Table des matières

Public : tout public

Gérer ses mots de passe avec KeePassXC

KeePassXC est un gestionnaire de mots de passe multiplateformes. Il fonctionne aussi bien sur Linux que sur macOS ou Windows, des clients sur Android et iOS sont disponibles.

Il **stocke les secrets** (essentiellement les mots de passe) dans un fichier KDBX. Ce fichier est à voir comme un **conteneur sécurisé** : il doit donc être **protégé par un « mot de passe fort »** (relire à ce sujet les recommandations du RSSI sur les comptes et mots de passe) et doit être très **soigneusement sauvegardé**.

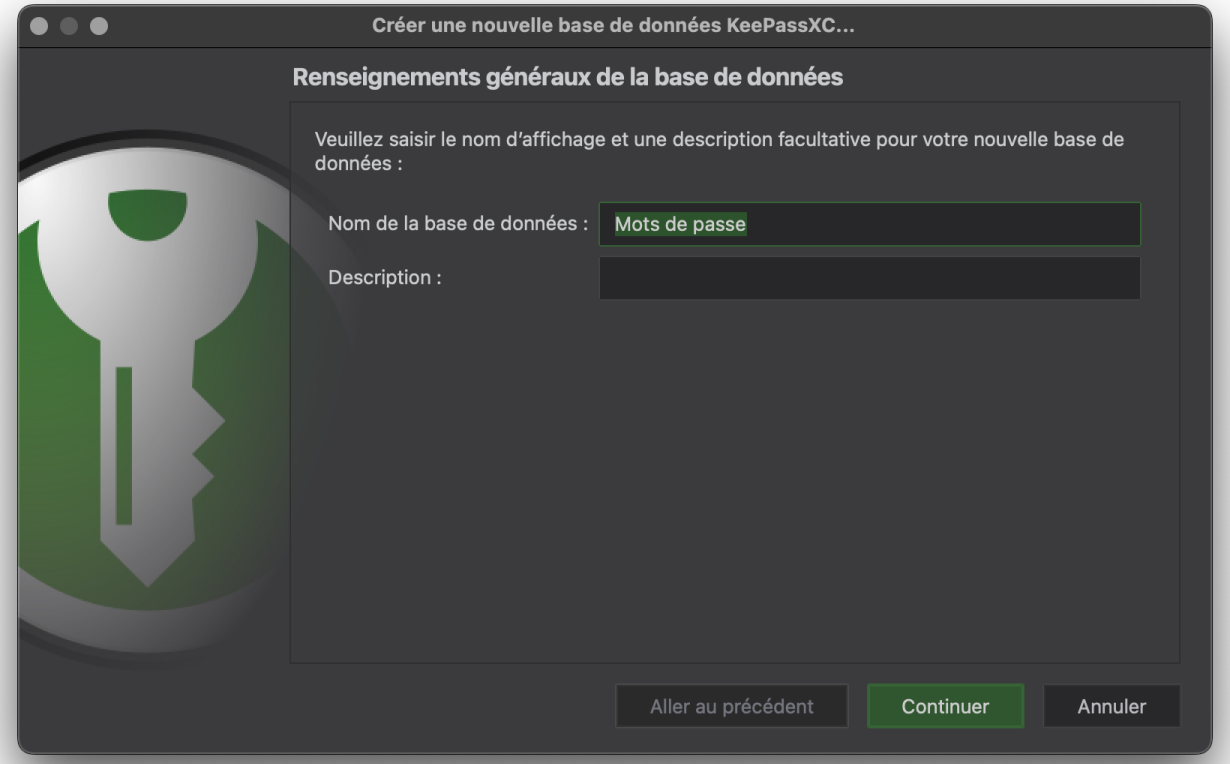
La suite constitue une prise en mains succincte. Se référer à la documentation officielle pour aller plus loin :

