EasyLock

Manuel de l’utilisateur Version 2.0.0.0

Manuel de l’utilisateur

COSOSYS

Table des matières

1. Introduction

La protection des données en transit est essentielle afin de s'assurer qu'aucun tiers n'ait pas l'accès aux données en cas où un dispositif est perdu, égaré ou volé. EasyLock permet aux dispositifs portables d'être identifiés comme TrustedDevices (en combinaison avec Endpoint Protector) et protège les données sur le dispositif par cryptage AES 256bit mode CBC approuvé par le gouvernement.

Avec l'interface intuitive glisser-déposer, les fichiers peuvent être rapidement copiés de et sur le dispositif pour un flux de travail rapide, sécurisé et efficace.

EasyLock est une application portable qui ne requiert aucun processus d'installation sur l'ordinateur hôte et est toujours portable. Partout où le dispositif portable de stockage est déplacé, EasyLock est enregistré sur le dispositif et peut être utilisé sur tous ordinateurs Windows, Mac ou Linux.

2. Configurations requises

Afin de configurer EasyLock, on a besoin d'un ordinateur avec un port USB disponible et un dispositif USB.

Les systèmes d'exploitation supportés sont:

- Windows 7 (toutes les versions)
- Windows Vista (toutes les versions)
- Windows XP (Service Pack 2 est recommandé)
- Mac OS 10.5 ou plus récente
- Linux - openSUSE 11.2 (d'autres systèmes peuvent être disponibles par demande).

On peut utiliser un dispositif USB de stockage tel qu'une clé USB, un disque dur externe, une carte de mémoire etc.

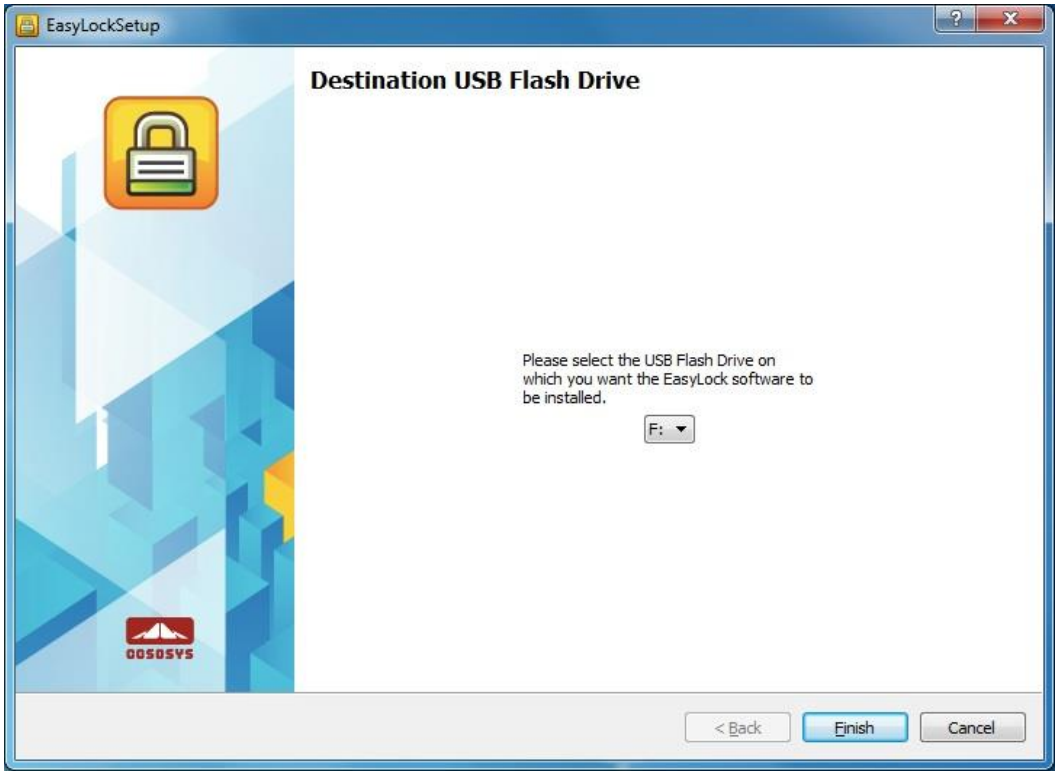
Si le dispositif portable de stockage detient un commutateur manuel de protection (verrouillage), il doit être dans la position non verrouillé (écriture permise) afin de pouvoir utiliser EasyLock.

