Les guides utilisateur 2020

KEEPASS, GESTIONNAIRE DE MOTS DE PASSE

Révision v1.1.1 du 02/10/2020

Table des matières

Index des figures et objets

GÉNÉRALITÉS[1]

Chiffrez vos mots de passe sur Windows et Mac

KeePass : retenez un seul mot de passe et chiffrez tous les autres

KeePass est sans conteste le **gestionnaire de mot de passe** le plus apprécié du moment et cela grâce à une myriade d'options qui apportent une fiabilité en sécurité hors du commun.

Sous licence GPL v2, KeePassKeePass est gratuit et le restera. Son code source est disponible pour tous les codeurs et développeurs du monde entier ce qui assure à KeePass des mises à jours et évolutions majeures au fil de ses versions.

Keepass 2.43 | Windows Keepass 2.43 | Portable MacPass (Fork) 0.7.9 | MacOS Keepass 2.xx | Linux

Lien vers les logiciels officiels et non officiels

Un gestionnaire de mot de passe simple et gratuit

Son principe est très simple : **KeePass sauvegarde tous vos mots de passe** dans une base de données qui lui est propre et qui est en réalité un fichier chiffré (« crypté »).

Cette base de données n'est alors accessible que grâce à votre mot de passe principal, le seul que vous avez à retenir et que vous aurez préalablement judicieusement choisi.

La sécurité de l'accès à cette base de données peut être alors encore renforcée très simplement en joignant « une clé » (à l'aide d'un fichier .key)

Un gestionnaire de mot de passe fiable et sécurisé

KeePass est disponible avec deux versions différentes de sécurisation pour choisir le degré de sécurité que vous souhaitez.

Vous aurez ainsi le choix entre **deux algorithmes de chiffrement** pour :

1 Extraits du site https://keepass.fr/

- une sécurisation par chiffrement **AES** (clé de 256 bits)
- une sécurisation par chiffrement **TwoFish** (clé de 256 bits + blocs de 128 bits)

Ces 2 méthodes de chiffrement sont actuellement les meilleurs du marché pour un **usage tout public et professionnel**.

Cependant, vous le savez, les failles de sécurité proviennent hélas le plus souvent de vos systèmes d'exploitations et KeePass est heureusement **multiplateforme**.

Un gestionnaire de mot de passe pour MacOS, Linux, FreeBSD et Windows

Qui dit système d'exploitation avec un monopole grand public dit aussi plus d'attaques pour exploiter les failles du dit système d'exploitation.

Sans pointer du doigt l'OS de la firme de Richmond, KeePass a été pensé pour **la sécurisation des mots de passe sur tous vos ordinateurs** et cela quel que soit la plateforme que vous utilisez.

Vous pouvez donc travailler en journée sur un poste sous **Windows** au bureau pour continuer à utiliser KeePass sur votre ordinateur personnel sous MacOS ou sous Linux à la maison par exemple.

Sous **Windows**, l'installation de KeePass est native. **Sous MacOS**, **Linux** et **FreeBSD** , l'installation native peut s'opérer grâce à la plateforme **Mono** (une plateforme de développement Microsoft .NET basée sur la **CLI** que nous vous proposons en téléchargement).

Pour les utilisateurs sous Windows, une seconde version de KeePass existe pour permettre de lier la base de données à un utilisateur Windows ainsi que de permettre l'incorporation de pièces jointes dans les entrées (pour les versions 2.x).

Un gestionnaire de mot de passe certifié ANSSI

C'est dans le cadre de ses missions pour la **défense et la sécurité nationale** que **l'ANSSI** (l'Agence Nationale de la Sécurité des Systèmes d'Information) teste les logiciels utilisés dans les administrations publiques françaises.

Depuis 2012, le Socle Interministériel de Logiciels Libres définit une liste de logiciels libres qui doivent être utilisés dans nos administrations, logiciels libres que l'ANSSI teste sur des aspects de sécurité.

C'est ainsi **depuis 2010 que l'ANSSI certifie KeePass** dans sa version 2.10. Son déploiement est national depuis 2012 dans toutes nos administrations publiques.

Un gestionnaire de mot de passe recommandé pour sa sécurité

En plus de l'ANSSI, l'**Office Fédéral de la Sécurité des Technologie de l'Information en Allemagne** rédigea une note à destination des PME en 2018 afin de leur recommander l'utilisation de KeePass.

La Commission Européenne ordonna un audit de sécurité à l'occasion du tout premier **EU-FOSSA** (le « Free and Open Source Software Audit » européen) de 2016 puis récidiva en 2019 dans le cadre du troisième « **bug bounty** » de KeePass qui récompense les généreux testeurs en sécurité qui rapportent les bugs et failles de sécurité aux développeurs.

Bref, avec KeePass vous atteignez des sommets en matière de **sécurité** et ce n'est pas nous qui le disons !

Gérez vos mots de passe aussi sur mobile

La base de données contenant vos mots de passe chiffrés (ou chiffrés si l'on veut utiliser le terme correct) peut être **synchronisée à distance**.

Avec **l'application KeePass** installée sur votre smartphone vous pourrez être synchronisé depuis un site distant en **FTP** sur votre **BlackBerry, Pocket PC, iPhone, Windows Phone 7** et bien évidemment sur **Android**.

Il existe des solutions de synchronisation plus simple grâce au **cloud** sur d'autres logiciels de gestion de mots de passe, cependant le degré de sécurisation du transport des données est alors plus problématique et bon nombre d'utilisateurs se méfient de solutions cloud comme **Dashlane** ou **Lastpass**.

KeePass est donc une excellente alternative aux **gestionnaires de mots de passe par cloud**.

Une interface en glisser/déposer très facile d'utilisation

Pour les entrées de votre fichier (votre base de données), vous aurez la possibilité de simplement glisser et déposer les informations nécessaires pour entrer le nom d'utilisateur puis ensuite le mot de passe associé. Toutes les entrées de la base de données peuvent ainsi être glissées et déposées.

Encore plus simple avec la saisie automatique de mot de passe

Si vous désirez **gagner encore plus de temps**, vous pouvez dans KeePass renseigner l'identifiant et le mot de passe à utiliser pour une application ou pour un site (grâce à son URL) afin que celui-ci les mettent **automatiquement** à chaque lancement de l'application ou du site internet.

C'est au sein de la base de données avec vos de mots de passe qu'il vous suffira d'ouvrir le menu contextuel par le clic droit sur une entrée pour sélectionner « **exécuter la saisie automatique** ».

Terriblement efficace et très simple pour pré-remplir les informations de connexion pour un site ou un logiciel demandant une authentification.

Comme toujours, la **saisie automatique** est bien évidemment **chiffrée et donc sécurisée** au sein même de KeePass, donc il n'y a aucune inquiétude quant à l'utilisation de cette option.

Vous changez souvent de mot de passe ?

Il faudrait avoir une mémoire phénoménale pour retenir le nombre de mots de passe importants qui régissent notre vie d'utilisateurs.

Il est évidemment très déconseillé d'utiliser toujours le même mot de passe et le même nom d'utilisateur, mais heureusement **KeePass est là pour tout gérer à votre place**.

Pour ce qui est des sites ou logiciels où vous changez régulièrement de mots de passe, KeePass est capable de garder une trace de ces anciens mots de passe grâce à un **historique des entrées de la base de données**.

COMMENTE ÇA MARCHE

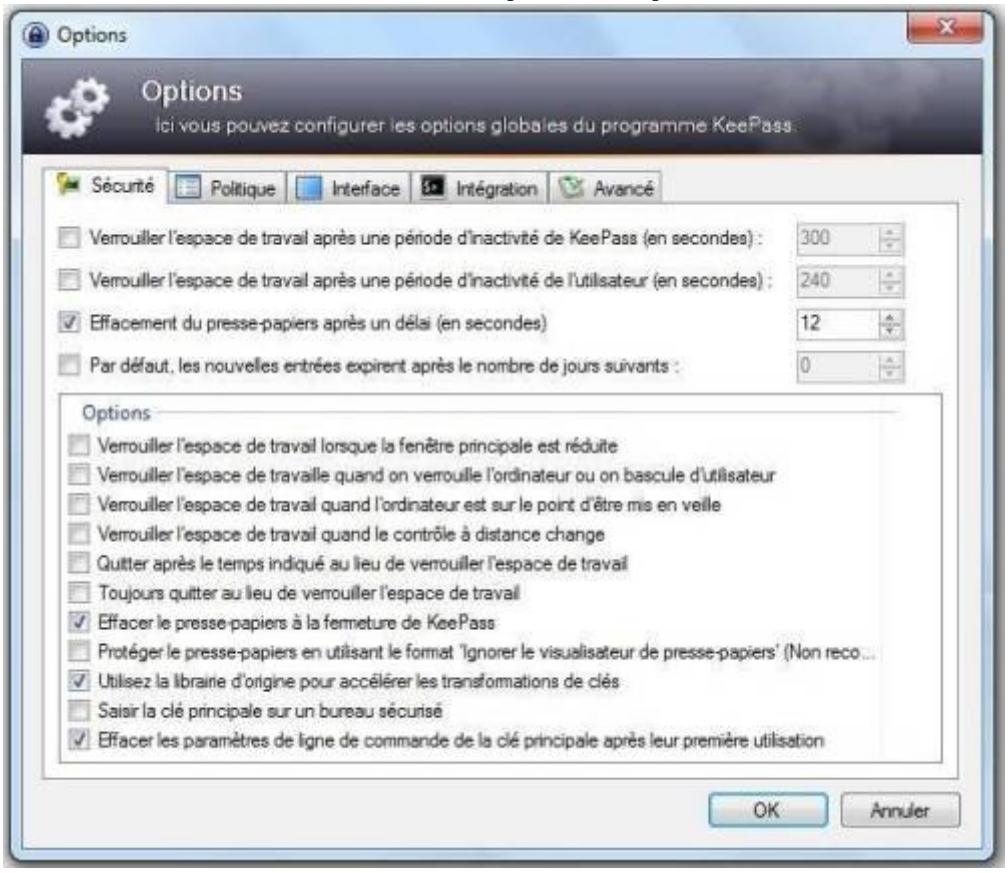
Vos mots de passe sont enregistrés dans KeePass dans sa base de données qui est un fichier chiffré au format **.kdb** (pour la v1) et **.kdbx** (pour la v2).

A chaque mot de passe une entrée dans cette base de données. Chaque entrée possède alors plusieurs champs dont le nom d'utilisateur, le mot de passe, l'adresse URL en question et des pièces jointes (à partir de la version 2) et bien évidemment le titre de cette entrée pour se repérer facilement dans la base de données.

Par souci de sécurité, KeePass garde en mémoire pour chaque entrée d'autres informations comme la date et l'heure de sa création, de sa dernière modification et de son dernier accès depuis votre base de données contenant vos mots de passe chiffrés.