- Getting Started Guide
- User Guide

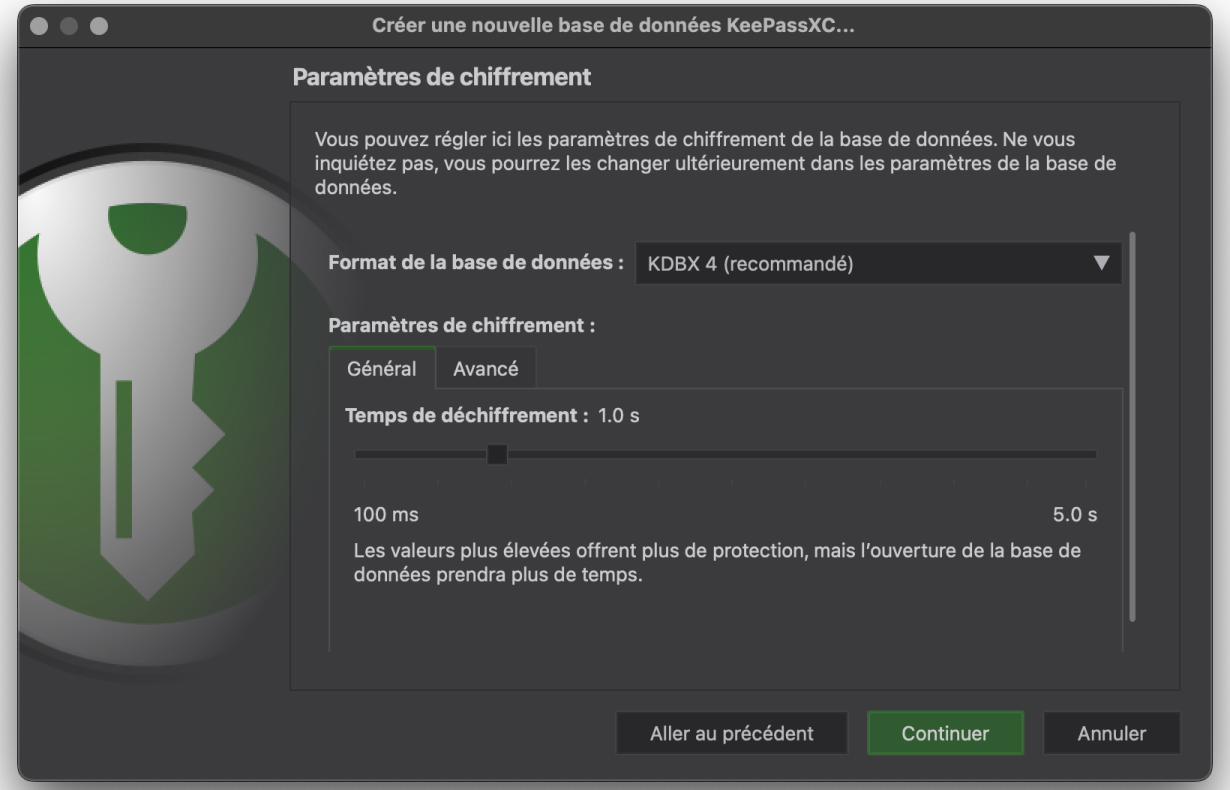
Premier lancement

Attention : sur Windows, depuis la vers 2.7.0 (21 mars 2022), des utilisateurs pourront avoir besoin d'installer aussi Microsoft Visual C++ Redistributable (si des messages d'erreur apparaissent, messages mentionnant des bibliothèques DLL manquantes).

Après installation, créer un nouveau conteneur : menu *Base de données* » *Nouvelle base* :



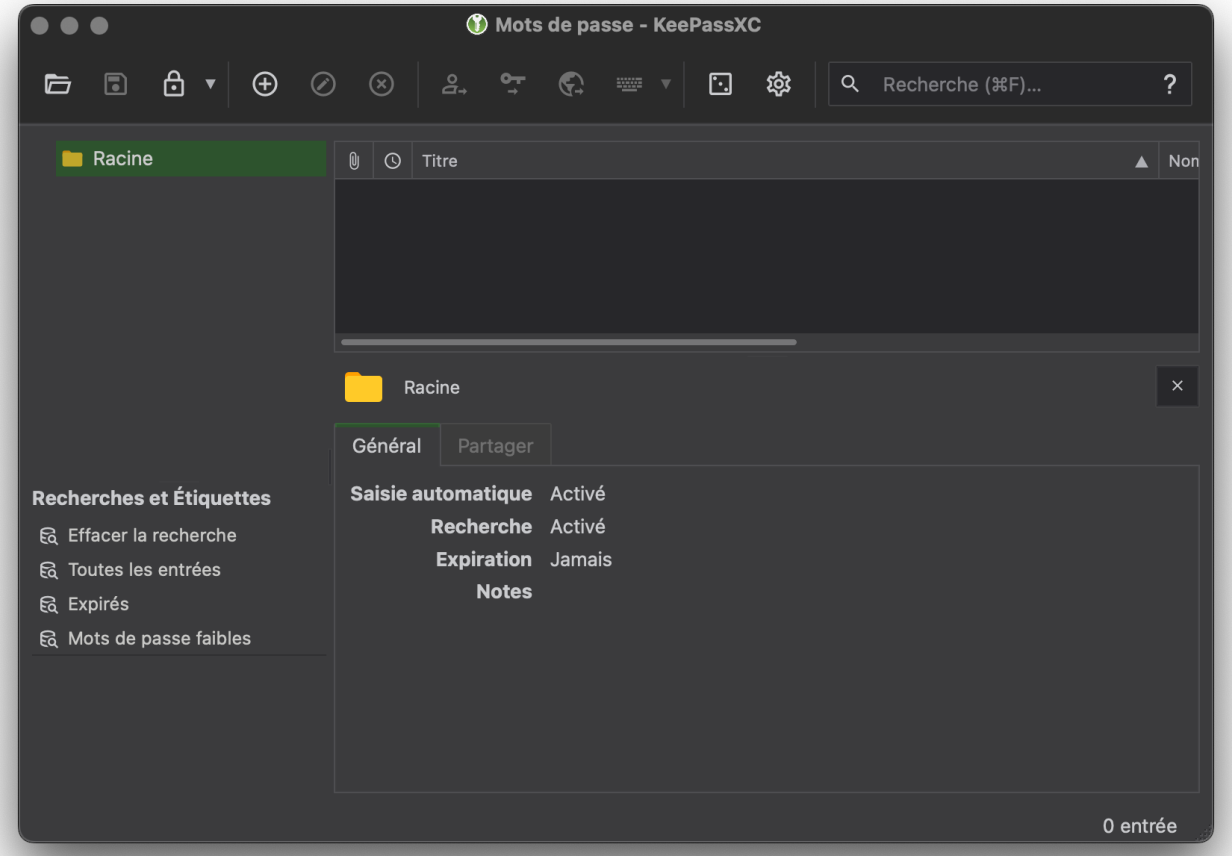
Se laisser guider en gardant les paramètres par défaut :



