

# Gestionnaire de mot passe

*L'outil de cette appropriation sera Keepass. Le choix s'est porté sur cet outil pour les raisons suivantes :*

- *C'est un logiciel libre (opensource)*
- *Il est gratuit*
- *Il est multiplateforme (Windows, Linux, MacOs...)*
- *Il permet de générer des mots de passe à la complexité élevée*
- *Il gère l'authentification à doubles facteurs*
- *La sécurité de stockage est importante*
- *Il est possible de partager la base de mots de passe entre plusieurs appareils*
- *Il permet l'importation / exportation de données dans de nombreux formats*
- *Il permet la saisie automatique des logins / mots de passe dans les différents logiciels*
- *Il permet la recherche et le tri avancé*
- *Il comporte un nombre de plug-ins conséquent*

## Sommaire

- 1) Elément déployé.
- 2) Où est stockée la base de données contenant les identifiants/mot de passe.
- 3) Comment s'effectue l'accès aux données de la base de données.
- 4) Comment sécuriser d'avantage l'accès à la base de données.
- 5) Comment le logiciel est utilisé du point de vue utilisateur, en étudiant le cycle de vie d'un mot de passe.
- 6) Comment installer un plug-in de votre choix et l'exploiter.

## 1) • Elément déployé →

- Le logiciel KeePass est un gestionnaire de mot passe fiable et sécurisé, celui-ci sauvegarde l'entièreté de vos mots de passe dans une base de données assurément chiffré (crypté) pouvant également être renforcée en joignant une clé. Celle-ci est seulement accessible via un mot de passe principale ;

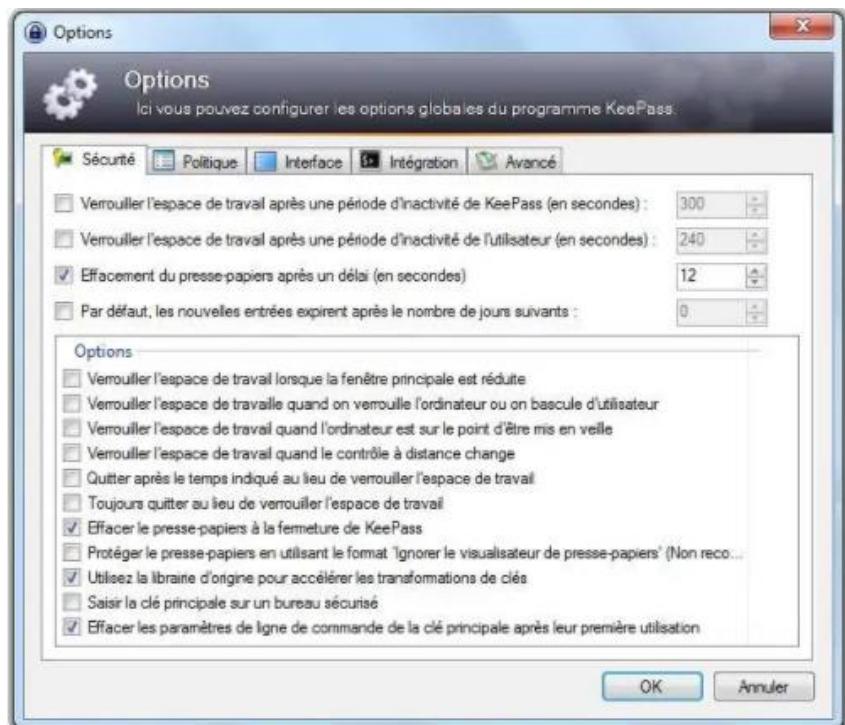
Ce logiciel est disponible sur une multitude de système d'exploitation, mais aussi sur mobile.

## 2) • Ou est stockée la base de données contenant les identifiants/mot de passe →

- La base de données sont des fichier chiffré au format (.kdb) ou (.kdbx) selon la version.

Les bases de données contenant vos mots de passe sont stockée sur un système de fichier crypté en cloud.

Vous avez également à disposition un menu d'options permettant une personnalisation de la sécurité globale du programme KeePass.



### 3) • Comment s'effectue l'accès aux données de la base de données →

- Pour se faire il faut au préalable créer une clé principale composée, là où vous pouvez donc définir le mot de passe principale de votre base de données interpréter précédemment, une estimation de la qualité de celui-ci est disponible.

Une feuille de secours est à disposition, elle doit être imprimée, remplie et par la suite stockée en lieu sûr afin d'assurer un accès à votre base de données en cas de problème.