Cela permet également à KeePass de vous **prévenir quand un mot de passe nécessite un changement** ce qui est très pratique et surtout automatique.

A. Fenêtre Options de Keepass



La meilleure option de KeePass selon nous

Une des failles majeures que l'on retrouve dans les gestionnaires de mots de passe est la gestion du presse papier lorsqu'un mot de passe est copié/collé.

KeePass permet alors de chiffrer les mots de passe en mémoire vive de votre ordinateur (et au passage de remplacer les caractères visibles par des astérisques).

Mais cela n'étant hélas pas suffisant pour garantir une sécurité optimale, **KeePass ne conserve en mémoire dans le presse papier que 12 secondes maximum un mot de passe copié/collé**.

Cette conservation temporaire dans le presse papier est une parfaite solution de contournement pour un problème de sécurité très épineux pour les logiciels de gestion de mots de passe.

Des versions légères et stables de KeePass : la version portable

KeePass est proposé en deux versions qui sont elles-mêmes disponibles en version classique et portable.

Une version portable de KeePass permet de jouir de son gestionnaire de mot de passe favori sur sa clef USB ou sur un tout autre support de stockage amovible comme une carte SD.

Il n'y aura alors plus besoin pour vous d'installer KeePass sur l'ordinateur que vous utilisez puisque c'est depuis votre clef USB que KeePass opèrera.

Toutefois, KeePass 1.x vous demandera le support de GDI+ si vous êtes sur un système plus ancien que Windows XP.

Pour KeePass 2.0, il vous faudra installer Microsoft .NET Framework 2.0.

Passer d'une v1 à une v2… ou depuis n'importe quel autre logiciel !

Grâce à une fonction d'importation très simple par fichier TXT ou CSV, vous pouvez passer de KeePass version 1 à KeePass version 2 sans aucun souci tout comme importer ces entrées **en provenance de n'importe quel autre logiciel de gestion de mots de passe**.

KeePass est donc « compatible » avec tous les autres logiciels pour l'importation tant que ceux-ci proposent une importation et une exportation au format **TXT** ou **CSV**.

Il existe également des plugins supplémentaires pour KeePass qui vous aideront grandement à importer les entrées des autres gestionnaires de mot de passe.

Pour l'exportation de vos mots de passe gérés par KeePass sur d'autres supports, nous avons prévu les formats **TXT, HTML, CSV et XML** pour une meilleure interopérabilité.

Vous parlez l'estonien, le croate ou encore le galicien ?

KeePass est disponible nativement en anglais mais vous pouvez ensuite ajouter des **traductions officielles** (grâce au travail chevronné de généreux bénévoles) dans **plus de 50 langues** et dialectes.

Ces fichiers de traduction sont disponibles au format **.lng** et **.lngx** selon votre version de KeePass.

Nos conseils pour sécuriser votre environnement

Nous vous recommandons très chaudement de vérifier s'il n'y a aucun **keylogger** installé sur votre système et qui pourrait tout simplement enregistrer tous vos clics, vos frappes clavier et le contenu du presse papier pouvant contenir justement votre mot de passe KeePass.

Ces logiciels malveillants aussi appelés « enregistreurs de frappe » sont détectables et supprimables depuis des logiciels de nettoyage tel que **Adware** ou **Spybot Search and Destroy**. Ceci est plus que vivement conseillé lorsque l'on sait que Windows 10 propose depuis sa v1009 un partage de l'historique du presse papier sur le cloud.

Mais la première faille de sécurité qui existe pour vos systèmes c'est vous ! Sachez qu'il existe des logiciels spécialisés dans le **cassage du chiffrement** de KeePass pour pouvoir découvrir vos mots de passe.

C'est ce que proposent **KeePass2john, KeePass Self-Bruteforcer et KeeCracker** et l'on remarque que des mots de passe complexes ne peuvent être « décryptés » par ces logiciels aux objectifs plus que douteux.

Des mots de passe « forts » et complexes vous permettent donc d'être à l'abri de ce type de tentatives de récupération malveillante de vos données.

Les plugins de KeePass

Puisque KeePass est sous **licence GPL** et est donc un **logiciel libre**, c'est toute une communauté qui fait vivre ce projet avec bien évidemment des **extensions (plugins)** très utiles qui approfondissent bien plus encore les possibilités qu'offre ce gestionnaire de mots de passe.

Nous pouvons vous donner comme exemple de plugins pour KeePass les utilisations suivantes :

- **l'enregistrement d'une sauvegarde de votre base de données** à chaque fois que celle-ci est mise à jour par de nouvelles entrées.
- l'utilisation de KeePass sur les **trois principaux navigateurs** que le grand public utilise avec **Chrome, Firefox et Internet Explorer**.
- l'utilisation de KeePass sur son **smartphone, sa tablette et ses ordinateurs** en les synchronisant sur un **cloud** contenant votre base de données.
- **l'importation et l'exportation** encore plus facile de vos données vers d'autres logiciels qui sont des gestionnaires de mot de passe concurrents à KeePass.
- l'utilisation d'une **protection par certificat** plutôt que par mot de passe permettant ainsi d'ajouter une sécurisation supplémentaire.
- la mise en ligne de la base de données sur un **serveur multi-utilisateurs** qui utilisera les protocoles sécurisés :
  SCP (Secure CoPy)
  SFTP (SSH File Transfer Protocol)
  FTPS (FTP SSL/TLS)

Nous devons toutefois vous avertir sur les risques potentiels liés à l'utilisation de ces plugins pour KeePass : ceux-ci ne peuvent être garantis par KeePass car ceux-ci ne sont pas compris dans les tests et audits de sécurité de notre logiciel.

De même qu'il vous faut vous assurer de la source de l'auteur du plugin et utiliser une vérification avec le hash MD5 pour s'assurer que le contenu du plugin n'a pas été altéré ou encore que ce plugin n'est tout simplement pas le fait d'une personne malveillante.

Il faut comprendre qu'un plugin pour KeePass aura accès à votre base de données et ses entrées, cela veut donc dire à tous vos mots de passe en clair.

Des forks et portages officieux de KeePass également disponibles

Un fork est un nouveau logiciel créé à partir du code source d'un autre logiciel.

KeePass étant open source, son code est donc libre et c'est ainsi que sont apparus des forks très sympathiques et surtout des portages forts intéressants :

- **KeePassXC** : il s'agit d'un fork basé sur l'ancien projet **KeePAsX** stoppé en 2016 et repris toujours sous licence GPL pour **Windows, MacOS et Linux**.
- **WinPass** : il s'agit d'un portage absolument génial les appareils tournant sous **Windows Mobile 8/10.**
- **KeePassB** : il s'agit d'un portage pour la plateforme de **BlackBerry**.
- **KeePass2Android et KeePassDroid** : encore des portages mais cette fois-ci pour la plateforme Android comme leurs noms l'indiquent.
- **MacPass** : c'est le portage de référence pour la plateforme **MacOS**.
- **KeeWeb** : il s'agit d'une application web qui permet une synchronisation de votre base de données via **Dropbox** pour un accès depuis n'importe quel appareil.

MISE EN ŒUVRE

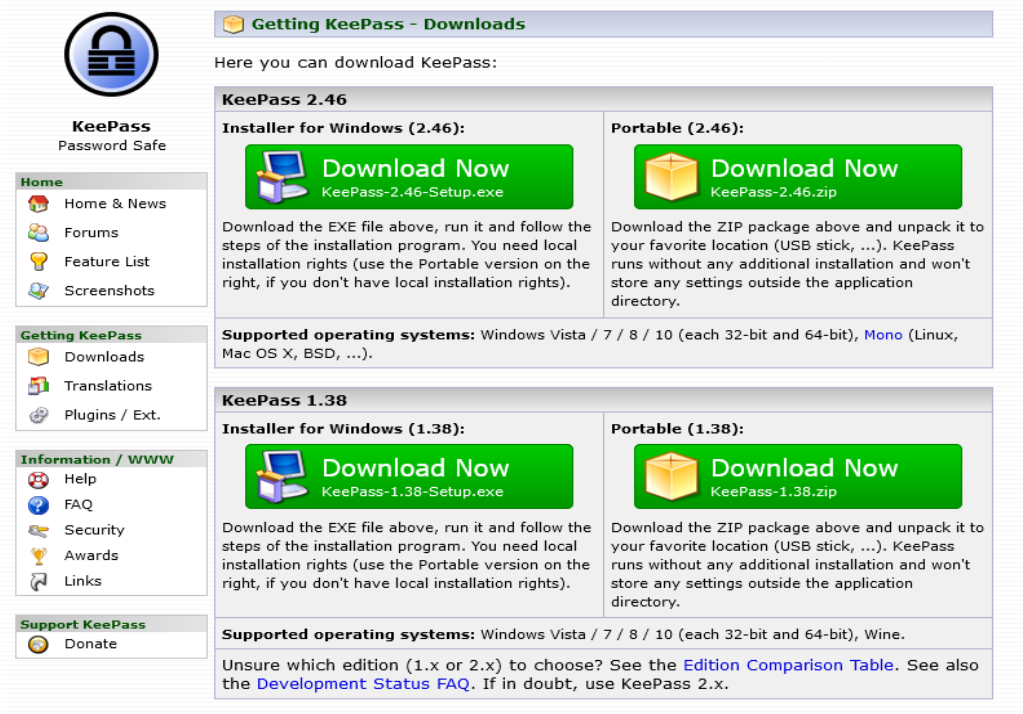
Vous pourrez trouver les dernières versions de KeePass sur notre site. Il s'agit **des versions officielles**.

Nous prenons ici l'exemple d'une utilisation sur PC pour la plateforme Windows.

Nous vous recommandons d'utiliser les versions 2.x qui sont bien plus complètes en options et fonctionnalités. Vous avez ensuite le choix entre une version classique et une version « portable » (légère pour clef USB).

Installation de KeePass et de la traduction FR

B. Site de Keepass (téléchargement fichier installation)



C. Site de Keepass (téléchargement fichier traduction)

KeePass
Password Safe

Home
- Home & News
- Forums
- Feature List
- Screenshots

Getting KeePass
- Downloads
- Translations
- Plugins / Ext.

Information / WWW
- Help
- FAQ
- Security
- Awards
- Links

Support KeePass
- Donate

Translations

Installation:

1. Left-click the download link of the language of your choice (for KeePass 1.x click the '[1.x+]' link; for KeePass 2.x click the '[2.x+]' link). Unpack the downloaded ZIP file (to the current directory).
2. In KeePass, click 'View' → 'Change Language' → button 'Open Folder'; KeePass now opens a folder called 'Languages'. Move the unpacked file(s) into the 'Languages' folder.
3. Switch to KeePass, click 'View' → 'Change Language', and select your language. Restart KeePass.

If you are using an old version, please have a look in the 1.x / 2.x translation archives.

