Table des matières

Premier lancement	3
Gestion des secrets	5
Intégration au navigateur	9
Gestion des mots de passe TOTP	11
Autres secrets	13
Protection de la base de données	14
Stockage	14
Durcissement	14

Public : tout public

Gérer ses mots de passe avec KeePassXC

KeePassXC est un gestionnaire de mots de passe multiplateformes. Il fonctionne aussi bien sur Linux que sur macOS ou Windows, des clients sur Android et iOS sont disponibles.

Il stocke les secrets (essentiellement les mots de passe) dans un fichier KDBX. Ce fichier est à voir comme un conteneur sécurisé : il doit donc être protégé par un « mot de passe fort » (relire à ce sujet les recommandations du RSSI sur les comptes et mots de passe) et doit être très soigneusement sauvegardé.

La suite constitue une prise en mains succincte. Se référer à la documentation officielle pour aller plus loin :

- Getting Started Guide
- User Guide

Premier lancement

Attention : sur Windows, depuis la vers 2.7.0 (21 mars 2022), des utilisateurs pourront avoir besoin d'installer aussi Microsoft Visual C++ Redistributable (si des messages d'erreur apparaissent, messages mentionnant des bibliothèques DLL manquantes).

Après installation, créer un nouveau conteneur : menu Base de données » Nouvelle base :

• • •	Créer une nouvelle base	de données KeePassXC
	Renseignements généraux (de la base de données
	Veuillez saisir le nom d'affichage données :	e et une description facultative pour votre nouvelle base de
	Nom de la base de données :	Mots de passe
	Description :	
		Aller au précédent Continuer Annu

Se laisser guider en gardant les paramètres par défaut :

Créer une nouvelle base de données KeePassXC
Paramètres de chiffrement
Vous pouvez régler ici les paramètres de chiffrement de la base de données. Ne vous inquiétez pas, vous pourrez les changer ultérieurement dans les paramètres de la base de données.
Format de la base de données : KDBX 4 (recommandé)
Paramètres de chiffrement :
Général Avancé
Temps de déchiffrement : 1.0 s
100 ms 5.0 s
Les valeurs plus élevées offrent plus de protection, mais l'ouverture de la base de données prendra plus de temps.
Aller au précédent Continuer Annule

Choisir un mot de passe « robuste » et enregistrer le fichier.



Le mot de passe doit être d'autant plus robuste qu'il sera la principale défense si le fichier finissait aux mains d'un acteur malveillant. Comme ce sera le seul ou presque dont il faut se souvenir, entre 16 et 20 caractères comprenant lettres, chiffres, caractères spéciaux, etc. sont un minimum.

Gestion des secrets

		2
E Racine	0 O Titre	▲ No
	Racine	×
	Général Partager	
Pacharahas at Étiquattas	Saisie automatique Activé	
ह्य Effacer la recherche	Recherche Activé	
ରେ Toutes les entrées	Expiration Jamais	
🛱 Expirés	Notes	
ର୍ଲ୍ Mots de passe faibles		
		0 entrée

Dans le menu Entrée, choisir Nouvelle entrée pour enregistrer un premier mot de passe :

n Itilisateur e passe example.com				
tilisateur e passe example.com				•
e passe example.com				
example.com				: •
/11/2024 14:39			▼ Pré	éréglages 🔻
	/11/2024 14:39	/11/2024 14:39	/11/2024 14:39	/11/2024 14:39 Pr é

Ici, le mot de passe est de piètre qualité comme l'indique le niveau de couleur jaune ambre en

dessous. Cliquer à droite au bout du cartouche du mot de passe sur l'icône : et le générateur de mot de passe s'ouvre :

JF3Gw7	/T2nZdz							\odot	G	Ê
Qualité du r	mot de pas	se : Faible					Entropie	: 71.45 bits		
Mot de	passe	Phrase d	e passe							
Longueu	ur:					12		¢	Avancé	
Types d	le caract	ères								
	A-Z	a	-z	0-9	/ * + 8	k	ASCII éten	du		
						Fermer	Appliqu	uer le mo	t de pass	e

Un mot de passe de seulement 12 caractères ne donne pas une entropie d'au moins 80 bits, il est considéré comme faible.

En théorie de l'information, l' nentropie de Shannon mesure la quantité d'information, le degré d'originalité, d'aléa, de désordre dans une information. Un mot de passe est considéré comme robuste au delà de 80 bits d'entropie.

Augmenter la longueur à 16 caractères et l'entropie devient bonne (le mot de passe est maintenant souligné en vert) :

			Générer	un mot de passe		
xFV4sJ1	LgUUw7zE	Kw				• C E
Qualité du mo	ot de passe :	Bon			Entropie : 87.4	0 bits
Mot de pa	asse Ph	rase de passe				
Longueur					16	Avancé
Types de	caractère	S				
	A-Z	a-z	0-9	/ * + &	ASCII étendu	
				Fermer	Appliquer le	e mot de passe

Enregistrer en cliquant sur OK en bas à droite.

Revenu à l'interface précédente, une entrée s'est ajoutée dans la fenêtre du haut.

Pour copier le mot de passe, sélectionner cette entrée et appuyer sur le raccourci clavier ctrl-c ou 光-c. En particulier, il n'y a pas besoin d'afficher le mot de passe pour le copier, ainsi il peut rester masqué.

