

# Tutoriel KEEPASS

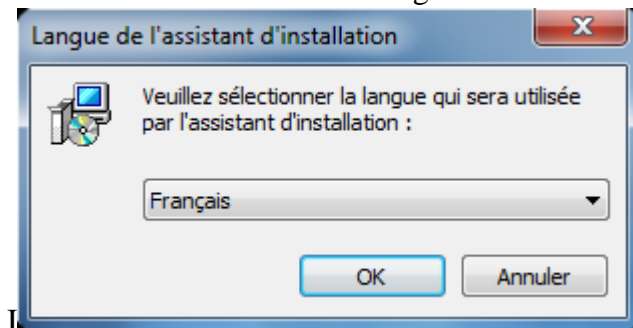
Téléchargez l'exécutable de Keepass (disponible pour Unix et Windows). Nous choisirons ici la version professionnelle 2.x. Une fois le fichier sur votre bureau, exécutez-le par un double clic.

**Nota :** Pour mettre KEEPASS en français, téléchargez et placez le fichier "French.Ingx " dans le répertoire d'installation de Keepass (par défaut dans "C:Program Files (x86)KeePass Password Safe 2").

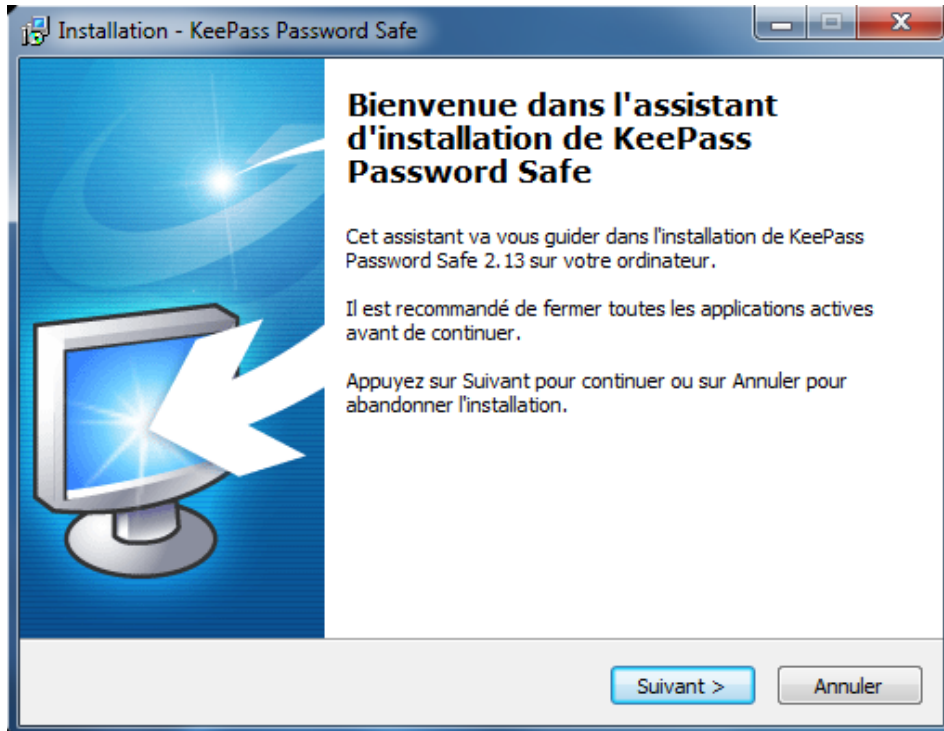
Ouvrez KeepPass puis allez dans le menu Affichage et sélectionnez "Modifier la langue", choisissez French et validez. Relancer KeepPass pour qu'il s'affiche en français.

Voici les étapes d'installations :

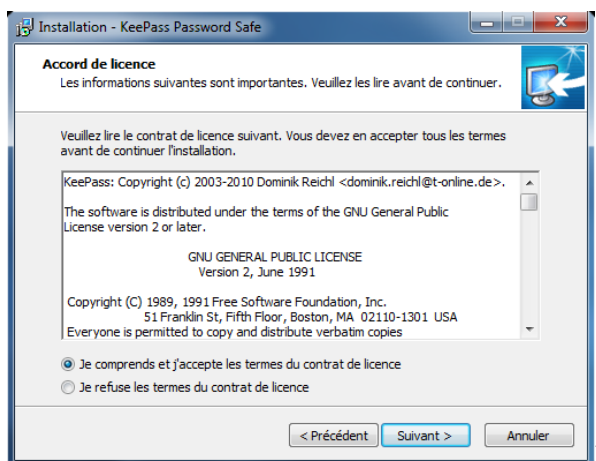
ETAPE 1 : Choisissez votre langue d'installation et cliquez sur « OK »



