I. OBJET ET DOMAINE D'APPLICATION

Acteurs	Complexité	Statut
Ensemble des utilisateurs Windows du CHU	***	[nouveau / ~~exécuté~~]

Ce document a pour but d'expliquer l'utilisation du logiciel KeePass pour une gestion des mots de passe sécurisée et conforme à la politique de l'établissement.

II. DÉFINITIONS ET ABRÉVIATIONS

II.1 DEFINITIONS

KeePass
Vidéos de tutoriels sur Epione
https://epione-simusante.fr/ecampus/mod/page/view.php?id=16842

Site d'information francophone :
https://keepass.fr/

C'est un logiciel de gestion des mots de passe, gratuit. **Il permet de sauvegarder vos identifiants et mots de passe** de manière sécurisée et certifiée par l'ANSSI. Il est déployé à l'échelle nationale dans l'administration publique depuis 2012.

Firefox
https://www.mozilla.org/fr/firefox/new/

C'est un logiciel gratuit de type navigateur internet. De par son niveau de sécurité, il est recommandé par la BSI (équivalent allemand de l'ANSSI).

L'utilisation de KeePass et de Firefox sur vos ordinateurs personnels est également recommandée.

II.2 ABREVIATIONS

ANSSI
https://www.ssi.gouv.fr/
Agence Nationale de la Sécurité des Systèmes d'Information

III. DESCRIPTION

Veiller à rattacher explicitement chaque action à un acteur
Interdiction de mentionner les login/mot de passe (occulter les informations sur les captures d'écran si nécessaire)
Prévoir une étape de contrôle de bon fonctionnement à l'issue de l'opération
Veiller à ce que le résultat de l'opération soit consigné (inscription du résultat en commentaire dans le ticket, accompagné d'une capture d'écran si nécessaire)
Indiquer la marche à suivre en cas d'échec ou d'erreur
Préférer l'utilisation de liens vers un annuaire lorsque des coordonnées doivent être communiquées (escalade, support technique, …)

Table des matières

Pourquoi cette démarche ?

Une personne malveillante en possession de l'un ou de plusieurs de vos mots de passe pourrait l'utiliser pour accéder à des données confidentielles et/ou critiques vous concernant, ou vos collègues, l'établissement du CHU, ou encore les patients.

Elle pourrait ensuite les détruire, ou les rendre inaccessibles et demander une rançon pour les restituer, ou encore les revendre, les diffuser sur Internet etc…

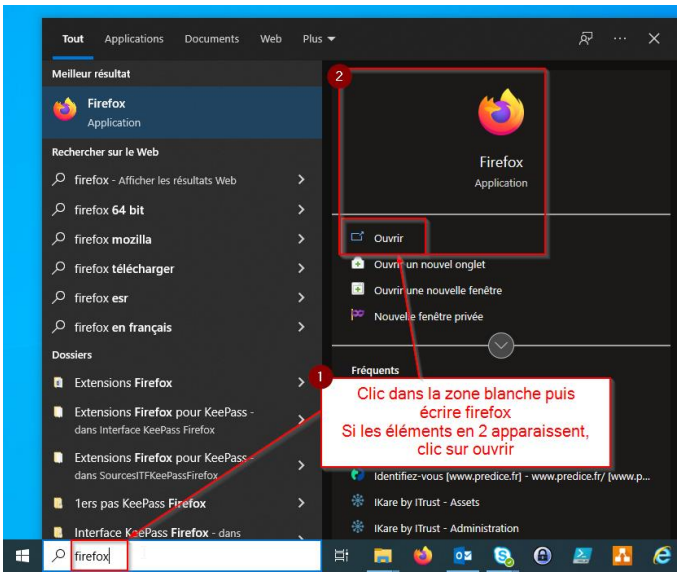
Cette démarche permet d'augmenter le niveau de sécurité des mots de passe.
Utiliser Firefox renforce également le niveau de confidentialité de vos activités sur Internet.

Prérequis d'installation

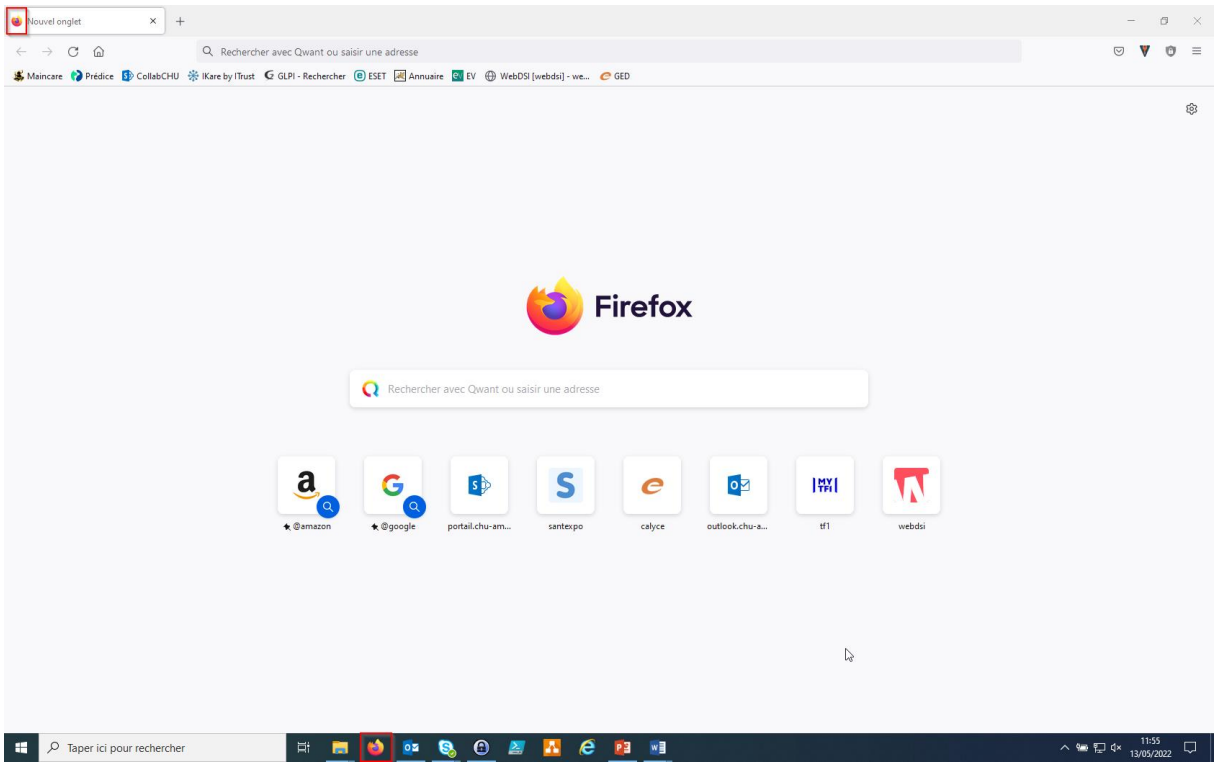
Firefox

Pour pouvoir bénéficier des avantages de Firefox, ainsi que du remplissage automatique de mot de passe pour vos applications web (exemples : SharePoint, Epione, Cloudfile, Web100T …), il faut que Firefox soit fonctionnel avant de procéder à l'installation du lien KeePass et Firefox.

Voici comment s'en assurer (images issues de Windows 10) :



Après le clic sur ouvrir, une fenêtre similaire à celle-ci doit apparaitre :



Si vous n'arrivez pas à ce type de fenêtre, alors il faut installer/Réinstaller Firefox via le centre logiciel.

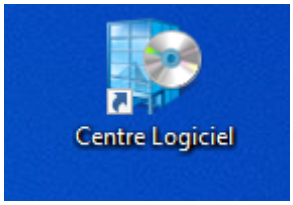
Préparation récupération accès KeePass professionnel

Pour avoir un accès de secours sécurisé à votre KeePass professionnel, nous conseillons un smartphone Android ou iPhone, avec reconnaissance d'empreinte digitale, ou faciale, et avec une connexion Internet.

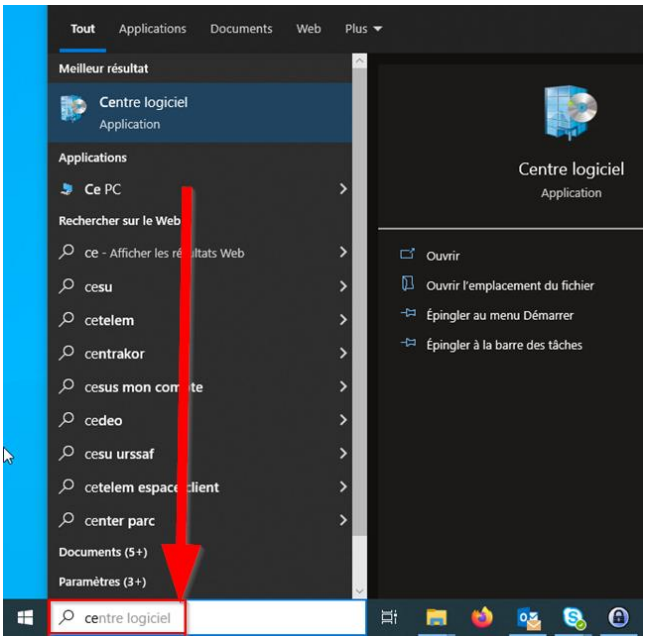
Installation

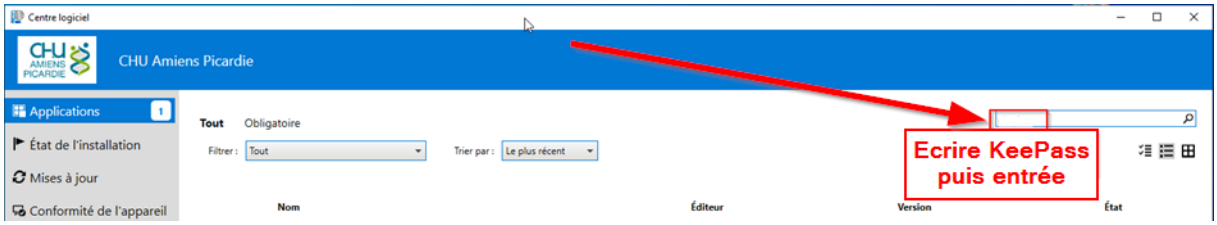
En vidéo sur :
https://epione-simusante.fr/ecampus/mod/page/view.php?id=16842&forceview=1

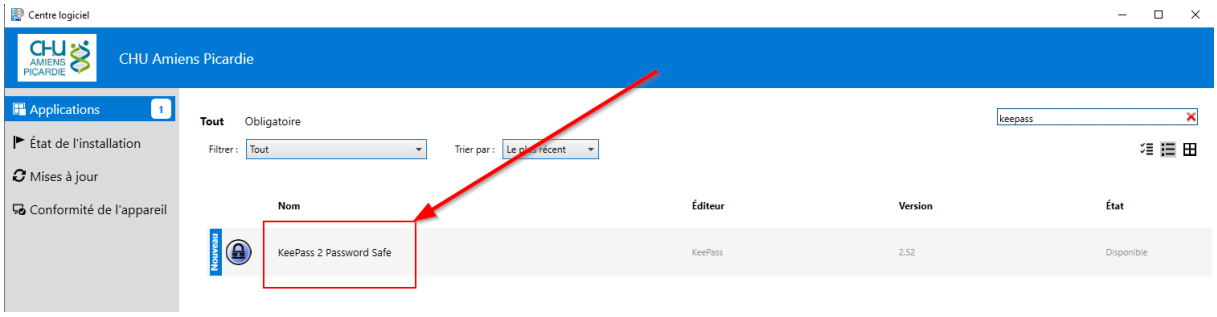
Vous pouvez procéder à cette installation même si KeePass est déjà installé, cela permettra une mise à jour.