EasyLock ne requiert pas de droits d'administration.

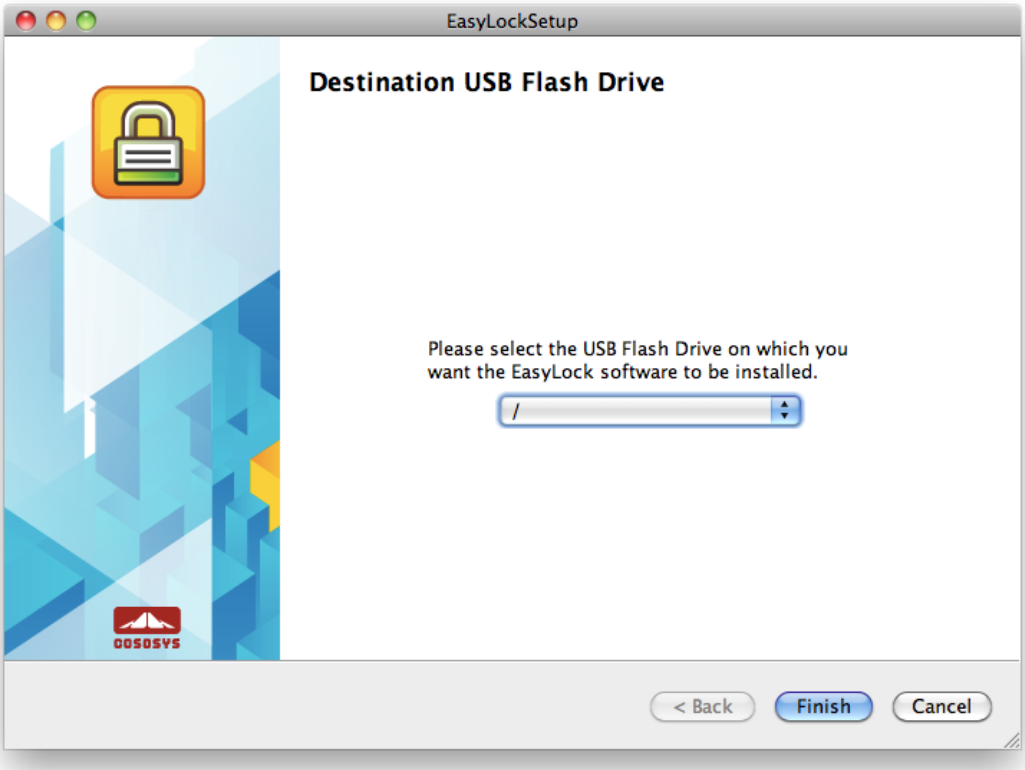
3. L’installation

Pour installer EasyLock sur une clé USB (ou d’autres dispositifs USB portables de stockage):