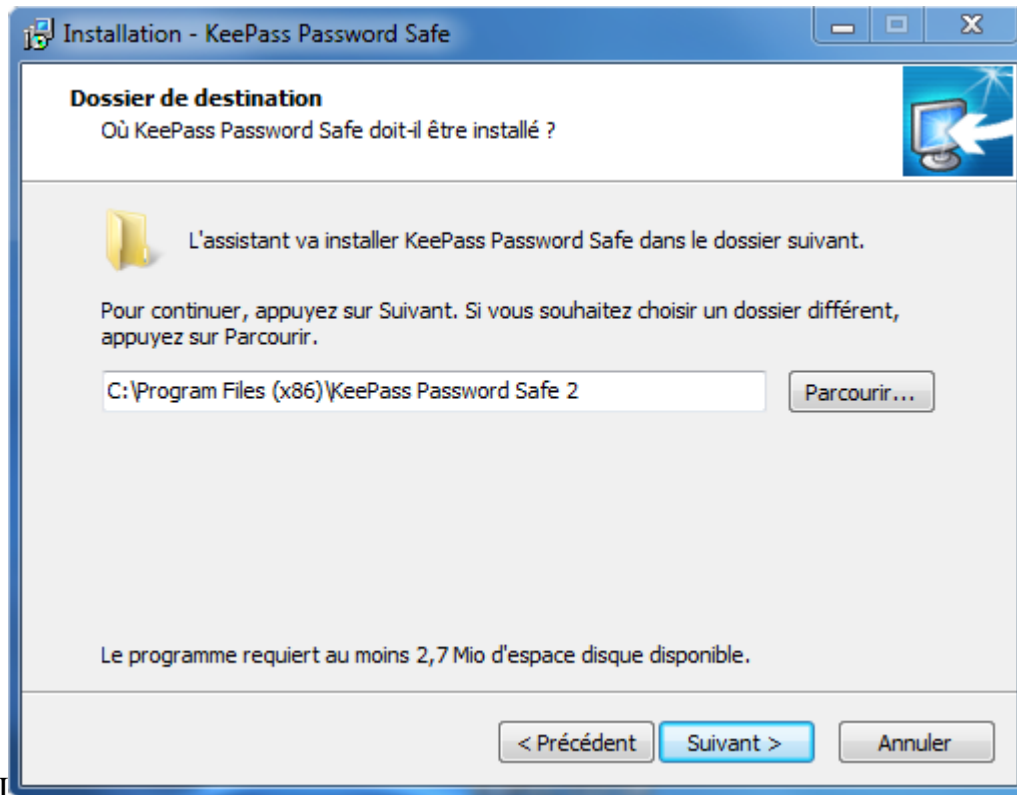
ETAPE 2 : Cliquez sur « Suivant »



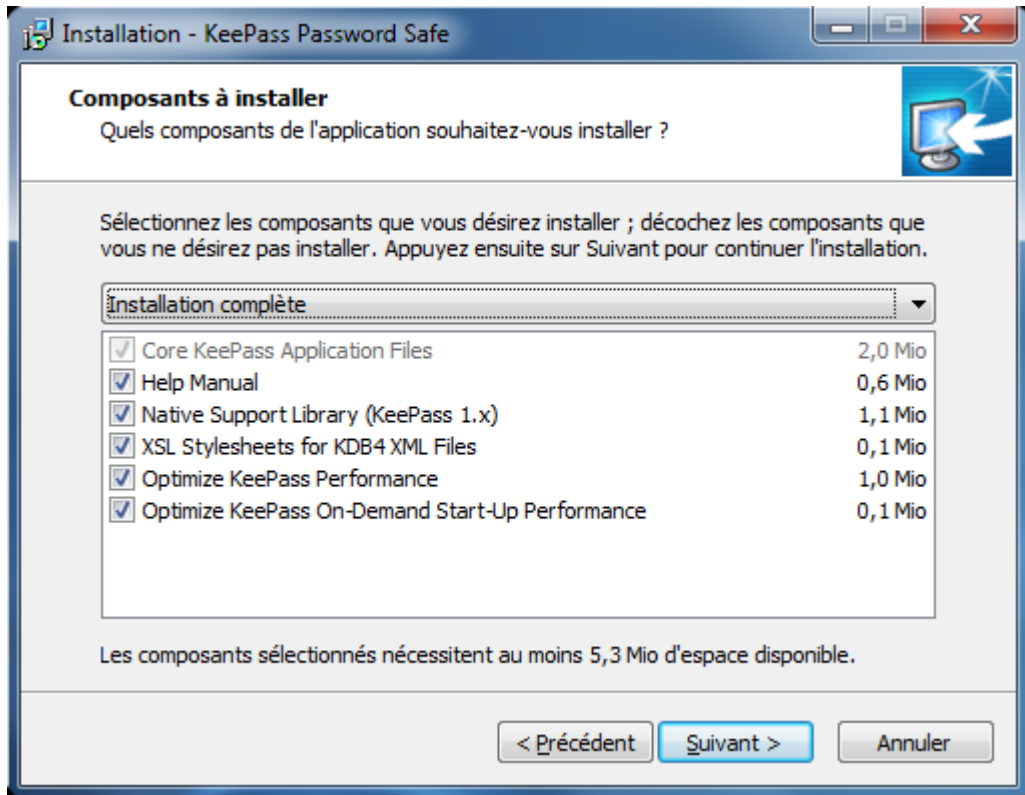
ETAPE 3 : Acceptez les termes du contrat de licence puis cliquez sur « Suivant »