Le mot de passe est copié pour une durée de 20 secondes :



Intégration au navigateur

Disposant maintenant d'un gestionnaire de mots de passe robuste et bien protégé, on peut l'intégrer aux navigateurs. Pour cela, ouvrir les préférences :

Paramètres de	l'application	
	Activer l'intégration aux navigateurs	
P	Général Avance	
Général	KeePassXC-Browser is needed for the browser integration to work. Download it for <u>Firefox</u> and <u>Google Chrome / Chromium / Vivaldi / Brave</u> and <u>Microsoft Edge</u> .	
	Activer l'intégration pour ces navigateurs :	
O Sécurité	Google Chrome ✓ Firefox Navigateur Tor Edge ✓ Chromium Vivaldi Brave	
	 Demander de déverrouiller la base de données si elle est verrouillée Correspondance du type d'URL (ex. : https://exemple.com) Retourner que les identifiants qui correspondent le mieux 	
Intégration aux navigateurs	Permettre de retourner des identifiants expirés Chercher les identifiants correspondants dans toutes les bases de données ouvertes	
>_ v		

Activer l'intégration et choisir les navigateurs à autoriser. Ajouter aux navigateurs considérés les plugins correspondants comme indiqué.

On note le logo de KeePassXC à droite du cartouche.

Mot de passe*	Adresse lecnam.net ou nom d'utilisateur*	
	Mot de passe*	۲

Lorsque le navigateur cherche à accéder à un secret dans KeePassXC, celui-ci demande une validation.



Le logo de KeePassXC est vert lorsqu'une entrée est trouvée dans le gestionnaire :

r and a second se	
Mot de passe*	۲

Gestion des mots de passe TOTP

Comme les mots de passe ne sont pas assez fiables, de plus en plus d'applications requièrent un second facteur d'authentification, souvent un mot de passe à usage unique (appelé TOTP pour *Timebased One Time Password*). KeePassXC est en mesure de gérer ces mots de passe à usage unique.

L'application et l'utilisateur doivent partager (à travers un canal fiable !) un secret. En conjuguant ce secret à l'heure courante¹⁾, on obtient un code sur 6 chiffres et valable 30 secondes²⁾.

Exemple avec le webmail (cf. Configurer l'authentification à deux facteurs sur webmail.cnam.fr) :

Authentification en deux étapes



Code de sauvegarde

724064466	819031104
174 626	155 1591
48:221432	820 1072
391, 1251	701 21578
4.19.96 (see	

Si vous ne pouvez pas recevoir les codes par Google Authenticator, vous pouvez utiliser les codes de sauvegarde pour vous connecter. Après avoir fait cela, il deviendra inactif.

Dans KeePassXC, ajouter une entrée webmail ; dans le menu Entrées, ouvrir TOTP puis Configurer TOTP et coller la clef dans le cartouche :



Ne pas toucher aux autres paramètres et enregistrer. Une horloge apparaît alors à gauche de l'entrée. Lorsque l'entrée est sélectionnée, le code et sa durée de vie apparaissent en bas à droite :



Autres secrets

KeePassXC permet de stocker des fichiers et toute sorte d'attributs, dont les codes de récupération fréquemment fournis par les applications requérant un second facteur :

	} ▼ (+)		e e	਼ਾ	Ð	 •	ſ•.]	කි	Rechei	rche (೫		
								Ъ.				
Racine • Ajou	ter une entr	ée										
	Attributs	supplément	aires									
										A	jouter	
Entrée											pprimer	
										Modi		
E,										✓	Protége	r
Avancé										R	évéler	
~	Fichiers je	oints										
\odot				Nom					Taille		Αјοι	ıter
lcône											Suppi	
•											Ouv	/rir
										Annu	ıler	ок
												3 entrées

Protection de la base de données

Stockage

Le fichier .kdbx contenant la base de données doit être protégé. Comme toute donnée importante, il doit être stocké :

- sur trois supports différents (disque, clef USB...),
- à trois endroits différents.

Ne jamais stocker de base de données de mots de passe « dans le cloud », même protégé par un mot de passe robuste.

Durcissement

Pour renforcer la sécurité de la base de données, un second facteur d'authentification peut être ajouté :

- soit un fichier de clef
- soit jeton matériel (comme OnlyKey Yubikey)

Dans le menu Base de données » Paramètres de la base de données » Sécurité :

E B V + Ø 8	음, 약 🐑 🐨 T 💽 韓 으 Recherche (兆F)		
, P.	Identifiants de la base de données Paramètres de chiffrement Mot de passe défini, cliquez pour le modifier ou le supprimer		
Général	Modifier le mot de passe Suppr	Supprimer le mot de passe	
Sécurité Definition aux navigateurs	Fichier clé Générez un nouveau fichier clé ou choisissez un fichier clé existant afin de p base de données. /Users/cp/fichier-clef-keepass.keyx Note : N'utilisez PAS un fichier qui pourrait être modifié, car cela vous empê déverrouiller votre base de données.	protéger votre (X) àchera de	Générer Parcourir Annuler
K eeShare ▼	Question-réponse If you own a <u>YubiKey</u> or <u>OnlyKey</u> , you can use it for additional security. The key requires one of its slots to be programmed as <u>HMAC-SHA1 Challen</u> g		
		An	inuler Ok

Attention : le fichier de clef et la base de données ne devraient jamais être sur le même support physique ! Par contre, ils doivent tous deux être sauvegardés.

1)

2)

Attention à bien garder les systèmes à l'heure, utiliser NTP.

Variante possible : 8 chiffres valable 60 secondes.

From: https://assistancedsi.cnam.fr/ - Assistance DSI

Permanent link: https://assistancedsi.cnam.fr/kb/1005

Last update: 2025/01/30 16:48

