outil à configurer au sein de son réseau local pour filtrer les connexions internet

Expliquez de quelle manière cet outil autorise ou non la demande de connexion à un site spécifique.

Grâce au filtrage DNS de périmètre 81 le gérant pourra:

Contrôle l'accès : empêchez les clients d'accéder à des sites non autorisés et dangereux.

Filtrage avancé: permet une gestion facile des filtres Web sur l'ensemble du Web.

Liste noire et liste blanche: Aide à mettre sur liste noire les adresses IP et les noms de domaine nuisibles, et sur liste blanche la liste des destinations de sites Web que les clients devraient visiter.

Blocage de catégorie: permettre de bloquer certains sites Web par catégorie, tels que les réseaux sociaux, les sites de jeux d'argent, les sites pornographiques, etc.

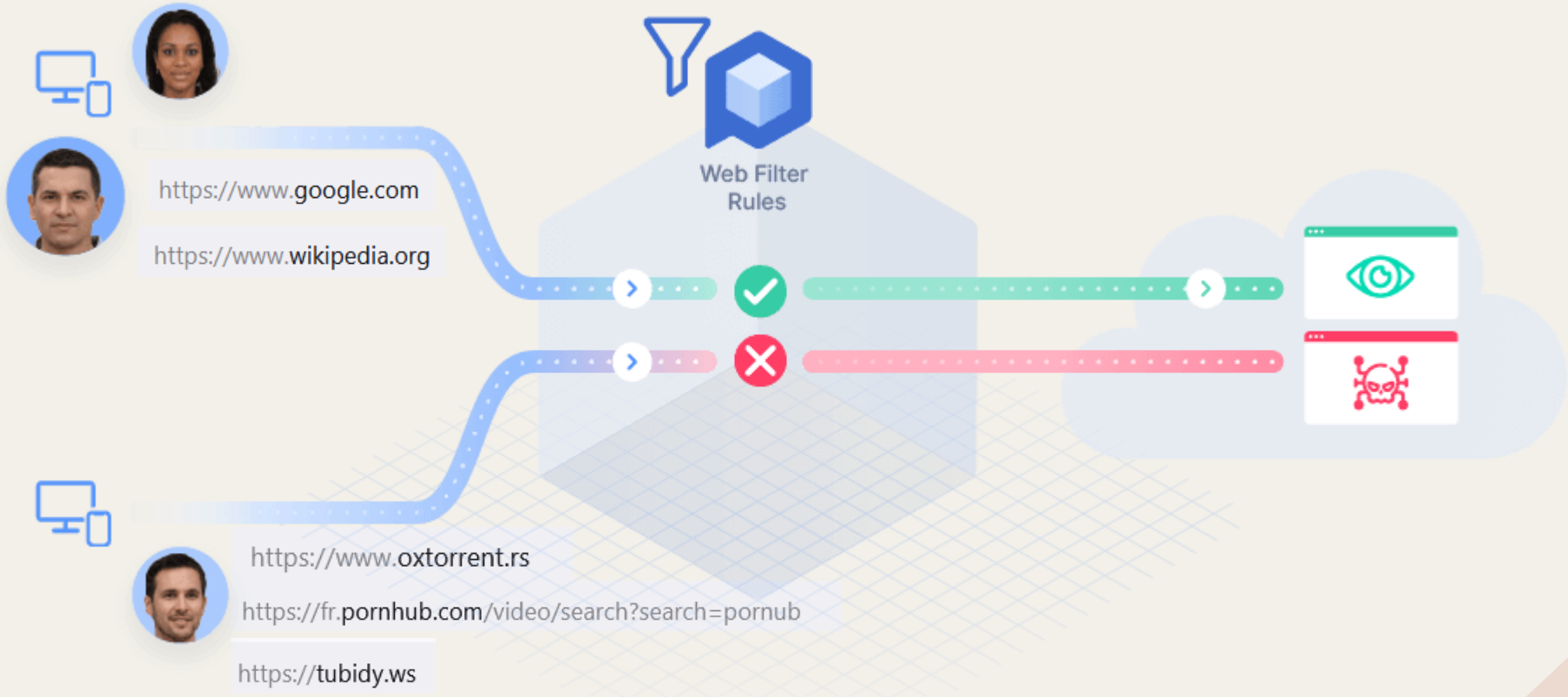
Sécurité améliorée: limitez les sites malveillants et les logiciels malveillants pour améliorer la sécurité de votre réseau.