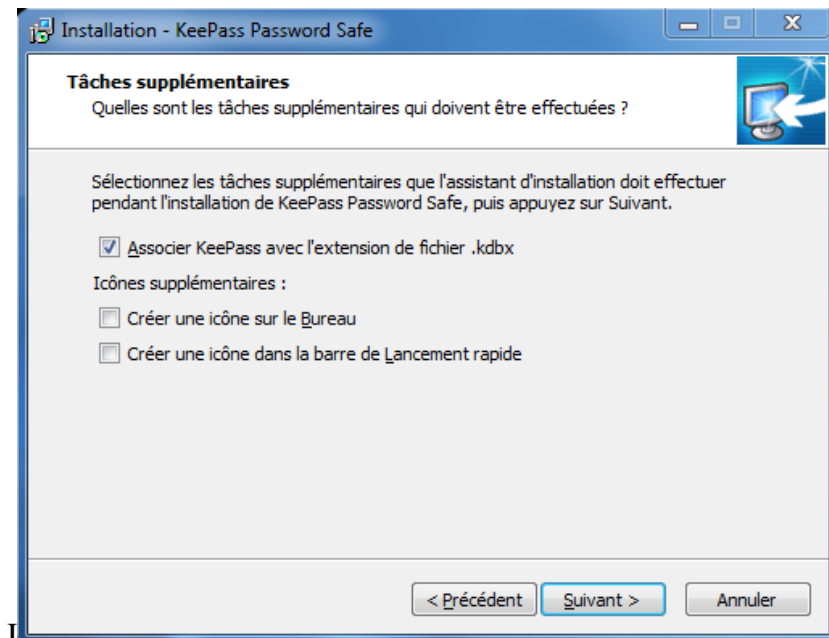
ETAPE 4 : Choisissez l'emplacement du programme sur le disque puis cliquez sur « Suivant »



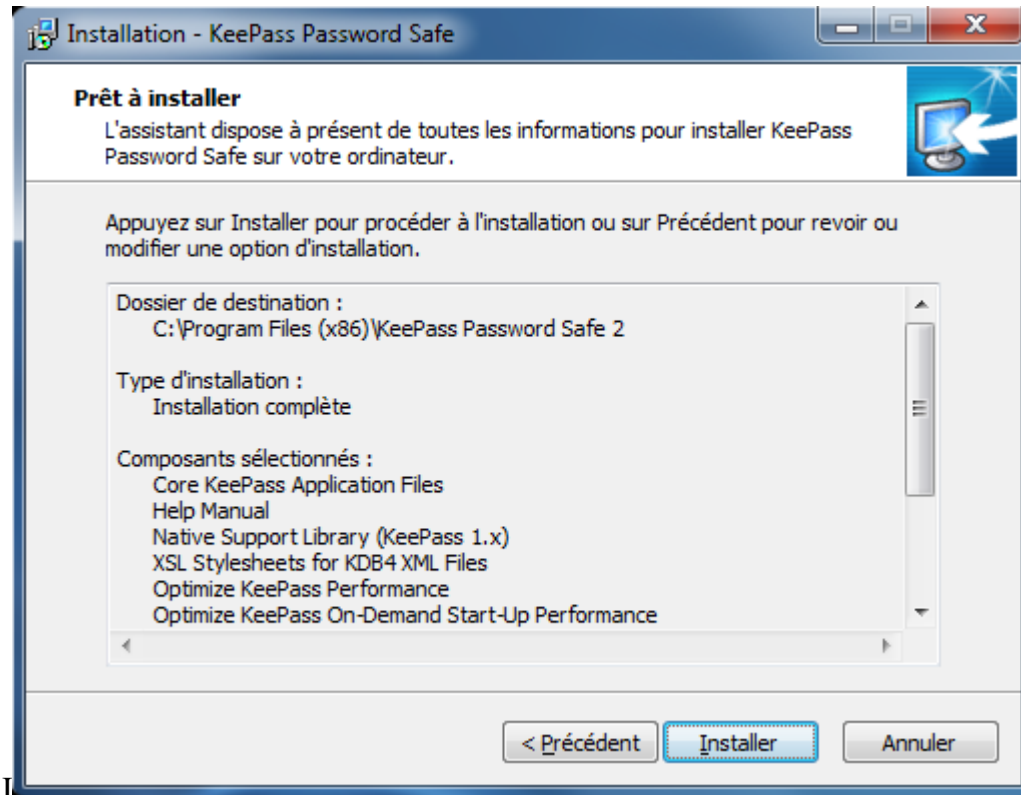
ETAPE 5 : Choisissez l'installation complète puis cliquez sur « Suivant »



ETAPE 6 : Choisissez les icônes de bureau puis cliquez sur « Suivant »



ETAPE 7 : Cliquez sur « Installer » pour confirmer l'installation.