**KeePass**  
**Feuille de secours**

07/02/2018

**Fichier de la base de données:**  
C:\Users\Administrateur\Documents\NouvelleBaseDeDonnées.kdbx

Vous devriez régulièrement créer une sauvegarde du fichier de la base de données (sur un équipement de stockage de données indépendant). Les sauvegardes sont stockées ici :

**Clé principale**  
La clé principale de ce fichier de base de données consiste en les composants suivants :

- **Mot de passe principal:**

**Instructions et informations générales**

- Une feuille de secours de KeePass contient toutes les informations importantes qui sont requises pour ouvrir une base de données. Elle devra être imprimée, remplie et stockée en lieu sûr, où seulement vous et d'autres personnes de confiance auront accès.
- Si vous perdez le fichier de la base de données ou bien tout composant de la clé principale (ou oubliez la composition), toutes les données stockées dans la base de données seront perdues. KeePass ne possède pas de fonctionnalité de commande interne pour la sauvegarde. Il n'y a pas de porte-arrière ou de clé universelle qui pourrait ouvrir votre base de données.
- La dernière version de KeePass peut être trouvée sur le site Web de KeePass: <https://keepass.info/>.

## 4) • Comment sécuriser davantage l'accès à la base de données →

- Différentes méthodes sont possible afin de renforcer et de sécuriser davantage l'accès à la base de données. Pour commencer deux types **d'algorithmes de chiffrement** sont possible, ce sont actuellement les meilleurs sur le marché pour tout usage, particulier ou bien professionnel :

-> AES (clé de 256 bits)

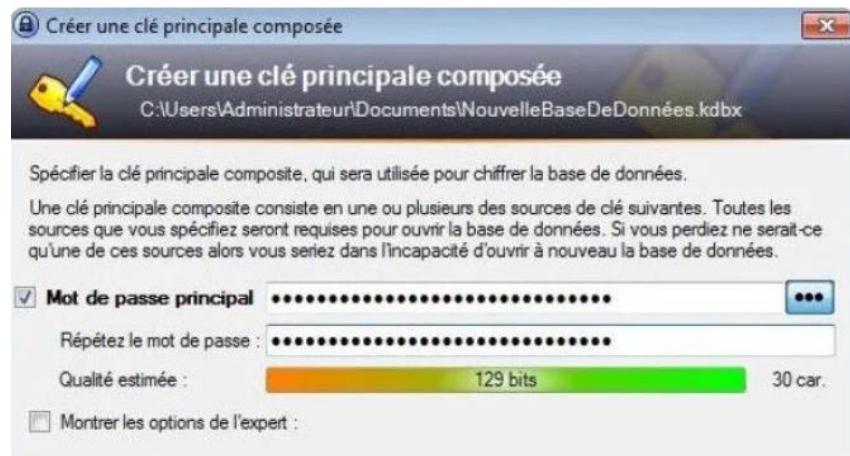
-> TwoFish (clé de 256 bits + bloc de 128 bits)

Evidemment il est recommandé de s'assurer de la non présence de keylogger positionné sur votre système, ou de la présence de logiciels tiers malveillants. Pour ce faire le logiciel **Adware** ou **Spybot Search and Destroy** permet un nettoyage de ces possibles malwares.

Le meilleur des méthodes reste de s'assurer d'avoir en sa possession un mot de passe avec une **sécurité complexe et forte**.

## 5) • Comment le logiciel est utilisé du point de vue utilisateur, en étudiant le cycle de vie d'un mot de passe →

- 1<sup>ère</sup> étape : *La création d'un mot de passe dans KeePass :*

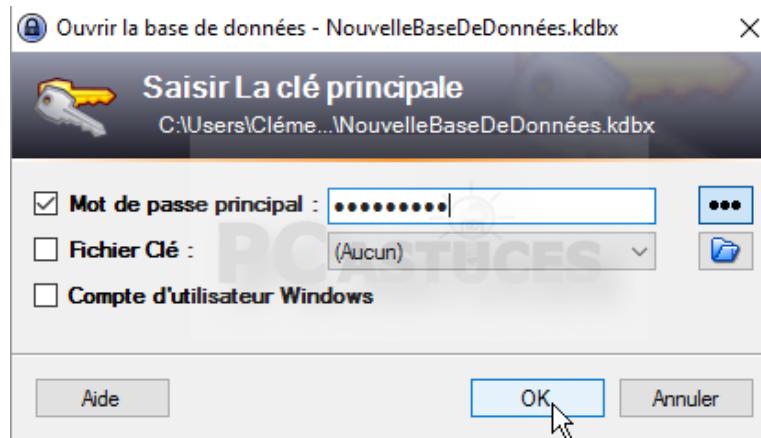


Pour commencer il est important de créer sa base de données et de déterminer son mot de passe principal. Le moyen le plus fiable pour obtenir un mot de passe sécurisé est d'utiliser une phrase longue au hasard qui n'a pas de lien direct avec vous ou votre quotidien.

