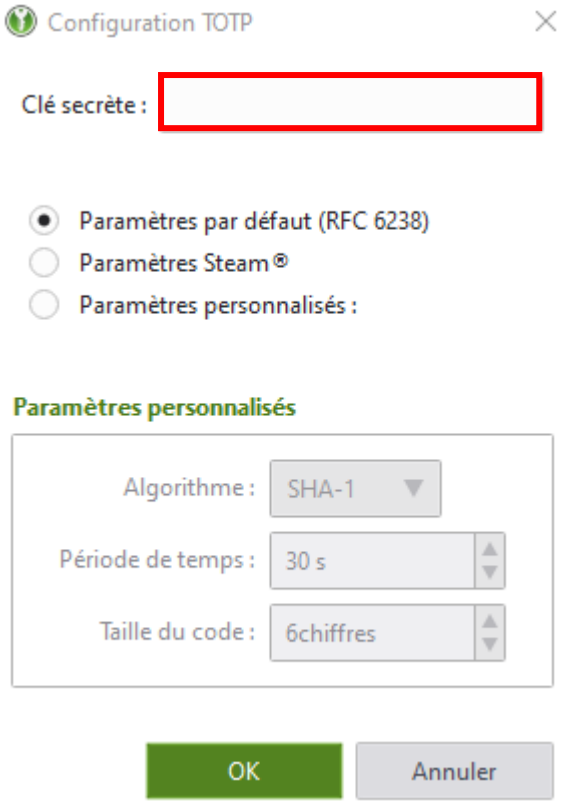
La double authentification est une méthode d'identification forte qui fait appel à une application préalablement paramétrée pour fournir un code unique et temporaire qui sera utilisé en complément du mot de passe.

Si un site ou un service propose l'activation d'une authentification à double facteur il est possible d'utiliser cette option depuis KeePass XC.



Après avoir sélectionné l'entrée concernée, rendez vous dans l'onglet Entrée pour choisir TOTP > Configurer TOTP

Paramétrage pratique



Pour paramétrer le TOTP, il faut fournir une clé proposée par le service en ligne correspondant à l'entrée sélectionnée dans KeePass XC.

La clé, si elle existe, se trouve généralement dans les paramètres de sécurité de votre compte en ligne sous « Double authentification » ou « 2FA ».

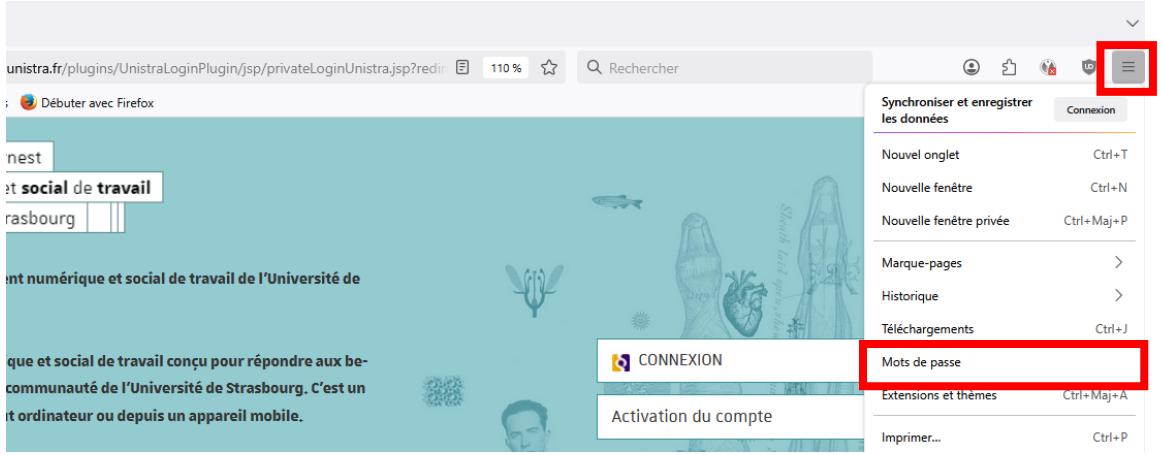
On vous proposera généralement de scanner un QR code mais vous trouverez dans la même section la possibilité de récupérer le code (clé secrète) que porte ce QR code (série de chiffres).

Note : Cette opération n'aura lieu qu'une seule fois et permettra au service en ligne de reconnaître l'authenticité du code TOTP que KeePass XC proposera.