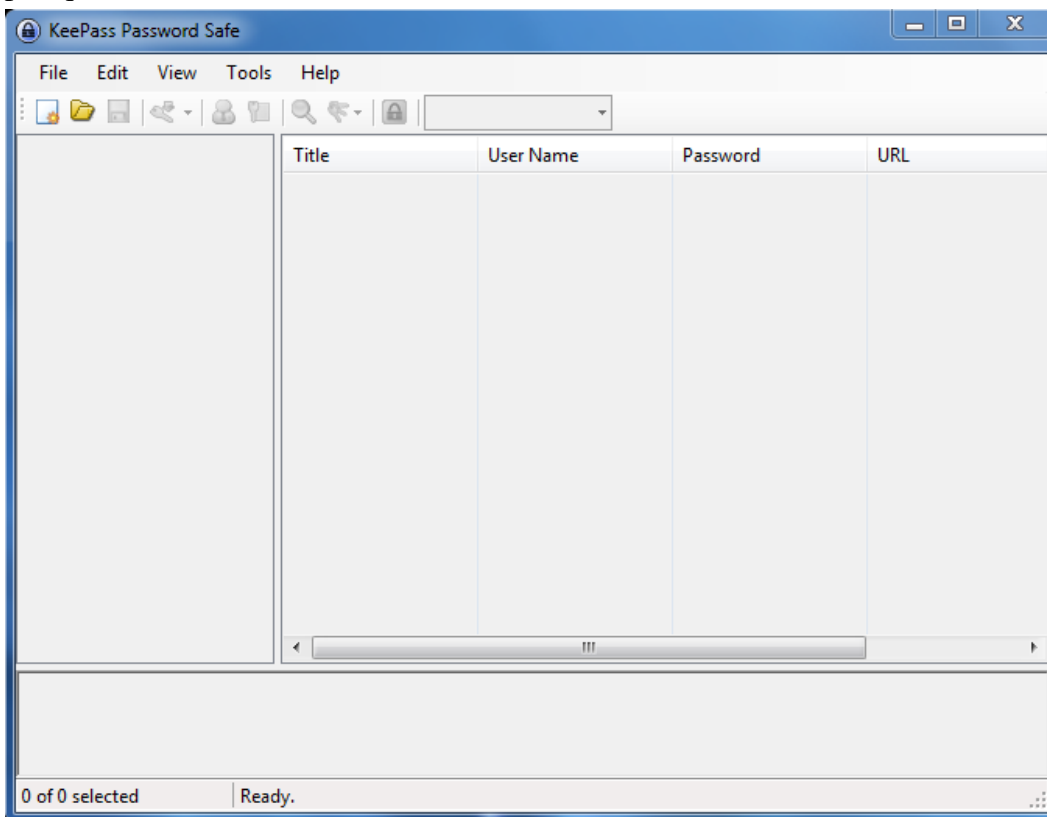
ETAPE 8 : Cliquez sur « Finish » pour démarrer KeePass maintenant.



L'installation de KeePass est maintenant terminée. Vous pouvez maintenant lancer le programme.

## Interface de KeePass et première configuration

Vous voilà sur l'interface principale de KeePass. Pour l'instant, tout est grisé ou presque et votre interface devrait ressembler à ceci :



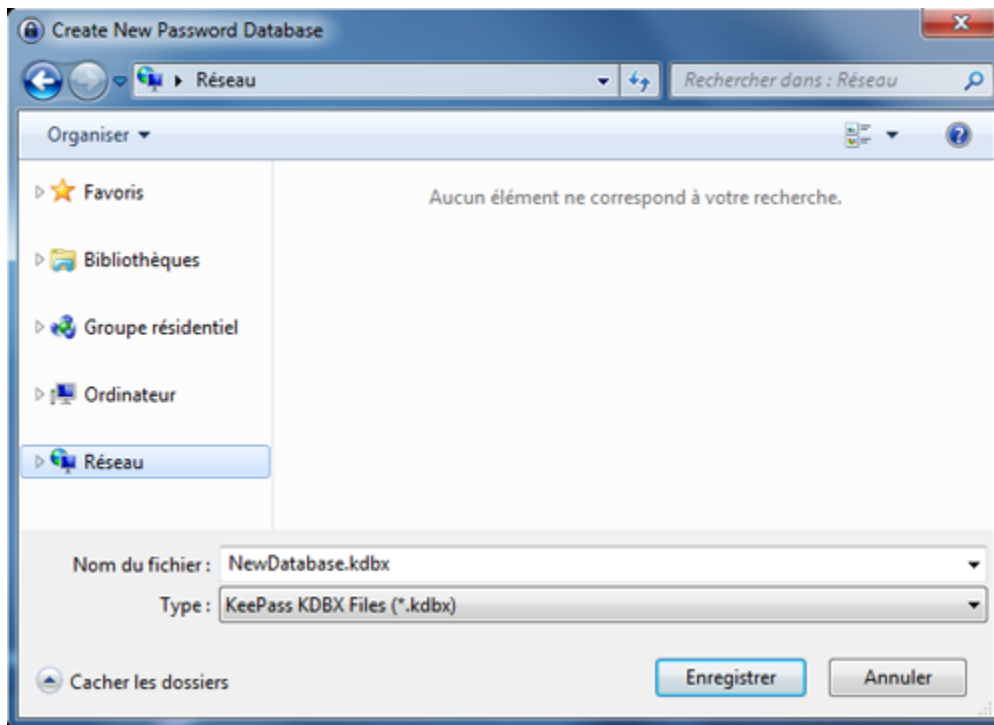
Pour commencer, nous allons devoir créer une nouvelle base de données de mots de passe dans laquelle nous allons stocker ceux-ci. Cliquez sur « New » en haut à droite de l'interface :



Vous devrez alors choisir l'emplacement du fichier de la base de données. Typiquement, vous pouvez la laisser dans « Mes documents » spécifié par défaut ou choisir un emplacement de votre choix. Une fois choisi, cliquez sur «

Enregistrer » pour valider.