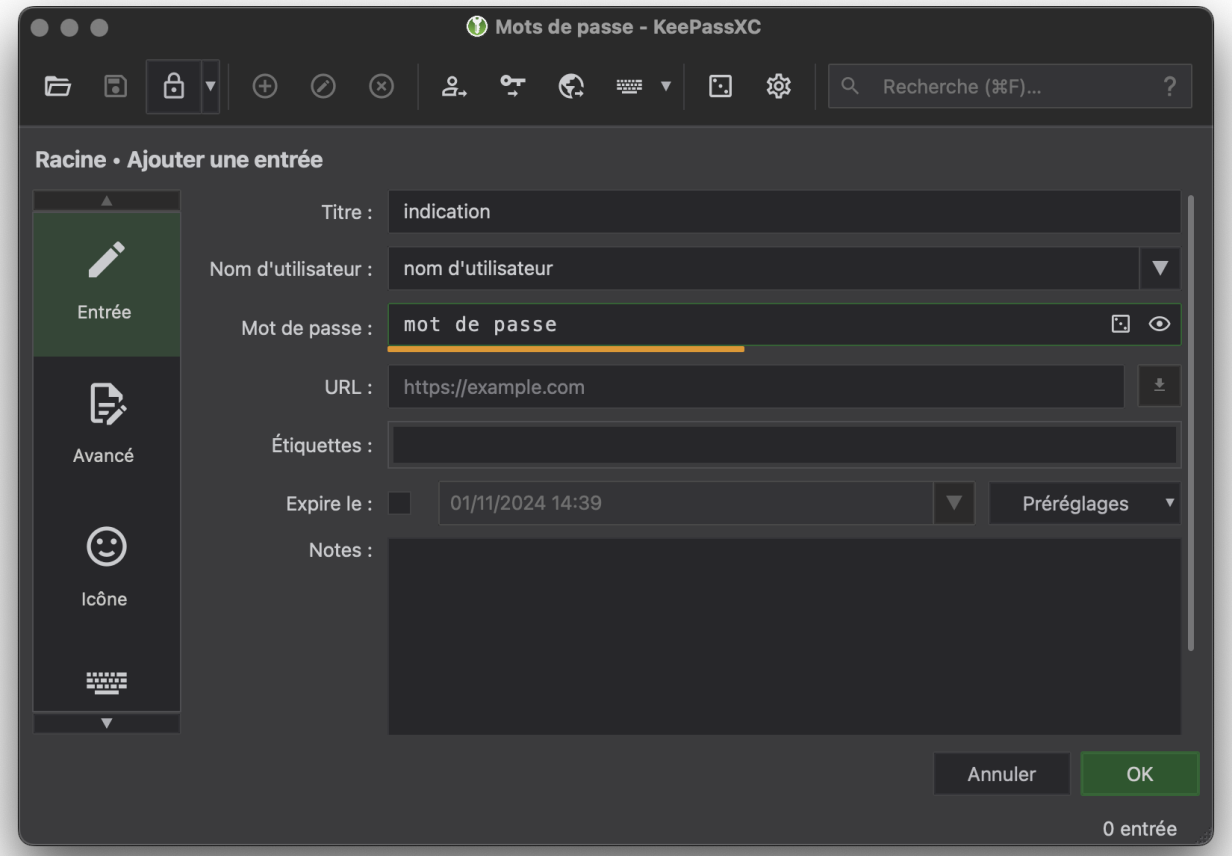
Choisir un mot de passe « robuste » et enregistrer le fichier.

Le mot de passe doit être d'autant plus robuste qu'il sera la principale défense si le fichier finissait aux mains d'un acteur malveillant. Comme ce sera le seul ou presque dont il faut se souvenir, entre 16 et 20 caractères comprenant lettres, chiffres, caractères spéciaux, etc. sont un minimum.

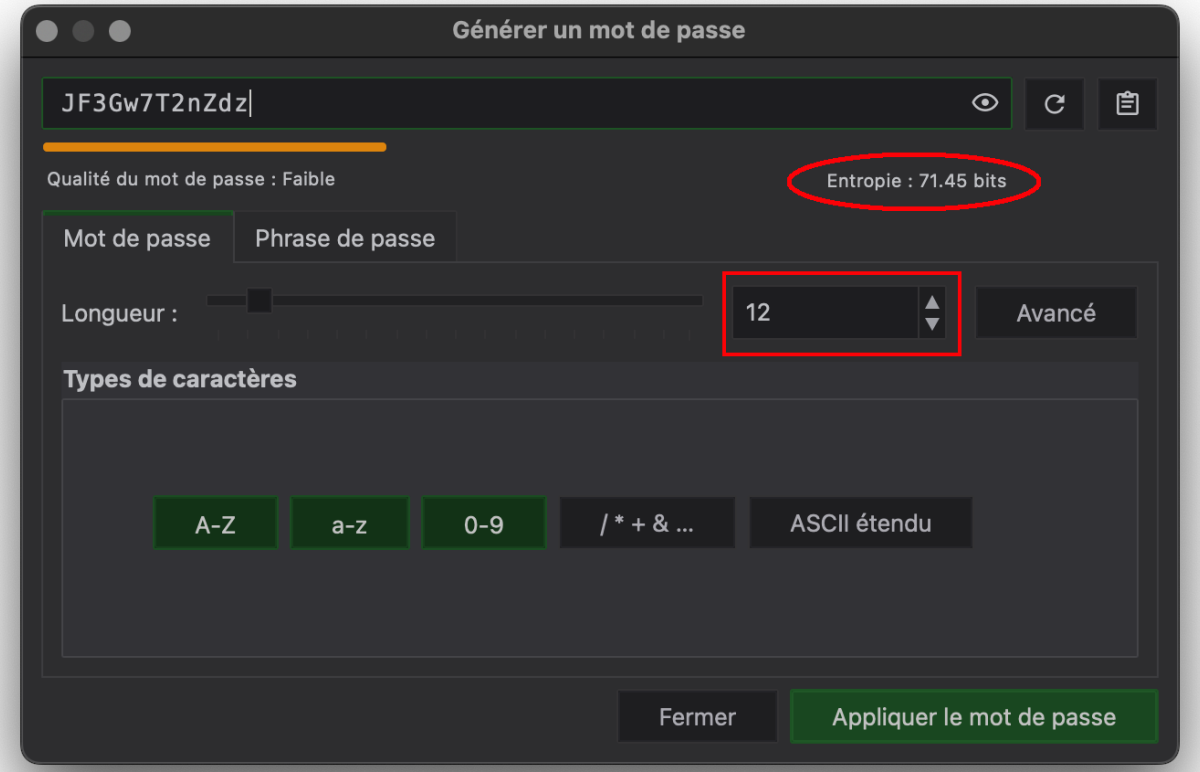
Gestion des secrets



Dans le menu Entrée, choisir Nouvelle entrée pour enregistrer un premier mot de passe :