Contrôles basés sur des stratégies: utilisez des contrôles basés sur des stratégies pour surveiller l'accès via le filtrage et le blocage.

Visibilité complète et segmentation précise: offre une visibilité complète, une segmentation précise et des solutions centrées sur l'utilisateur.

Évolutivité: hautement évolutif, permettant une transition facile vers les environnements cloud.

Montrez comment l'outil que vous avez proposé peut prendre en charge ces pratiques



Précisez-s ’il permet de se protéger contre les intrusions malwares.

Oui, Perimeter 81 offre une protection contre les malwares:

•Perimeter 81 inspecte le trafic web (y compris les téléchargements de fichiers, HTML, JavaScript, CSS, etc.) et recherche d’éventuels malwares avant de permettre l’accès.

Si une menace est détectée, elle est bloquée et les utilisateurs voient une page de notification.

il est activée lorsqu’un utilisateur se connecte à l’agent, et applique automatiquement un niveau supplémentaire de protection sans impacter l’expérience utilisateur.

il a l’avantage unique de protéger les utilisateurs lorsqu’ils sont connectés au réseau d’entreprise ainsi que lorsqu’ils accèdent directement à Internet.

Il utilise un apprentissage automatique avancé pour accélérer la détection et fournir une protection contre les menaces sophistiquées, notamment les APT, les attaques Zero Day et les ransomwares.

Indiquez comment peut-il intervenir sur les postes de travail pour contrôler l'utilisation des supports USB

Pour contrôler l'utilisation des supports USB sur les postes de travail des cybercafés, le responsable peut prendre les mesures suivantes :

- Désactivez le pilote USBSTOR (le pilote USBSTOR est un pilote de port de stockage USB fourni par Microsoft pour gérer les périphériques de stockage de masse USB à l'aide du pilote de classe de stockage natif de Microsoft) : cela empêche l'utilisation du périphérique de stockage USB.
- Utiliser les solutions d'analyse et de désinfection sur support amovible (CD ou DVD, disque dur externe, clé USB) avant chaque utilisation.
- Interdire l'exécution d'applications téléchargées à partir de sources non fiables.
- Restreindre l'utilisation des applications qui nécessitent des autorisations de niveau administrateur pour s'exécuter.

Expliquez quelle précaution supplémentaire il doit prendre pour être certain que la configuration réalisée précédemment soit pérenne.

Pour assurer la pérennité de la configuration, le responsable doit prendre les précautions supplémentaires suivantes:

1. **Mettre à jour régulièrement les logiciels**: Cela permet de bénéficier des dernières mises à jour de sécurité.
2. **Installer un pare-feu** (firewall) logiciel sur le poste et limiter l'ouverture des ports de communication à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail.
3. **Prévoir un mécanisme de verrouillage automatique de session** en cas de non-utilisation du poste pendant un temps donné.
4. **Limiter les droits des utilisateurs** au strict minimum en fonction de leurs besoins sur les postes de travail.
5. **Effectuer des sauvegardes régulières** pour prévenir la perte de données.
6. **Crypter les données sensibles** pour protéger les informations importantes.
7. **Sensibiliser les utilisateurs** aux risques liés à l'utilisation de supports amovibles.

. Indiquez quelle application native sous windows permet d'avoir une version récente du système d'exploitation.

L'application native sous Windows qui permet d'avoir une version récente du système d'exploitation est **Windows Update**. Cette application est intégrée à Windows et permet de télécharger et d'installer les dernières mises à jour du système d'exploitation.

7. Démontrez que celle-ci peut également agir sur les failles de sécurité.

Windows Update peut également agir sur les failles de sécurité.