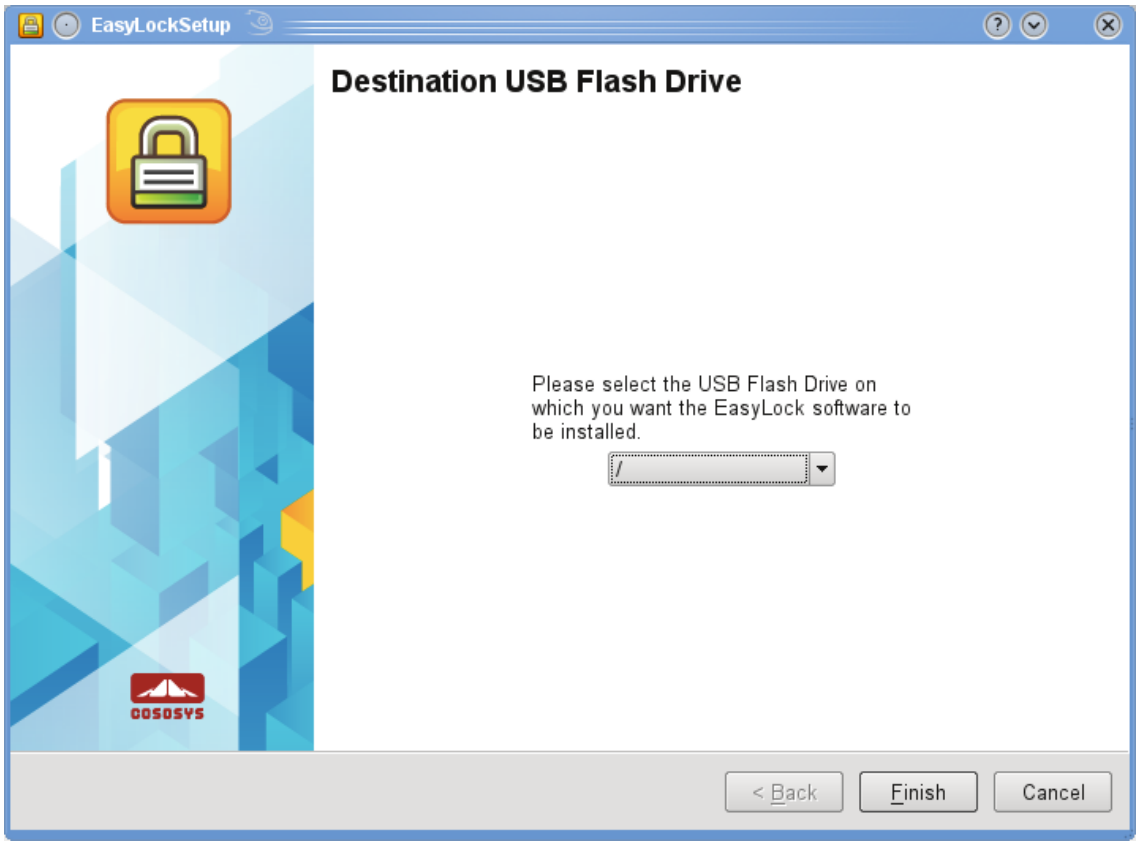
- **Sur le SO Windows**: exécutez le fichier “EasyLockSetup.exe”, sélectionnez la lettre du lecteur correspondant au dispositif USB et appuyez sur “Finish”. L’application EasyLock sera installée automatiquement dans le répertoire racine du dispositif sélectionné.



- **Sur le SO MAC**: exécutez le fichier "EasyLockSetup.dmg", sélectionnez la lettre du lecteur correspondant au dispositif USB et appuyez sur "Finish". L'application EasyLock sera installée automatiquement dans le répertoire racine du dispositif sélectionné.



