TP B3 : Synthèse :

HEGO Maxence

Cybercafé :

Dans un premier temps on veut sécuriser les équipements du cyber-café en contrôlant les accès à Internet.

Pour cela on peut utiliser un serveur Proxy.

Serveur Proxy :

Un serveur proxy agit comme un intermédiaire entre les appareils du cyber café et internet.

Il permet entre autres de restreindre l'accès à certains sites internet.

Pour ce cyber café on utilise pfsense.

Pfsense est une solution Open-source qui permet de configurer à la fois un pare-feu et un proxy dans un réseau local.

Pfsense :

Voyons comment cet outil autorise ou non la demande de connexion à un site.

Squid :

On peut configurer dans pfsens Squid qui est un proxy web.

Squid intercepte toutes les requêtes HTTP et HTTPS. Lorsque quelqu'un tente de se connecter à un site, la requête passe d'abord par **Squid,** qui peut analyser l'URL et la comparer à une liste de règles de filtrage.

Si l'URL du site est dans la liste de filtrage (sites sensibles), alors la requête est bloquée.

Téléchargements illégaux :

On veut également protéger le cyber café des téléchargements illégaux qui amènent des risques de malware.

Pfsense permet de se protéger contre les intrusions de malware.

Pour le téléchargement illégal :

- Blocage des sites avec Squid
- Possibilité de limiter les ports utilise en P2P

Pour la protection contre les intrusions et malwares :

- Pare feu qui bloque connexions extérieures
- Snort/Suricata : installation d'un IDS/IPS pour bloquer les intrusions.
- Fonctions VPN et filtrage web possible

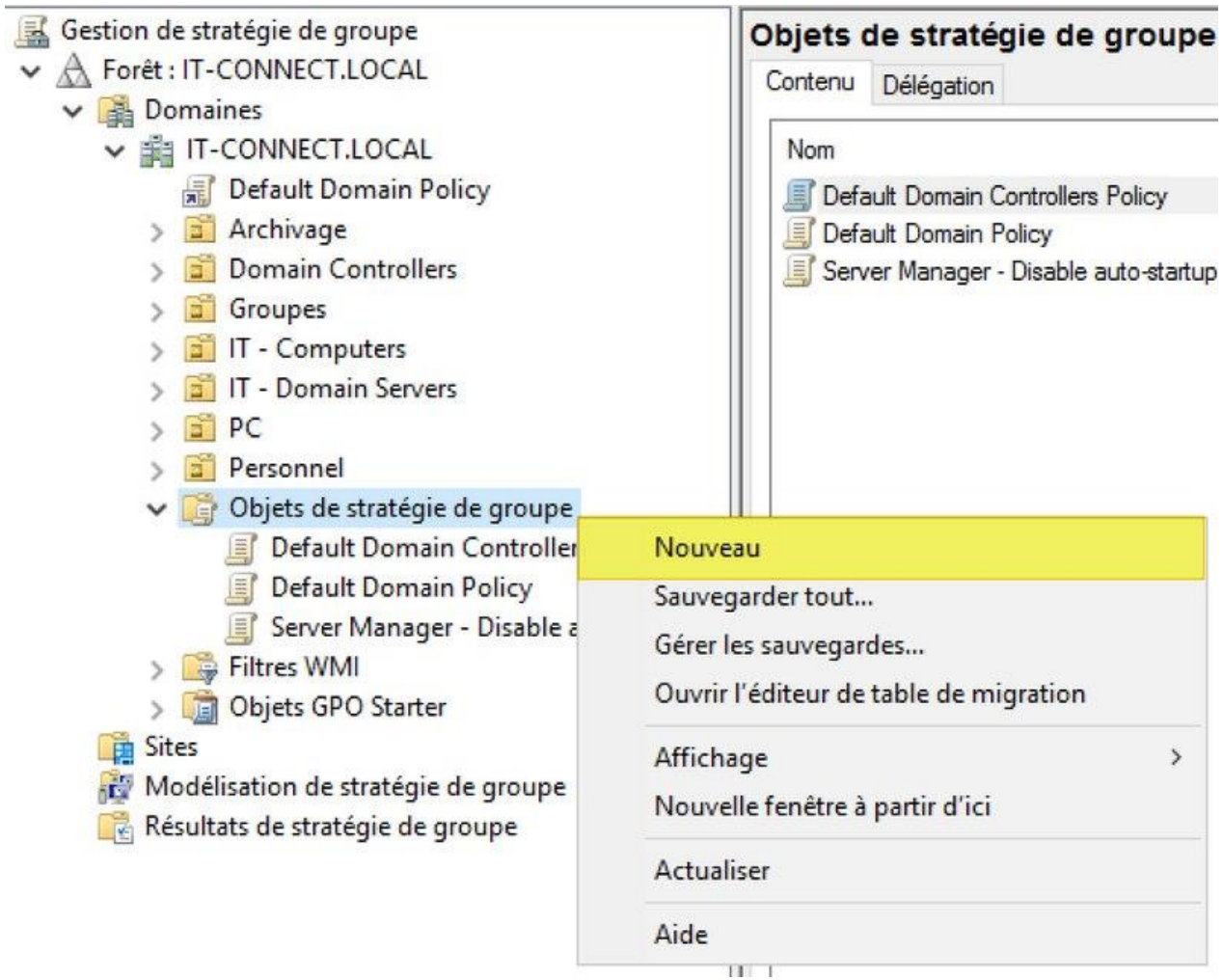
Ports USB :

