Utilisation

Création d'une nouvelle base de données

1. Ouvrez KeePassXC.
2. Cliquez sur "Fichier" > "Nouvelle base de données".
3. Suivez les instructions pour définir un mot de passe maître.
4. Enregistrez la base de données sur votre disque.

Ajout de mots de passe

1. Cliquez sur "Entrée" > "Ajouter une entrée".
2. Remplissez les champs : Titre, Nom d'utilisateur, Mot de passe, URL, etc.
3. Cliquez sur "OK" pour enregistrer l'entrée.

Générateur de mots de passe

1. Dans la fenêtre d'ajout d'une entrée, cliquez sur l'icône du générateur de mots de passe.
2. Personnalisez les options (longueur, caractères, etc.).
3. Cliquez sur "Insérer" pour ajouter le mot de passe généré à l'entrée.

Sauvegarde et synchronisation

- Pour sauvegarder votre base de données, cliquez sur "Fichier" > "Enregistrer sous" et choisissez un emplacement.
- Vous pouvez synchroniser votre base de données via des services de cloud comme Dropbox ou Google Drive en enregistrant la base de données dans le dossier synchronisé.

Autofill et intégration navigateur

1. Installez l'extension KeePassXC-Browser pour votre navigateur (Chrome, Firefox, etc.).
2. Dans KeePassXC, allez dans "Outils" > "Extensions du navigateur" et activez l'intégration.
3. Suivez les instructions pour connecter l'extension à KeePassXC.

Sécurité

- Utilisez un mot de passe maître fort.
- Activez l'authentification à deux facteurs si disponible.
- Sauvegardez régulièrement votre base de données.