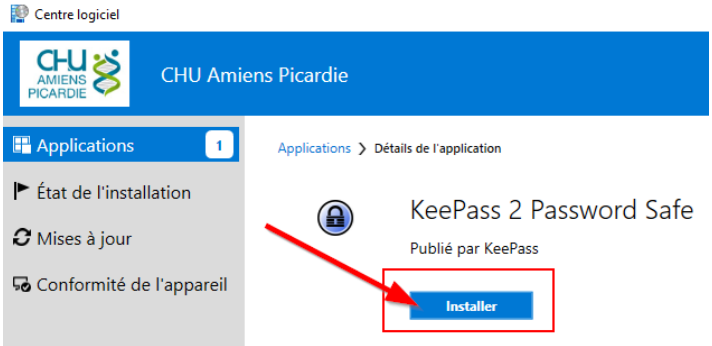


Sur le bureau vous devez avoir cette icône, sinon écrire « centre logiciel » ici :





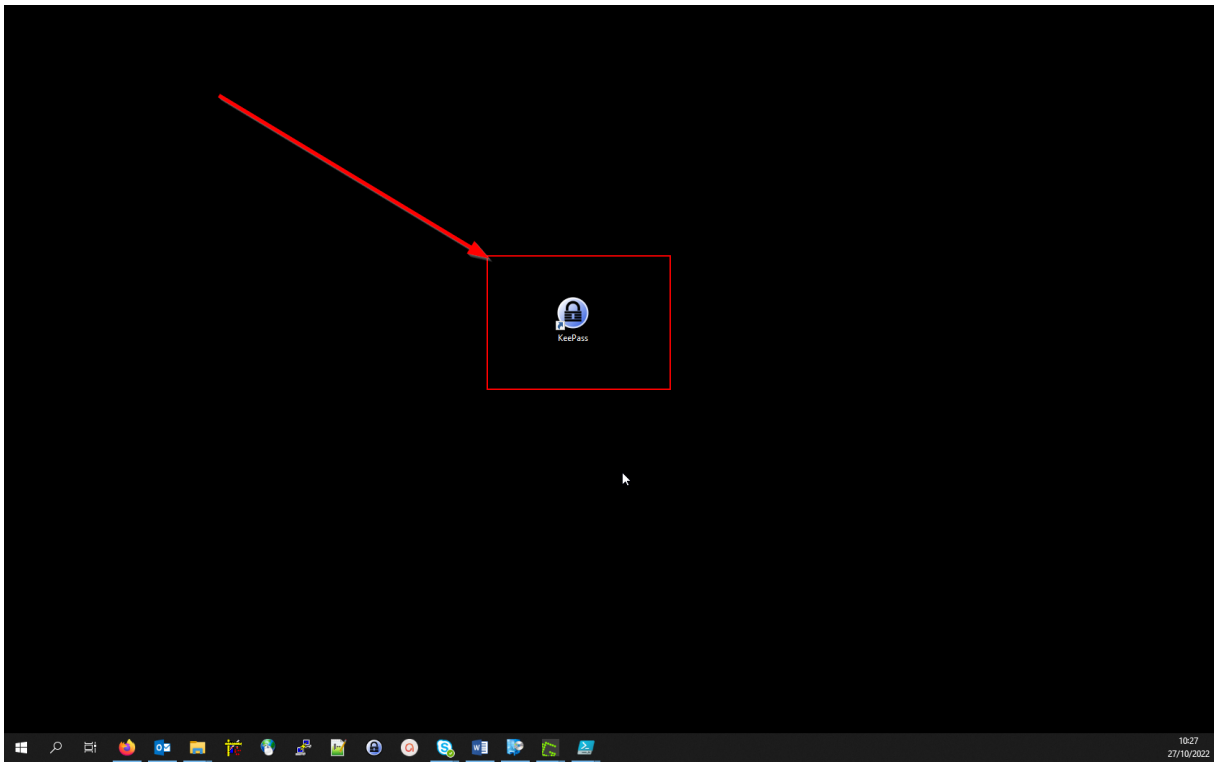




Plus bas on trouve les liens utiles vers les vidéos de formation et la politique de mots de passe.

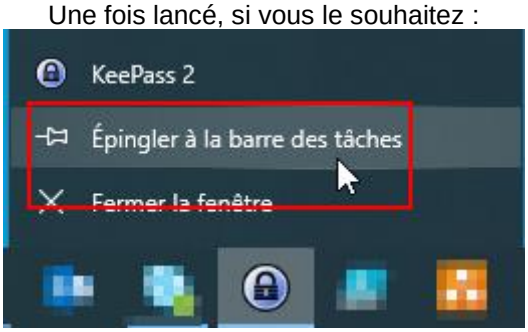
Configurer pour la 1ère utilisation

Prenez l'habitude d'utiliser le raccourci bureau.



Il permet de sauvegarder vos coffres forts de mots de passe, (si vous avez une connexion avec votre homedir U :), mais aussi une proposition d'ouvrir le dernier coffre-fort que vous avez enregistré.

Une fois lancé, si vous le souhaitez :

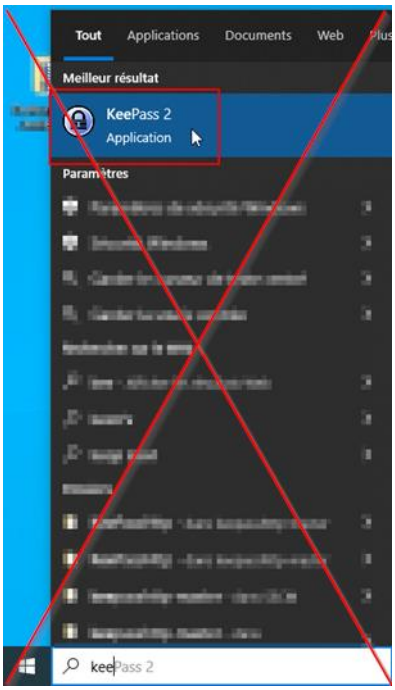


Pour pouvoir y retourner plus facilement

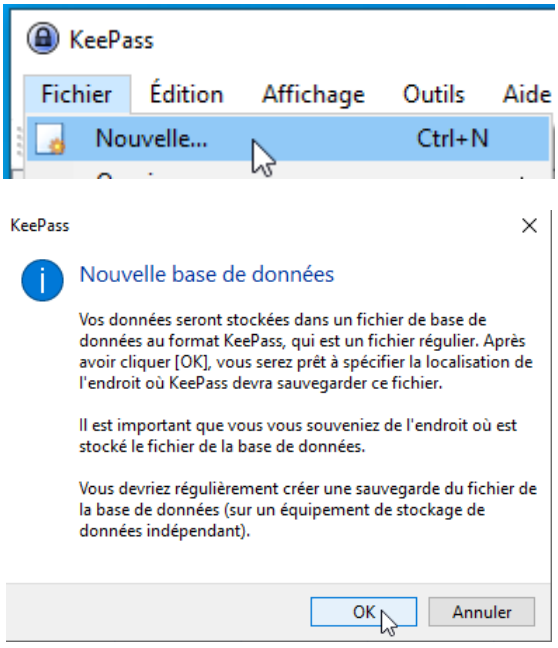
Vous n'aurez pas la sauvegarde, et la proposition d'ouverture se fera sur le dernier coffre ouvert, si vous ouvrez KeePass par les autres moyens, comme :

Taper 'Kee' dans la zone recherche en bas à gauche de l'écran :

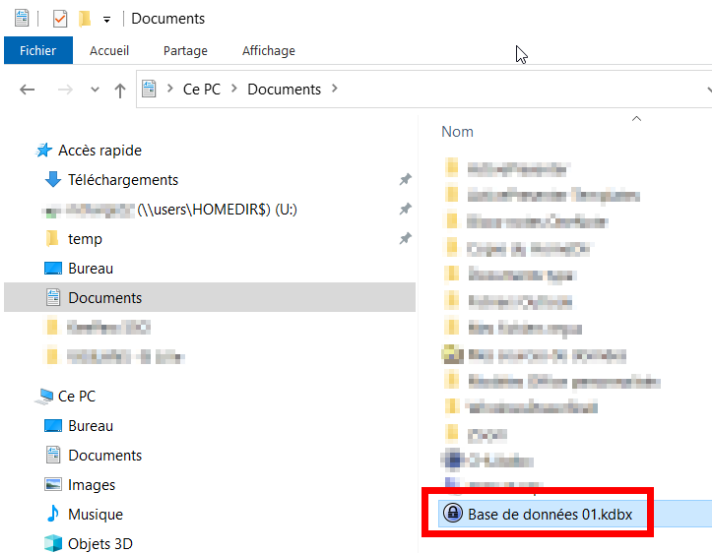
A ne faire que si l'ouverture par le raccourci ne fonctionne pas !



Créer votre coffre-fort (base de données)



Il faut enregistrer sa base de données dans le répertoire Documents, c'est le répertoire par défaut qui va être proposé par l'application, et permettre des accès aux fichiers plus rapides.



Toute base dans Documents sera copiée pour sauvegarde au lancement de KeePass sur le lecteur HOMEDIR, U:\Backup\KeePass, à condition d'utiliser le raccourci personnalisé mis en place par le CHU, et que la connexion à U : soit possible.

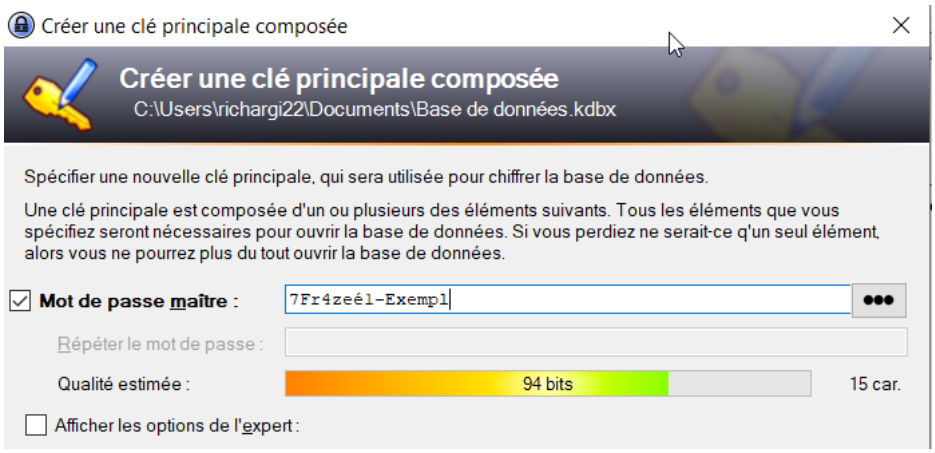
Exception : Sur un poste partagé, avec ou sans connexion automatique à Windows, il ne peut y avoir de connexion à un lecteur HOMEDIR, donc il n'y a pas de copie de sauvegarde.

Sur ces postes, même si cela reste **à éviter**, il est possible de créer une base de données nominative dans le répertoire document, ou d'en récupérer une par mail ou encore via https://cloudfile.chu-amiens.fr.

Il faut alors être attentif aux différences entre les bases de données : les modifications faites sur le poste partagé ne seront reprises sur un autre poste que si on y copie la base modifiée.

Lancer KeePass par ce raccourci permet par ailleurs de préparer l'ouverture (il ne reste que le mot de passe à entrer) de la dernière base de données ouverte dans Documents.

Il faut inclure dans le nom de quoi identifier pour vous facilement qu'il s'agit de votre base de mots de passe uniquement professionnelle.



L'étape suivante est le choix de votre mot de passe maître.

L'accès à votre KeePass professionnel **doit être sécurisé par un mot de passe maître fort.**

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. En effet, un algorithme permet de les créer, mais il est possible de trouver l'algorithme pour les deviner à partir de celui de création.

La meilleure méthode actuelle pour choisir un mot de passe fort, et donc complexe à déchiffrer, est d'utiliser une phrase longue que vous choisissez au hasard, en suivant la Politique d'établissement sur les mots de passe

Ici « 7Fr4zeé1-Exempl » correspond à la phrase « Cette (=7) phrase (=Fr4ze) est un (=é1) exemple.