En fait, Microsoft publie régulièrement des mises à jour de sécurité pour corriger les vulnérabilités découvertes dans le système d'exploitation.

Ces mises à jour peuvent corriger des vulnérabilités que des attaquants pourraient exploiter pour exécuter du code à distance sur votre ordinateur.

De plus, il n'est pas recommandé de continuer à utiliser les anciennes versions de Windows car votre ordinateur ne recevra plus de mises à jour de sécurité.

Précisez quel outil supplémentaire peut être installé sur un poste de travail pour garantir sa sécurité

Pour sécuriser du poste de travail, certains outils supplémentaires peuvent être installés. Parmi eux, on peut citer :

KeePass pour la gestion sécurisée des mots de passe

TrueCrypt pour le cryptage des données

AxCrypt pour le cryptage/déchiffrement des fichiers. Ces outils, associés à une utilisation prudente et à des mises à jour régulières du système d'exploitation et des applications, peuvent contribuer à renforcer la sécurité des postes de travail.

En vous appuyant sur les informations données par l'ANSSI, indiquez les spécifications qui doivent être mentionnés dans le guide au sujet de la création des mots de passe utilisés par les étudiants pour leurs connexions au réseau local

D'après les informations fournies par l'ANSSI dans le Guide d'hygiène informatique, voici les spécifications qui doivent être mentionnées dans le guide au sujet de la création des mots de passe utilisés par les étudiants pour leurs connexions au réseau local :

1.Longueur minimale : Le mot de passe doit comporter au moins 12 caractères pour un compte d'utilisateur standard, et au moins 16 caractères pour un compte d'administrateur ou un compte sensible.

2.Complexité : Le mot de passe doit être composé de caractères aléatoires de différentes catégories (lettres majuscules, lettres minuscules, chiffres, symboles). Il ne doit pas contenir de mots du dictionnaire, de noms propres, de dates, de séquences répétitives ou prévisibles, ni d'informations personnelles.

3.Renouvellement : Le mot de passe doit être changé au moins une fois par an, ou plus fréquemment en cas de suspicion de compromission. Il ne doit pas être réutilisé pour plusieurs comptes ou services.

4.Mémorisation : Le mot de passe doit être mémorisé par l'utilisateur et non écrit sur un support physique ou stocké dans un fichier non protégé. Si l'utilisateur a besoin d'un outil pour gérer ses mots de passe, il doit utiliser un gestionnaire de mots de passe sécurisé.

5.Confidentialité : Le mot de passe doit être gardé secret et ne doit pas être partagé avec d'autres personnes, même de confiance. Il ne doit pas être saisi sur un ordinateur ou un réseau non sécurisé, ni transmis par un moyen de communication non chiffré. Il ne doit pas être divulgué en réponse à une sollicitation frauduleuse (phishing, hameçonnage, etc.).

Précisez les recommandations à suivre pour la gestion des mots de passe durant les deux années de BTS

Pour la gestion des mots de passe durant les deux années de BTS, les recommandations sont les suivantes:

- **L'Utilisation d'un mot de passe unique pour chaque compte** : Chaque compte doit avoir un mot de passe unique, en particulier pour les comptes les plus sensibles comme les adresses mails et les usages professionnels.
- **Le Changement régulier des mots de passe** : Les mots de passe doivent être changés régulièrement pour assurer une sécurité optimale.
- **La Non-communication des mots de passe** : Les mots de passe ne doivent pas être communiqués à d'autres personnes.
- **L'Activation de l'authentification à double facteur** : Lorsqu'elle est disponible, l'authentification à double facteur doit être activée pour une sécurité accrue.

Expliquez les deux méthodes utilisées pour définir un mot de passe par passphrase.

Pour définir un mot de passe par passphrase, deux méthodes peuvent être utilisées:

1.La phrase de passe : Plutôt que de retenir un mot de passe complexe, la phrase est plus longue qu'un mot de passe et plus facile à mémoriser. Elle augmentera considérablement la robustesse de vos accès.