- 2<sup>ème</sup> étape : Utilisation d'un mot de passe stocké dans KeePass, dans un autre logiciel (par exemple dans Firefox) :



L'installation du Plug-in KeeFox sur le moteur de recherche Firefox est nécessaire afin d'utiliser et de pouvoir accéder à sa base de données.



Par la suite l'accès à KeePass est disponible, ainsi nous pouvons entrer notre mot de passe principale pour avoir accès à notre base de données.

**Se connecter**

**Pseudo / E-mail**  
cjoathon

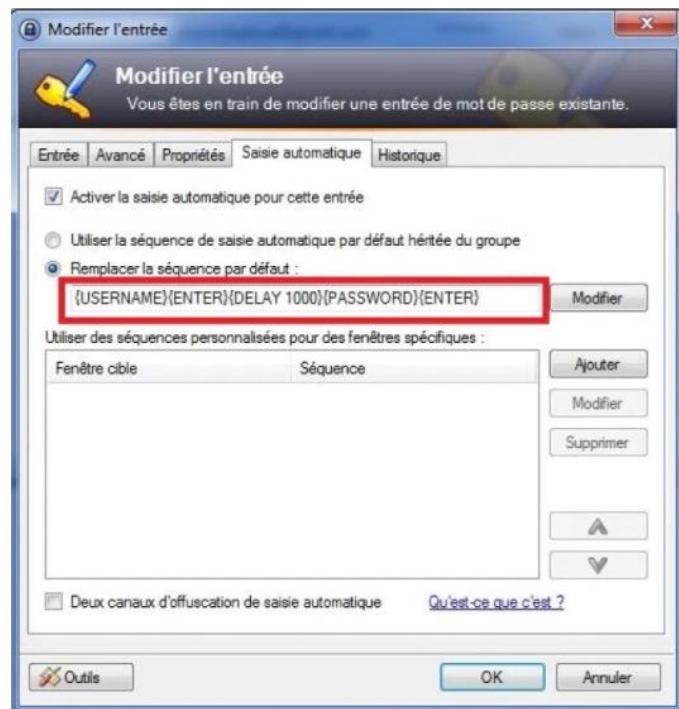
**Mot de passe**  
\*\*\*\*\*

Rester connecté **Connexion**

[Problème de connexion ?](#)

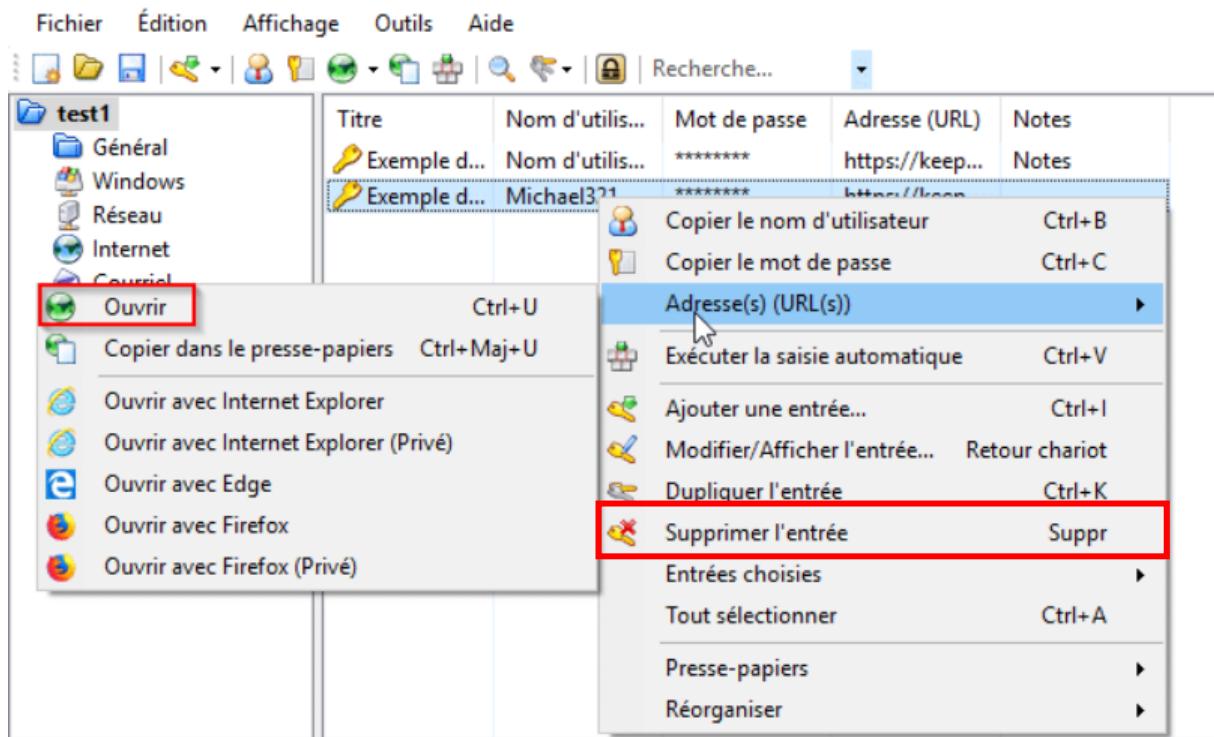
KeeFox détecte ainsi automatiquement les champs de formulaire de connexion sur les sites où les identifiants sont enregistrés dans KeePass, il rentre donc de lui-même vos informations de connexions.