Language	Author	Downloads	
Arabic	M. Abdulaziz (2.x), S. Al-Farhood and A. Gharbeia (1.x)	[1.11+]	[2.39+]
Belarusian	Andrew Gavrushenko	[1.18+]	[2.x] N/A
Bulgarian	I. Georgiev (2.x), DonAngel (1.x)	[1.10+]	[2.46+]
Burmese	T. Hlaing (2.x), R. Kyaw (1.x)	[1.23+]	[2.19+]
Catalan	Albert Morera	[1.38+]	[2.46+]
Chinese, Simp.	Leo Dou	[1.38+]	[2.45+]
Chinese, Trad.	Kao Shiang-Yuan	[1.38+]	[2.46+]
Croatian	I. Bunjevac (2.x), D. Vuković (1.x)	[1.14+]	[2.29+]
Czech	M. Pavelka and M. Klíma and R. Tlapák (2.x), T. Glabasňa and P. Chramosta (1.x)	[1.37+]	[2.44+]
Danish	Christian Staal	[1.38+]	[2.45+]
Dutch	Hilbrand Edskes	[1.38+]	[2.46+]
English	Dominik Reichl	Built-in, no download	
Estonian	A. Kuhlberg (2.x), A. Viiand (1.x)	[1.14+]	[2.38+]
Finnish	K. Eveli (2.x), A. Tähtinen (1.x)	[1.11+]	[2.46+]
French	Ronan Plantec	[1.38+]	[2.46+]
Galician	Jesús Amieiro	[1.10+]	[2.x] N/A

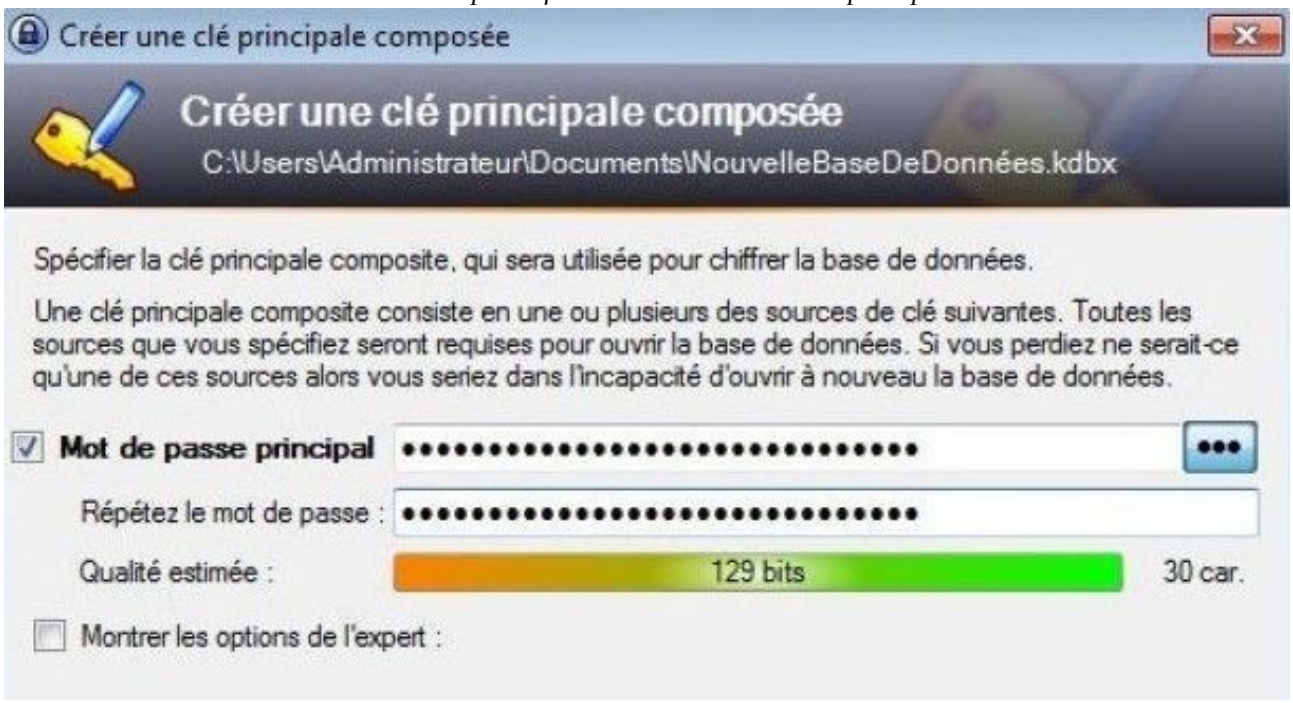
Il n'y a absolument aucune difficulté à l'installation sur Windows, l'Installer étant des plus simple et habituel.

Toutefois, KeePass est installé par défaut en langue anglaise et il vous faudra télécharger le **pack de traduction français**.

Ce fichier au format .lgnx est à placer dans votre dossier « Program Files\KeePass Password Safe 2\Languages » une fois décompressé. C'est depuis le menu « View ➔ Change language » que vous pourrez enfin sélectionner notre langue.

Créer la base de données

D. Keepass : fenêtre de création de la clé principale



Rendez-vous dans le menu « Fichier ➔ Nouvelle… » et choisissez le nom que vous désirez pour votre fichier **KDBX**. C'est ce fichier qui sera votre base de données contenant tous vos mots de passe qui sont chiffrés (cryptés).

L'étape suivante est le choix de votre mot de passe principal, ce qui est appelé sous KeePass votre « clé principale ».

Nous ne vous conseillons pas d'utiliser les mots de passe aléatoires qui même s'ils ont un aspect austère ne sont pas suffisamment sécurisés.

La meilleure méthode pour choisir un mot de passe fort et donc complexe à déchiffrer est d'utiliser une phrase longue que vous choisissez au hasard.

C'est évidemment un moyen qui en plus d'être sécurisé permet de mémoriser cette clé principale beaucoup plus facilement.

Il est vrai que nous vous conseillons d'ajouter des chiffres et caractères spéciaux dans votre clé principale, mais cela dépend de votre capacité à vous en souvenir.

Une phrase longue est amplement suffisante dans la majorité des cas.

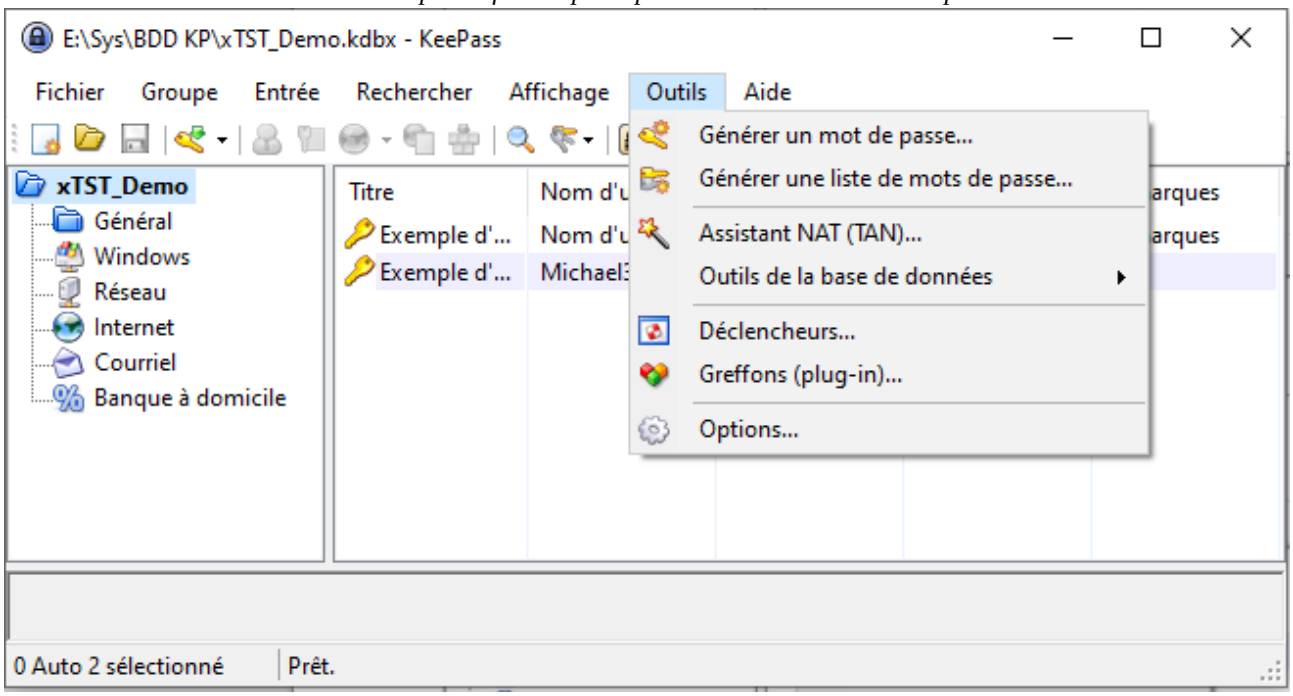
E. Keepass : Fenêtre Feuille de secours

Si vous possédiez d'autres logiciels de gestionnaire de mot de passe comme **Dashlane, Lastpass, 1Password ou encore Mozilla**, c'est le moment d'importer leurs bases de données que vous aurez préalablement exportées depuis ceux-ci.

Tout se passe dans le menu « Fichier ➔ Importer » où il ne vous restera plus qu'à choisir le fichier à importer tout en conservant son arborescence et ses entrées intacts.