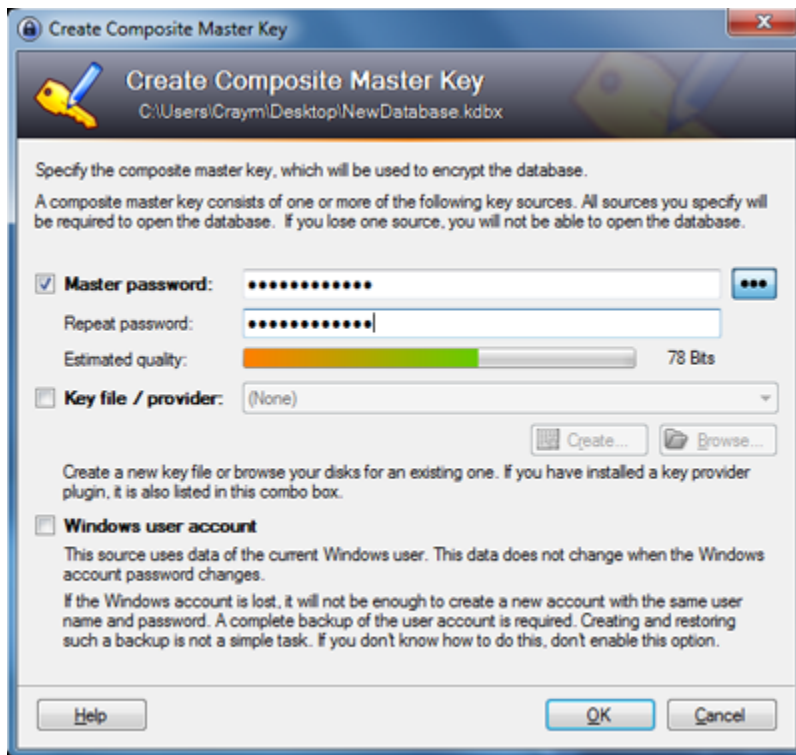
Emplacement base de données KeePass



Vous devez alors choisir votre UNIQUE mot de passe à retenir. Notez le bien car une fois perdu, un retour n'est pas possible et il n'y a aucun moyen de le retrouver. Néanmoins, un seul mot de passe, c'est vraiment simple à retenir ! Vous pouvez aussi créer un mot de passe à partir de votre compte windows actuel mais si vous changez plus tard de mot de passe, celui de KeePass ne changera pas... Il est donc conseillé de choisir un nouveau « Master Password ».

Une barre vous indiquera le niveau de force de votre mot de passe. Plus celui-ci est élevé, mieux c'est. Choisissez typiquement un mot de passe d'au moins 10 caractères avec des chiffres (1,2,3,...,9,0), des MAJUSCULES et des caractères spéciaux (%\$#"... etc.). Vous constaterez que si vous utilisez ceux-ci, le mot de passe gagne bien plus en force qu'avec de simple caractères !

## Choix de la master Key Keepass



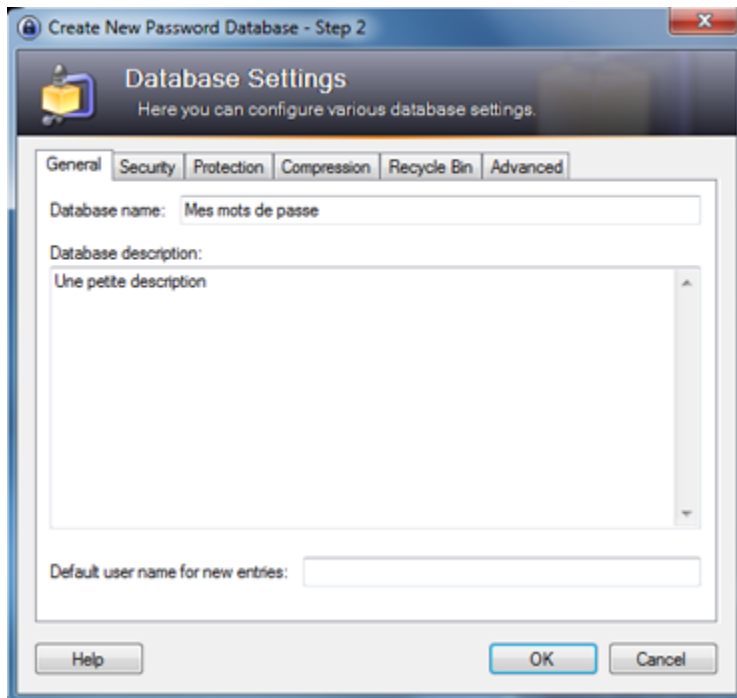
Une fois validé, vous accédez à la configuration avancé de votre base de données. Donnez lui tout d'abord un nom puis vous pouvez lui ajouter une petite description si vous souhaitez en créer plusieurs pour vous y retrouver. Cliquez ensuite sur l'onglet « Security » comme dans l'image ci-dessous pour accéder au paramètre de sécurité.