- 3<sup>ème</sup> étape : Modification d'un mot de passe dans KeePass :



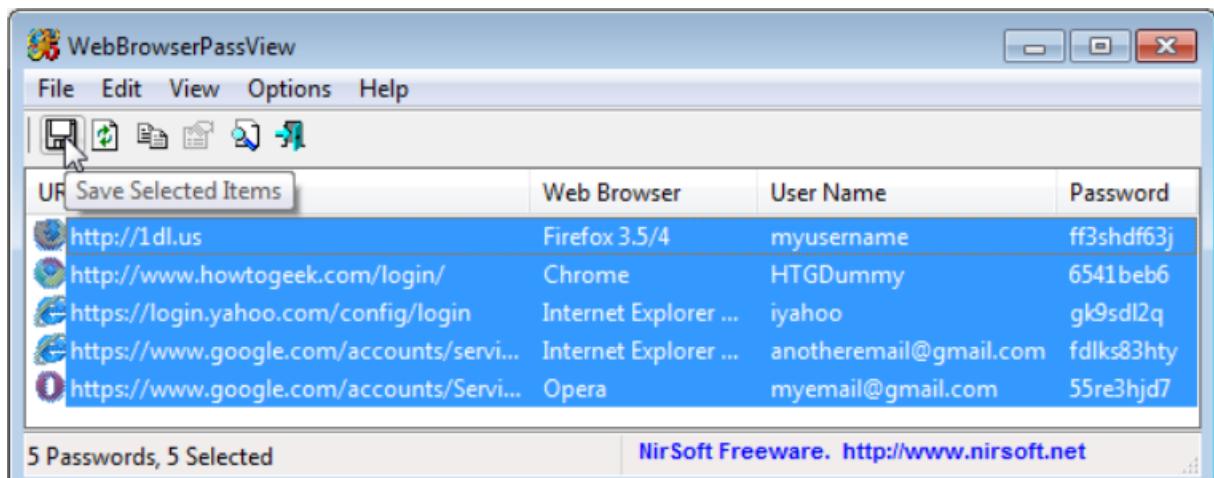
En cas d'une fuite de donnée, ou une demande de renouvellement de mot de passe automatiquement demander par KeePass. Il est donc préférable de se rendre dans l'onglet pour modifier l'entrée de ou des mots de passe concernés.

- 4<sup>ème</sup> étape : Suppression de mot de passe dans KeePass :

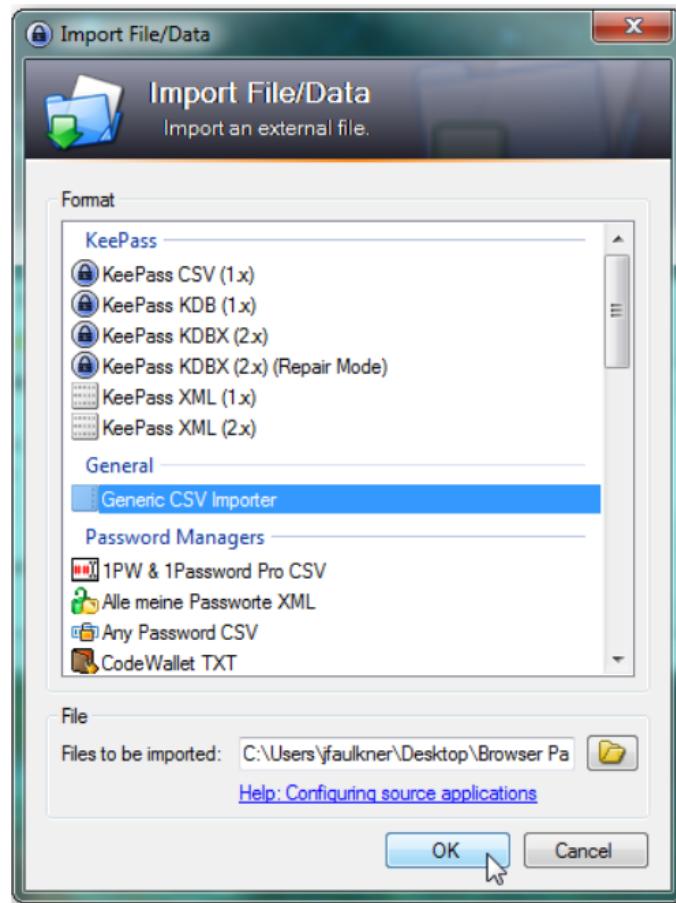


Une fois sur le gestionnaire KeePass, la modification de tous les mots de passe est possible. Il faut donc choisir l'entrée concerné puis sélectionner « Supprimer l'entrée ». (Encadré en rouge).