2.L'utilisation d'un coffre-fort de mots de passe : Si vous possédez trop de comptes pour vous souvenir de l'ensemble de vos phrases de passe, vous pouvez également faire appel à l'aide d'un coffre-fort de mots de passe.

Indiquez quelles manipulations ne sont pas souhaitables et expliquez pourquoi

Les manipulations qui ne sont pas souhaitables lors de l'utilisation des identifiants de connexion sont :

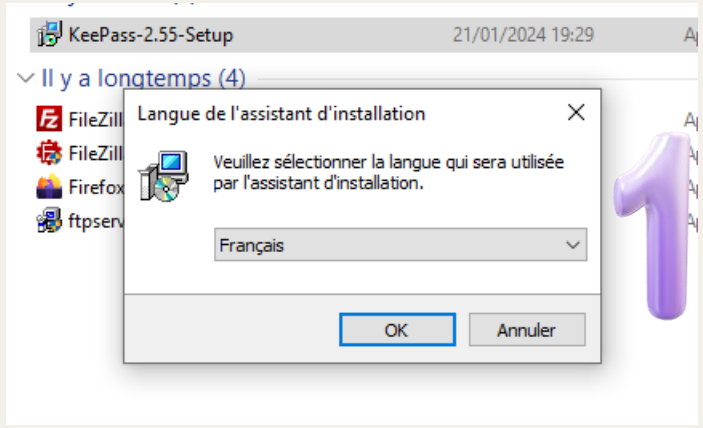
- **Utiliser le même identifiant et le même mot de passe pour tous les sites ou logiciels** : cela augmente le risque de piratage et de vol d'informations personnelles ou professionnelles.
- **Enregistrer les identifiants de connexion dans le navigateur ou le logiciel** : cela facilite l'accès aux sites ou logiciels, mais cela rend aussi les identifiants de connexion plus vulnérables aux attaques informatiques ou aux accès non autorisés.
- **Partager les identifiants de connexion avec d'autres personnes** : cela compromet la sécurité et la confidentialité des données et des travaux réalisés avec les identifiants de connexion.
- **Utiliser des identifiants de connexion trop simples ou évidents** : cela facilite le devinage ou le craquage des identifiants de connexion par des personnes malveillantes. Il est préférable d'utiliser des identifiants de connexion complexes et variés, comprenant des lettres, des chiffres et des symboles.

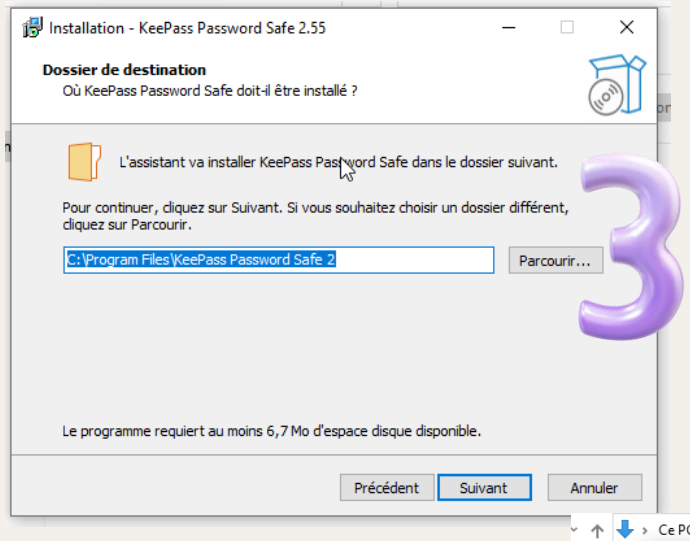
Expliquez le rôle des différentes stratégies de sécurité locales présentées ci-dessous.