C'est 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.

Avant de valider votre mot de passe maître, il faut installer KeePass sur votre téléphone et y enregistrer votre nouveau mot de passe maitre pour pouvoir le récupérer de manière sécurisée.

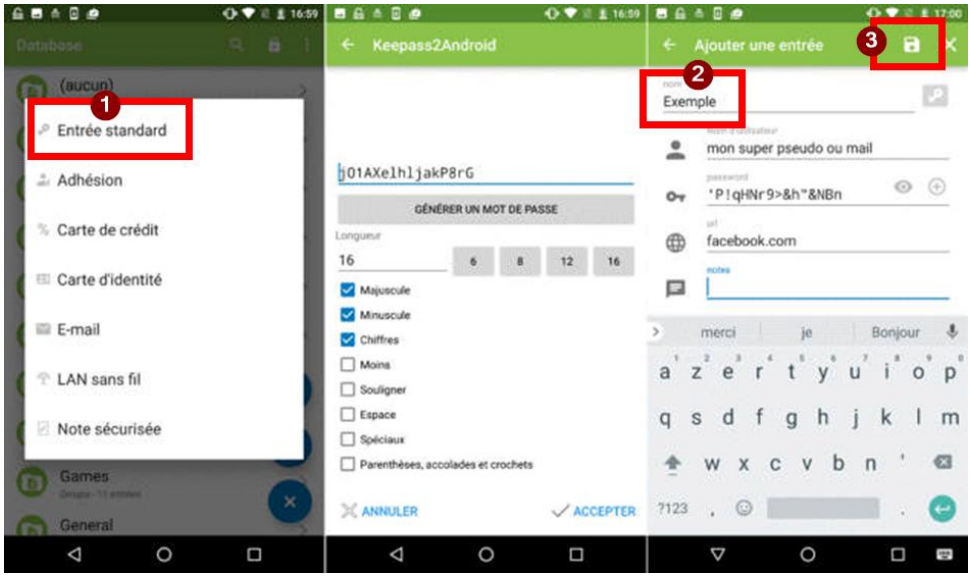
Installer KeePass sur votre téléphone

Ce chapitre permet l'installation d'une version de KeePass avec déverrouillage par votre empreinte digitale.

En effet, un autre KeePass accessible par mot de passe n'a pas d'intérêt, ça ferait juste un nouveau mot de passe à retenir en plus.

Comment installer : téléphone Google Play (Android) reconnaissance empreinte digitale

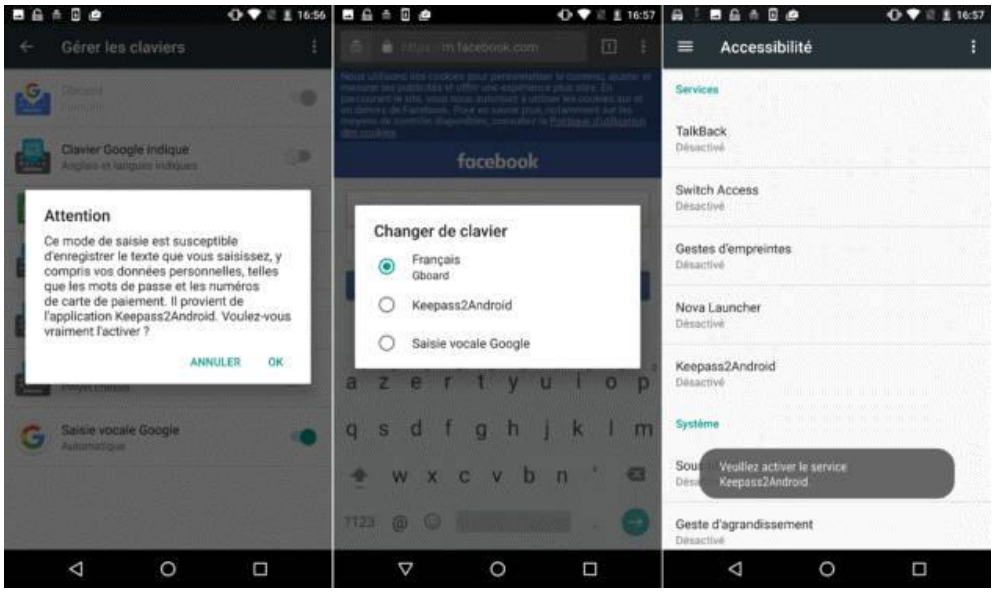
- Depuis Google Play, installer puis ouvrir KeePass2Android
- Créer une base de données locale (pas de connexion à un service cloud pour assurer plus de sécurité)
- Ajouter une entrée avec le nom de votre base KeePass professionnelle (il pourra être modifié: Pour cela, petit + puis « Entrée standard » (1). Dans nom, là où on voit sur l'image « Exemple » (2), mettre le nom de votre base de données professionnelle, par exemple « CHU », enregistrer avec la disquette (3).



- Paramètres > Base de données > Déverrouillage par empreinte digitale > Activer le déverrouillage par empreinte digitale.

  Avec cette méthode de connexion, vous n'aurez plus à retaper tous les identifiants et mots de passe enregistrés dans les entrées de KeePass2Android.

-



Rendez-vous ensuite dans les paramètres d'Android pour activer le clavier Keepass2Android qui vous permettra de pouvoir remplir tous les champs d'authentification par login/mot de passe automatiquement.
Dans les paramètres Android donc, rendez-vous dans Langues et saisies (ou Accessibilité) puis sélectionnez le clavier **KeePass2Android**.

Il vous suffit alors de vous rendre sur une page de connexion et de cliquer sur la touche clavier en forme de cadenas qui se trouve juste à gauche de la barre espace.

Continuez en sélectionnant la seconde option mais si jamais KeePass2Android ne vous propose pas la bonne entrée, alors cliquez sur « Sélectionner une autre entrée » puis taper le bon identifiant et mot de passe.
Pour passer d'un clavier à l'autre, il vous suffit de taper de nouveau sur cette touche en forme de cadenas à côté de la barre espace.

Comment installer : sur iPhone avec reconnaissance empreinte digitale

-Sur votre iPhone, activer la reconnaissance d'empreinte digitale Touch ID
https://support.apple.com/fr-fr/guide/iphone/iph672384a0b/ios : Touch ID

(à tester avec Face ID, reconnaissance faciale)

-Sur votre iPhone, depuis App Store, chercher et télécharger KeePass Touch
-Créer une base de données
-Créer une entrée, avec en nom celui de votre future base de données pour le CHU
-KeePass Touch permet de faire des copier/coller des identifiants vers les autres applis

Pour tous les types de téléphone, après l'installation

N'hésitez pas à renseigner vos identifiants et mots de passe personnels sur le KeePass de votre téléphone !

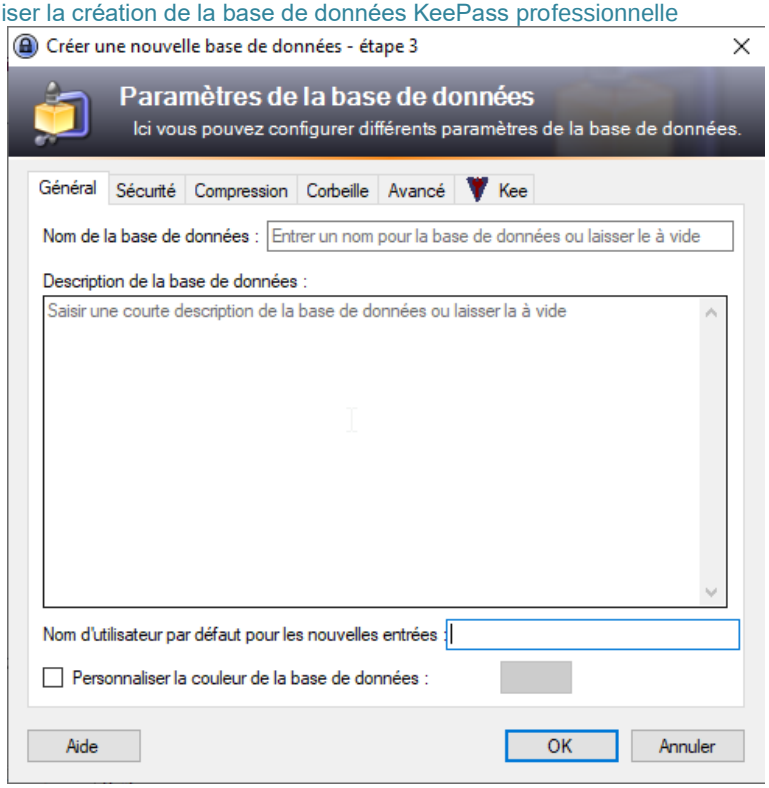
Une fois habitué(e) à KeePass, vous n'aurez besoin que du mot de passe principal du KeePass professionnel pour pouvoir accéder à tous vos identifiants et mots de passe professionnels, et vous pouvez le retrouver sur votre téléphone si besoin.

Sur l'ordinateur, valider votre mot de passe maitre KeePass professionnel, et **n'oubliez pas de l'enregistrer aussi sur votre KeePass de téléphone** !

Enregistrer également sur votre téléphone :
-identifiants de comptes de connexion Windows (AD) ;
-si vous avez un ordinateur portable, code BitLocker de démarrage.

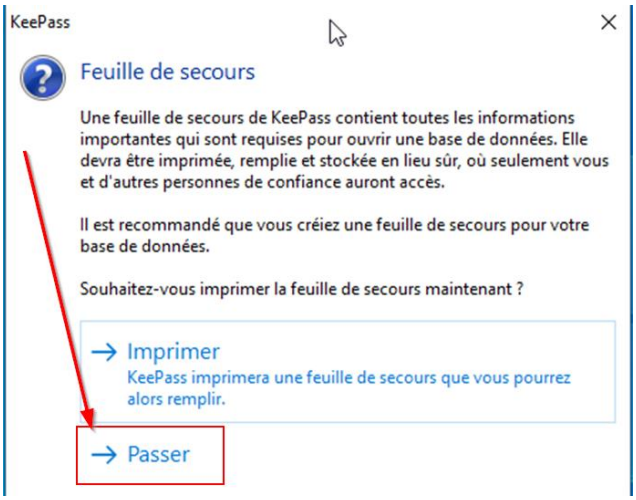
Ainsi vous aurez sur votre téléphone, en cas de besoin, tous les mots de passe nécessaires pour pouvoir débloquer l'accès à votre poste de travail.

Sur l'ordinateur, finaliser la création de la base de données KeePass professionnelle



A ce stade, nous conseillons de ne rien modifier, mais libre à vous d'inspecter les options possibles.

Dans notre cadre, nous déconseillons ensuite l'impression d'une feuille de secours, en effet l'intrusion de personnes malveillantes, ou laisser la possibilité à d'autres personnes dans l'hôpital d'accéder à vos mots de passe est trop risquée pour en laisser des versions imprimées :



Récupération d'anciens mots de passe

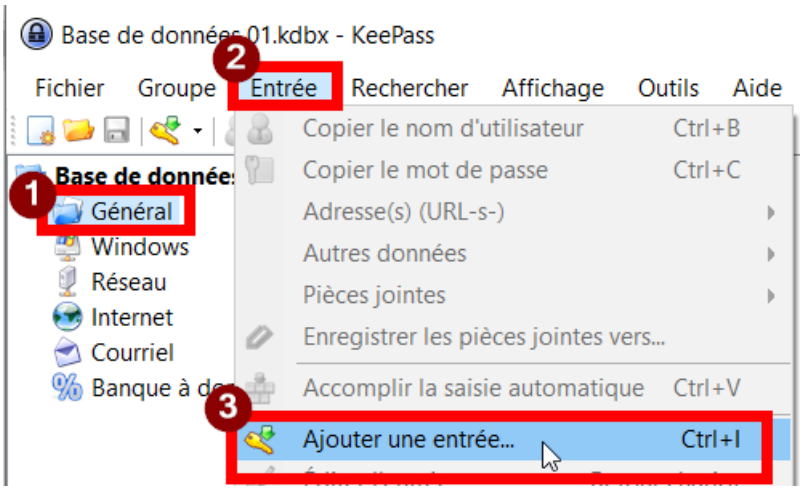
Si vous disposez de fichiers ou vous aviez inscrits vos identifiants et mots de passe, ou d'applications où vous avez enregistré des mots de passe (exemple Firefox, Google Chrome), sachez qu'il est possible techniquement d'en extraire la liste, puis de l'importer dans KeePass.