- 5<sup>ème</sup> étape : importation d'identifiants à partir de logiciel tiers, dans la base de données Keepass :



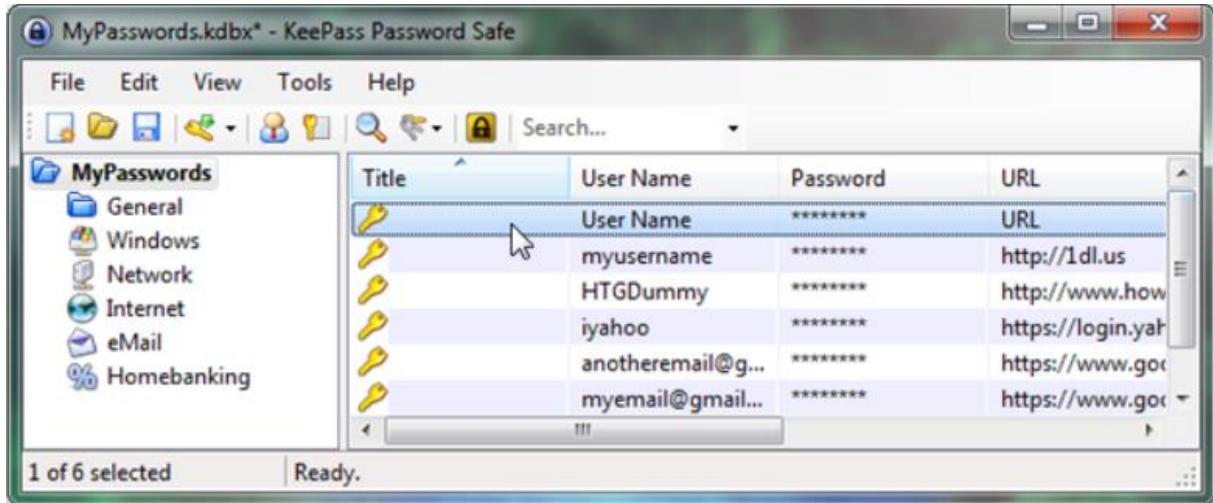
Le logiciel WebBrowserPassView permet de faciliter cette manipulation, ce dernier récupère directement vos identifiants et mots de passe étant enregistré sur les moteurs de recherches.



Par la suite vous pourrez enregistrer le travail effectué du logiciel en fichier CSV, fichier qu'il est possible d'importer dans la base de données de KeePass.

Imported entries preview:						Refresh
Title	User Name	Password	URL	Notes	Custom 1	
User Name						
myusername		ff3ehdf63j	http://1d1.us			
HTGDummy		6541beb6	http://www.howtoge...			
@yahoo		gk9edl2q	https://login.yahoo.c...			
anotheremail@gmail....		fdiks83hty	https://www.google....			
myemail@gmail.com		55re3hjd7	https://www.google....			

Une fois le fichier importé une boîte de dialogue s'ouvre effectuant ainsi la prise en compte et la récupération des identifiants dans KeePass.