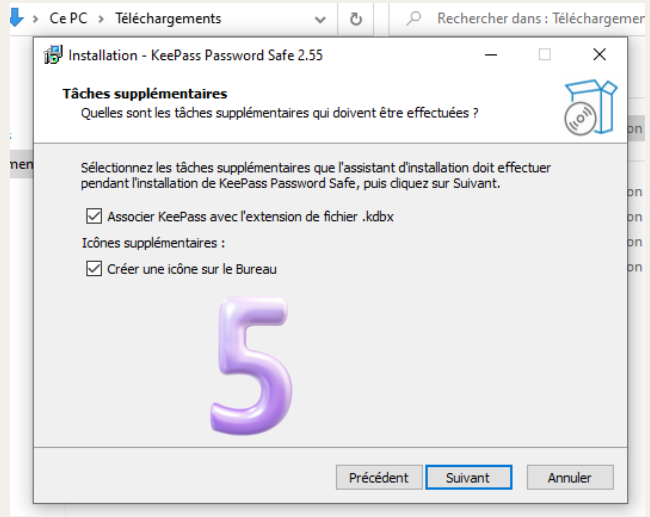
1. L'audit de la longueur minimal du mot de passe : C'est une stratégie qui vérifie que le mot de passe a une longueur adapter qui respecter les recommandations de la sur la longueur du mot de passe.
2. Conserver l'historique des mots de passe :Cette stratégie permet que aucun mot de passe ne soit enregistré ni conserver sur le poste ce qui permet plus de sécurité lors d'une attaque.
3. Durée de vie maximale du mot de passe : Cette stratégie permet que au bout de 'é jours le mot de passe n'est plus utilisable donc à respecter les recommandations de changement régulier du mot de passe.
4. Durée minimale d'un mot de passe: Cette stratégie permet de changer le mot de passe au bout de 0 jour minium.
5. Enregistrement de mot de passe en utilisant le chiffrement réversible :Cette stratégie est utilisée pour prendre en charge les applications qui nécessitent le mot de passe de l'utilisateur pour l'authentification.
6. Le stockage des mots de passe chiffrés d'une manière réversible signifie que les mots de passe chiffrés peuvent être déchiffrés. Sur l'exemple elle est désactivée car elle présente un risque de sécurité car un attaquant compétent capable d'interrompre ce chiffrement peut alors se connecter aux ressources réseau à l'aide du compte compromis.
7. Le mot de passe doit respecter des exigences de complexité: cette stratégie sert à renforcer la sécurité des comptes utilisateurs. Elle impose certaines règles pour la création de mots de passe, ce qui rend plus difficile pour les attaquants de deviner ou de craquer les mots de passe.
8. Longueur minimale du mot de passe: Cette stratégie sert à définir une longueur obligatoire pour chaque mot de passe qui sera créer.