Toutefois, il est préférable de changer vos mots de passe. En effet, les anciens mots de passe ont pu facilement être récupérés. Le fait de passer à KeePass est un bon moment pour changer de mot de passe et repartir sur la sécurité apportée par des mots de passe récents.

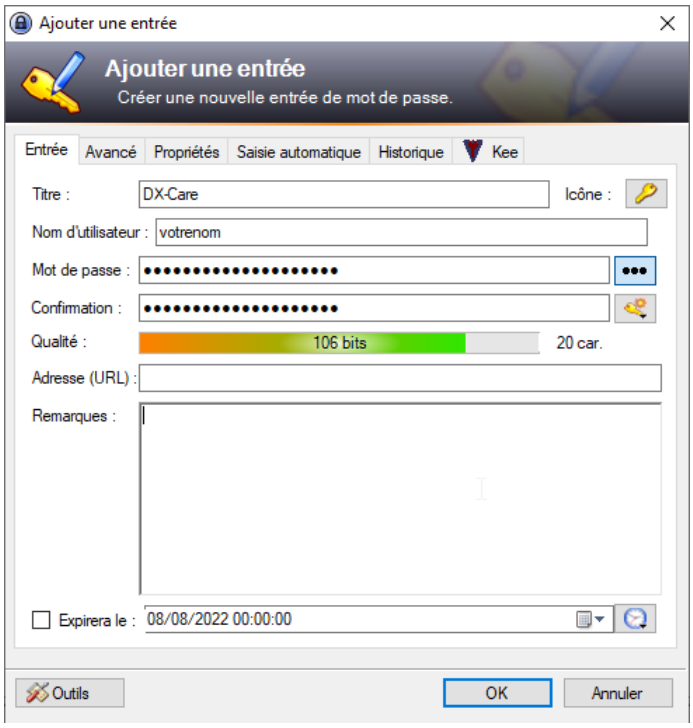
Enregistrement identifiant + mot de passe pour logiciel « client lourd »

Il est plus pratique de ne créer ainsi des entrées avec cette méthode uniquement pour s'identifier sur des applications qui ne s'ouvrent pas sur un navigateur internet, par exemple DX-Care, ou encore sur des navigateurs internet autres que Firefox.

Une fois le groupe (dossier) voulu de l'arborescence sélectionné (1), faites (2)(3) :



(on peut déplacer les entrées ensuite dans les groupes)



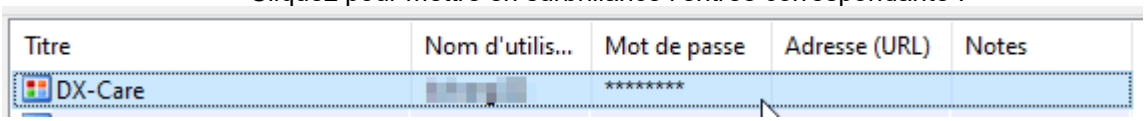
On reprend ici le nom d'utilisateur et le mot de passe actuellement dans l'application.

Se connecter à une application avec saisie semi-automatique de l'identifiant et du mot de passe

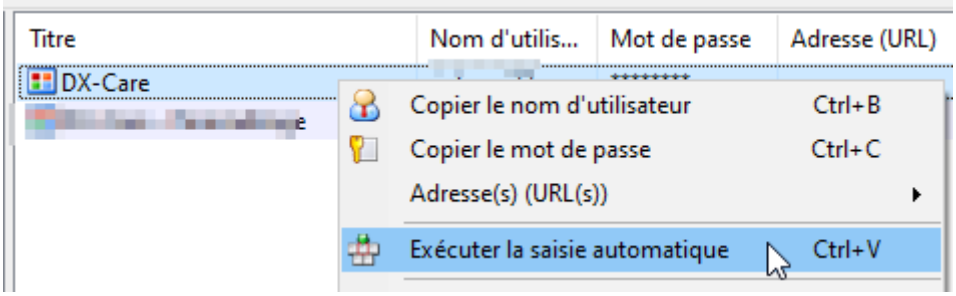
Pour vous connecter sur votre application désormais, avec remplissage automatique de l'identifiant et du mot de passe :

Cliquez sur la zone identifiant de connexion de l'application :

Cliquez pour mettre en surbrillance l'entrée correspondante :



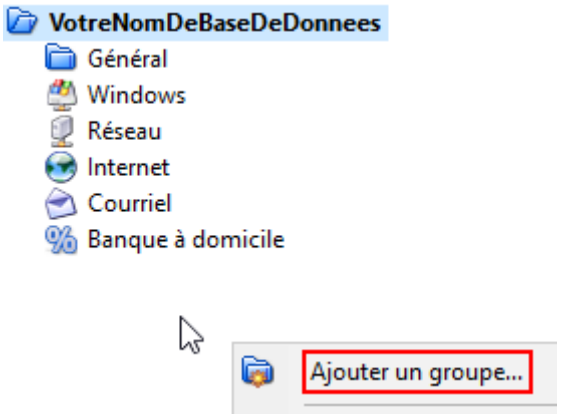
Utilisez la combinaison des touches Ctrl + V
Ou bien avec le clic droit de la souris :



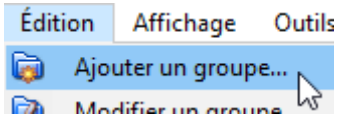
Création d'un groupe

Un groupe est un dossier dans lequel on range des entrées.

On crée un groupe en cliquant avec le bouton de droite de la souris dans cette zone blanche :



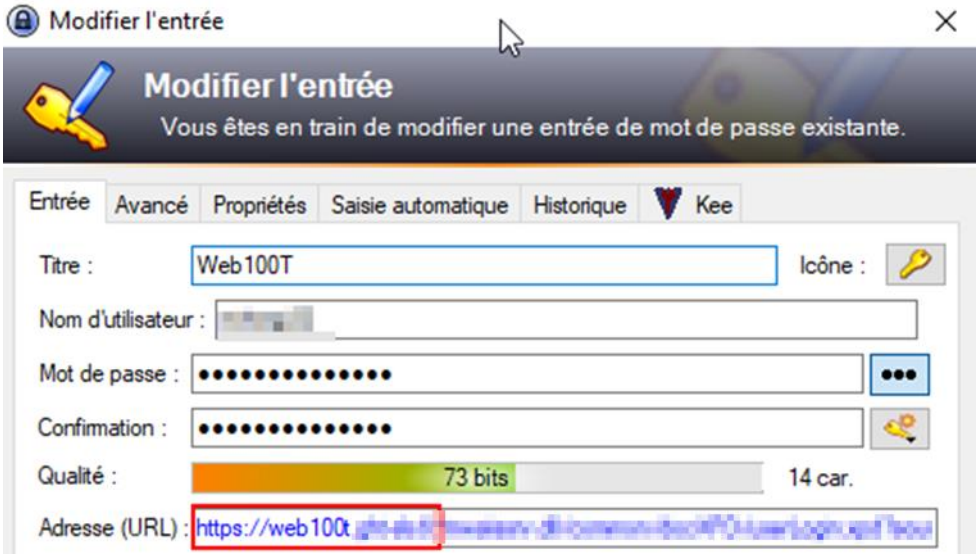
Ou bien :



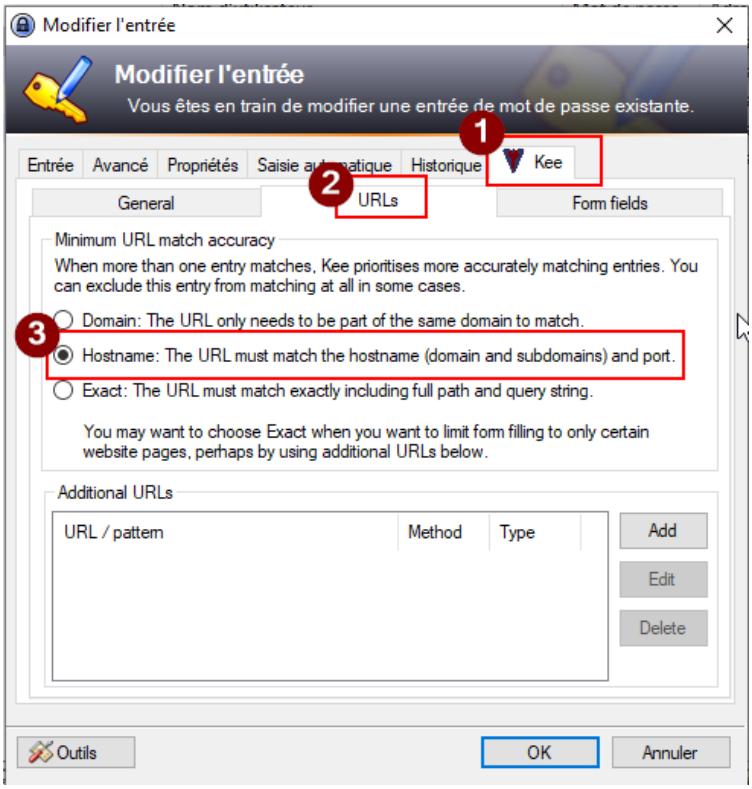
Créer une entrée identifiant / mot de passe par Firefox

Si vous avez plusieurs entrées pour un même domaine, par exemple plusieurs adresses (URL) de sites qui finissent par « ghtxXXX.fr », alors par défaut Firefox va toutes vous les proposer et il faudra à chaque fois choisir, ce qui peut prendre du temps au cumulé.

Pour ces cas, on peut configurer une entrée pour qu'elle ne soit proposée que sur le site correspondant à ce qui est inscrit ici :



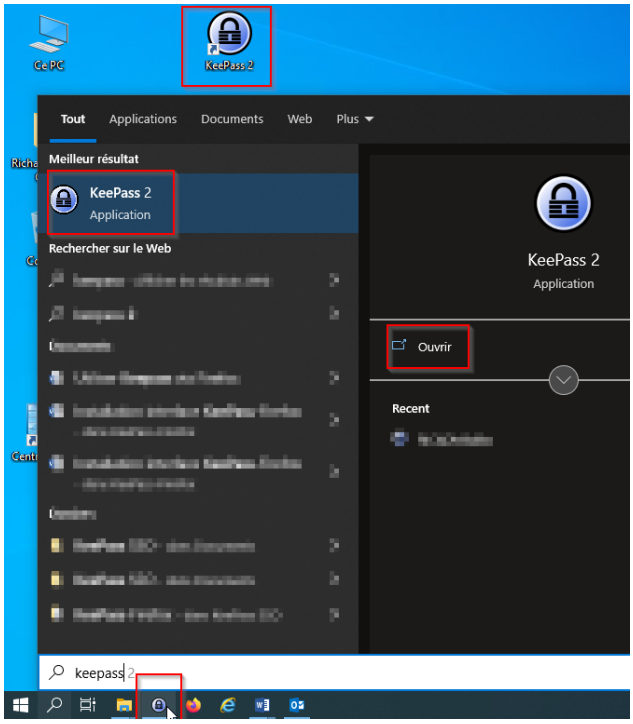
, par exemple web100t.ghtXXXX.fr, au lieu de tous les sites avec .ghtXXXXXX.fr :



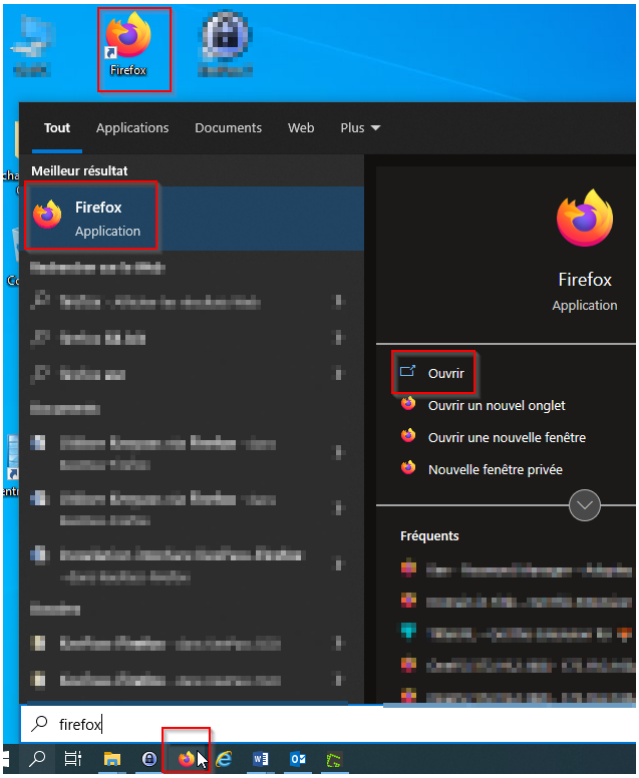
L'option « Exact » permet même de ne proposer le remplissage automatique identifiant / mot de passe sur l'adresse complète indiquée dans URL, plus la liste des adresses en dessous.