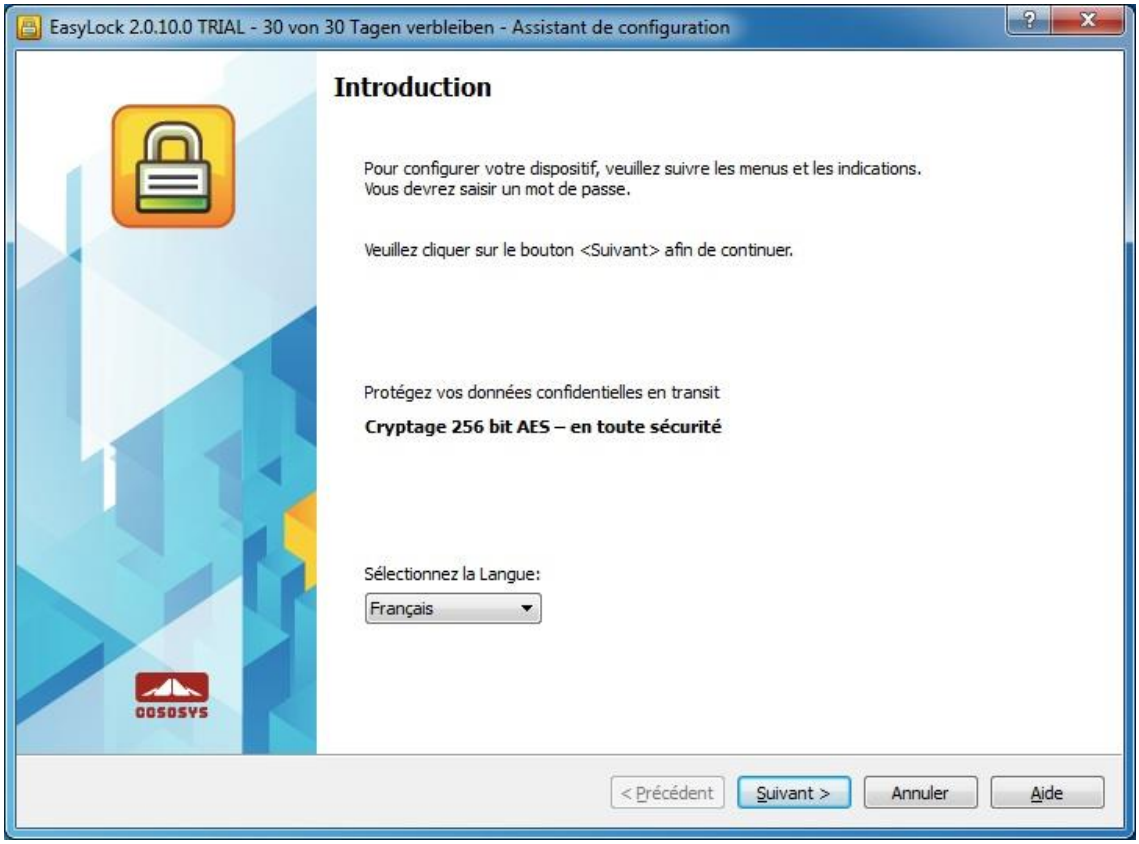
- **Sur le SO Linux**: exécutez le fichier EasyLockSetup, sélectionnez la lettre du lecteur correspondant au dispositif USB et appuyez sur "Finir". L'application EasyLock sera installée automatiquement dans le répertoire racine du dispositif sélectionné.



3.1. Configurer EasyLock

Pour lancer EasyLock double-cliquez sur le fichier EasyLock sauvegardé dans le répertoire racine du dispositif portable de stockage.

Lors de l'utilisation du dispositif portable de stockage comme un TrustedDevice en combinaison avec Endpoint Protector, l'ordinateur client auquel le dispositif est connecté doit avoir reçu l'autorisation du serveur Endpoint Protector, sinon le dispositif ne sera pas accessible sur un ordinateur protégé par Endpoint Protector ou EasyLock ne démarrera pas automatiquement.



3.2. Configurer un mot de passe

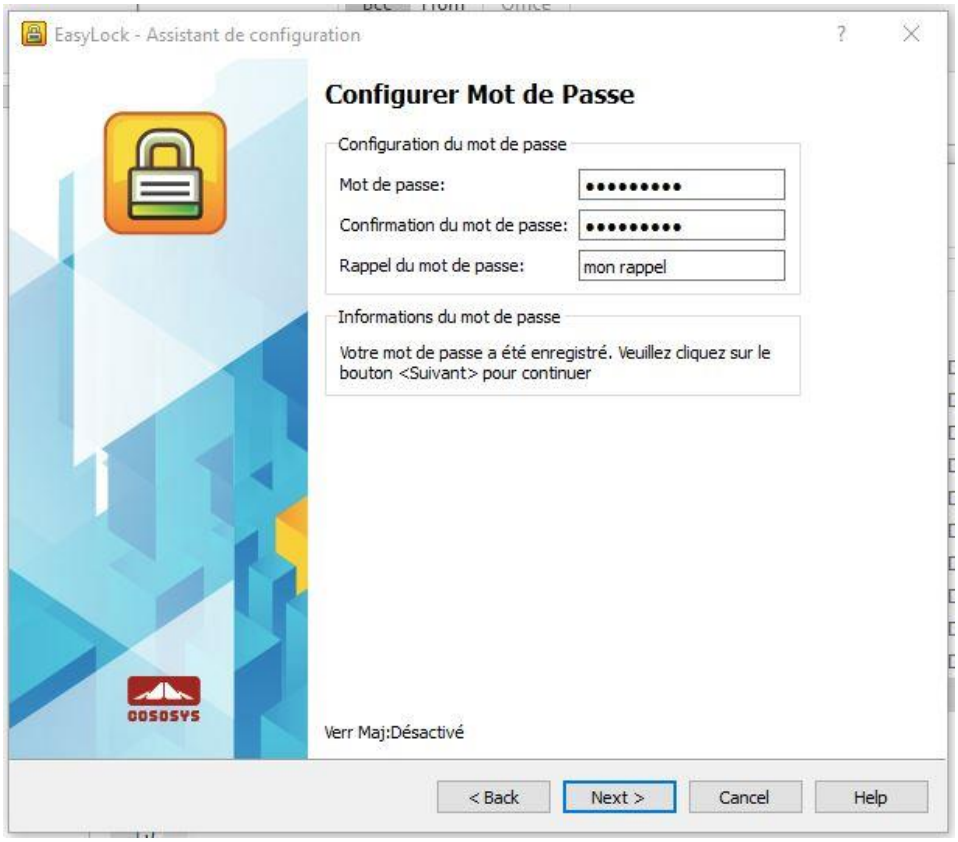
Pour sécuriser (crypter) vos données, vous devez configurer un mot de passe. Le mot de passe doit avoir au moins 6 (six) caractères.