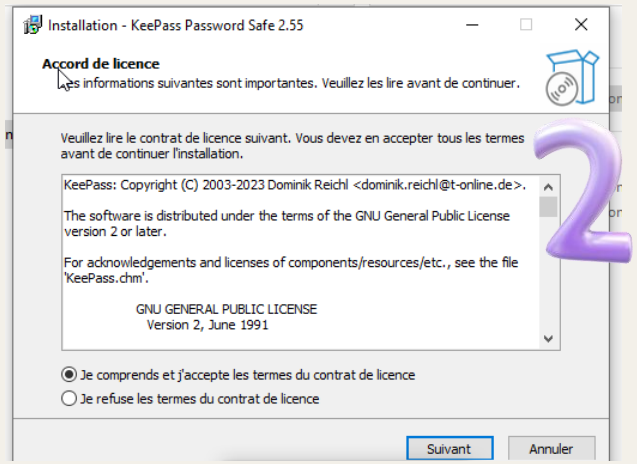
II. Gestion des mots de passe

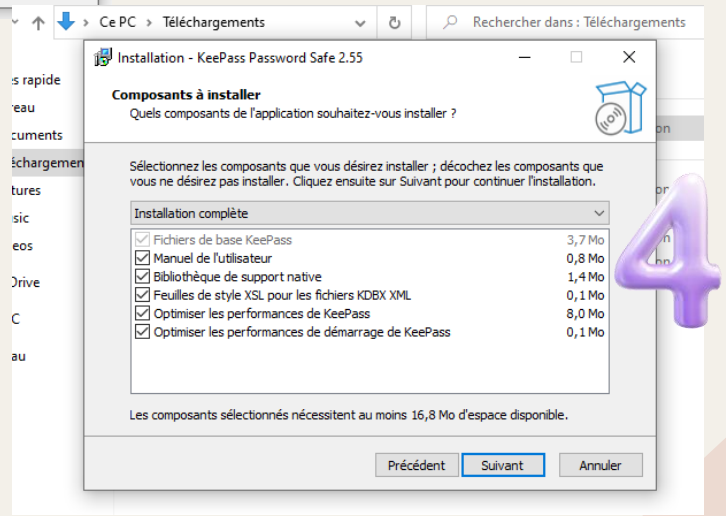
Installez l'outil Keepass sur une VM.