Afin de prévenir de l'installation de malware, on doit également interdire l'usage des clés USB.

On peut pour cela définir une stratégie de groupe si les PC utilisent Windows.

Une autre solution est de désactiver les ports USB via le BIOS/UEFI

(Voir TP B2: AD DNS)



Mises à jour Windows:

Enfin, pour garantir la sécurité, on doit également prévoir des mises à jour.

Pour cela on utilise l'application Windows Update qui télécharge et installe automatiquement les MAJ du système.

Afin d'augmenter la sécurité on peut aussi installer un antivirus ou encore un pare-feu.

Pour utiliser windows update :

Allez dans **Paramètres** > **Mise à jour et sécurité** > **Windows Update**.

Windows Update permet d'agir sur les failles de sécurité en :

- Corrigeant les vulnérabilités critiques
- Mettant à jour Microsoft Defender
- Maintenant les pilotes et protocoles à jour.

Lycée :

On veut maintenant réaliser un guide des bonnes pratiques pour encadrer les usages des étudiants.

Dans un premier temps on définit les règles pour les mots de passe.

Pour plus d'informations voir TP : B3 : Identifier les menaces

Règles pour bon mot de passe :

- 12 ou plus caractères
- Utilisation de majuscule, minuscule, caractères spéciaux, chiffres
- Mot de passe unique
- Changement régulier de mots de passes (tous les 3 mois recommandés)

Il est conseillé également de prendre un mot de passe sans lien personnel pour éviter les vulnérabilités liées à l'OSINT.

Afin de trouver un bon mot de passe, on peut utiliser la technique de phrase de passe.

Bonnes pratiques :

En plus des mesures recommandées par l'ANSSI, d'autres bonnes pratiques sont également à respecter.

Bonnes pratiques :

- Ne pas partager les mots de passe
- Utiliser un mot de passe différent pour chaque compte
- Utiliser un coffre-fort de mot de passe pour la mémorisation ou phrase de passe.
- Utilisation de l'authentification double facteur si possible

Phrase de Passe :