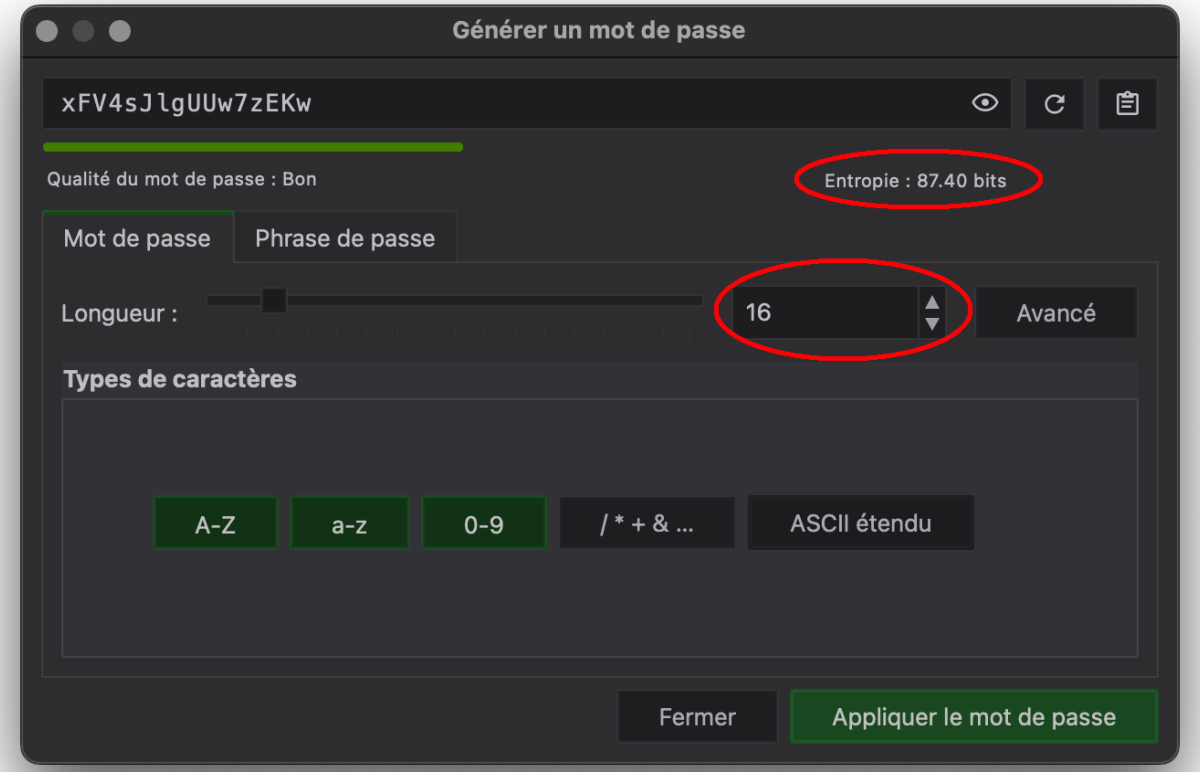
Ici, le mot de passe est de piètre qualité comme l'indique le niveau de couleur jaune ambre en dessous. Cliquer à droite au bout du cartouche du mot de passe sur l'icône :  et le générateur de mot de passe s'ouvre :



Un mot de passe de seulement 12 caractères ne donne pas une entropie d'au moins 80 bits, il est considéré comme faible.

En théorie de l'information, l'entropie de Shannon mesure la quantité d'information, le degré d'originalité, d'aléa, de désordre dans une information. Un mot de passe est considéré comme robuste au delà de 80 bits d'entropie.

Augmenter la longueur à 16 caractères et l'entropie devient bonne (le mot de passe est maintenant souligné en vert) :