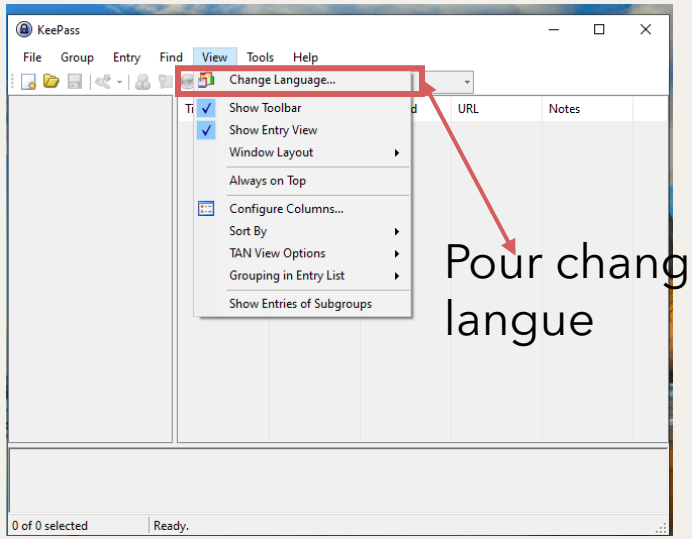






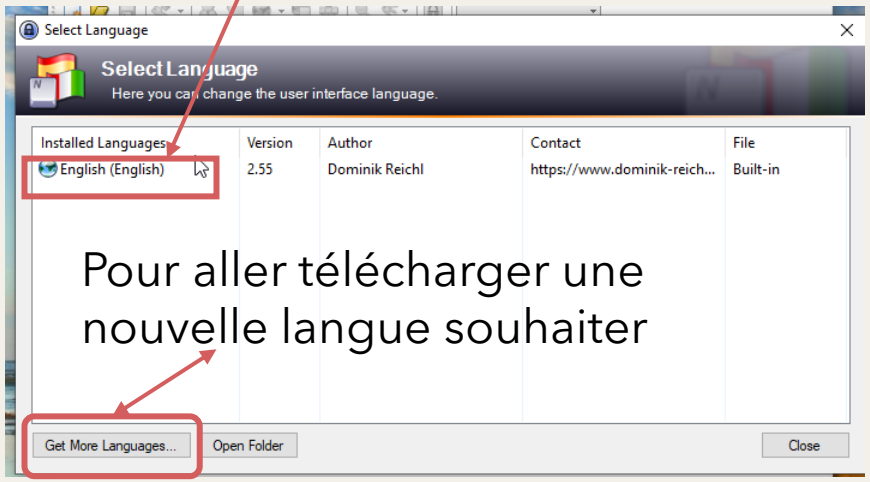


Changement de langue



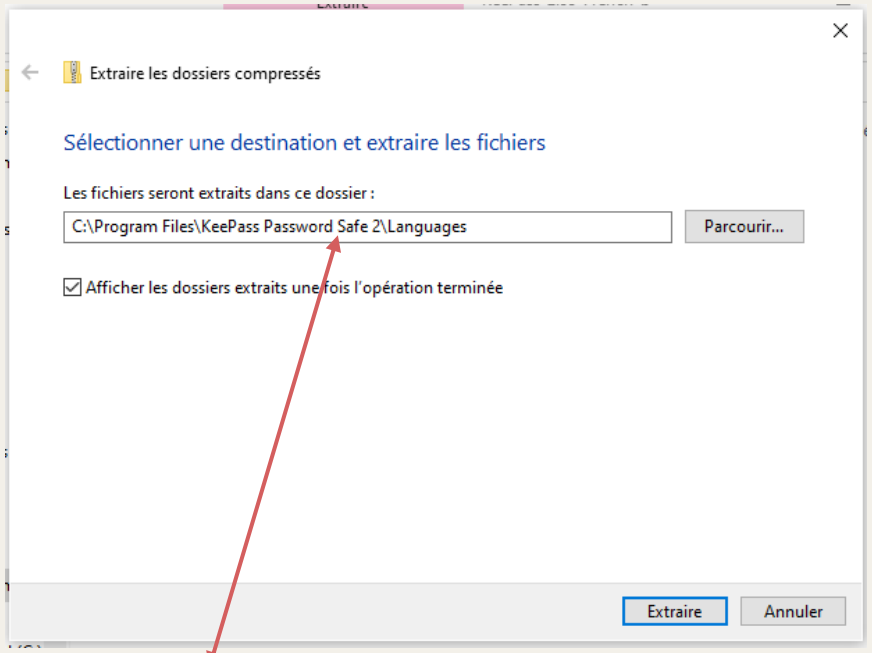
Pour changer la langue

Ici il n'y a pas encore le français dans le répertoire de la

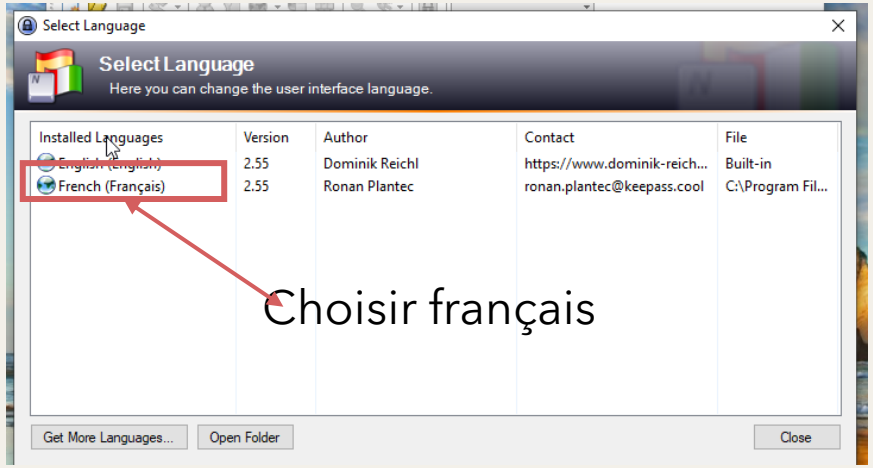


Pour aller télécharger une nouvelle langue souhaiter

Dans notre cas c'est le français donc choisir la même version que le keepass

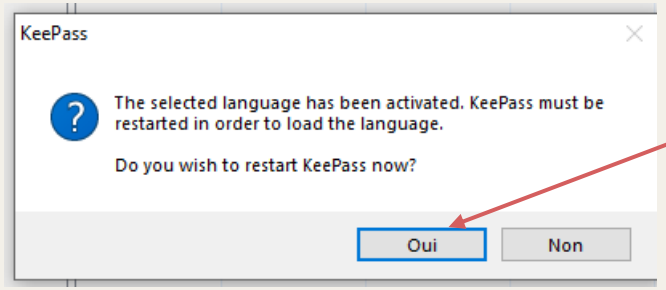


Extraire le fichier télécharger et le mettre dans le fichier langue qui se trouve au même endroit que votre fichier keepass



Choisir français

Ouvrer keepass une nouvelle fois et aller dans modifier la langue



Accepter que la keepass soit redémarrer en cliquant sur oui

La barre d'outils est maintenant en français

Créer une base de données pour stockés les mots de passe