Pour rendre une attaque sur votre base de données plus difficile, vous pouvez ajouter une constante de temps d'environ une seconde qui se base sur les performances de votre ordinateur. Typiquement, les mots de passes subiront, par défaut ici sur l'image 6000, des transformations en boucle avant d'être cryptés. Cela rend le décryptage très complexe et protège d'autant mieux vos codes. Pour évaluer cette constante, cliquez simplement sur « 1 second delay » en dessous du champ « 6000 ». La nouvelle valeur viendra alors s'inscrire toute seule dans ce champ.

Si vous le souhaitez, vous pouvez gérer d'autres paramètres avec les autres onglets.

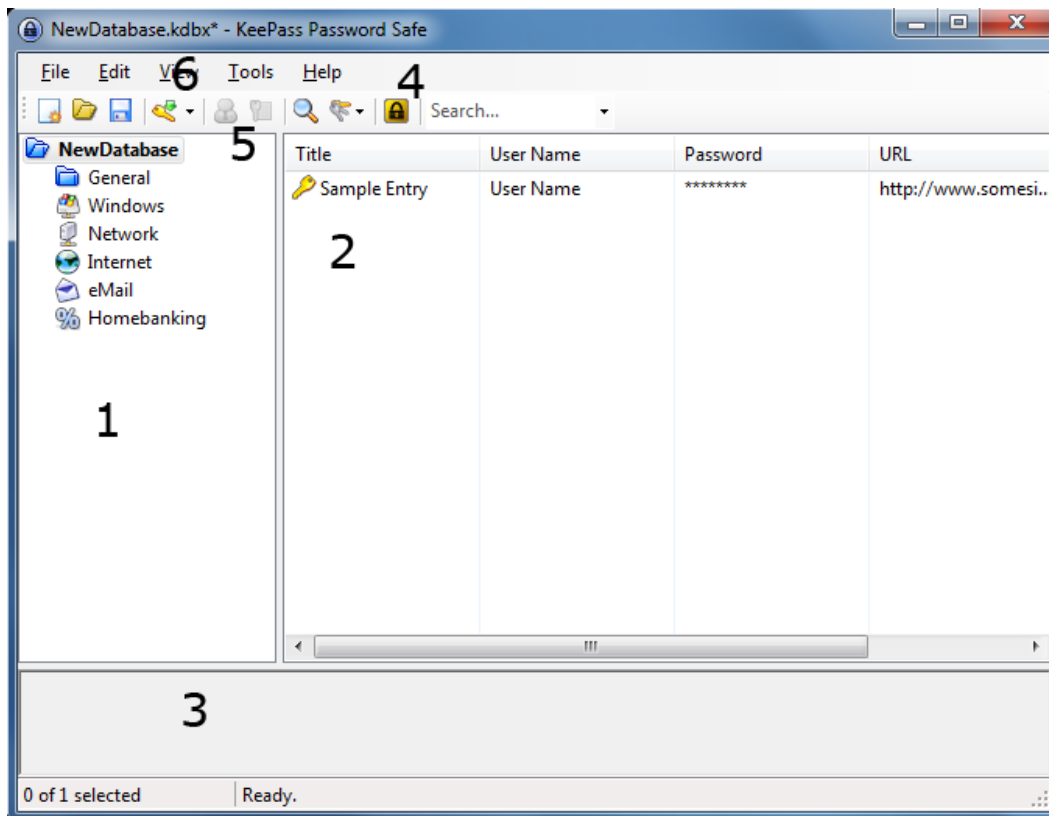
Une fois terminé, cliquez sur « OK » pour valider votre configuration





Vous avez terminé la création de votre base de données de mots de passe !

L'interface est maintenant disponible avec de nombreux éléments. Vous pouvez voir que vous êtes logué sur la base « NewDatabase.kdbx » :



## Interface Keeppass ouvert

L'interface comporte toutes les fonctions essentielles. Voici sa description :

1 - A gauche, avec les petits icones se trouvent des catégories dans lesquelles vous pourrez trier et ranger vos mots de passe par thèmes. Vous pouvez créer, supprimer et modifier les catégories.

2 - Au centre, vous trouvez vos mots de passe actuellement entrés dans la base de données. Vous pouvez y voir figurer le titre de la clef, son nom d'utilisateur, le mot de passe associé et l'URL de la page web correspondante.

3 - Ici se trouve toutes les informations relatives à la clef sélectionné comme le groupe, la date de création, de la dernière utilisation ou modification... etc.

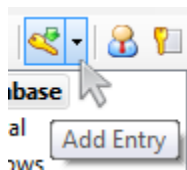
4 - Le petit cadenas juste en dessus de « Title » vous permettra de bloquer votre base de données lorsque vous aurez besoin de vous éloigner de votre machine. Par défaut, Keeppass enregistre et sauvegarde votre base de donnée à chaque lock ou fermeture du programme.

5 - Ces deux petites icônes servent à copier le nom d'utilisateur ou le mot de passe d'une clef sélectionnée dans la base sans avoir à taper quoi que ce soit sur le clavier. Vous n'aurez plus qu'à coller le dans le formulaire.