Pour des raisons de sécurité, il est recommandé d'inclure des lettres, des chiffres et des symboles dans le mot de passe.

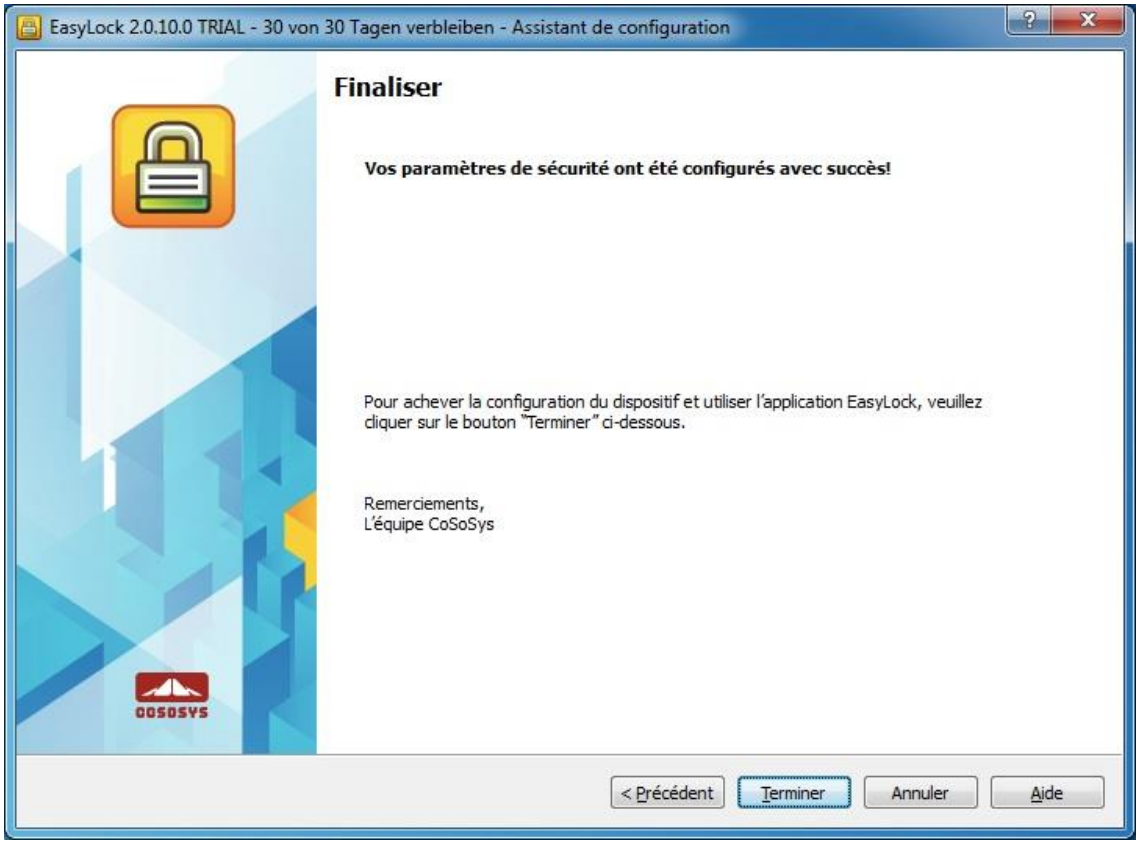
Entrez le mot de passe, puis confirmez-le.