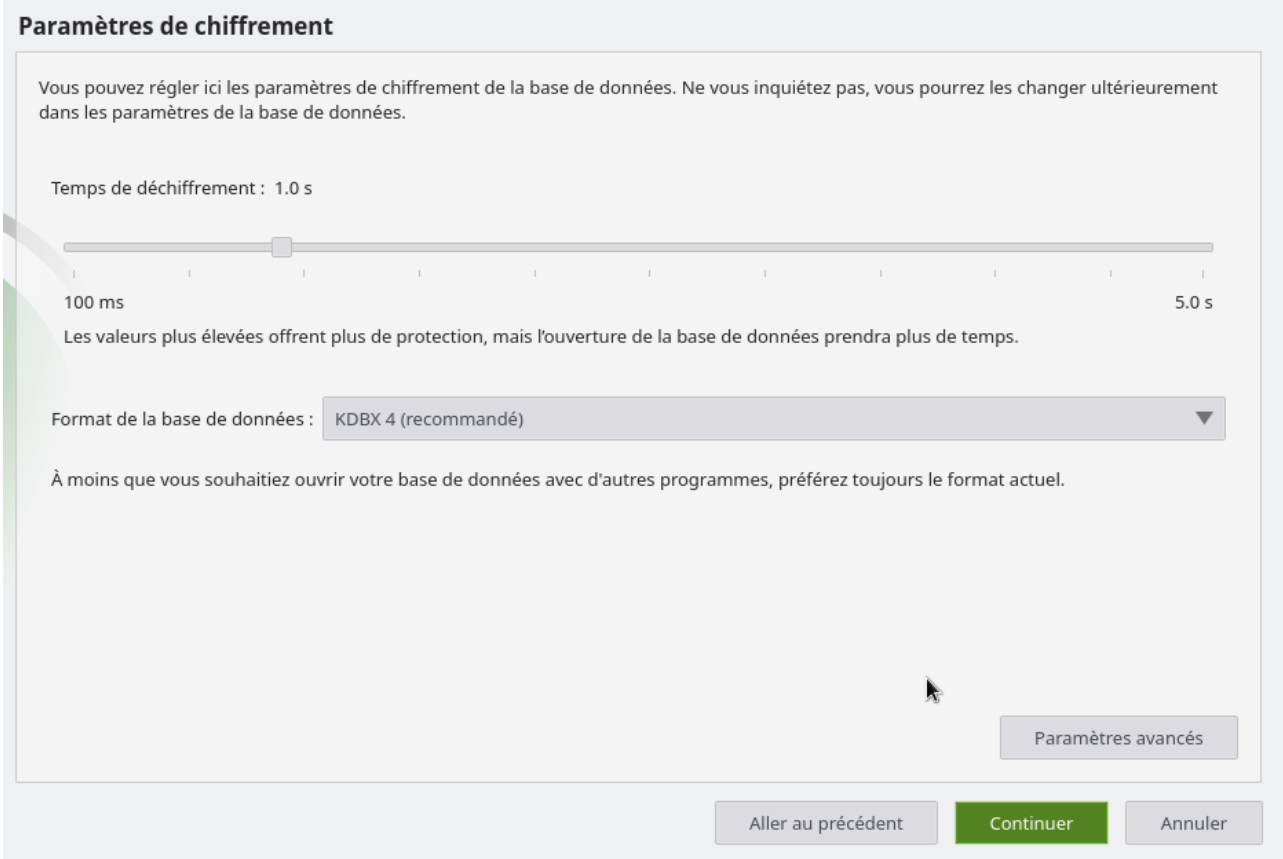
Conclusion

KeePassXC est un outil puissant pour gérer vos mots de passe en toute sécurité. N'hésitez pas à consulter la documentation officielle pour plus de détails.

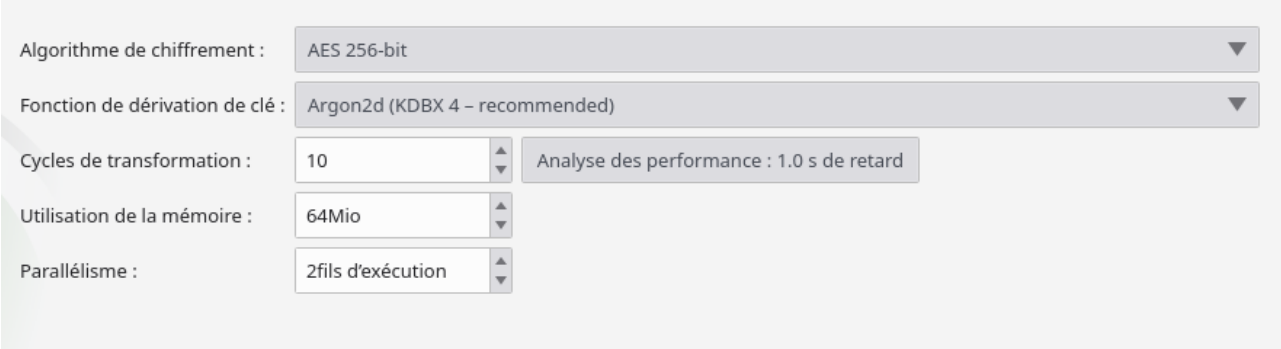
Spécificités de KeePassXC

KeePassXC est un gestionnaire de mots de passe qui offre plusieurs fonctionnalités de sécurité avancées :