Connecter KeePass et Firefox

Il faut tout d'abord ouvrir KeePass et vous connecter.

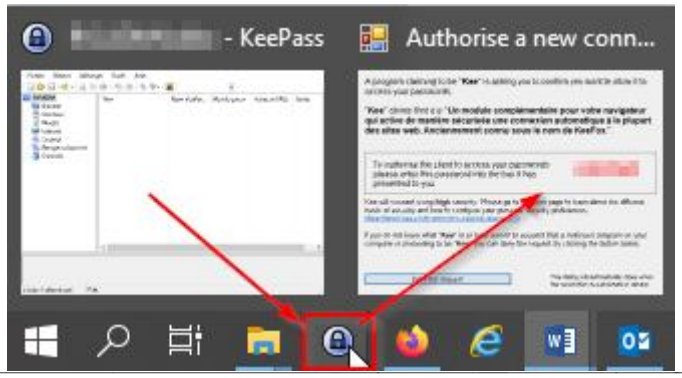


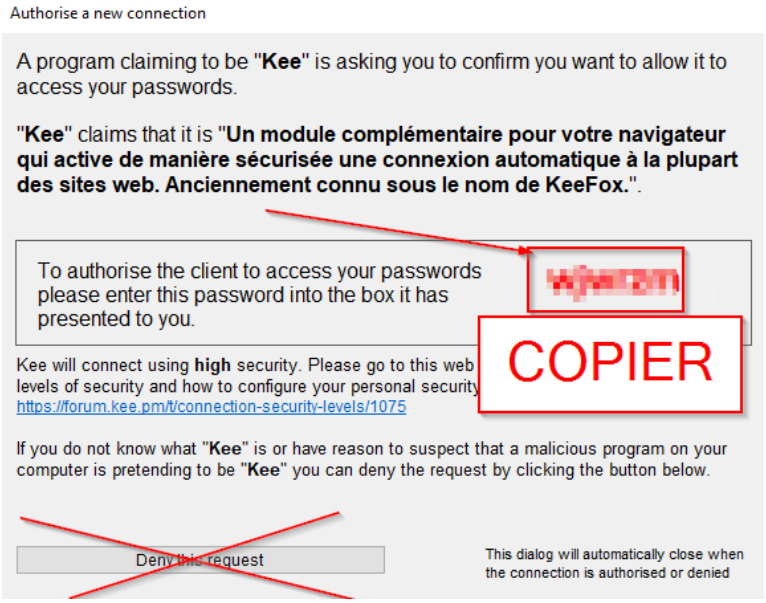
Il faut ensuite ouvrir Firefox



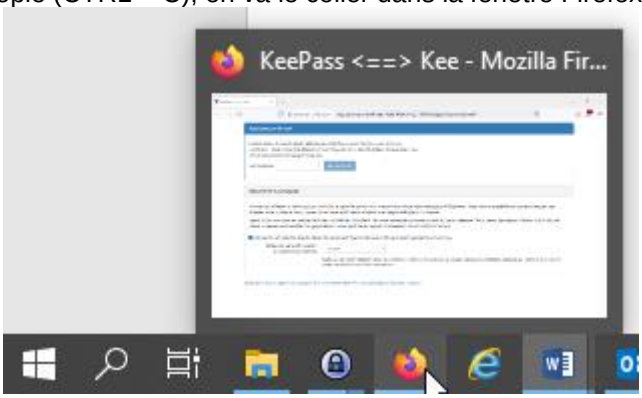
A chaque ouverture de Firefox, on doit indiquer un mot de passe pour sécuriser l'utilisation de votre base de données KeePass et éviter que vos identifiants soient utilisés par une autre personne.

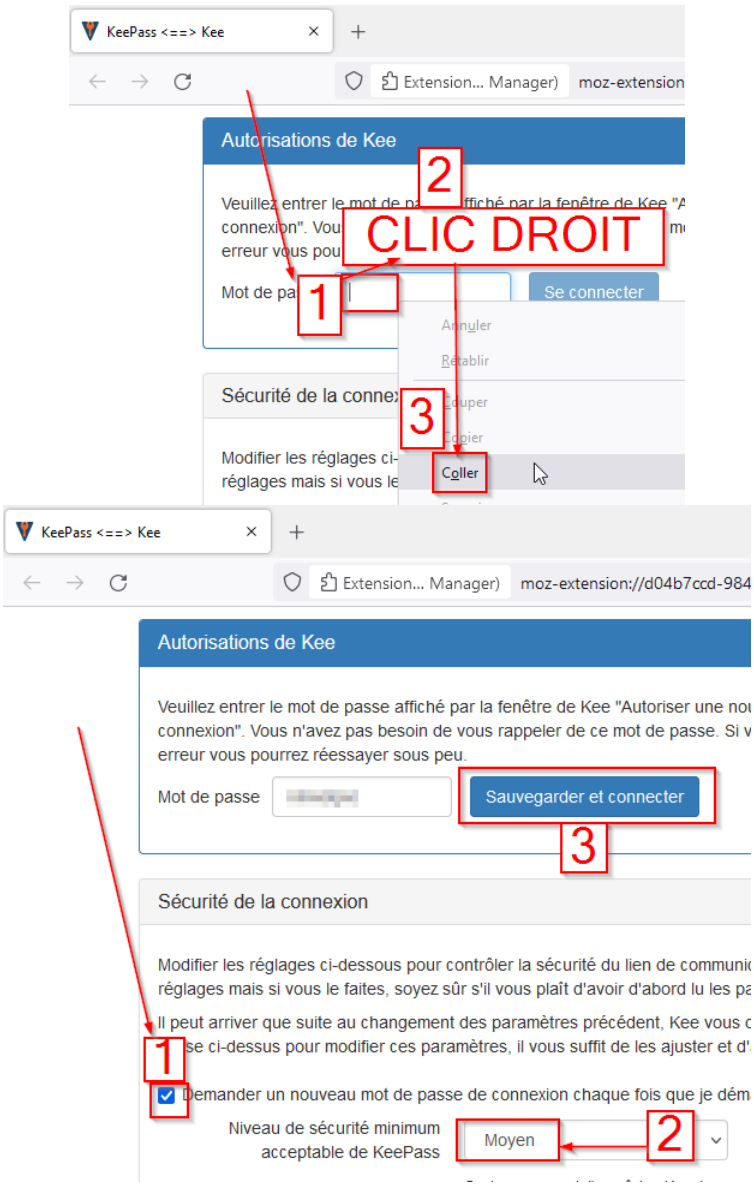
Une autre fenêtre KeePass s'ouvre donc avec ce mot de passe, on y accède ainsi :





Une fois copié (CTRL + C), on va le coller dans la fenêtre Firefox suivante :



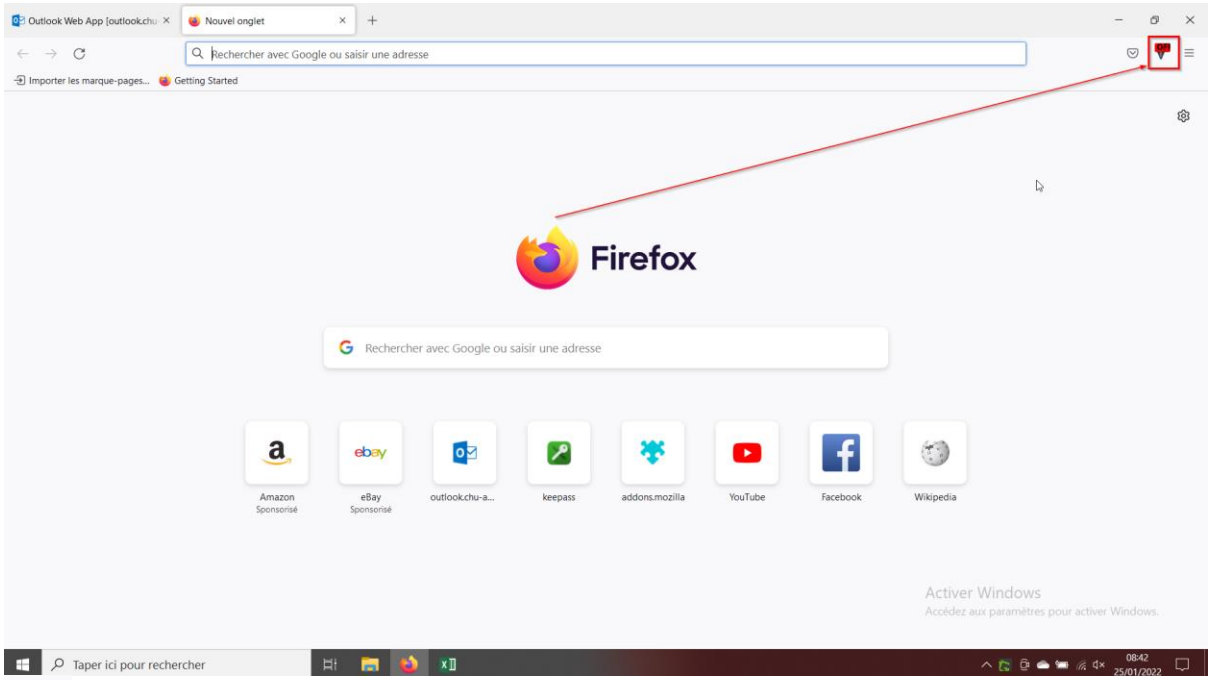


Veuillez ne pas choisir le niveau de sécurité minimum « Elevé » qui a posé problème lors des tests avec des messages d'alertes intempestifs.

Veuillez ne pas prendre en compte la fenêtre suivante proposant « KeeVault ».

Vérifier l'état de la connexion KeePass - Firefox

A tout moment, une icône indique dans Firefox l'état de connexion avec KeePass

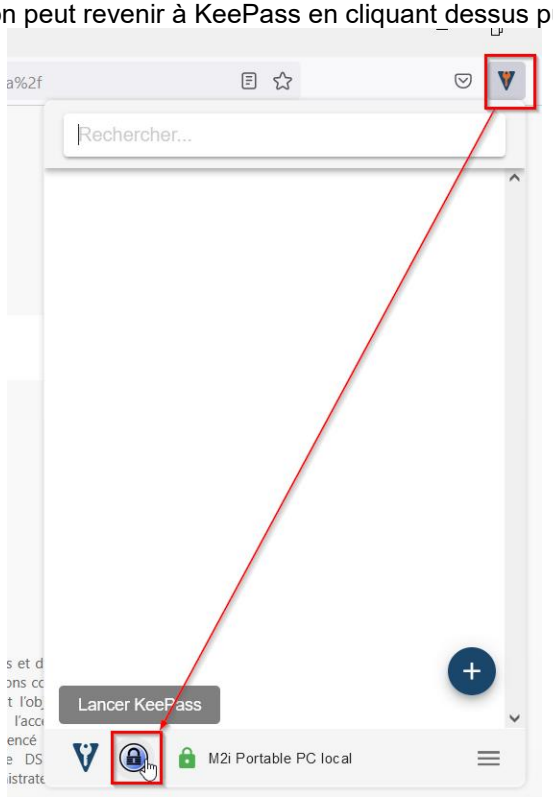


(rouge) indique que KeePass n'est pas ouvert.