Il est recommandable de définir un indice du mot de passe qui aidera en cas d'avoir oublié le mot de passe.

Cliquez "Suivant" pour continuer.



Cliquez "Finir" pour terminer de paramétrer le mot de passe et commencer à utiliser l'application.



3.3. Re-essais du mot de passe

Pour des raisons de sécurité, le mot de passe sera requis à chaque démarrage de l’application.

Au cas où le disque est perdu ou volé le nombre des re-essais du mot de passe est limité à 10 (dix). Après la saisie erronée du mot de passe 10 fois consécutives, EasyLock supprimera en sécurité tous les fichiers cryptés gardés sur le dispositif portable de stockage.

Les données sur le dispositif portable de stockage ne peuvent pas être récupérées ou recrées ultérieurement. Elles sont définitivement supprimées.

3.4. Paramètres d'affichage

Dans la barre d’outils EasyLock il y a plusieurs options disponibles pour personnaliser la fenêtre d’affichage EasyLock.

Panneaux de commutation – pour changer l’affichage des panneaux entre la clé USB et Mon Ordinateur

Afficher ou Cacher le Panneau de Mon ordinateur – pour afficher le Panneau de Mon ordinateur

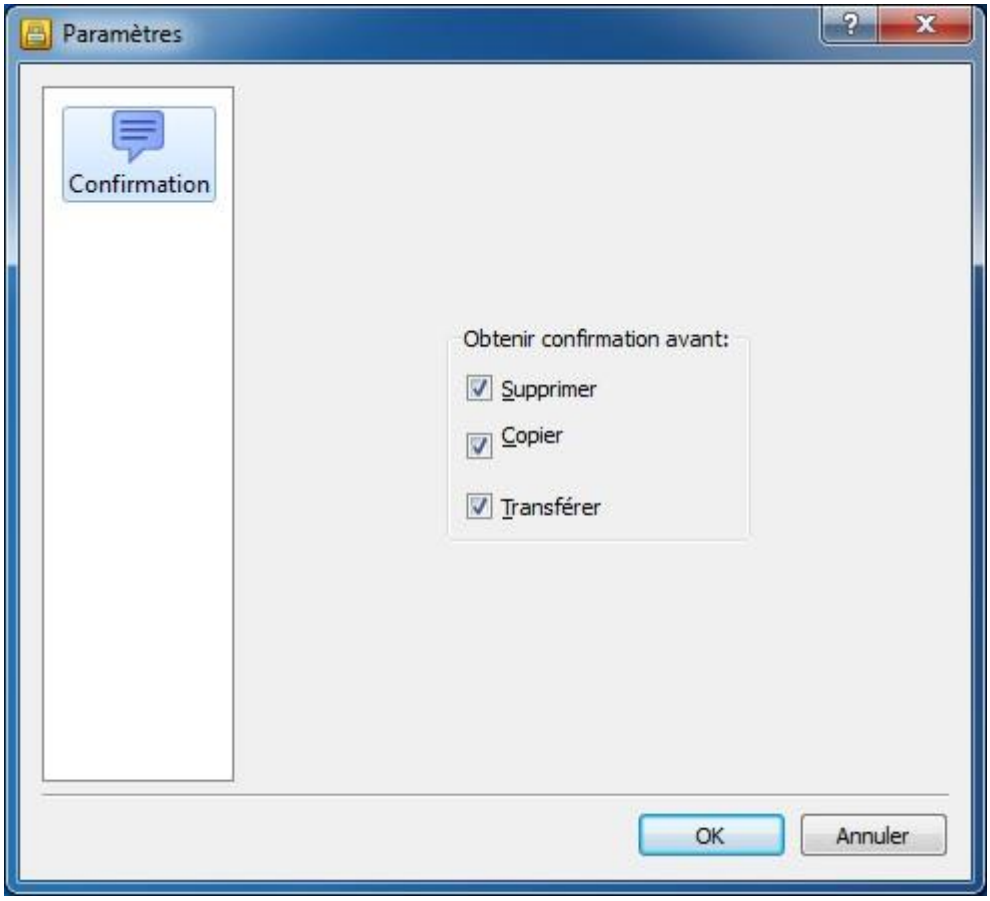
Afficher la Vue Arborescente – pour afficher une structure arborescente