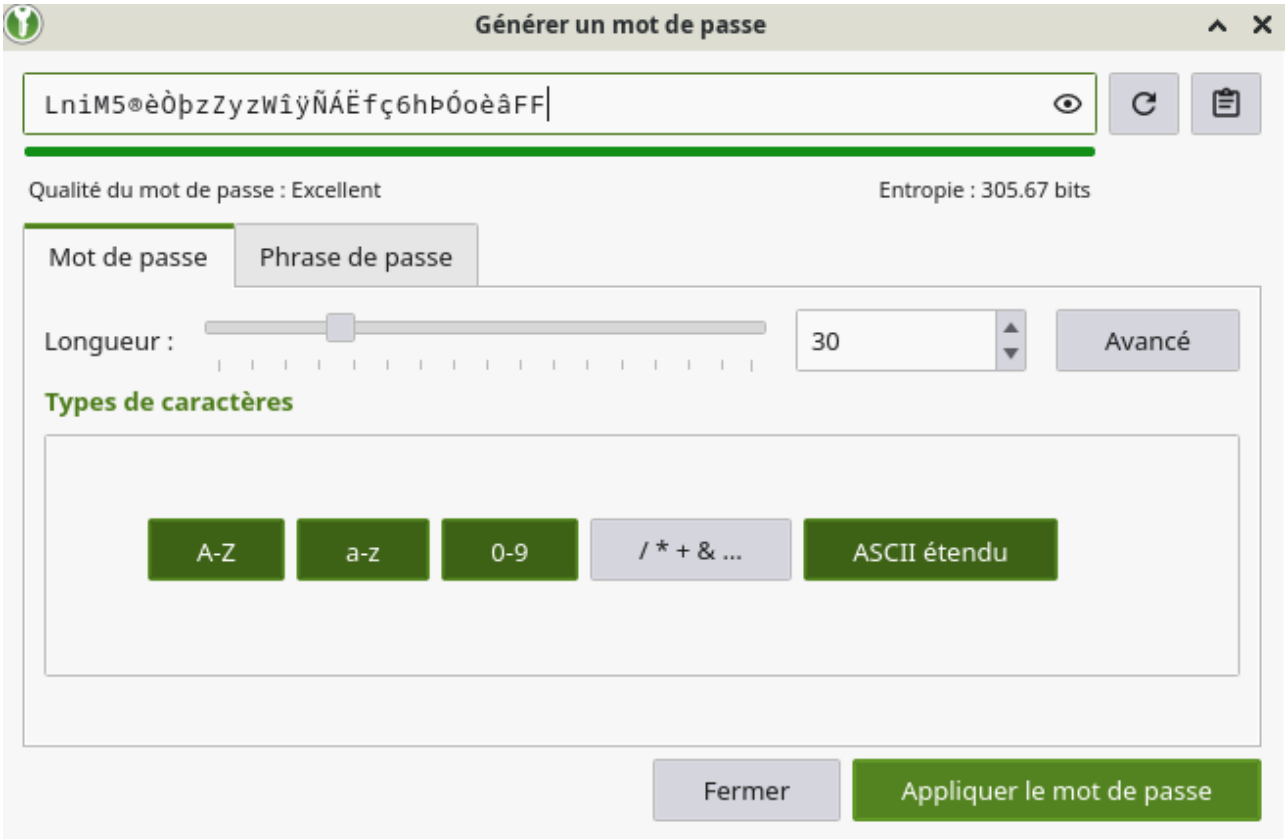
- **Chiffrement des données** : KeePassXC utilise le chiffrement AES (Advanced Encryption Standard) avec une clé de 256 bits, garantissant un niveau élevé de sécurité pour vos mots de passe.
- **Temps de chiffrement** : Le chiffrement AES est considéré comme très rapide, permettant un chiffrement et déchiffrement presque instantanés, en fonction de la taille de la base de données et des ressources système.



- **Algorithmes de hachage** : Pour protéger le mot de passe maître, KeePassXC utilise des algorithmes de hachage comme Argon2, qui sont résistants aux attaques par force brute et offrent une protection supplémentaire.



- **Format de base de données** : KeePassXC utilise le format de base de données KDBX, qui est compatible avec d'autres clients KeePass, facilitant l'importation et l'exportation de données.
- **Générateur de mots de passe intégré** : KeePassXC dispose d'un générateur de mots de passe personnalisable, permettant de créer des mots de passe forts et uniques pour chaque entrée, in peut choisir ; sa longeur (128 caractére max) / Types de caractére / si c'est un mdp ou une phrase.



- **Autofill sécurisé** : L'intégration avec les navigateurs permet de remplir automatiquement les formulaires de connexion de manière sécurisée.

- **Multiplateforme** : KeePassXC est disponible sur plusieurs systèmes d'exploitation, y compris Windows, macOS et Linux, avec une interface utilisateur cohérente.
- **Open Source** : En tant que projet open-source, KeePassXC permet aux utilisateurs de vérifier le code source et de contribuer au développement.

Ces spécificités font de KeePassXC un choix solide pour la gestion de mots de passe en toute sécurité.