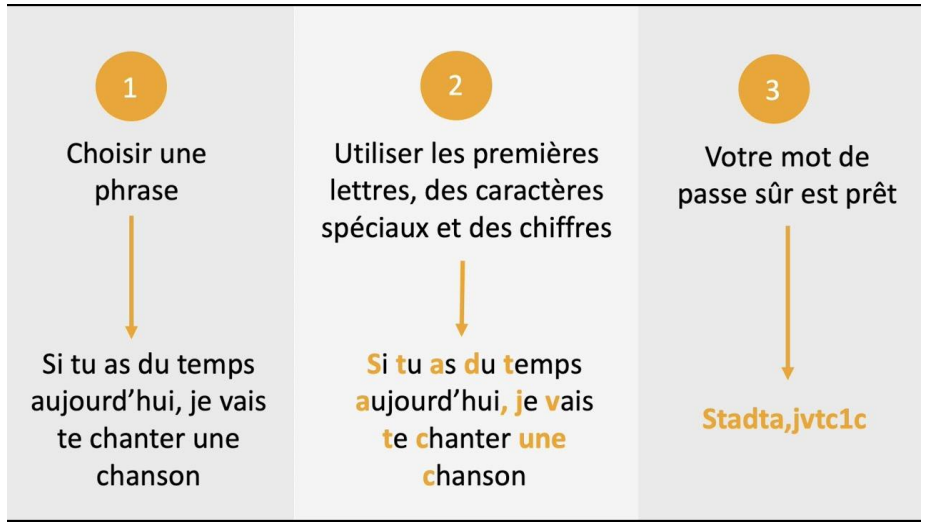
Afin de créer une phrase de passe, on peut utiliser deux principales méthodes.

1. Méthode des mots aléatoires (ou méthode "diceware")

- Choisir plusieurs mots aléatoires issus d'une liste prédéfinie (par exemple, une liste de mots du dictionnaire).

2. Méthode mémotechnique basée sur une phrase personnelle

- Créer une passphrase à partir d'une phrase significative en prenant les premières lettres de chaque mot.

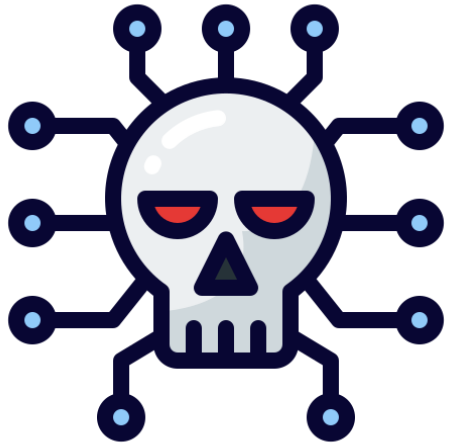


Mauvaises pratiques :

Certaines pratiques concernant les mots de passes sont à proscrire :