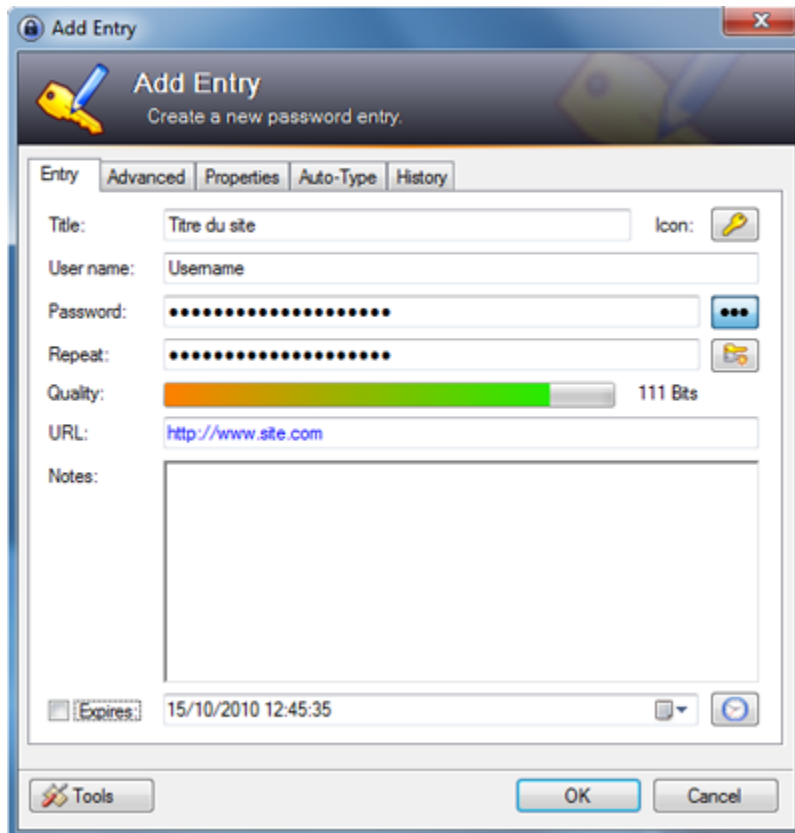
6 - Cette clef avec une flèche verte permettra l'insertion de nouvelles clefs dans la base de données.

## Insertion de clefs

Nous allons maintenant ajouter un premier mot de passe à notre base. Pour cela cliquez sur le bouton « Add Entry » :



Vous obtiendrez alors une fenêtre pour rentrer les paramètres et les mots de passe de la nouvelle clef :



## Création clef KeePass

Dans « Title », entrez le nom de la clef que vous souhaitez enregistrer. Typiquement « Facebook » ou « Banque A » par exemple.

« Username » est le nom associé à votre mot de passe. Très souvent, ce champ est en fait votre pseudo.

« Password » est implicite. Notez que vous pouvez l'afficher en clair en cliquant sur les 3 points à droite. La petite clef à droite permet quant à elle de générer un mot de passe via un générateur (détaillé plus bas)

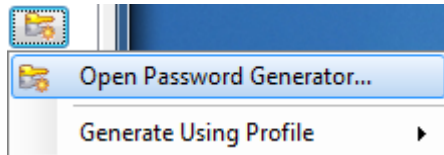
« URL » est assez important car elle permettra d'utiliser l'auto-complétion une fois que l'on aura installé le plug-in Keyfox pour KeePass.

Une fois votre mot de passe entré, vous pouvez le valider en cliquant sur « OK ».

Vous avez terminé d'ajouter votre premier mot de passe ! Celui-ci apparaît alors dans l'interface en dessous de la première clef que l'on voit sur l'image plus haut.