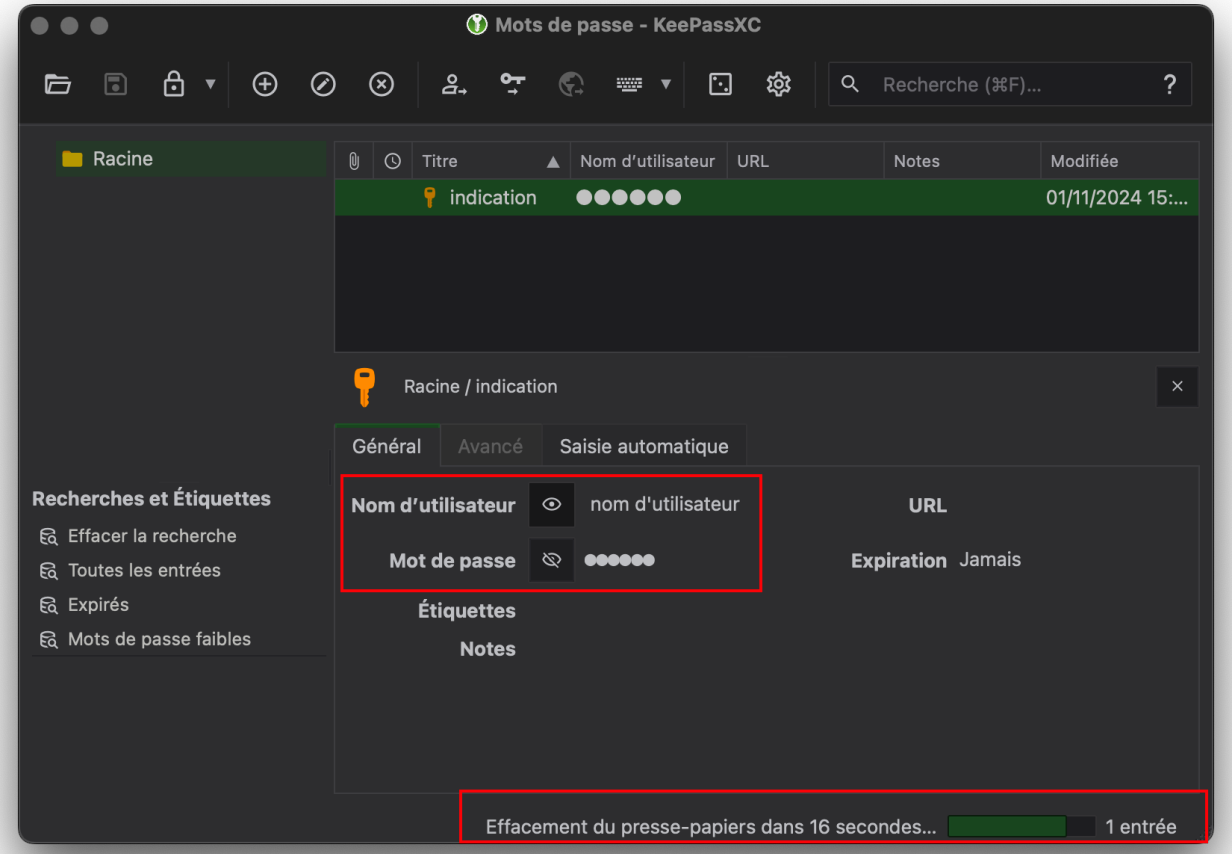


Enregistrer en cliquant sur OK en bas à droite.

Revenu à l'interface précédente, une entrée s'est ajoutée dans la fenêtre du haut.

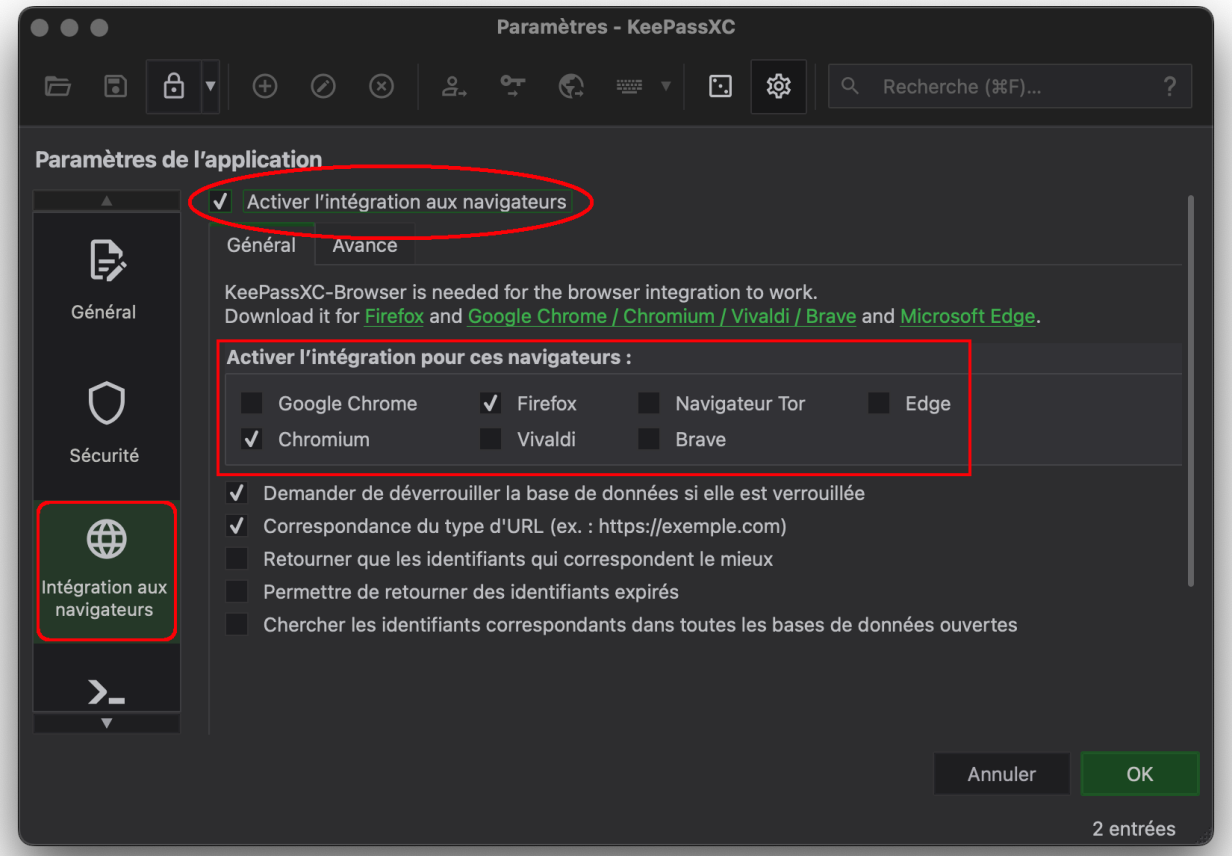
Pour copier le mot de passe, sélectionner cette entrée et appuyer sur le raccourci clavier ctrl-c ou ⌘-c. **En particulier, il n'y a pas besoin d'afficher le mot de passe pour le copier, ainsi il peut rester masqué.**

Le mot de passe est copié **pour une durée de 20 secondes** :