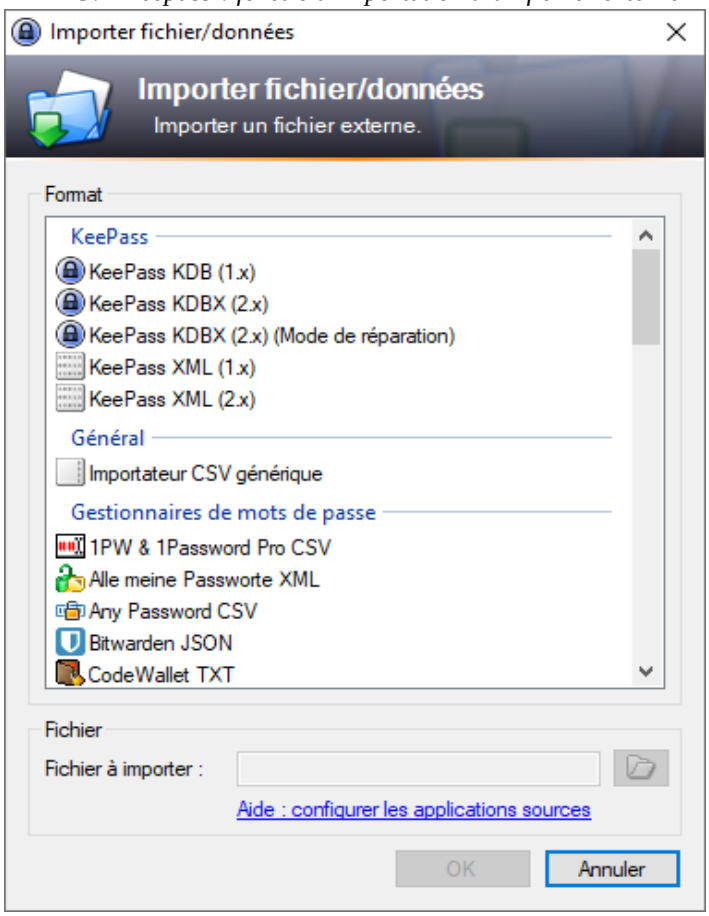
Ajuster les options de l'application

F. Keepass : fenêtre principale – sous-menu Outils > Options



Mettre en place la saisie automatique de vos mots de passe

G. Keepass : fenêtre d'importation d'un fichier externe



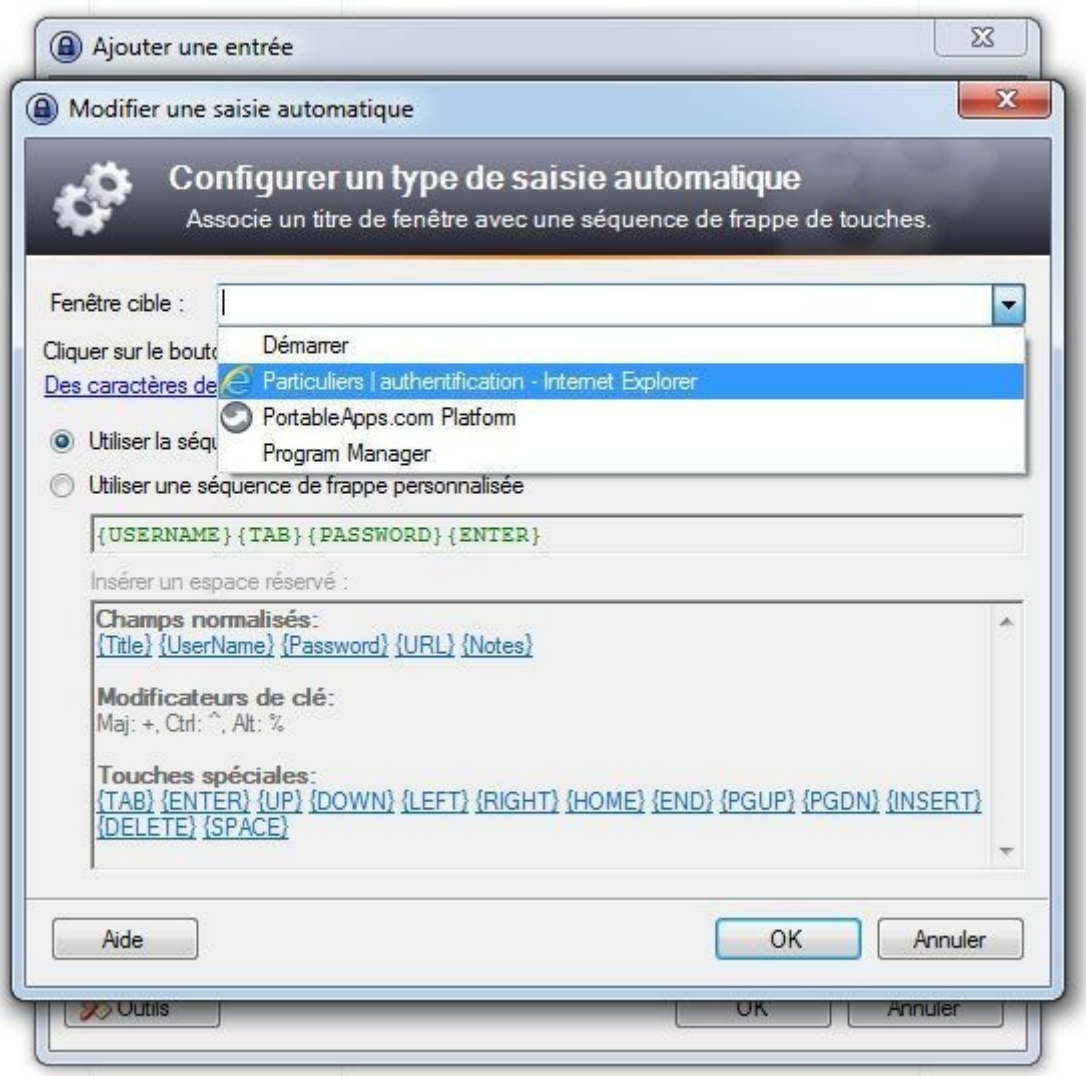
Dans son utilisation la plus basique, KeePass vous proposera vos mots de passe avec leurs noms d'utilisateurs que vous pourrez copier/coller dans les formulaires de connexion de vos logiciels ou de vos sites préférés.

Cela peut être particulièrement agaçant pour une utilisation domestique et c'est pourquoi KeePass propose un mode de **saisie automatique**.

Ainsi, dès lors que l'on vous demande d'entrer un nom d'utilisateur et un mot de passe, ceux-ci seront déjà pré-remplis par KeePass et il procédera même à l'envoi du formulaire de connexion.

C'est aussi simple que cela avec la saisie automatique.

H. Keepass : fenêtre de configuration de la saisie automatique 1



Pour les utilisateurs que nous sommes, concrètement cela donne une utilisation totalement transparente de KeePass qui va remplir les champs de nom d'utilisateur et de mot de passe par magie dès lors que vous aurez fait un clic droit sur le premier champ pour sélectionner « **Exécuter la saisie automatique** ».

Le gain de temps est non-négligeable grâce à ce simple clic droit sur le premier champ de vos formulaires de connexion.

KeePass fonctionne de base sur un modèle de formulaire de connexion où il vous est demandé le nom d'utilisateur puis le mot de passe associé, ce qui donne un enchaînement {USERNAME}{TAB}{PASSWORD}{ENTER}.

Il peut cependant arriver pour certain sites que vous ayez à modifier cet enchaînement pour permettre à la saisie automatique de fonctionner, comme c'est le cas par exemple avec les sites qui vont vous demander votre nom d'utilisateur puis de valider pour seulement ensuite vous demander dans une nouvelle fenêtre votre mot de passe.

Pas de panique, KeePass sait très bien le gérer par le simple enchaînement {USERNAME}{ENTER}{DELAY 1000}{PASSWORD}{ENTER}.

Vous l'aurez compris, nous venons tout simplement d'ordonner à KeePass d'ajouter un délai de 1 000 ms (soit 1 seconde) entre le nom d'utilisateur et le mot de passe afin que la page suivante puisse s'afficher et être validée à son tour.

I. Keepass : fenêtre de configuration de la saisie automatique 2

Comme l'univers de KeePass regorge de plugins très utiles et puissants, vous pouvez vous aider de **KeePassHttp** qui vous permettra alors de transmettre de manière automatique vos identifiants à un plugin comme **ChromeIPass**, nous vous parlons plus en détail ci-dessous.

Et aussi...

Installer le plugin KeePassHttp pour utiliser le plugin ChromeIPass

Pour installer un plugin (dans cet exemple **KeePassHttp et ChromeIPass**) il vous suffira de télécharger un fichier **.plgx** (comme KeePassHttp.plgx) et de la placer dans le répertoire « Program Files\KeePass Password Safe 2\Plugins ».

Pour faire fonctionner **ChromeIP** il vous faudra simplement cliquer sur « Connecter » où KeePass vous demandera alors d'entrer votre clé de connexion.

Il faut donner l'autorisation à KeePass de pouvoir exécuter des tâches en mode administrateur pour que le plugin puisse alors reconnaitre automatiquement les mots de passe associés aux sites internet que vous visitez.

Il faut bien dire que cette méthode par le plugin **ChromeIPass** ne fonctionne pas à 100% et produit quelques erreurs, c'est donc bien la première solution, celle native de KeePass que nous vous expliquions juste avant qui est bien la meilleure.

Vous venez néanmoins **d'apprendre à installer un plugin pour KeePass**.

Sauvegarde de vos mots de passe et synchronisation

Nous espérons sincèrement que vous avez déjà une solution de **sauvegarde automatique** sur votre ordinateur et dans ce cas, votre base de données de KeePass est alors sauvegardée avec le reste.

Toutefois et surtout en cas de panne matérielle, il est tout de même plus intéressant de mettre sa sauvegarde sur un autre support (un disque dur externe par exemple ou carrément sur le cloud).

Votre base de données KeePass est chiffrée et donc indéchiffrable dans les sauvegardes, il n'y a donc aucun risque à avoir sur une clef USB ou tout autre support sa sauvegarde KeePass.

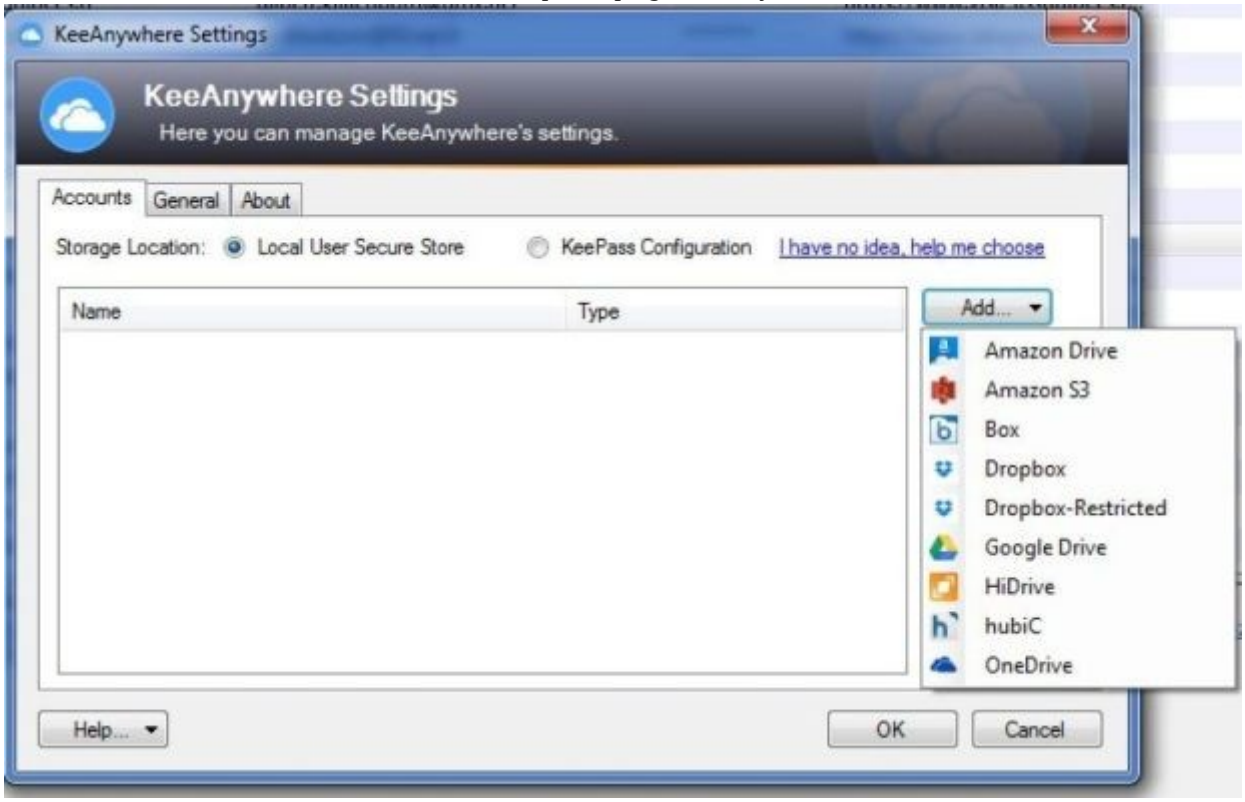
Il vous suffit alors de tout simplement faire une copie régulièrement de votre fichier **KDBX** afin d'avoir l'esprit tranquille.