(orange) indique que KeePass est ouvert, mais le mot de passe n'a pas été validé.

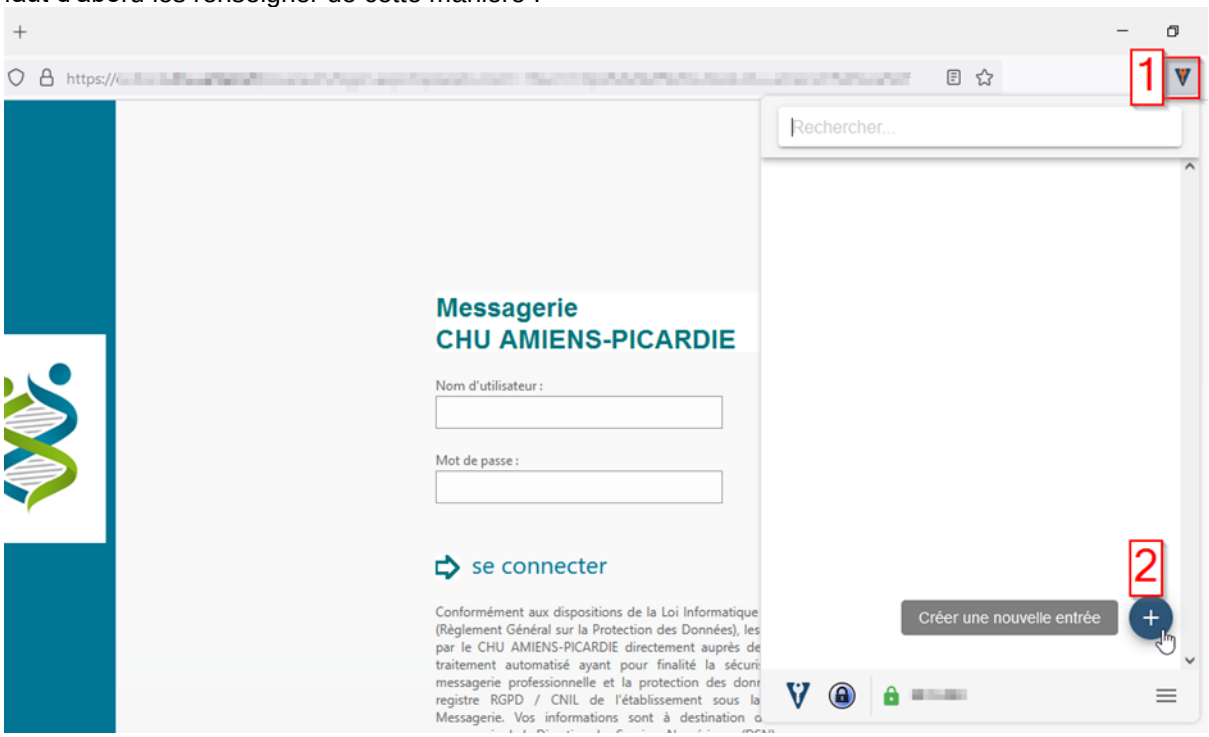
est l'icône obtenue quand tout est prêt !

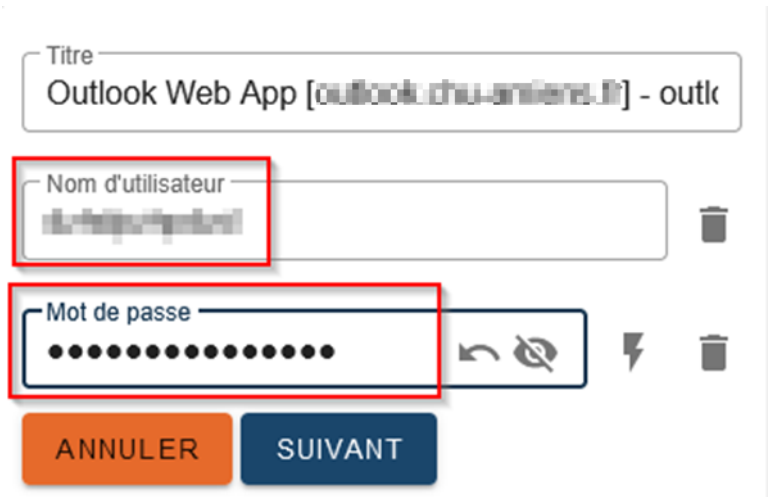
Avec l'icône dans cet état, on peut revenir à KeePass en cliquant dessus puis :



Sauvegarder dans KeePass les identifiants de sites Internet

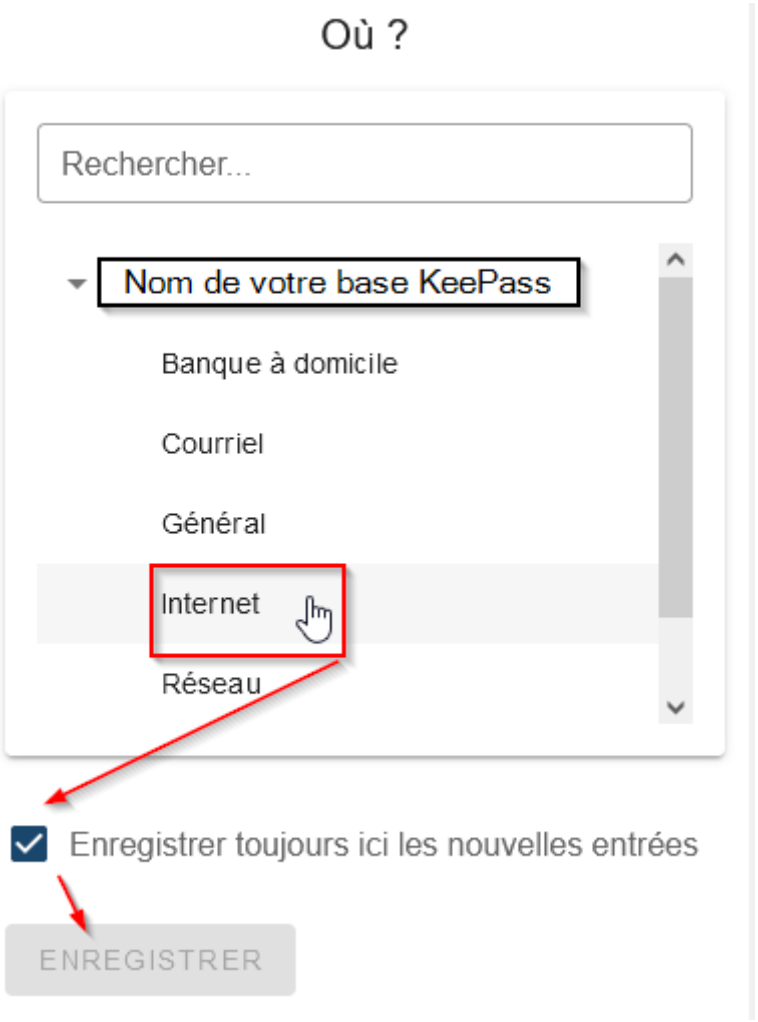
Pour chaque site Internet où vous avez besoin de stocker un identifiant associé d'un mot de passe, il faut d'abord les renseigner de cette manière :



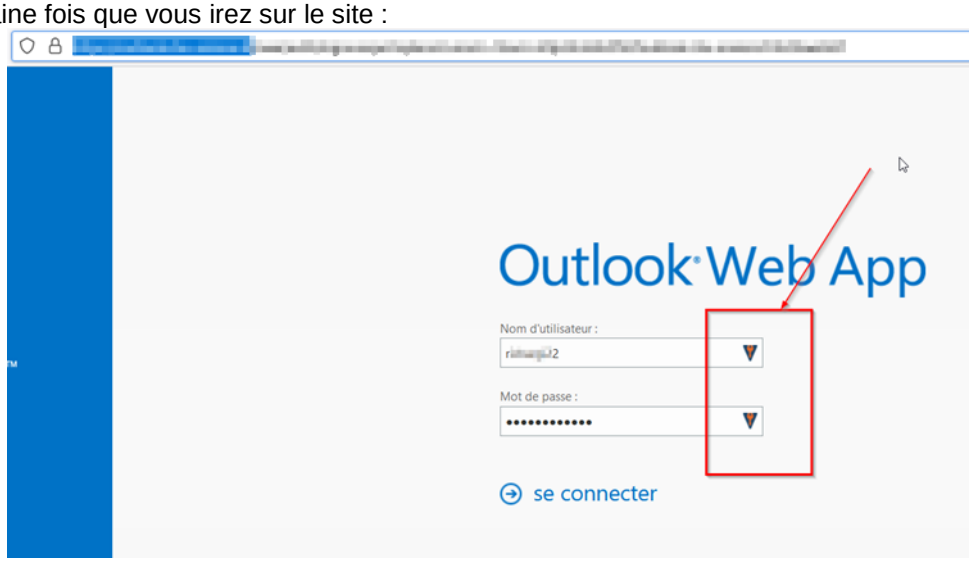


Pour les sites où vous avez déjà un identifiant et un mot de passe, pour que la connexion automatique puisse fonctionner, il vous faut stocker ici les mêmes informations.

Pour les nouveaux sites où vous créez un compte, n'oubliez pas que ces mots de passe seront dans votre KeePass, et renseignés automatiquement sur les sites via Firefox, il n'y a donc pas besoin de les retenir, donc autant les rendre complexes en suivant la politique d'établissement pour éviter qu'ils soient subtilisés via Internet : Politique d'établissement sur les mots de passe



La prochaine fois que vous irez sur le site :

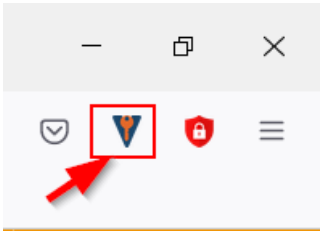


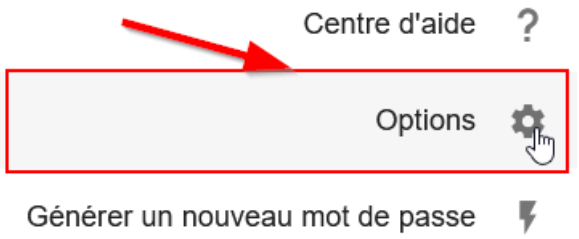
Les champs sont renseignés automatiquement avec cette icône montrant que les informations sont bien issues de KeePass et sont sécurisées.