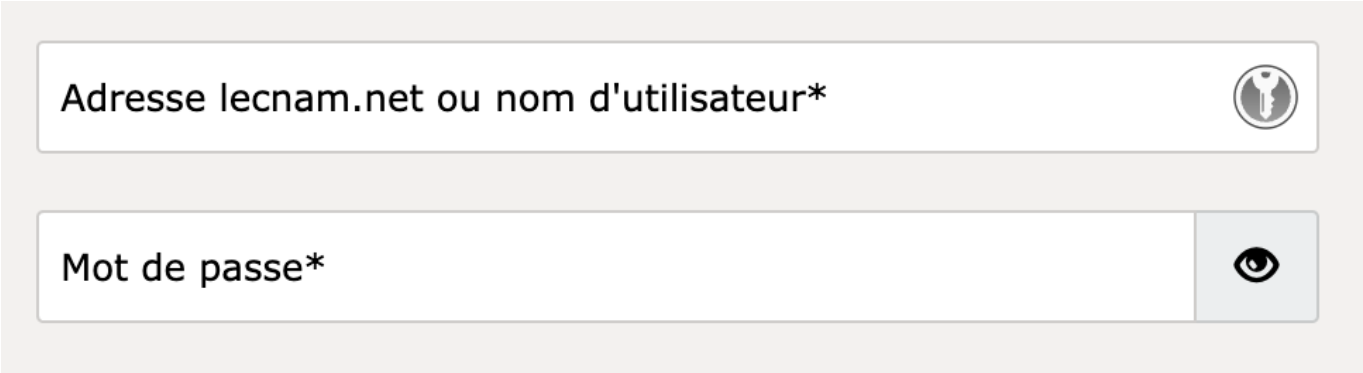
Intégration au navigateur

Disposant maintenant d'un gestionnaire de mots de passe robuste et bien protégé, on peut l'intégrer aux navigateurs. Pour cela, ouvrir les préférences :

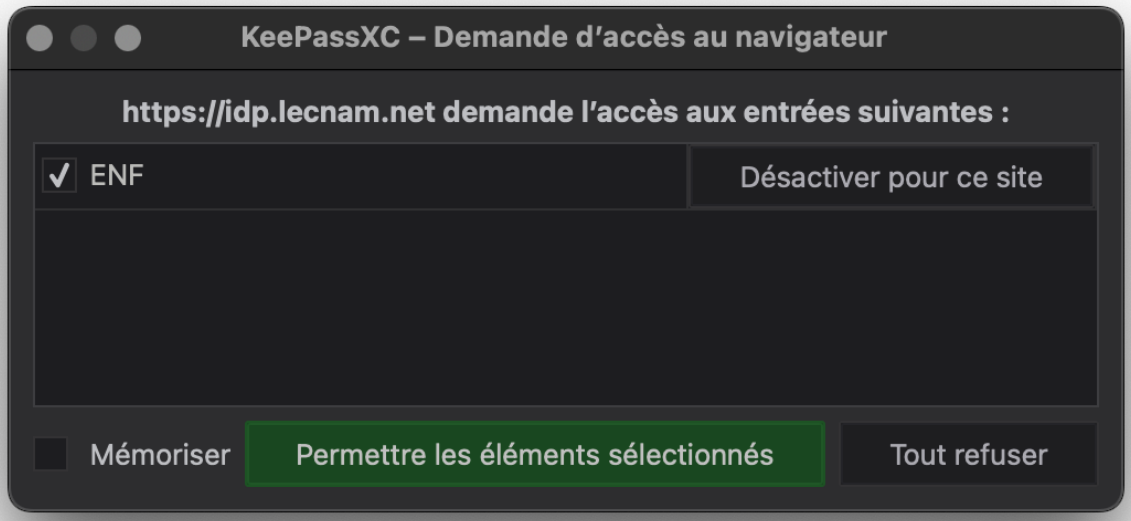


Activer l'intégration et choisir les navigateurs à autoriser. Ajouter aux navigateurs considérés les plugins correspondants comme indiqué.

On note le logo de KeePassXC à droite du cartouche.



Lorsque le navigateur cherche à accéder à un secret dans KeePassXC, celui-ci demande une validation.



Le logo de KeePassXC est vert lorsqu'une entrée est trouvée dans le gestionnaire :