Pour ceux qui ont des espaces de stockage en ligne, KeePass peut utiliser les protocoles **FTP, HHTP ou WebDAV** pour **sauvegarder et synchroniser votre base de données à distance**.

Le plus intéressant reste bien évidemment de s'installer son propre serveur FTP mais cela n'est pas à la portée de tous et peut être que vous utilisez déjà des services de **cloud**, il serait donc dommage de ne pas les utiliser.

Vous pourrez y arriver très facilement grâce au plugin **KeeAnywhere** qui vous permettra une synchronisation (et donc sauvegarde) de votre base de données sur **Dropbox, Google Drive, OneDrive, Box ou encore Amazon**. Vous savez déjà comment installer un plugin pour KeePass, tout le reste se passe dans le menu « Outils ➔ KeeAnywhere Settings » une fois installé.

J. Keepass : plugin KeeAnywhere



Utiliser KeePass Portable : mes mots de passe partout

Il est évident que si en journée vous êtes sur un poste au travail et le reste du temps sur deux autres ordinateurs à la maison, retrouver ses mots de passe sur chacun d'eux serait l'idéal et cela est possible très facilement.

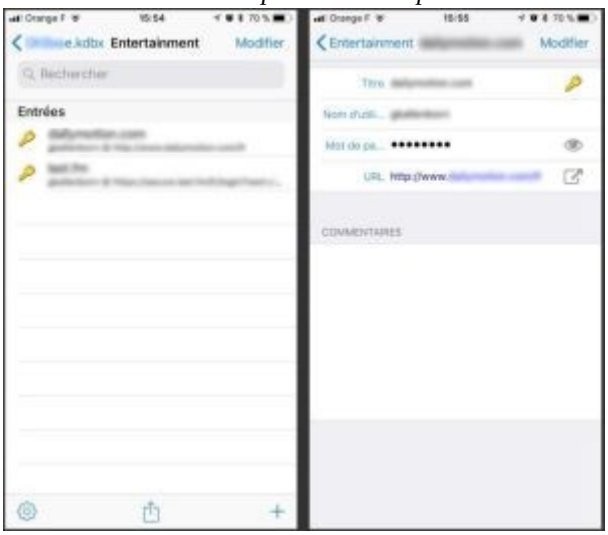
Souvenez-vous que nous vous présentions la version Portable de KeePass qui est suffisamment légère pour tenir sur une clef USB. Il n'y a alors pas besoin d'installer KeePass sur l'ordinateur que vous utilisez au travail (puisque le plus souvent vous n'avez pas les droits administrateurs pour faire cela) ou sur les autres ordinateurs à la maison puisque tout est déjà installé et fonctionnel depuis votre clef USB (qui contient du même coup la base de données et donc tous vos mots de passe du quotidien).

Télécharger KeePass Portable est donc la toute première étape pour avoir un gestionnaire de mot de passe sur **clef USB**.

L'étape suivante est des plus simples puisqu'il suffit de copier le fichier **.Exe** lors de votre téléchargement sur la clef USB et… c'est tout. Vous savez déjà comment importer une base de données (la vôtre avec vos mots de passe) et désormais **KeePass sera disponible et utilisable partout, tout le temps, sur n'importe quel ordinateur**.

KeePass sur smartphone

K. Keepass sur smartphone



Que vous soyez sur **iOS, Android, Blackberry** ou d'autres plateformes de smartphones, il est certain que vous trouverez votre bonheur par les **plugins KeePass**.

Toutes ces extensions sont évidemment compatibles avec la base **KDBX** de KeePass.

Nous pouvons citer pour les possesseurs d'Iphone l'excellent plugin MiniKeePass qui permet très simplement de gérer sa base de données (et donc ses mots de passe) en ajoutant/modifiant des entrées (voir la capture ci-dessus) et bien évidemment de jouir d'un aussi bon gestionnaire de mot de passe sécurisé sur ses **appareils mobiles** (pratique pour les **tablettes tactiles** par exemple).

Voir l'article de Keepass dédié aux smartphone iOS et Android

KeePass sous MacOS et Linux

Bien sûr que n'ont pas été oubliés les utilisateurs qui sont sur des ordinateurs avec des OS autres que ceux de Microsoft.

Nous vous citions les forks (qui ne sont pas des versions officielles de KeePass) mais il existe bon nombre de « portages » pour d'autres plateformes qui permettent d'utiliser directement toutes les fonctionnalités de KeePass sur un logiciel spécifiquement conçu pour **Linux, FreeBSD** ou encore **MacOS**.

C'est exactement comme pour les portages de KeePass sur les différentes plateformes de **smartphones (iOS, Android…)**.

Être sur **MacOS** ou **Linux** n'est donc pas un souci pour l'utilisation simplifiée de KeePass grâce à ses portages.

Si vous désirez KeePass (le seul et l'unique !) sans passer par un portage, il vous faudra alors installer une couche de compatibilité grâce à **Microsoft .NET** (cela se fait facilement grâce à **Mono**), ce qui vous permettra de bénéficier de KeePass avec exactement les mêmes fonctionnalités et avec la même interface que sur **Windows**.

Il n'y a alors plus rien de déroutant à passer de **Windows** au travail à **Mac OS** sur son ordinateur multimédia et à Linux sur son ordinateur pour développer, tout sera à l'identique dans sa présentation et dans son fonctionnement. Parfait non ?

En conclusion

Que vous utilisiez KeePass pour vous **simplifier la vie** et ne plus avoir à retenir ou noter sur des post-it volants vos mots de passe ou alors pour une **sécurisation accrue** de vos codes d'accès, ce sont bien ces deux avantages conséquents que vous retrouverez grâce à ce logiciel.

Tous les membres toujours plus nombreux de cette belle et grande communauté sur le **projet open source KeePass** sont à remercier : grâce à eux, KeePass est sans conteste le gestionnaire de mots de passe chiffrés le plus populaire et cela n'a été rendu possible que grâce à la communauté libre faisant évoluer depuis des années cet excellent logiciel.

Vous pouvez bien évidemment retrouver **KeePass dans ses versions Portables et Classiques** pour **Windows, MacOS X, Linux, BSD** et bien d'autres systèmes encore. Pour les portages sur d'autres plateformes, les **forks et les plugins KeePass**, suivez le guide !

Keepass 2.43 | Windows Keepass 2.43 | Portable MacPass (Fork) 0.7.9 | MacOS Keepass 2.xx | Linux

Lien vers les logiciels officiels et non officiels

FONCTIONNALITÉS DÉTAILLÉES[2] [3]

Saisie automatique (Auto-Type)

Fonction puissante qui envoie des pressions de touches simulées à d'autres applications.

- Informations de base sur la saisie automatique
- Invoquer la saisie automatique
  - Menu contextuel : Commande'Exécuter la saisie automatique
  - Raccourci clavier global de saisie automatique
- Spécification des séquences de touches et des fenêtres cibles
- Séquences de touches de saisie automatique
- Filtres de la fenêtre cible
- Modifier la séquence de saisie automatique par défaut
- Exemple d'utilisation

Informations de base sur la saisie automatique (Basic Auto-Type Information)

KeePass dispose d'une fonctionnalité "Auto-Type". Cette fonction vous permet de définir une séquence de pressions de touches que KeePass peut effectuer automatiquement pour vous. Les pressions de touches simulées peuvent être envoyées dans n'importe quelle autre fenêtre actuellement ouverte de votre choix (fenêtres du navigateur, boîtes de dialogue de connexion, ...).

Par défaut, la séquence de touches envoyée est {USERNAME}{TAB}{PASSWORD}{ENTER}, c'est-à-dire qu'elle tape d'abord le nom d'utilisateur de l'entrée sélectionnée, puis la touche Tab, puis le mot de passe de l'entrée et enfin la touche Entrée.

Pour les entrées TAN, la séquence par défaut est {MOT DE PASSE}, c'est-à-dire qu'il suffit de taper le TAN dans la fenêtre cible, sans appuyer sur Entrée.

> *KeePass 1.x uniquement*
>
> Vous pouvez définir librement votre propre séquence de saisie automatique : il vous suffit d'écrire la séquence dans le champ notes de l'entrée, préfixée par "Auto-Type :". Vos notes pourraient ressembler à ceci :
>
> Vous pouvez écrire n'importe quelles notes ici.
>
> Mon e-mail que j'ai utilisé pour m'inscrire : me@example.com
>
> saisie automatique : {USERNAME}{TAB}{TAB}{TAB}Une chaîne fixe{TAB}{PASSWORD}{ENTER}{ENTER

2 Voir site web : https://keepass.info/help/base/index.html
3 Traduction avec www.DeepL.com/Translator (version gratuite)

Ici vous pouvez continuer avec vos notes si vous le souhaitez..…

Comme vous pouvez le voir, la seule chose importante est que la séquence de saisie automatique soit préfixée à l'aide de "Auto-Type :" et soit d'une seule ligne. Une séquence de saisie automatique ne peut pas être définie en utilisant deux lignes ou plus.

Si vous définissez deux ou plusieurs séquences de saisie automatique, la première est utilisée.

KeePass 2.x uniquement

La saisie automatique peut être configuré individuellement pour chaque entrée à l'aide de la page à onglet Saisie automatique de la boîte de dialogue de saisie (sélectionnez une entrée → Modifier l'entrée). Sur cette page, vous pouvez spécifier une séquence par défaut et personnaliser les associations fenêtre/séquence spécifiques.

L'obscurcissement de saisie automatique à deux canaux est pris en charge (ce qui rend la saisie automatique résistant aux enregistreurs de frappe).