Afficher la Vue Détaillée – pour afficher des informations supplémentaires des fichiers

Afficher la Vue Liste – pour afficher les éléments comme une liste

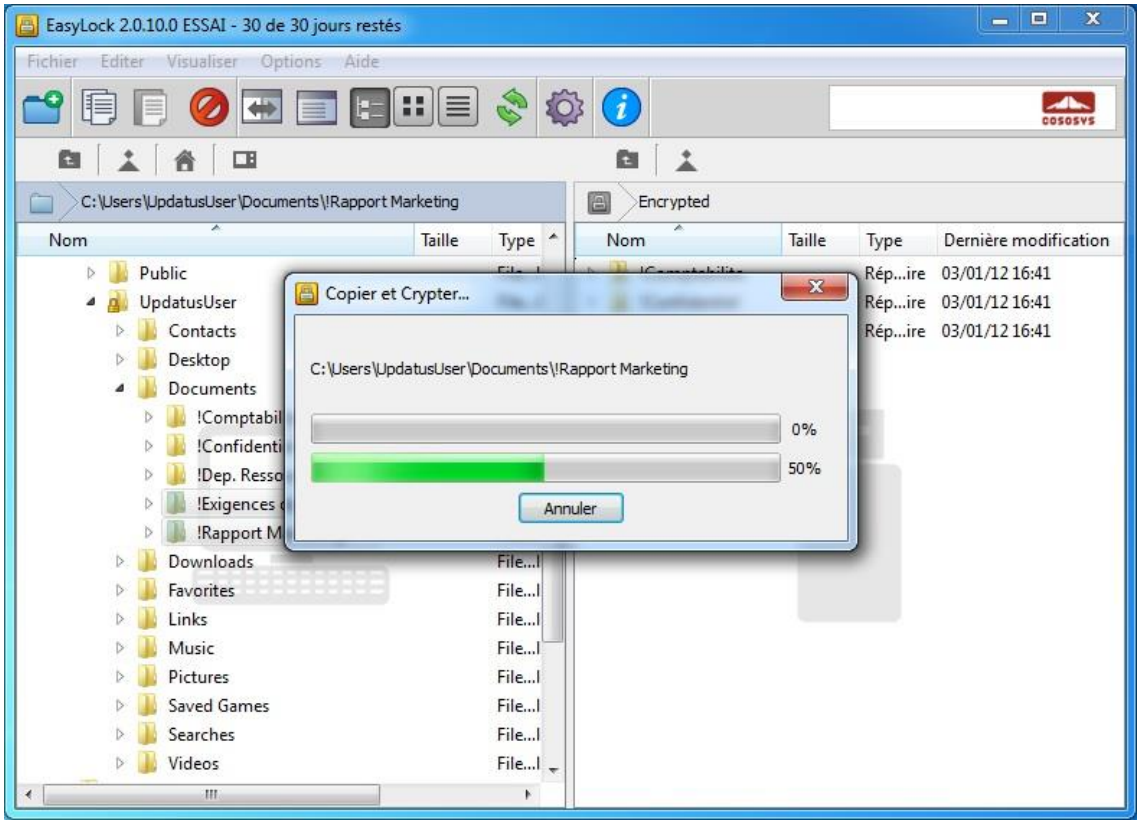
Les options disponibles peuvent être sélectionnées aussi directement du menu principal, de la section Vue.

Une nouvelle option, Préférences, permet de choisir si on veut faire apparaître un message de confirmation avant de supprimer, copier ou déplacer des fichiers.