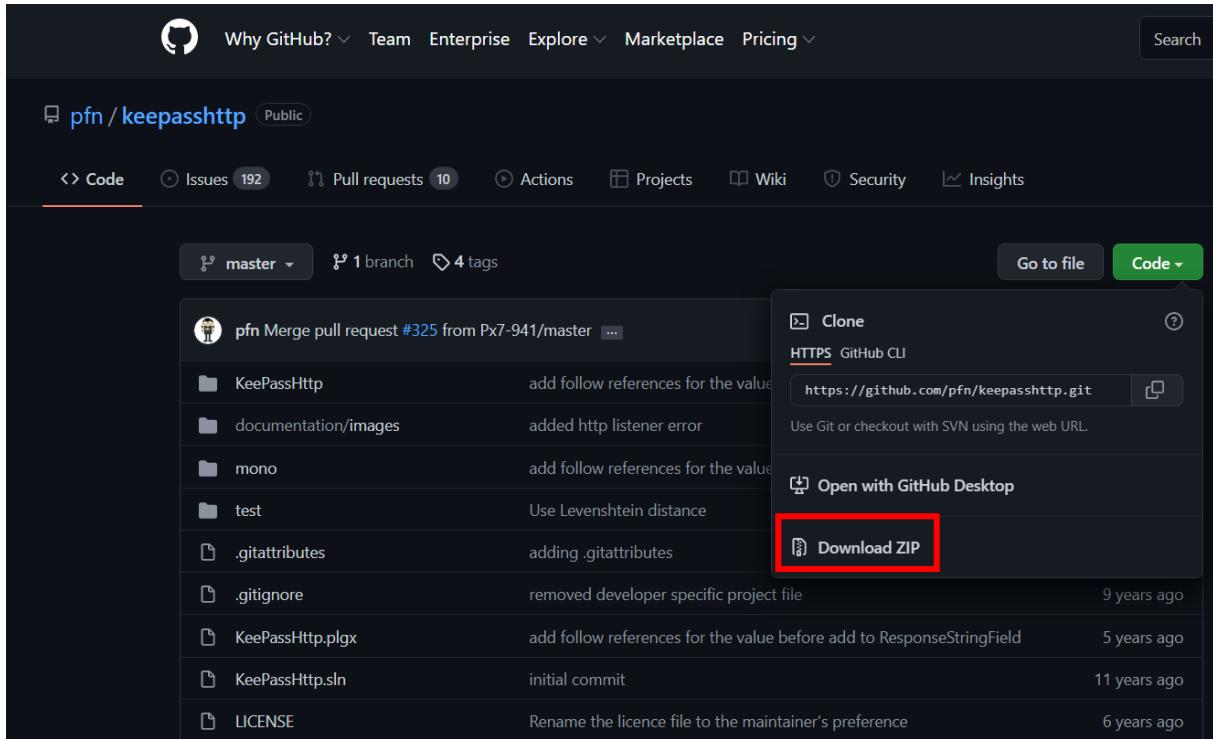


Une fois terminé KeePass à donc enregistré tout les identifiants et mots de passe présent dans le fichier **CSV**, KeePass connaît donc les informations de connexions à vos comptes enregistré sur le moteur de recherche.

## 6) • Comment installer un plug-in de votre choix et l'exploiter →

Category	Plugin Name	Description
Integration & Transfer	<a href="#">KeeForm</a>	Opens websites and fills in the login data automatically.
	<a href="#">Kee</a>	Bridges between KeePass and web browsers.
	<a href="#">Passafari</a>	Integrates KeePass and the Safari browser.
	<a href="#">KPFloatingPanel</a>	Displays an always on top KeePass floating panel.
	<a href="#">KeePassHelper</a>	Browser extension that retrieves credentials from KeePass.
	<a href="#">KeeOTP</a>	Generates TOTP/P/OTP authentication codes.
	<a href="#">KeeTrayTOTP</a>	Generates TOTP authentication codes.
	<a href="#">TwoFactorQRCodeReader</a>	Creates 2FA placeholder parameters from QR codes or OTP URLs.
	<a href="#">Character Copy</a>	Allows copying individual characters from entry strings.
	<a href="#">Password Change Assistant</a>	Helps to change passwords.
Import	<a href="#">1P2KeePass</a>	Imports 1Password 1P1F files.
	<a href="#">AnyPassword Import</a>	Imports CSV files reported by 'AnyPassword'.
	<a href="#">CardFileKeePass</a>	Imports CRD files created by 'Cardfile'.
	<a href="#">CodeWallet 3 Import</a>	Imports TXT files exported by 'CodeWallet 3'.
	<a href="#">CodeWallet 6 Konverter</a>	Converts TXT files exported by 'CodeWallet 6' to importable CSV files.
	<a href="#">eWallet Import</a>	Imports TXT files exported by 'eWallet'.
	<a href="#">eWallet Data Import</a>	Export data from 'eWallet' and import it into KeePass.
	<a href="#">eWallet Data Liberator</a>	Export data from 'eWallet' and import it into KeePass.
	<a href="#">eWallet2KeePass</a>	Migrates 'eWallet' data to KeePass.
	<a href="#">KeePassBrowserImporter</a>	Imports credentials from various browsers.
Backup	<a href="#">KeePassIrefoxImporter</a>	Imports credentials from Firefox.
	<a href="#">MSDN/TechNet Key Importer</a>	Imports MSDN/TechNet key files.
	<a href="#">OnePif</a>	Imports 1Password 1P1F files.
	<a href="#">OneVault</a>	Imports 1Password OPVault files.
	<a href="#">Oubliette Import</a>	Imports Oubliette password database files.
	<a href="#">Passcommand Import</a>	Imports Password Commander CSV files.
	<a href="#">Password Minder Import</a>	Imports Password Minder data.
	<a href="#">PINs Import</a>	Imports text files exported by 'PINs'.
	<a href="#">PwSafeDBImport</a>	Directs import Password Safe database files.
	<a href="#">SafeInCloudImport</a>	Imports SafeInCloud XML files.
I/O & Synchronization	<a href="#">SpnImport</a>	Imports Steganos Password Manager files.
	<a href="#">VariousImport</a>	Imports several different file formats.
	<a href="#">Vault3Importer</a>	Imports Vault3 XML files.
	<a href="#">VaultSyncPlugin</a>	Imports HashiCorp Vault data.
	<a href="#">AdvancedConnect</a>	Allows to specify applications for direct connections.
	<a href="#">Breach/Leak Checkers</a>	Check entries against breach lists.
	<a href="#">ColoredPassword</a>	Allows to define colors for password characters.
	<a href="#">Custom Icon Dashboard</a>	Statistics and management features for custom icons.
	<a href="#">DataBaseReorder</a>	Reorders groups alphabetically.
	<a href="#">GlobalSearch</a>	Allows searching in all open databases at once.
<a href="#">GroupColumn</a>	Provides a column showing the group of an entry.	
Utilities	<a href="#">AdvancedConnect</a>	Allows to specify applications for direct connections.
	<a href="#">Breach/Leak Checkers</a>	Check entries against breach lists.
	<a href="#">ColoredPassword</a>	Allows to define colors for password characters.
	<a href="#">Custom Icon Dashboard</a>	Statistics and management features for custom icons.
	<a href="#">DataBaseReorder</a>	Reorders groups alphabetically.
	<a href="#">GlobalSearch</a>	Allows searching in all open databases at once.
	<a href="#">GroupColumn</a>	Provides a column showing the group of an entry.
	<a href="#">KeeAgent</a>	Adds SSH agent support to KeePass.
	<a href="#">KeePassRest</a>	Allows KeePass to supply credentials via REST.
	<a href="#">KeePassRPC</a>	Allows KeePass to supply credentials via RPC.
<a href="#">KeePassHttp</a>	Allows KeePass to supply credentials via HTTP.	
<a href="#">KeePassCommander</a>	Allows KeePass to supply credentials via named pipes.	
<a href="#">KeePassNatMsg</a>	Allows KeePass to supply credentials via Native Messaging.	
<a href="#">Remote Desktop Manager Plugin</a>	Allows KeePass to supply credentials to Remote Desktop Manager.	