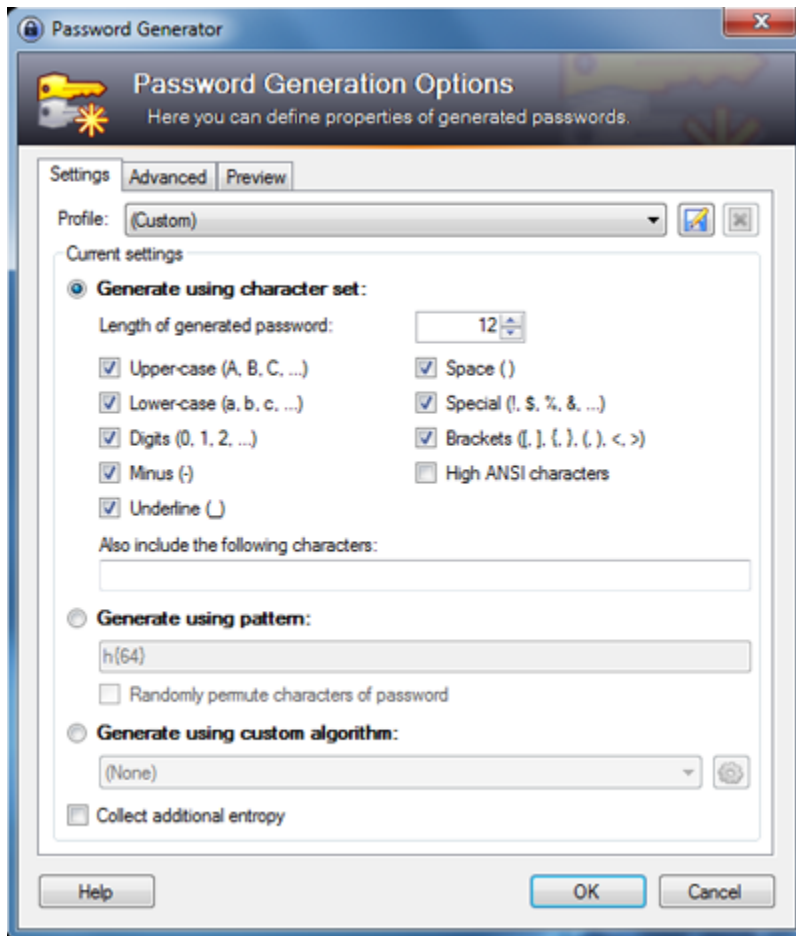
## Password Générateur

Retournons rapidement sur le générateur de mot de passe :



Générateur de mot de passe Keepass

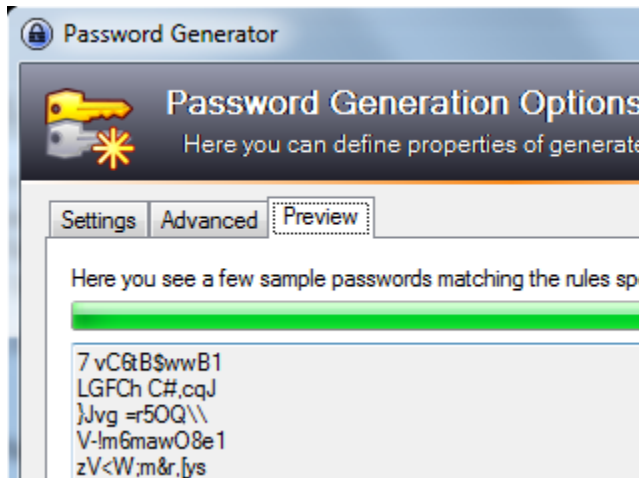
C'est la petite clef à côté de la confirmation comme sur l'image ci-dessus. Il ressemble à ceci :



## Mot de passe généré avec keepass

Pour générer un mot de passe puissant mais toujours quelque peu lisible (dans la mesure du possible), sélectionnez tous les cases comme sur l'image ci-dessus. Cela correspond à toutes les touches que l'on peut taper sur un clavier classique. Vous pouvez aussi choisir la longueur du mot de passe qui ici a été fixé à 12.

Une fois fait, vous pouvez obtenir une preview des mots de passe en cliquant en haut dans l'onglet correspondant. Vous obtiendrez quelque chose comme ceci :



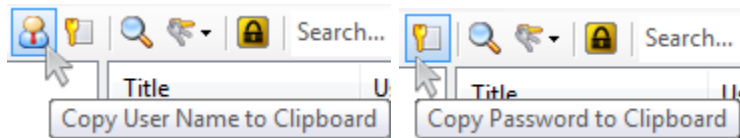
Vous pouvez voir que de nombreux mots de passe ont été générés. Vous pouvez en copier un et l'utiliser comme mot de passe, sinon cliquez simplement sur « Valider » pour que Keefox choisisse lui-même un mot de passe et vous l'ajoute à votre clef. Comme c'est lui qui va vous donner vos mots de passe lorsque vous en aurez besoin, il n'y a aucune raison, excepté par curiosité, ni de le voir, ni de le retenir non plus. Vous avez seulement besoin de vous assurer qu'il est assez puissant pour être très difficilement crackable par un hacker ce que vous avez fait en choisissant les paramètres comme dans l'image.

Notez que vous pouvez générer toute une quantité de mot de passe qui ont tous de grandes qualités de sécurité. Amusez-vous à explorer un petit peu ce générateur qui est très bien fait.

### Utiliser une clef

Une fois que vous avez enregistré vos mots de passe, vous souhaitez bien sûr pouvoir vous en servir. Pour cela, rien de plus simple, tout le travail a déjà été effectué en amont ! Sélectionnez simplement la clef dont vous voudriez copier l'utilisateur ou le mot de passe.

Cliquez alors sur une des deux icônes illustrées ci-dessous pour copier respectivement l'username ou le password.



Copy username KeePass Copy password KeePass

Il vous suffira alors de coller votre mot de passe / nom d'utilisateur dans votre formulaire de connexion et le tour est joué ! Vous avez entré votre login sans même avoir touché au clavier !

Vous n'aurez alors plus à vous soucier de cette clef pour votre prochaine visite !

KeePass peut être configuré pour soumettre automatiquement les formulaire à votre place. Pour cela, il suffit de cocher les cases correspondantes dans les options de KeePass :

Keefox OptionsOptions Keefox

Vous voilà maintenant en mesure de naviguer rapidement sur le web tout en évitant les problèmes des mots de passe à retenir et à remplir à chaque connexion sur vos sites préférés.

Félicitation ! Vous êtes arrivé à la fin de ce tutoriel ! Merci d'avoir pris le temps de nous lire !

<https://craym.eu/tutoriels/utilitaires/keepass.html>