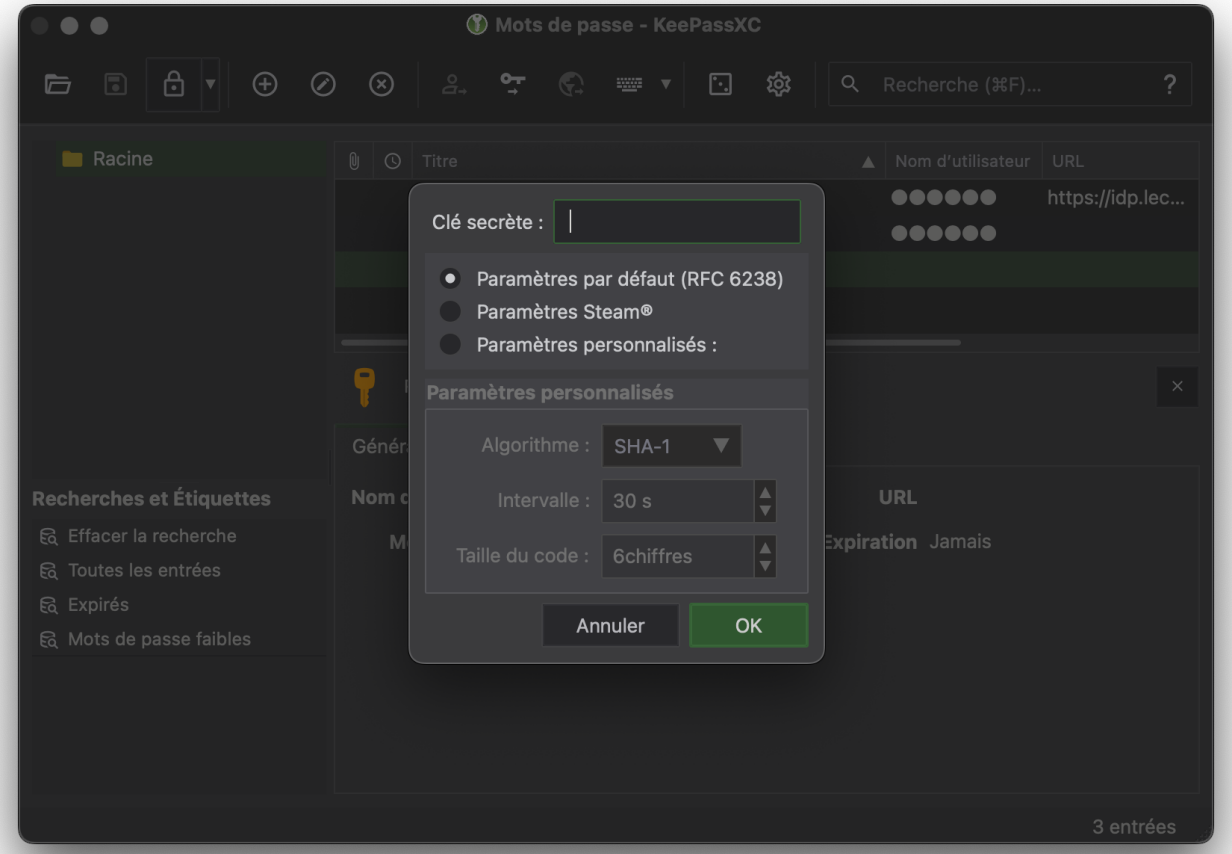
Gestion des mots de passe TOTP

Comme les mots de passe ne sont pas assez fiables, de plus en plus d'applications requièrent un second facteur d'authentification, souvent un mot de passe à usage unique (appelé TOTP pour *Time-based One Time Password*). KeePassXC est en mesure de gérer ces mots de passe à usage unique.

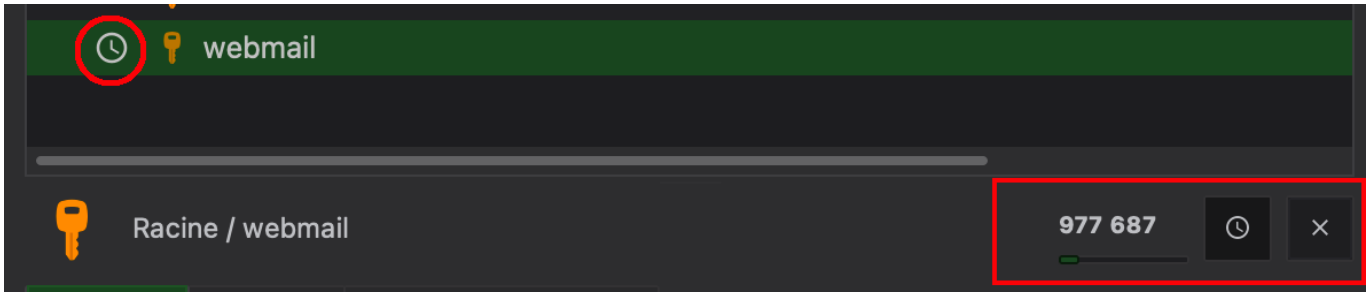
L'application et l'utilisateur doivent partager (à travers un canal fiable !) un secret. En conjuguant ce secret à l'heure courante[1)], on obtient un code sur 6 chiffres et valable 30 secondes[2)].

Exemple avec le webmail (cf. Configurer l'authentification à deux facteurs sur webmail.cnam.fr) :

Dans KeePassXC, ajouter une entrée `webmail` ; dans le menu Entrées, ouvrir TOTP puis Configurer TOTP et coller la clef dans le cartouche :