En outre, vous pouvez créer des associations fenêtre/séquence personnalisées qui remplacent la séquence par défaut. Vous pouvez spécifier différentes séquences de touches pour différentes fenêtres pour chaque entrée. Par exemple, imaginez une page Web, à laquelle vous voulez vous connecter, qui a plusieurs pages où vous pouvez vous connecter. Ces pages pourraient toutes avoir un aspect un peu différent (sur l'une d'entre elles, vous pourriez également avoir besoin de cocher une case à cocher - comme c'est souvent le cas dans les forums). Ici, la création d'associations fenêtre/séquence personnalisées résout le problème : il vous suffit de spécifier différentes séquences de saisie automatique pour chaque fenêtre (identifiées par leur titre).

Utiliser la saisie automatique :

Il y a trois méthodes différentes pour utiliser la saisie automatique :

- Utiliser la saisie automatique d'une entrée à l'aide de la commande de menu contextuel Exécuter la saisie automatique lorsque l'entrée est sélectionnée.
- Sélectionnez l'entrée et appuyez sur Ctrl+V (c'est le raccourci du menu contextuel ci-dessus).
- Utilisation de la touche de raccourci de saisie automatique à l'échelle du système. KeePass recherchera les séquences correspondantes dans toutes les entrées de la base de données actuellement ouverte.

Toutes les méthodes sont expliquées en détail ci-dessous.

Définition du point d'entrée (Input Focus) :

Notez que la saisie automatique commence à taper dans le contrôle de la fenêtre cible qui a le focus d'entrée. Ainsi, par exemple, pour la séquence par défaut, vous devez vous assurer que le focus d'entrée est défini sur le contrôle du nom d'utilisateur de la fenêtre cible avant d'appeler la saisie automatique en utilisant l'une des méthodes ci-dessus.

Droits (Rights) :

Pour que la saisie automatique fonctionne, KeePass doit s'exécuter avec les mêmes droits ou des droits supérieurs à ceux de l'application cible. En particulier, si l'application cible s'exécute avec des droits d'administration, KeePass doit également s'exécuter avec des droits d'administration. Pour plus de détails, voir Conception du mécanisme d'intégrité de Windows.

Ordinateurs de bureau distants et machines virtuelles (Remote Desktops and Virtual Machines) :

KeePass ne connaît pas la disposition du clavier qui a été sélectionnée dans un bureau distant ou une fenêtre de machine virtuelle. Si vous voulez taper automatiquement dans une telle fenêtre, vous devez vous assurer que le système local et le système virtuel/distant utilisent la même disposition de clavier.

Menu contextuel Texte : Commande 'Exécuter la saisie automatique' 

Cette méthode est celle qui nécessite le moins de configuration et qui est la plus simple, mais elle a l'inconvénient que vous devez sélectionner l'entrée dans KeePass que vous voulez saisir automatiquement.

La méthode est simple : cliquez avec le bouton droit de la souris sur une entrée de votre base de données actuellement ouverte et cliquez sur 'Exécuter la saisie automatique' (ou bien appuyez sur le raccourci Ctrl+V pour cette commande). La fenêtre qui a obtenu le focus précédemment (c'est-à-dire celle dans laquelle vous avez travaillé avant de passer à KeePass) sera mise au premier plan et les types automatiques de KeePass seront affichés dans cette fenêtre.

La séquence de saisie automatique dépend du titre de la fenêtre. Si vous n'avez pas spécifié d'association fenêtre/séquence personnalisée, la séquence par défaut est envoyée. Si vous avez créé des associations, KeePass utilise la séquence de la première association correspondante. Si aucune des associations ne correspond, la séquence par défaut est utilisée.

Touche d'accès rapide de saisie automatique global de texte 

C'est la méthode la plus puissante, mais elle nécessite aussi un peu plus de travail/connaissances avant de pouvoir être utilisée.

Exemple simple de saisie automatique global :

- Créez une entrée dans KeePass intitulée Bloc-notes avec les valeurs du nom d'utilisateur et du mot de passe.
- Démarrez Notepad (sous'Programmes' →'Accessoires').
- Appuyez sur Ctrl+Alt+A dans Notepad. Le nom d'utilisateur et le mot de passe seront saisis dans Notepad.

Le titre de l'entrée KeePass Notepad correspond au titre de la fenêtre Notepad et la séquence de type automatique par défaut est tapée.

Comment ça marche - Détails :

KeePass enregistre un raccourci clavier à l'échelle du système pour la saisie automatique. L'avantage de cette touche de raccourci est que vous n'avez pas besoin de passer à la fenêtre KeePass et de sélectionner l'entrée. Il vous suffit d'appuyer sur le raccourci clavier tout en ayant la fenêtre cible ouverte (c'est-à-dire la fenêtre qui recevra les touches simulées).

Par défaut, le raccourci clavier global est Ctrl+Alt+A (c.-à-d. maintenez les touches Ctrl et Alt enfoncées, appuyez sur A et relâchez toutes les touches). Vous pouvez modifier cette hotkey dans la boîte de dialogue des options (menu principal -'Outils' -'Options', onglet'Intégration'/'Avancé') : ici, cliquez dans la zone de texte sous "Global Auto-Type Hot Key Combination" et appuyez sur la hotkey que vous souhaitez utiliser. Si la touche de raccourci est utilisable, elle apparaîtra dans la zone de texte.

Lorsque vous appuyez sur la touche de raccourci, KeePass regarde le titre de la fenêtre actuellement ouverte et recherche les entrées utilisables dans la base de données actuellement ouverte. Si KeePass trouve plusieurs entrées qui peuvent être utilisées, il affiche une boîte de dialogue de sélection. Une entrée est considérée comme utilisable pour le titre de la fenêtre en cours lorsqu'au moins l'une des conditions suivantes est remplie :

- Le titre de l'entrée est une sous-chaîne du titre de la fenêtre actuellement active.
- L'entrée a une association fenêtre/séquence, dont le spécificateur de fenêtre correspond au titre de la fenêtre actuellement active.

La deuxième condition a déjà été mentionnée, mais la première est nouvelle. En utilisant les titres d'entrée comme filtres pour les titres de fenêtres, le montant de la configuration pour la saisie automatique est presque nul : vous n'avez qu'à vous assurer que le titre de l'entrée est contenu dans le titre de la fenêtre dans laquelle vous voulez que l'entrée soit saisie automatiquement. Bien sûr, ce n'est pas toujours possible (par exemple, si une page web a un titre très générique comme "Welcome"), vous devez ici utiliser des associations fenêtre/séquence personnalisées.

KeePass 1.x uniquement

Les associations de fenêtres/séquences personnalisées peuvent être spécifiées à l'aide du champ Notes des entrées.

Mon e-mail que j'ai utilisé pour m'inscrire : me@example.com

Type automatique : {USERNAME}{TAB}{TAB}{TAB}Une chaîne fixe{TAB}{PASSWORD}{ENTER}{ENTER

Fenêtre de saisie automatique : Quelques sites Web – Bienvenue*

Ici vous pouvez continuer avec vos notes si vous le souhaitez..…

Si vous avez maintenant une fenêtre ouverte qui commence par "Some Website - Welcome" et appuyez sur la combinaison de touches de raccourci clavier globale de saisie automatique, KeePass exécute la séquence de saisie automatique ci-dessus.

Certains sites, notamment les banques, utilisent des schémas de connexion multi-pages. Vous pouvez utiliser les chaînes de caractères de la fenêtre de saisie automatique pour automatiser ces sites. Vous pouvez également utiliser les chaînes de caractères de la fenêtre de saisie automatique pour normaliser votre connexion au réseau local dans une entrée KeePass.

Il est possible de définir autant de chaînes de caractères Auto-Type-Window par entrée que vous le souhaitez.

De plus, une séquence peut être utilisée pour plusieurs fenêtres. Pour cela, définissez d'abord un couple fenêtre/séquence comme d'habitude, puis continuez en ajoutant'-' et un nombre, en commençant par 1. exemple :

Type automatique : {NOMD'UTILISATEUR}{ONGLET}{MOT DE PASSE}{ENTRER}{NOMD'UTILISATEUR}{TAB}{MOT DE PASSE}{ENTRER

Fenêtre de saisie automatique : Quelques dialogues - *

Auto-Type-1 : {USERNAME}{ENTER}{ENTER}

Auto-Type-Window-1 : * - Editeur

Auto-Type-Window-1 : * - Bloc-notes

Auto-Type-Window-1 : * - WordPad

Auto-Type-2 : {MOT DE PASSE}{ENTER}{ENTER}

Auto-Type-Window-2 : Quelques pages Web - *

Ici, la séquence Auto-Type-1 sera utilisée pour toutes les fenêtres Auto-Type-Window-1.

Les associations de fenêtres personnalisées remplacent le titre de l'entrée KeePass. Si des associations de fenêtres personnalisées sont spécifiées, elles seront les seuls éléments utilisés pour déterminer une correspondance et le titre de l'entrée KeePass sera ignoré.KeePass 2.x uniquement

KeePass 2.x uniquement

Les associations de fenêtre/séquence personnalisées peuvent être spécifiées dans la page à onglet'Auto-Type' de chaque entrée.

Les associations complètent le titre d'inscription KeePass. Toute association spécifiée sera utilisée en plus du titre de l'inscription KeePass pour déterminer une correspondance.

Les définitions des fenêtres de type automatique, les titres des entrées et les URL sont compilés par Spr, c'est-à-dire que les espaces réservés, les variables d'environnement, les références de champs, etc. peuvent être utilisés.

Séquences de touches de type automatique

Une séquence de touches de type automatique est une chaîne d'une ligne qui peut contenir des caractères génériques et des codes de touches spéciaux.

Une liste complète de tous les espaces réservés pris en charge se trouve sur la page Placeholders. Les codes des touches spéciales se trouvent ci-dessous.

Au-dessus, vous avez déjà vu que la saisie automatique par défaut est {USERNAME}{TAB}{PASSWORD}{ENTER}. Ici, {USERNAME} et {PASSWORD} sont des caractères de remplacement : lorsque la saisie automatique est effectuée, ceux-ci sont remplacés par les valeurs de champ appropriées de l'entrée. {TAB} et {ENTER} sont des codes de touches spéciaux : ils sont remplacés par les touches appropriées. Les codes de touches spéciales sont le seul moyen de spécifier des touches spéciales telles que Flèche vers le bas, Majuscule, Echap, etc.

Bien entendu, les séquences de touches peuvent également contenir des caractères simples à envoyer. Par exemple, la chaîne suivante est parfaitement valide comme chaîne de séquence de touches :

{NOM D'UTILISATEUR}{TAB}Un texte à envoyer!{ENTRE}.

KeePass 1.x uniquement

Les codes spéciaux des touches sont sensibles à la casse.

KeePass 2.x uniquement

Les codes spéciaux des touches sont insensibles à la casse.