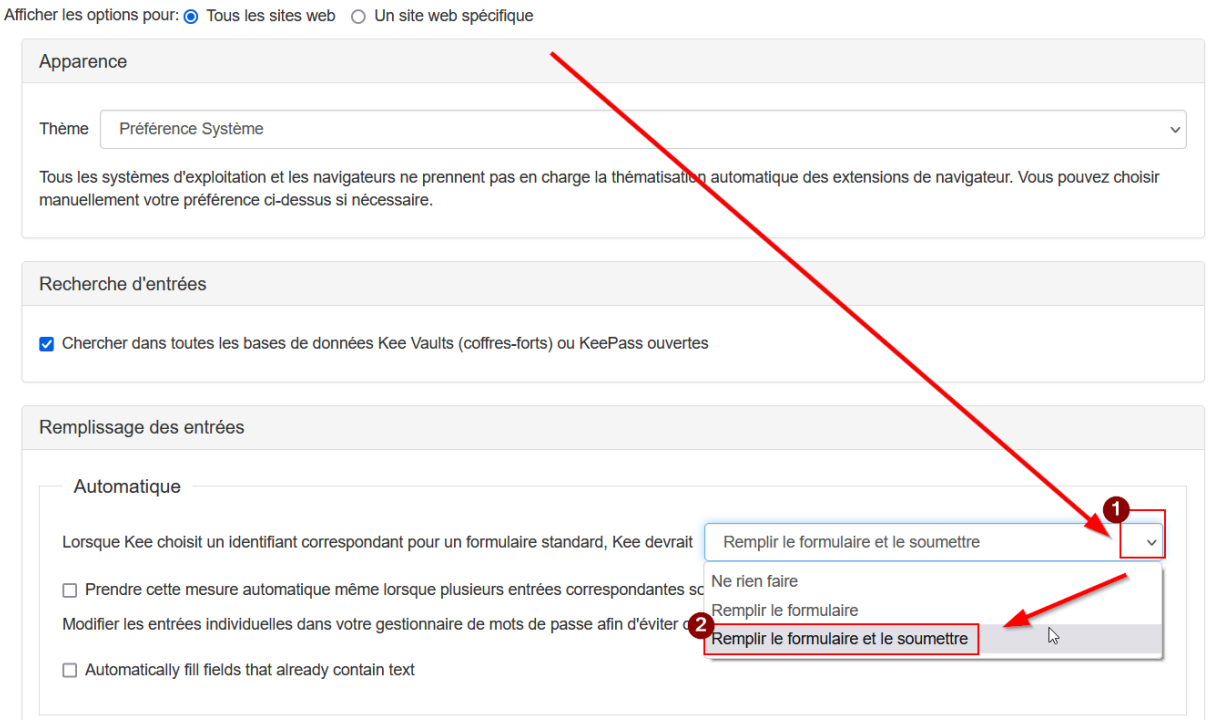
Si ce fonctionnement automatique n'est pas opérationnel, alors il faut utiliser les données depuis la fenêtre KeePass, en les recopiant ou copiant vers la fenêtre Firefox. **Il ne faut en aucun cas enregistrer ces informations dans Firefox comme proposé ci-dessous :**

Rendre automatique la connexion aux sites avec identifiants connus de KeePass

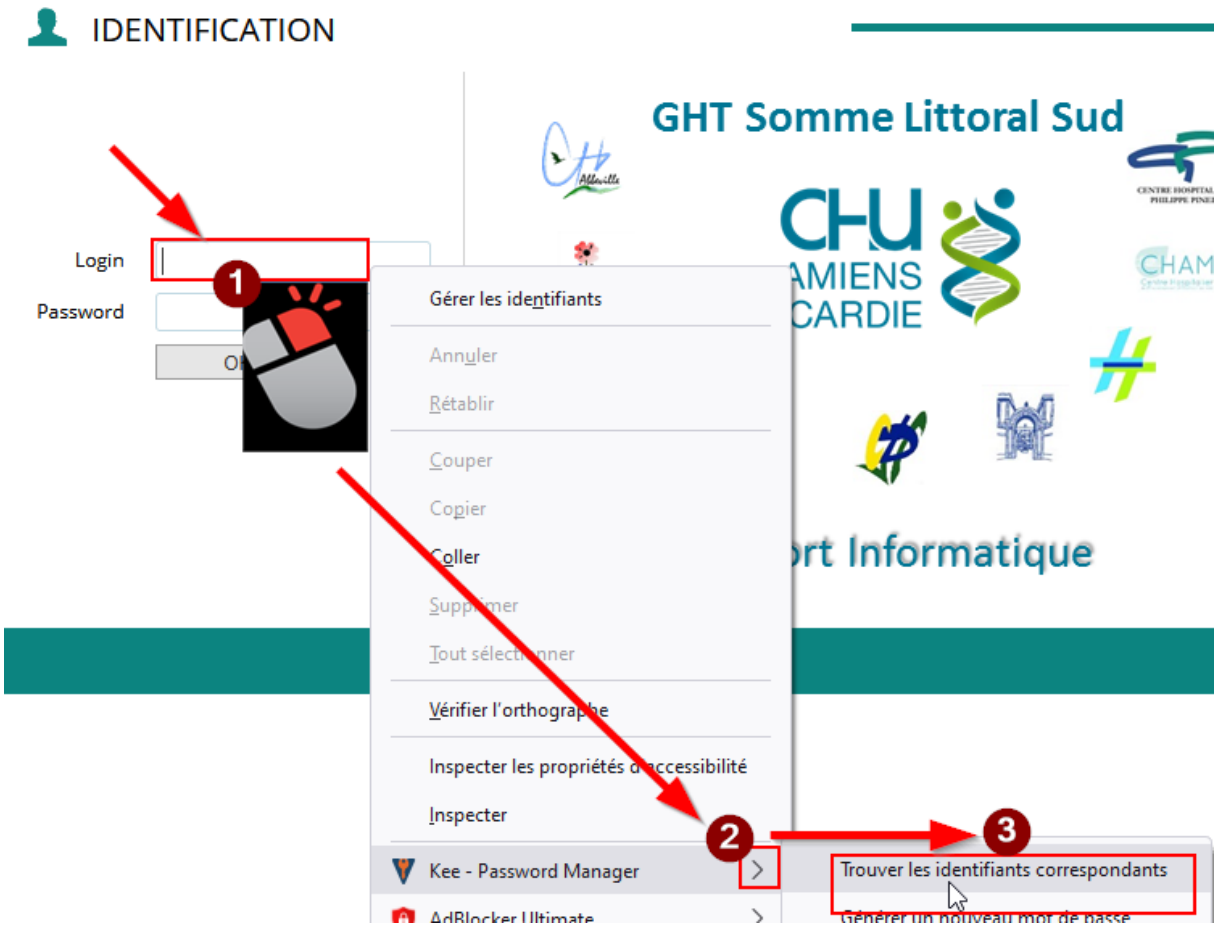
Dans Firefox :







Quand les identifiants KeePass ne sont pas automatiquement proposés dans Firefox



Si cette manipulation ne donne toujours rien, alors il faut vérifier que vous avez bien une entrée KeePass créée pour ce site.

Une fois familiarisé(e) à KeePass, les habitudes à changer :

Ne plus enregistrer de mots de passe sur d'autres supports que KeePass (dont le papier)

Sur les navigateurs Internet, il est parfois proposé de les enregistrer :

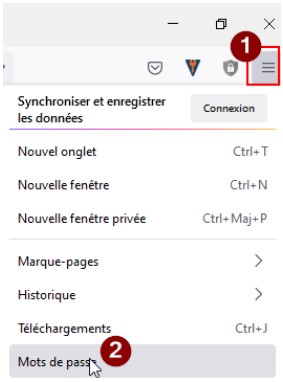
Il est largement déconseillé d'enregistrer vos mots de passe de cette manière.

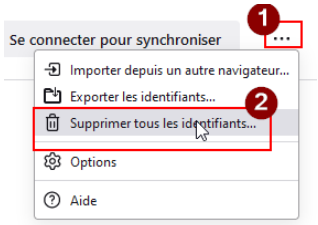
Dans tous ces cas, un hacker peut plus facilement accéder à vos identifiants / mots de passe que sur KeePass.

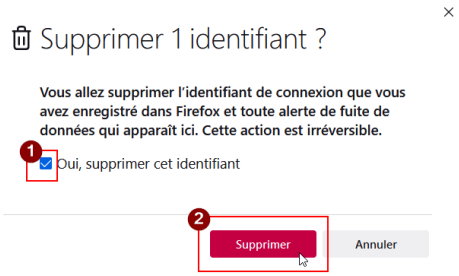
Supprimer les mots de passe déjà enregistrés sur le navigateur

Si vous avez déjà des mots de passe enregistrés dans vos navigateurs, veuillez les reporter dans KeePass, puis supprimer les de votre (vos) navigateur (s) :

Sur Firefox :

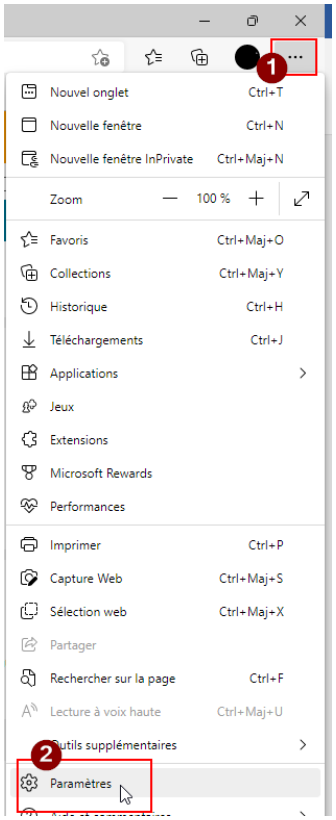


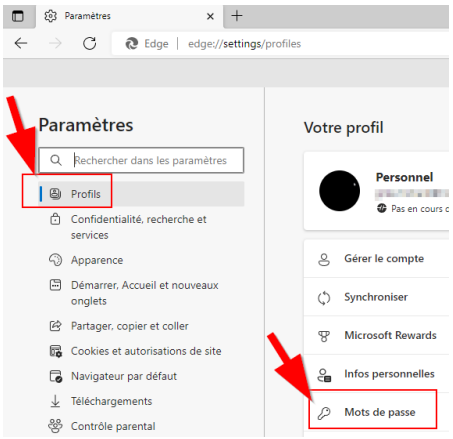


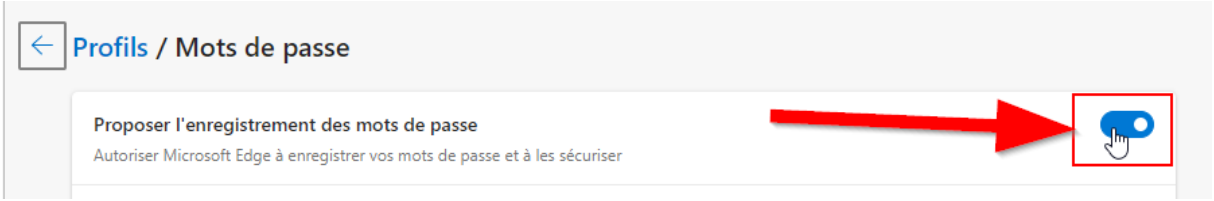


L'installation du plugin KeePass pour Firefox désactive les propositions d'enregistrement d'identifiant et mots de passe de Firefox.