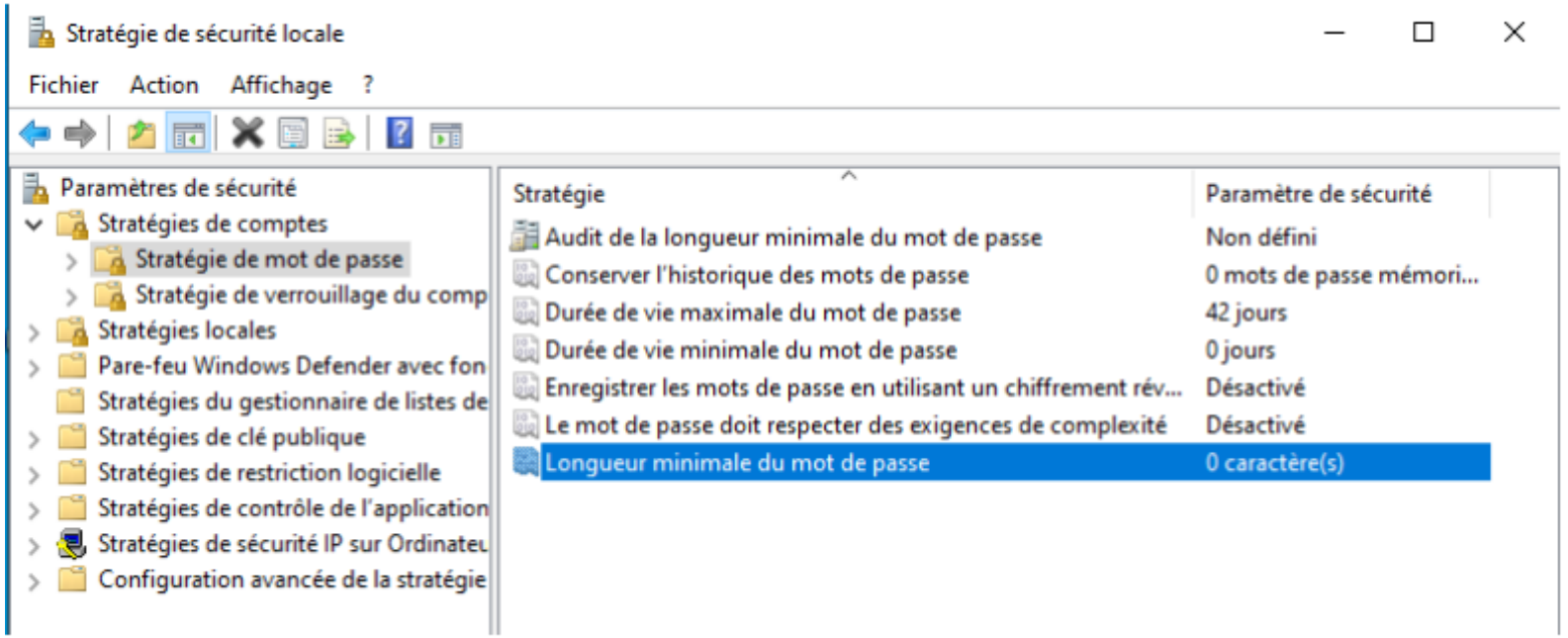
Mauvaises pratiques :

- Enregistrer les mots de passes dans les navigateurs : Risque de sécurité
- Ne pas vérifier les sites internet et le protocole utilisé
- Utiliser des connexions non sécurisées : réseau wifi public
- Télécharger des logiciels dont l'éditeur est inconnu
- Réutiliser un ancien mot de passe ou le modifier que très légérement.



Stratégies de sécurité global :

Voyons les stratégies définies ci-contre :



Rôle des stratégies :

Longueur minimal : taille du mot de passe

Exigence de complexité : pas réutiliser le login et autres exigences de complexité