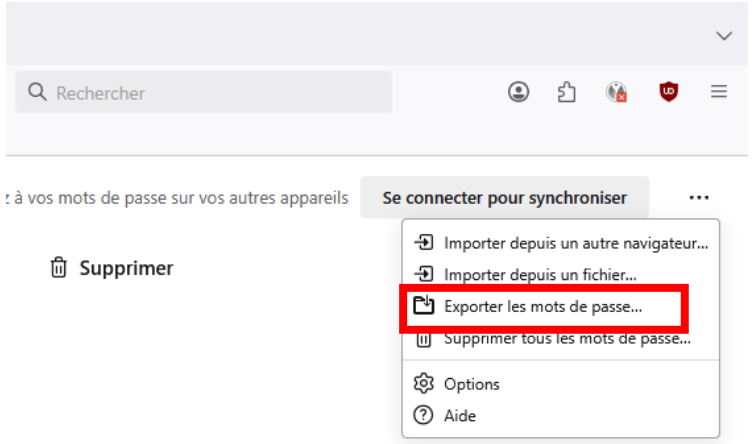
Note sur l'importation d'une base de données

Si vous avez enregistré vos mots de passe dans le navigateur (par exemple, Firefox) vous pouvez les importer facilement dans le gestionnaire KeePass XC

1. Rendez-vous dans les paramètres de Firefox et choisissez l'option « Mots de passe »



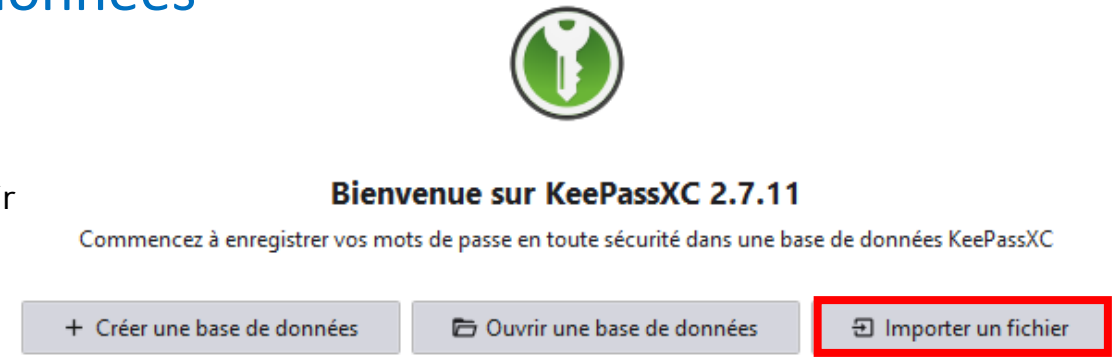
2. Dans la fenêtre suivante, cliquez sur « Exporter les mots de passe » puis passez le message d'avertissement.



3. Enregistrez le fichier au format csv comme proposé. **Retenez bien l'emplacement du fichier.**

Note sur l'importation d'une base de données

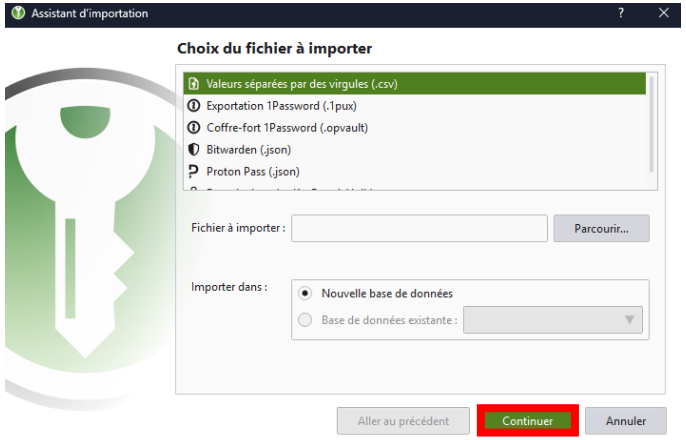
4. Dans KeePass XC. Lors de la création du coffre fort, juste après avoir démarré l'application, choisissez « Importer un fichier »



5. Choisissez « valeurs séparées par des virgules » (.csv)

6. Chercher le fichier à importer, celui que vous avez téléchargé depuis votre navigateur et cliquez sur continuer.

La suite est identique au processus de création d'un base de données



Note : vous pouvez également récupérer vos mots de passe une fois le coffre KeePass créé.

Important : N'oubliez pas de supprimer le fichier CSV que vous avez créé lors de l'exportation depuis le navigateur.