Un site web de **KeePass** propose une grande liste de plug-in disponible au téléchargement afin de le ou les ajoutés à votre logiciel.



Code Issues 192 Pull requests 10 Actions Projects Wiki Security Insights

master 1 branch 4 tags

pfn Merge pull request #325 from Px7-941/master ...

KeePassHttp add follow references for the value  
documentation/images added http listener error  
mono add follow references for the value  
test Use Levenshtein distance  
.gitattributes adding .gitattributes  
.gitignore removed developer specific project file  
KeePassHttp.plgx add follow references for the value before add to ResponseStringField  
KeePassHttp.sln initial commit  
LICENSE Rename the licence file to the maintainer's preference

HTTPS GitHub CLI  
https://github.com/pfn/keepasshttp.git

Use Git or checkout with SVN using the web URL.

Open with GitHub Desktop

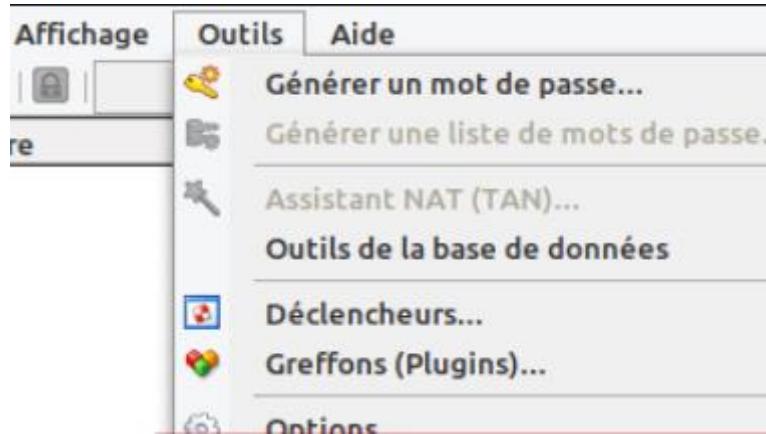
Download ZIP

Prenons l'exemple du plug-in KeePassHTTP, une fois sur la page de celui-ci, il faut donc installer le fichier zip.