Touches spéciales :

Les codes suivants pour les touches spéciales sont pris en charge :

Special Key	Code
Tab	`{TAB}`
Enter	`{ENTER}` or `~`
Arrow Up	`{UP}`
Arrow Down	`{DOWN}`
Arrow Left	`{LEFT}`
Arrow Right	`{RIGHT}`
Insert	`{INSERT}` or `{INS}`
Delete	`{DELETE}` or `{DEL}`

Home	{HOME}
End	{END}
Page Up	{PGUP}
Page Down	{PGDN}
Space	{SPACE}
Backspace	{BACKSPACE}, {BS} or {BKSP}
Break	{BREAK}
Caps-Lock	{CAPSLOCK}
Escape	{ESC}
Windows Key	{WIN} (equ. to {LWIN})
Windows Key: left, right	{LWIN}, {RWIN}
Apps / Menu	{APPS}
Help	{HELP}
Numlock	{NUMLOCK}
Print Screen	{PRTSC}
Scroll Lock	{SCROLLLOCK}
F1 - F16	{F1} - {F16}
Numeric Keypad +	{ADD}
Numeric Keypad -	{SUBTRACT}
Numeric Keypad *	{MULTIPLY}
Numeric Keypad /	{DIVIDE}
Numeric Keypad 0 to 9	{NUMPAD0} to {NUMPAD9}
Shift	+
Ctrl	^
Alt	%

KeePass 1.x uniquement

Special Key	Code
+	{PLUS}
%	{PERCENT}
^	{CARET}
~	{TILDE}
(,)	{LEFTPAREN}, {RIGHTPAREN}
{, }	{LEFTBRACE}, {RIGHTBRACE}
@	{AT}
Windows Key (as modifier)	@

KeePass 2.x uniquement

Special Key	Code
+	{+}
%	{%}
^	{^}
~	{~}
(,)	{(}, {)}
[,]	{[}, {]}
{, }	{{}, {}}

De plus, certaines commandes spéciales sont prises en charge :

Command Syntax	Action
{DELAY *X*}	Retards X millisecondes.
{DELAY=*X*}	Règle le délai par défaut à X millisecondes pour toutes les pressions de touches suivantes.
{CLEARFIELD}	Efface le contenu du champ d'édition qui a actuellement le focus (uniquement les champs d'édition d'une seule ligne).
{VKEY *X*}	Envoie la clé virtuelle de la valeur X.
{APPACTIVATE *WindowTitle*}	Active la fenêtre "WindowTitle".
{BEEP *X Y*}	Bip avec une fréquence de X hertz et une durée de Y millisecondes.

KeePass 2.x uniquement

Command Syntax	Action
{VKEY-NX *X*}	Envoie la clé virtuelle non étendue de la valeur X. Si possible, utilisez {VKEY X} à la place.
{VKEY-EX *X*}	Envoie la clé virtuelle étendue de la valeur X. Si possible, utilisez {VKEY X} à la place.

KeePass 2.x uniquement

Les touches et les touches spéciales (et non les espaces réservés ou les commandes) peuvent être répétées en ajoutant un numéro dans le code. Par exemple, {TAB 5} appuie 5 fois sur la touche Tabulation.

Pour plus de détails sur la façon d'envoyer des clés spéciales pour lesquelles il n'existe pas de codes spéciaux explicites, veuillez consulter : Comment la saisie automatique peut-elle envoyer d'autres clés spéciales ?

Enfin, quelques exemples :

{TITLE}{TAB}{USERNAME}{TAB}{TAB}{PASSWORD}{ENTER}

Tapez le titre de l'entrée, un onglet, le nom d'utilisateur, un onglet, le mot de passe de l'entrée actuellement sélectionnée et appuyez sur Entrée.

{TAB}{PASSWORD}{ENTER}

Appuyez sur la touche Tabulation, entrez le mot de passe de l'entrée et appuyez sur Entrée.

{USERNAME}{TAB}^v{ENTER}

Tapez le nom d'utilisateur, appuyez sur Tab, appuyez sur Ctrl+V (qui colle les données du presse-papiers Windows dans la plupart des applications), et appuyez sur Entrée.

Activer les cases à cocher :

Parfois, vous trouverez des cases à cocher sur les sites Web (" Rester connecté sur cet ordinateur " par exemple). Vous pouvez activer ces cases à cocher en envoyant un espace (' ') lors de la saisie automatique. Par exemple :

{USERNAME}{TAB}{PASSWORD}{TAB} {TAB}{ENTER}

S'il y a un formulaire Web avec un champ nom d'utilisateur, un champ mot de passe et une case à cocher, cette séquence devrait entrer le nom d'utilisateur, le mot de passe et activer la case à cocher qui suit le contrôle du mot de passe.

Appuyer sur les boutons non par défaut :

L'appui sur des boutons autres que ceux par défaut fonctionne de la même manière que le basculement des cases à cocher : envoyer un caractère espace (' '). Notez que ceci ne doit être utilisé que pour les boutons qui ne sont pas par défaut ; pour les boutons par défaut, {ENTER} doit être envoyé à la place.

Caractères ANSI supérieurs :

La fonction de type automatique prend en charge l'envoi de caractères ANSI supérieurs compris entre 126 et 255. Cela signifie que vous pouvez envoyer des caractères spéciaux comme ©, @, etc. sans aucun problème ; vous pouvez les écrire directement dans la définition de la séquence de touches.

Filtres de la fenêtre cible

Lorsque vous créez une association fenêtre/séquence personnalisée, vous devez indiquer à KeePass à quoi ressemblent les titres des fenêtres correspondantes. Ici, KeePass prend en charge les caractères génériques simples :

chaîne	Signification
chaîne	Correspond à tous les titres de fenêtres qui s'appellent exactement "*chaîne*"
*chaîne**	Correspond à tous les titres de fenêtres qui commencent par "*chaîne*".
**chaîne*	Correspond à tous les titres de fenêtres qui se terminent par "*chaîne*".
chaîne	Correspond à tous les titres de fenêtre qui ont "*chaîne*" quelque part dans le titre de la fenêtre. Ceci inclut le fait que la chaîne de caractères se trouve directement au début ou à la fin du titre de la fenêtre.

KeePass 1.x uniquement

Les autres caractères génériques ne sont pas pris en charge. Le caractère générique * ne doit pas être au milieu d'une chaîne de caractères.

Par exemple, *Windows*Explorer* ne correspondra pas à l'explorateur Windows, mais seulement à Windows*Explorer, c'est-à-dire que le caractère du milieu * est traité comme un caractère texte'*' au lieu d'un caractère générique.

KeePass 2.x uniquement

Des caractères génériques peuvent également apparaître au milieu des motifs. Par exemple, *Windows*Explorer* correspondrait à Windows Internet Explorer.

De plus, la correspondance à l'aide d'expressions régulières est prise en charge. Pour indiquer à KeePass que le motif est une expression régulière, enfermez-le dans //. Par exemple, //B.?g Window// correspondrait à Big Window, Bug Window et Bg Window.

En utilisant des caractères génériques, vous pouvez rendre vos associations de type automatique indépendantes du navigateur. Voir les exemples d'utilisation pour plus d'informations.

Changement de texte par défaut Séquence de type automatique

La séquence de saisie automatique par défaut (c'est-à-dire celle qui est utilisée lorsque vous ne spécifiez pas de séquence personnalisée) est {USERNAME}{TAB}{PASSWORD}{ENTER}. KeePass vous permet de modifier cette séquence par défaut. Normalement, vous n'aurez pas besoin de le modifier (utilisez plutôt des définitions de fenêtres/séquences personnalisées !), mais il est très utile lorsqu'une autre application interfère avec KeePass (par exemple un logiciel de sécurité qui vous demande toujours la permission avant d'autoriser KeePass à saisir automatiquement).

KeePass 1.x uniquement

La séquence de saisie automatique par défaut peut être modifiée dans la boîte de dialogue de configuration de la saisie automatique. Ce dialogue se trouve dans'Outils' →'Options' →'Options' →'Avancé' →'Auto-Type'.

KeePass 2.x uniquement

Par défaut, les entrées héritent de la séquence de type automatique de leur groupe contenant. Les groupes héritent également de la séquence de type automatique de leurs groupes parents. Il n'y a qu'un seul groupe supérieur (le premier groupe contient tous les autres groupes). Par conséquent, si vous modifiez la séquence de saisie automatique de ce tout premier groupe, tous les autres groupes et leurs entrées utiliseront cette séquence. En pratique, il s'agit d'une dérogation globale. Pour le changer, cliquez avec le bouton droit de la souris sur le premier groupe, choisissez'Modifier le groupe' et passez à l'onglet'Auto-Type'.

Exemple d'utilisation

Voyons maintenant un exemple concret : la connexion à un site Web. Dans cet exemple, utiliserons-nous le raccourci clavier global pour remplir la page de connexion ?

Ouvrez d'abord la page de test, puis créez une nouvelle entrée dans KeePass avec le titre Test Form et un nom d'utilisateur et un mot de passe de votre choix.

Supposons que le raccourci clavier global de saisie automatique est réglé sur Ctrl+Alt+A (la valeur par défaut). KeePass s'exécute en arrière-plan, vous avez ouvert votre base de données et l'espace de travail est déverrouillé.

Lorsque vous accédez à la page de test et que vous êtes invité à entrer votre nom d'utilisateur et votre mot de passe, cliquez simplement dans le champ nom d'utilisateur et appuyez sur Ctrl+Alt+A. KeePass saisit le nom d'utilisateur et le mot de passe pour vous !

Pourquoi cela a-t-il fonctionné ? Le titre de la fenêtre de votre navigateur était "Formulaire de test - KeePass - Internet Explorer" ou "Formulaire de test - KeePass - Mozilla Firefox", selon le navigateur que vous utilisez. Parce que nous avons donné à l'entrée dans KeePass le titre Test Form, le titre de l'entrée est contenu dans le titre de la fenêtre, donc KeePass utilise cette entrée.

Ici vous voyez les énormes avantages de l'auto-saisie : non seulement elle ne nécessite aucun logiciel de navigation supplémentaire (le navigateur ne sait rien de KeePass - il n'y a aucun plugin d'aide requis), mais elle est également indépendante du navigateur : la seule entrée que vous avez créée dans KeePass fonctionne pour Internet Explorer et Mozilla Firefox (et autres navigateurs) sans exiger aucune modification ou définition.

Lorsque vous utilisez des associations fenêtre/séquence (au lieu d'une correspondance de titre d'entrée), vous pouvez obtenir le même effet indépendant du navigateur en utilisant des caractères génériques : vous auriez par exemple pu utiliser Test Form - KeePass - * comme filtre de fenêtre. Ce filtre correspond à la fois à Internet Explorer et à la fenêtre Firefox.

Clé maîtresse (Composite Master Key)

Ce document décrit comment KeePass verrouille les bases de données.