Note sur l'utilisation d'un cloud pour la base de données (exemple de Seafile)

Pour une utilisation du cloud sur votre ordinateur

Dans tous les cas la base de données doit être accessible dans l'arborescence de l'ordinateur. Pour cette raison, il faudra disposer du client Seafile sur votre ordinateur (idem pour les autres « clouds » qui devront également être intégrés à l'arborescence).

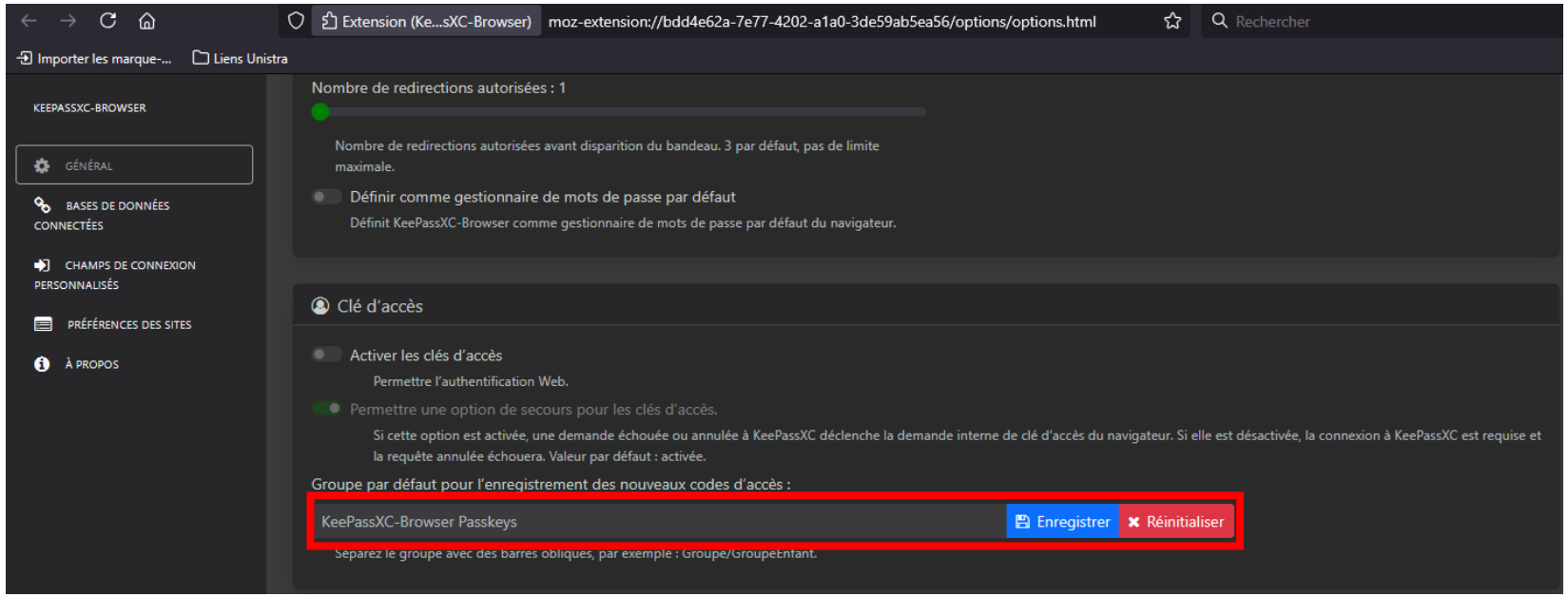
L'usage d'un cloud exclue une utilisation sur n'importe quel ordinateur.

Pour une utilisation sur votre mobile (exemple de KeePass2Android : KP2A).

Si vous utilisez Seafile pour stocker la base de données, il faudra installer l'application Seafile et l'ouvrir. Lors du paramétrage de l'application KP2A choisissez « sélecteur de fichier système » et dans « parcourir les fichiers…. » cherchez Seafile. Il suffit ensuite de localiser le fichier .kdbx.

Vous utilisez des clés d’accès?

Les clés d’accès se gèrent depuis l’extension du navigateur « KeePassXC Browser » avec KeePass XC actif et la base ouverte.



Définissez le groupe qui stockera les clés dans KeePassXC
Sur le site web sur lequel vous cherchez à vous identifier, rendez vous dans les paramètres de sécurité et cherchez la clé d’accès à enregistrer. Suivez simplement les instructions.

Merci pour votre attention