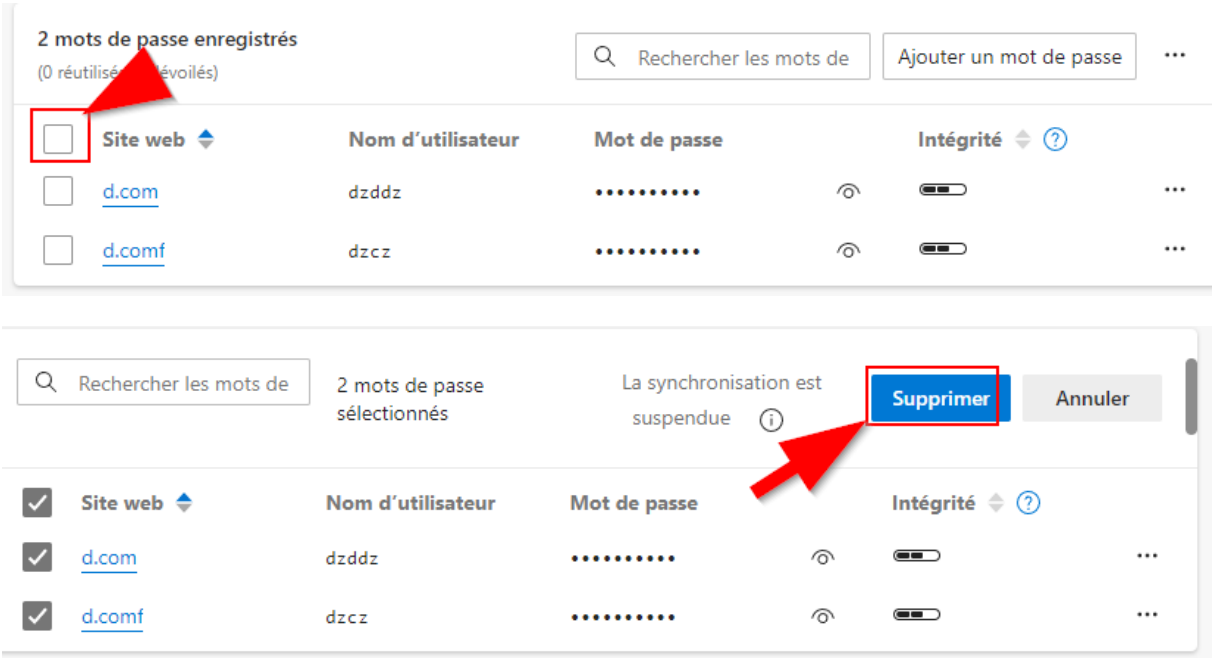
Sur Edge :





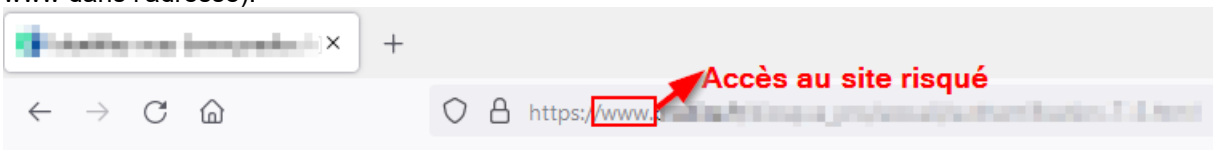


Cliquer pour désactiver (le rond blanc doit être à gauche, et il passe au noir)



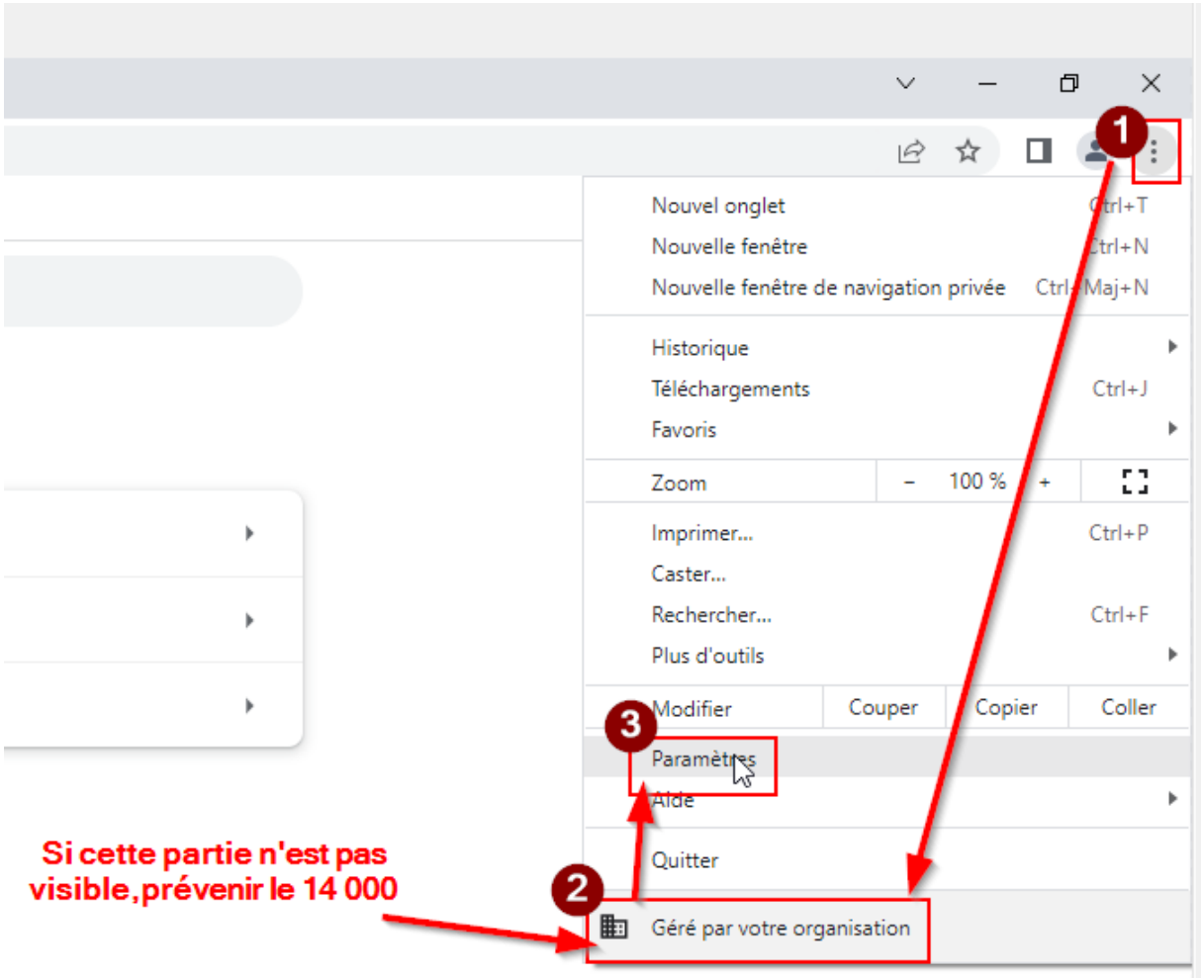
Sur Chrome :

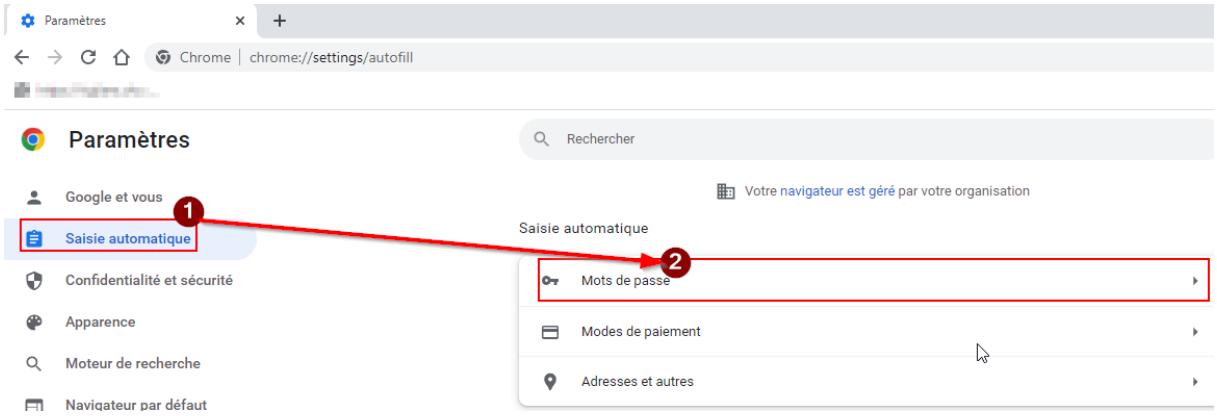
L'utilisation de Chrome doit être évitée au maximum ; pour des sites internes uniquement (pas de www dans l'adresse).

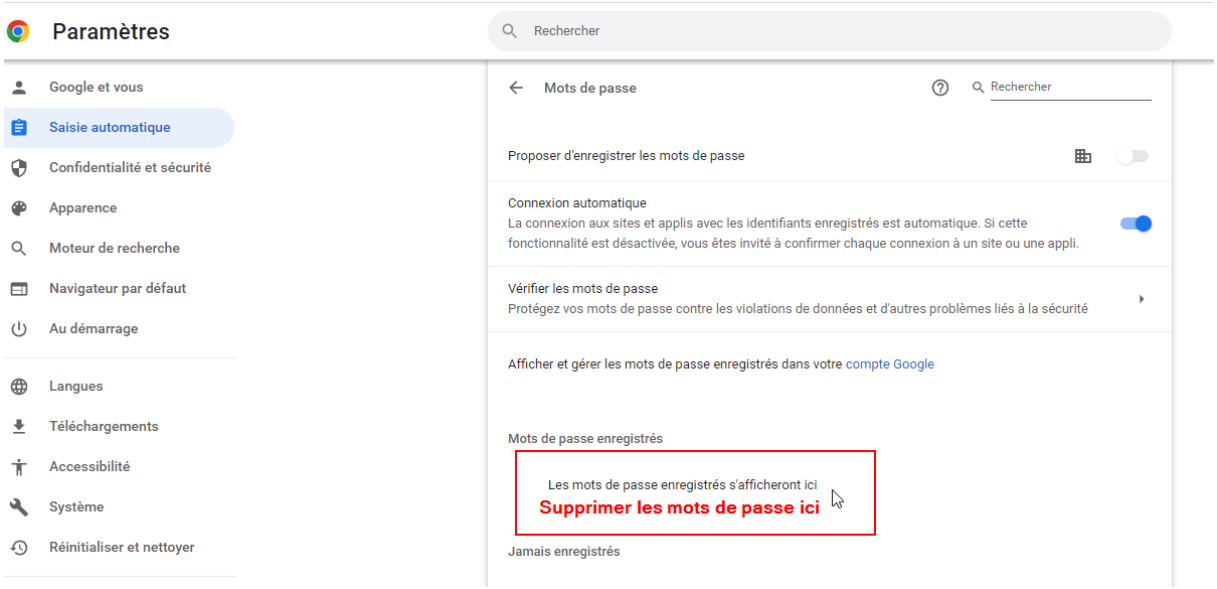


L'enregistrement des mots de passe y est désactivée par défaut, par politique de déploiement interne.

Pour supprimer des mots de passe éventuellement enregistrés avant mise en place de cette politique, suivre ces étapes :


1
Nouvel onglet Ctrl+T
Nouvelle fenêtre Ctrl+N
Nouvelle fenêtre de navigation privée Ctrl+Maj+N
Historique
Téléchargements Ctrl+J
Favoris
Zoom – 100 % +
Imprimer... Ctrl+P
Caster...
Rechercher... Ctrl+F
Plus d'outils
Modifier Couper Copier Coller
3
Paramètres
Aide
Quitter
2
Géré par votre organisation
Si cette partie n'est pas visible, prévenir le 14 000


Paramètres
Chrome | chrome://settings/autofill
Paramètres
Rechercher
Google et vous
Saisie automatique
Confidentialité et sécurité
Apparence
Moteur de recherche
Navigateur par défaut
Votre navigateur est géré par votre organisation
Saisie automatique
1
2
Mots de passe
Modes de paiement
Adresses et autres



IV. RÉFÉRENCES

V. ÉVALUATION

VI. DOCUMENTS ASSOCIÉS

VII. HISTORIQUE DU DOCUMENT

Date	Acteur	Objet
29/11/2022	Gilles RICHARD	Ajout informations pour poste partagé / en autologon
27/10/2022	Gilles RICHARD Ingénieur Référent Application, Pôle Fonctions Support et investissement, Services Numériques, Cellule Sécurité	Rédaction initiale

VIII. RÉDACTION, VALIDATION, APPROBATION

Groupe de travail :

NOMS ET FONCTIONS DES SIGNATAIRES	DATES DE SIGNATURE
Relecture qualité	
Ingénieur qualité, Pôle Efficience, Finances et Qualité	
Rédaction	
RICHARD Gilles, Ingénieur Référent Application, Pôle Fonctions Support et investissement, Services Numériques, Cellule Sécurité	**18/11/2022**
Validation	
ROUSSELLE Julien, Ingénieur Responsable de la Sécurité des Systèmes Informatiques, Pôle Fonctions Support et investissement, Services Numériques	18/11/2022
Approbation	
Directeur qualité, Pôle Efficience, Finances et Qualité	