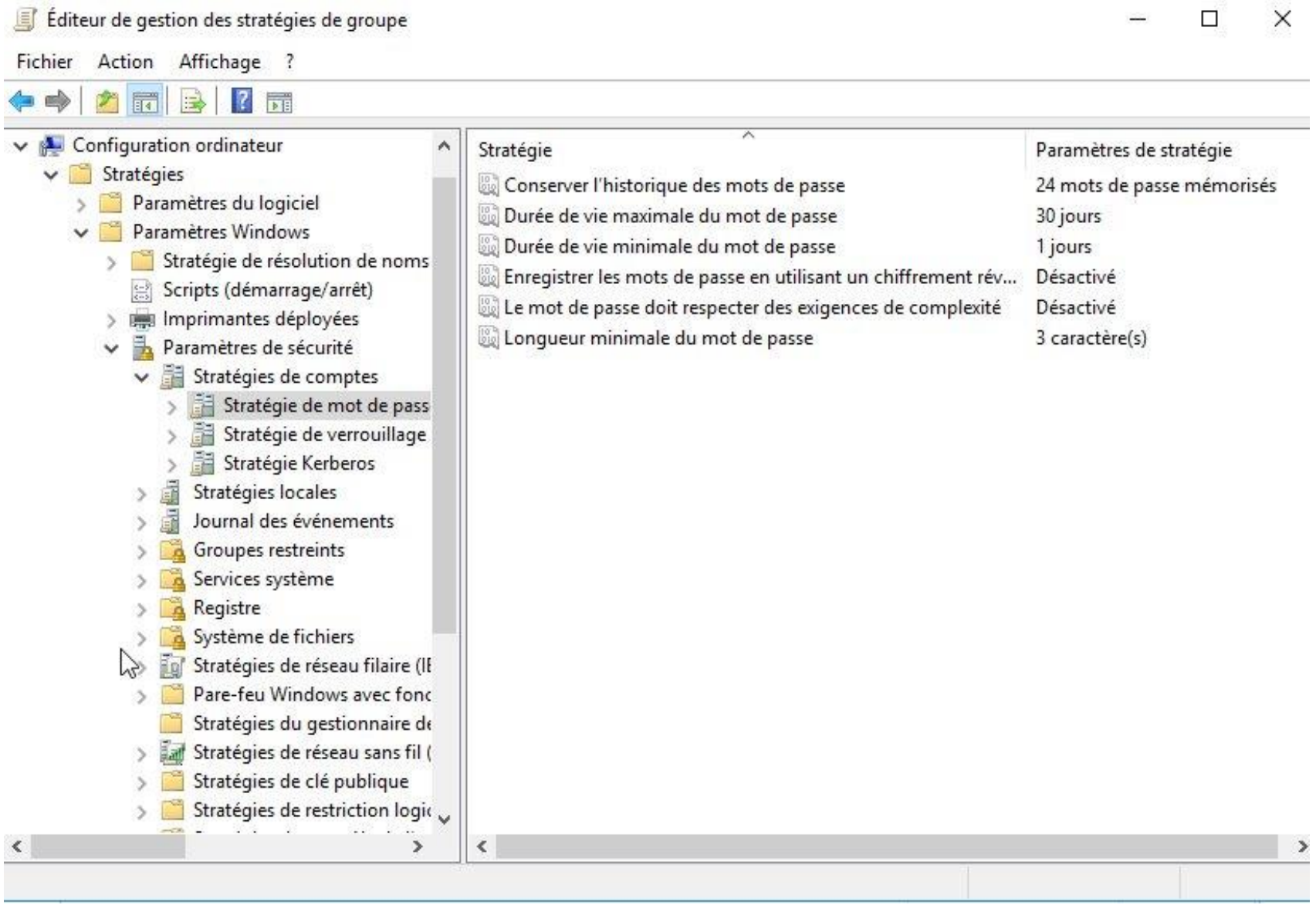
Durée de vie des mots de passes : temps avant changment obligatoire

Historique des mots de passe : si on peut réutiliser un ancien mdp

Utiliser un chiffreemnt : si les mots de passes sont stocké en clair ou non

Stratégies de sécurité mdp :

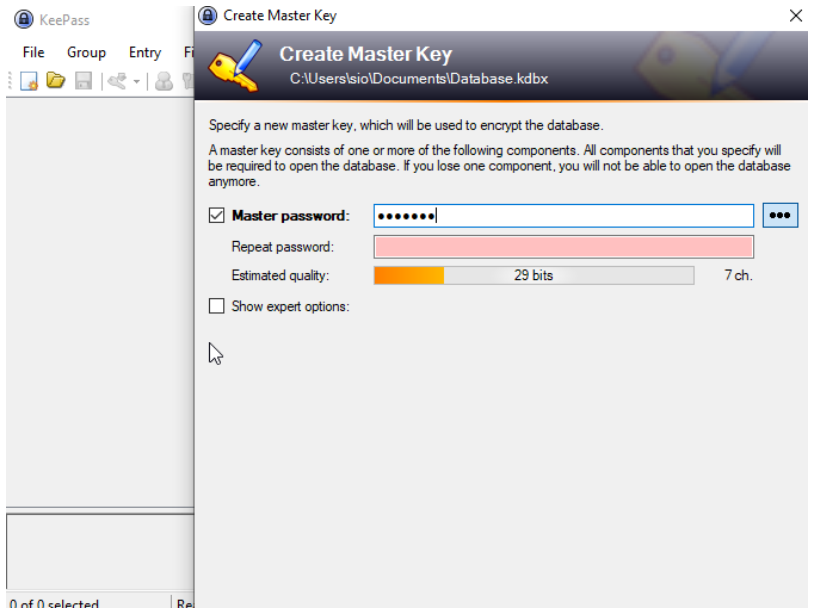
On applique ces stratégies sur la VM Windows :