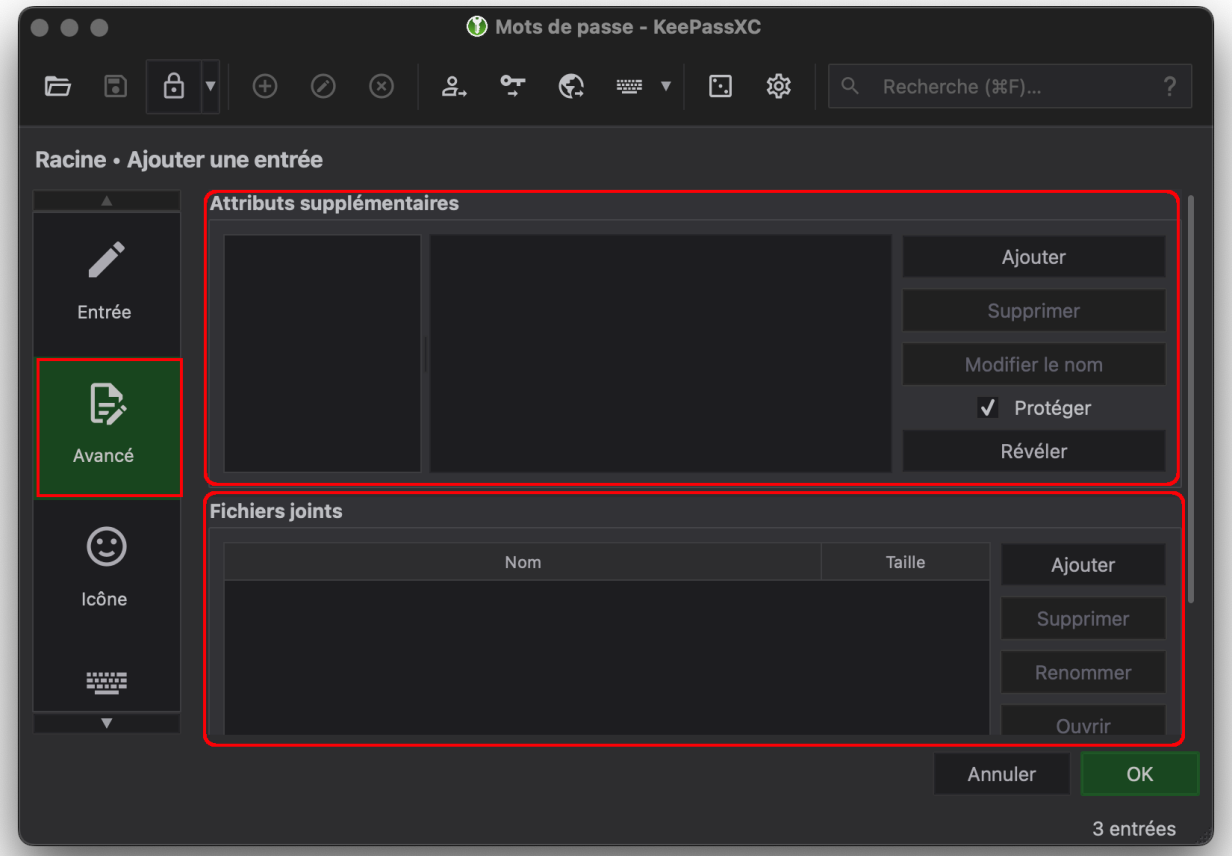


Ne pas toucher aux autres paramètres et enregistrer. Une horloge apparaît alors à gauche de l'entrée. Lorsque l'entrée est sélectionnée, le code et sa durée de vie apparaissent en bas à droite :



Autres secrets

KeePassXC permet de stocker des fichiers et toute sorte d'attributs, dont les codes de récupération fréquemment fournis par les applications requérant un second facteur :



Protection de la base de données

Stockage

Le fichier `.kdbx` contenant la base de données doit être protégé. Comme toute donnée importante, il doit être stocké :

- sur trois supports différents (disque, clef USB...),
- à trois endroits différents.

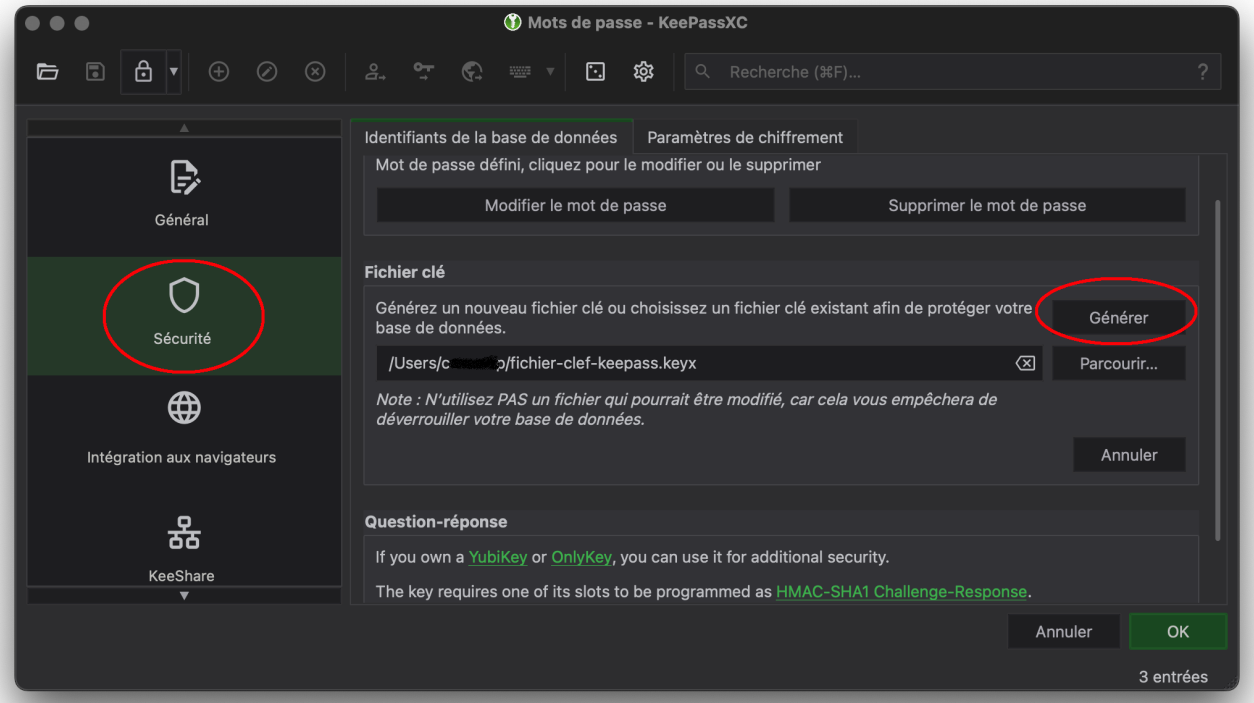
> Ne jamais stocker de base de données de mots de passe « dans le cloud », même protégé par un mot de passe robuste.

Durcissement

Pour renforcer la sécurité de la base de données, un second facteur d'authentification peut être ajouté :

- soit un fichier de clef
- soit jeton matériel (comme OnlyKey Yubikey)

Dans le menu Base de données » Paramètres de la base de données » Sécurité :



Attention : le fichier de clef et la base de données ne devraient jamais être sur le même support physique ! Par contre, ils doivent tous deux être sauvegardés.

1)

Attention à bien garder les systèmes à l'heure, utiliser NTP.

2)

Variante possible : 8 chiffres valable 60 secondes.