- Mots de passe maîtres
- Fichiers clés
- Compte utilisateur Windows
- Pour les administrateurs : Spécification des propriétés minimales des clés maîtresses

KeePass stocke vos mots de passe en toute sécurité dans un fichier crypté (base de données). Cette base de données est verrouillée avec un mot de passe maître, un fichier de clés et/ou les détails du compte Windows actuel. Pour ouvrir une base de données, toutes les sources clés (mot de passe, fichier de clés, etc.) sont nécessaires. Ensemble, ces sources clés forment la clé passe-partout composite.

KeePass ne supporte pas l'utilisation alternative des clés, c'est-à-dire qu'il n'est pas possible d'ouvrir votre base de données avec un mot de passe ou un fichier de clés. Utilisez soit un mot de passe, soit un fichier de clés, soit les deux à la fois (tous deux requis), mais pas de façon interchangeable.

Mots de passe maîtres (Master Passwords)

Si vous utilisez un mot de passe maître, vous n'avez qu'à vous souvenir d'un seul mot de passe ou phrase de passe (qui devrait être bon !) pour ouvrir votre base de données. KeePass offre une protection contre les attaques par force brute et les attaques du dictionnaire sur le mot de passe maître, consultez la page d'informations sur la sécurité pour en savoir plus.

Si vous oubliez ce mot de passe maître, tous les autres mots de passe de la base de données sont également perdus. Il n'y a pas de porte dérobée ou de clé permettant d'ouvrir toutes les bases de données. Il n'y a aucun moyen de récupérer vos mots de passe.

Fichier Clé (key file)

Vous n'avez même pas besoin de vous souvenir d'une longue et compliquée phrase de passe maîtresse. La base de données peut également être verrouillée à l'aide d'un fichier clé. Un fichier de clé est essentiellement un mot de passe maître dans un fichier. Les fichiers de clés sont généralement plus forts que les mots de passe maîtres, parce que la clé peut être beaucoup plus compliquée, mais il est aussi plus difficile de les garder secrets.

- Un fichier clé peut être utilisé à la place d'un mot de passe, ou en plus d'un mot de passe (et du compte utilisateur Windows dans KeePass 2.x).
- Un fichier clé peut être n'importe quel fichier que vous choisissez, bien que vous devriez en choisir un avec beaucoup de données aléatoires.
- Un fichier clé ne doit pas être modifié, cela vous empêchera d'ouvrir la base de données. Si vous souhaitez utiliser un fichier de clés différent, vous pouvez modifier la clé maître et utiliser un fichier de clés nouveau/différent.
- Les fichiers clés doivent être sauvegardés ou vous ne pourrez pas ouvrir la base de données après un crash/reconstruction du disque dur. C'est la même chose que d'oublier le mot de passe principal. Il n'y a pas de porte dérobée.
- Ne sauvegardez pas le fichier clé au même emplacement que la base de données, utilisez un répertoire ou un disque différent. Testez l'ouverture de votre base de données sur une autre machine pour confirmer que votre sauvegarde fonctionne. Pour une discussion détaillée sur la différence entre la sauvegarde du fichier clé et la sauvegarde de la base de données, consultez la FAQ ABP.

Emplacement.

L'intérêt d'un fichier clé est que vous avez quelque chose pour vous authentifier (contrairement aux mots de passe maîtres, où vous savez quelque chose), par exemple un fichier sur une clé USB. Le contenu du fichier clé (c'est-à-dire les données clés contenues dans le fichier clé) doit rester secret. Le but n'est pas de garder secret l'emplacement du fichier clé - sélectionner un fichier parmi des milliers existant sur votre disque dur n'augmente pas du tout la sécurité, car il est très facile pour les malware/attaqueurs de trouver le bon fichier (par exemple en observant les derniers temps d'accès des fichiers, la liste des fichiers récemment utilisés de Windows, les journaux du scanner de malware, etc). Essayer de garder secret l'emplacement du fichier clé est la sécurité par l'obscurité, c'est-à-dire qu'il n'est pas vraiment efficace.

Type de fichier et fichiers existants.

KeePass peut générer des fichiers clés pour vous, mais vous pouvez aussi utiliser n'importe quel autre fichier déjà existant (comme une image JPG, un document DOC, etc.).

KeePass 1.x uniquement

Pour utiliser un fichier existant comme fichier clé, cliquez sur le bouton avec l'image "Enregistrer" dans la boîte de dialogue de création de la clé principale et sélectionnez le fichier existant. Après avoir accepté la boîte de dialogue, KeePass vous demandera si vous souhaitez écraser ou réutiliser le fichier (voir la capture d'écran).

KeePass 2.x uniquement

Pour utiliser un fichier existant comme fichier clé, cliquez sur le bouton "Parcourir" dans la boîte de dialogue de création de la clé principale.

Références des champs 

Comment mettre des références à des données dans les champs d'autres entrées.

- Introduction
- Syntaxe des caractères génériques
- Exemple

Introduction 

KeePass peut insérer des données stockées dans différentes entrées dans les champs d'une entrée. Cela signifie que plusieurs entrées peuvent partager un champ commun (nom d'utilisateur, mot de passe,...), et en modifiant l'entrée de données réelle, toutes les autres entrées utiliseront également la nouvelle valeur.

Pour créer une référence de champ, vous pouvez soit utiliser l'assistant pratique de références de champ (dans la fenêtre d'édition des entrées, cliquez sur le bouton'Outils' en bas à gauche et sélectionnez'Insérer référence de champ'), soit insérer le caractère de remplissage manuellement (voir la syntaxe ci-dessous).

Notez que les références de zone sont destinées à faire référence à des données enregistrées dans des entrées différentes. Si vous voulez insérer des données à partir de la même entrée ou d'une entrée courante, vous devez utiliser des caractères génériques locaux, comme {TITLE} et {S:FieldName} ; voir Caractères génériques.

Syntaxe du caractère de remplissage de texte 

La syntaxe des caractères génériques pour les références de zone est la suivante :

Réf:<WantedField>@<SearchIn>:<Text>} {REF:<WantedField>@<SearchIn>:<Text>}

Les parties WantedField et SearchIn doivent être remplacées par des codes à une lettre identifiant le champ :

Code	Field
T	Titre
U	Nom d'utilisateur
P	Mot de passe
A	URL
N	Notes
I	UUID
O	Autres chaînes personnalisées (*KeePass 2.x uniquement*)

La partie Texte est la chaîne de recherche qui décrit le(s) texte(s) qui doit (doivent) apparaître dans la zone spécifiée d'une entrée pour correspondre.

Si plusieurs entrées correspondent au critère de recherche spécifié, la première entrée sera utilisée. Pour éviter toute ambiguïté, les entrées peuvent être identifiées par leurs UUID, qui sont uniques. Exemple : {REF:P@I:46C9B1FFBD4ABC4BBBBB260C6190BAD20C} insérerait le mot de passe de l'entrée ayant 46C9B1FFBD4ABC4BBBB260C6190BAD20C comme UUID.

KeePass 2.x uniquement

Le référencement des champs d'autres entrées ne fonctionne qu'avec des champs standard, pas avec des chaînes utilisateur personnalisées. Si vous voulez référencer une chaîne utilisateur personnalisée, vous devez placer une redirection dans un champ standard de l'entrée avec la chaîne personnalisée, en utilisant {S:<Name>}, et référencer le champ standard.

Les chaînes personnalisées peuvent être référencées localement (c'est-à-dire dans une entrée) en utilisant {S:<Nom>}, voir la page Caractères de remplissage pour plus de détails.

Vous pouvez utiliser le code O pour que KeePass recherche dans la base de données des champs de chaînes personnalisés (pour identifier l'entrée source référencée), mais O ne peut pas être utilisé pour récupérer les données des champs personnalisés (c'est-à-dire que le code ne peut être utilisé comme WantedField).

Exemple

Supposons que vous ayez deux entrées : l'une avec le titre "Example Website" et l'autre avec "Example Forum", et que vous voulez insérer le nom d'utilisateur du compte du site dans l'URL de l'entrée du forum. Dans l'URL de l'entrée du forum, vous pouvez référencer le nom d'utilisateur de la manière suivante :

https://forum.example.com/?user={REF:U@T:Example Website}

Support TAN

KeePass prend en charge les numéros d'authentification de transaction (TAN Transaction Authentication Numbers).

- Utilisation de l'assistant TAN pour ajouter des TANs (Using the *TAN Wizard* to add TANs)
- Utilisation des NAV

KeePass prend en charge les TAN, c'est-à-dire les mots de passe qui ne peuvent être utilisés qu'une seule fois. Ces mots de passe spéciaux sont utilisés par certaines banques : vous devez confirmer les transactions en utilisant ces TAN. Ceci offre une sécurité supplémentaire, car un espion ne peut pas effectuer de transactions, même s'il connaît le mot de passe de votre compte bancaire.

Utilisation de l'Assistant TAN pour ajouter des TANs

Vous pouvez utiliser l'assistant KeePass TAN Wizard pour ajouter plusieurs TAN à la fois à votre base de données. Ouvrez simplement la boîte de dialogue de l'assistant TAN (menu Outils - Assistant TAN) et entrez tous vos TANs. Le formatage n'a pas vraiment d'importance, KeePass utilise simplement toutes les chaînes alphanumériques, c'est-à-dire que les caractères comme les sauts de ligne, les tabulations, les espaces, les points, etc. sont interprétés comme séparateurs.

L'assistant génère alors plusieurs entrées TAN à partir des données que vous avez saisies dans la boîte de dialogue. Chaque TAN est une entrée KeePass standard. Le titre d'une entrée TAN est toujours réglé sur "<TAN>". Ceci indique à KeePass que l'entrée est une entrée TAN. Vous ne pouvez pas modifier le titre, le nom d'utilisateur et l'URL d'un NAV. Mais vous pouvez librement ajouter des notes à une entrée TAN, si vous le souhaitez.

Utilisations de TANs (Using TANs)

Lorsque vous utilisez le TAN (par exemple, exécutez la commande "Copier le mot de passe"), sa date d'expiration sera réglée sur l'heure actuelle, qui expire l'entrée. Il obtiendra un X rouge comme icône. Si vous voulez savoir plus tard quand vous avez utilisé un TAN spécifique, vous pouvez simplement jeter un coup d'oeil à sa date d'expiration.

Lors de la copie d'un TAN dans le presse-papiers, la base de données est marquée comme modifiée. Vous devez enregistrer le fichier afin de vous souvenir de l'utilisation d'un TAN.

Si vous avez accidentellement utilisé un NAV sans en avoir besoin, vous pouvez le réinitialiser (c'est-à-dire supprimer le X rouge et l'afficher à nouveau comme NAV valide). Pour ce faire, ouvrez l'entrée TAN (cliquez dessus avec le bouton droit de la souris et choisissez'Modifier/visualiser l'entrée...'). Ici, décochez la case'Expire'. Cliquez sur[OK] pour fermer la boîte de dialogue.

Suite à venir ?