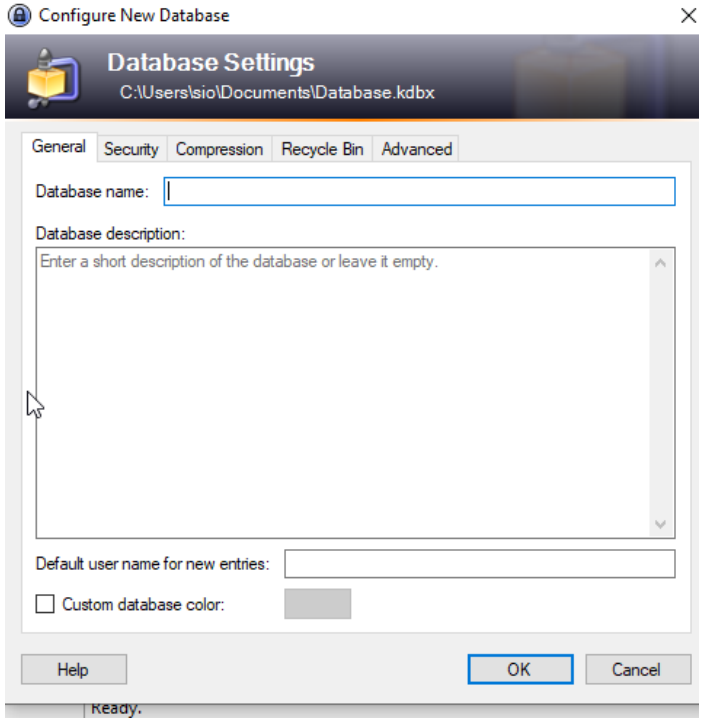
Gestion des mots de passe :

Afin de gérer les mots de passe on utilise un coffre-fort de mot de passe. On choisit d'utiliser KeePass.

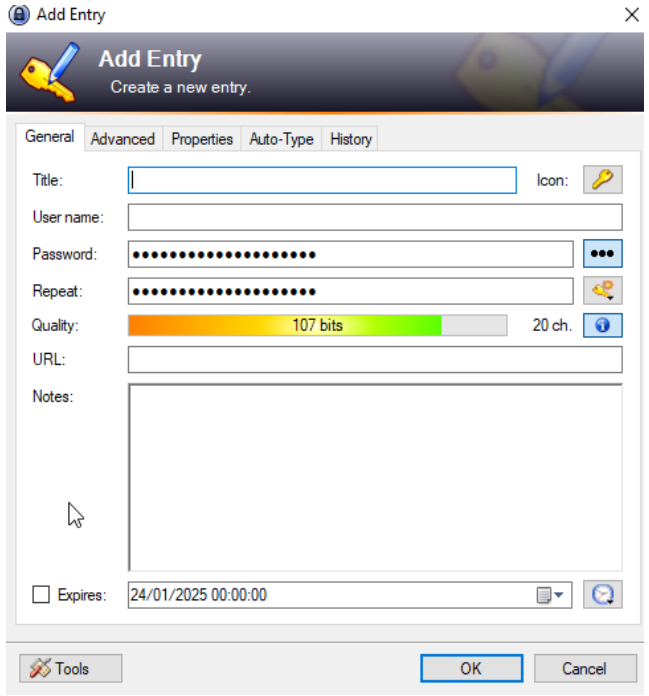
1. On créer une base de donnés
2. On paramètre la base de données
3. On définie le mdp



1



2



3

Avantages et inconvénients :

Voici un tableau récapitulatif des avantages et inconvénients :

Avantages	Inconvénients
Open source et gratuit	Sécurité depend du mdp initial
Relativement facile d'utilisation	Interface utilisateur inférieur aux concurents
Chiffrement des mdp pour une meilleur sécurité	Pas de stockage cloud des mots de passes, syncronisation à faire sur chaque appareil
Facilite la gestion des mots de passe	