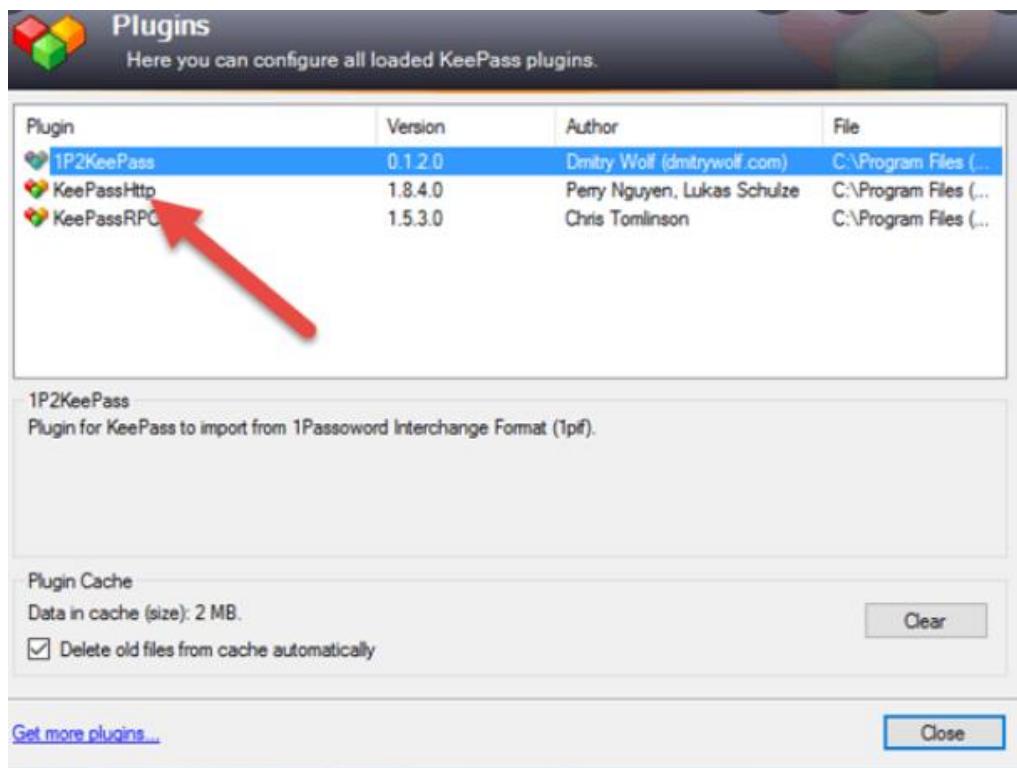
Nom	taille	Compressé	type
..			Dossier de fichier
test			Dossier de fichier
mono			Dossier de fichier
KeePassHttp			Dossier de fichier
documentation			Dossier de fichier
update-version.txt	24	24	Document texte
README.md	17 740	6 272	Fichier source MD
logo.png	54 308	54 308	Fichier PNG
LICENSE	35 147	12 119	Fichier
latest-version.txt	24	24	Document texte
KeePassHttp.sln	927	363	Fichier SLN
KeePassHttp.plgx	160 836	159 931	Fichier PLGX
build.bat	610	347	Fichier de commandes
.gitignore	111	90	Fichier source Git
.gitattributes	14	14	Fichier source Git

Une fois téléchargé, il faut donc extraire le fichier puis se rendre dans les dossiers afin d'exécuter le fichier nommé « build.bat ».

Par la suite un fichier est généré « KeePassHttp.plgx », il faut donc le copié afin de le collé dans le dossier plug-in du logiciel KeePass que vous trouverez par ce chemin : C:\Program Files (x86)\KeePass Password Safe 2\ Plugins.



Pour finaliser la manipulation, rendez-vous sur le logiciel KeePass et dans outils sélectionner **Greffons (Plugins)**.



Ici vous observer donc que le plugin **KeePassHttp** est bien pris en compte par le logiciel.

## Comment utiliser le plugin KeePassHttp ?

- 1) Cliquez sur *Outils*, puis sur **KeePassHttp Options....**  
Une nouvelle fenêtre s'ouvre, cliquez sur l'onglet *Advanced*.
- 2) Cochez les cases **Always allow access to entries** et **Always allow updating entries**.  
Cliquez ensuite sur **Save**.
- 3) Vous devez installer une extension à votre navigateur :
  - Pour Google Chrome : [ChromelPass](#)
  - Pour Firefox : [PasslFox](#)  
(Ajouter l'extension à votre navigateur.)
- 4) Cliquez sur l'icône de Keepass puis sur **Connect**.
- 5) Indiquez un nom de votre clé, (vous pouvez indiquer ce que souhaitez).  
Cliquez ensuite sur **Save**.
- 6) Allez sur un site que vous avez enregistré dans votre base de registre.  
Vous pouvez voir que les champs *utilisateur* et *mot de passe* sont automatiquement remplis.  
Cliquez sur **OK** pour vous connectez.