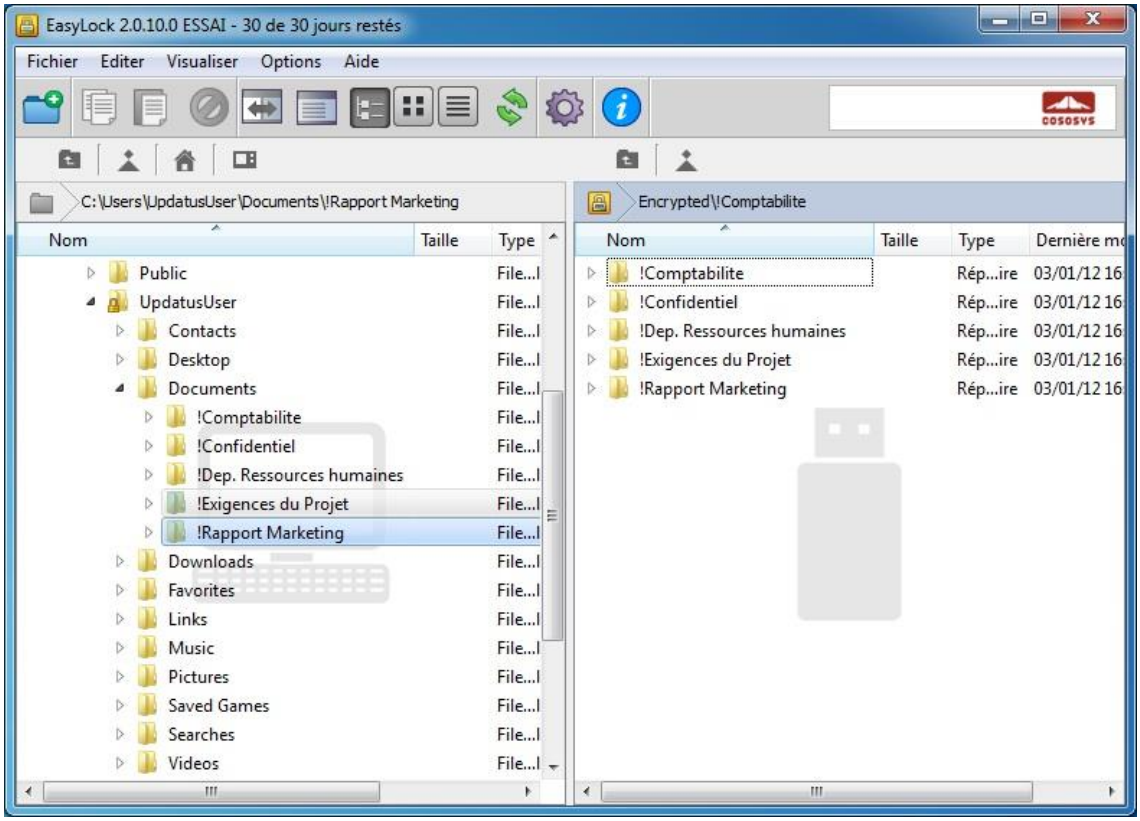


3.5. Utiliser glisser-déposer pour copier des fichiers

Une fonctionnalité-clé de EasyLock est la fonctionnalité glisser-déposer qui permet de simplement glisser le(s) fichier(s) et/ou le(s) répertoire(s) qu'on veut copier sur le dispositif et le(s) déposer dans la fenêtre EasyLock. Ces fichiers seront automatiquement cryptés, en s'assurant que les données restent en sécurité et privées.



Le cryptage des fichiers et le statut du transfert peuvent être vu à l'aide de la barre de progression. Quand la barre arrive à la fin, les fichiers ont été copiés et cryptés.



En cliquant-droite sur un élément on aura l'accès aux options comme "Rafraîchir", "Copier" et "Supprimer".

Attention! Copier des fichiers du disque dur sur le dispositif portable de stockage en utilisant l'Explorateur Windows est pas recommandable!

Nous recommandons d'utiliser soit la commande glisser-déposer, soit les raccourcis pour copier et coller Ctrl+C et Ctrl+V pour transférer des données sur le dispositif portable de stockage par l'interface EasyLock.

Dans la barre d'outils EasyLock on peut trouver des icônes supplémentaires qu'on peut également utiliser pour copier et crypter les fichiers.

Veuillez noter que les fichiers enregistrés sur le dispositif portable de stockage ne sont pas visibles après le cryptage, que si EasyLock roule.

Pour quitter EasyLock, sélectionnez le menu Fichier et choisissez "Quitter", ou cliquez simplement sur le bouton "X" du coin supérieur droite de la fenêtre de l'application.

3.6. Ouvrir et modifier des fichiers dans EasyLock

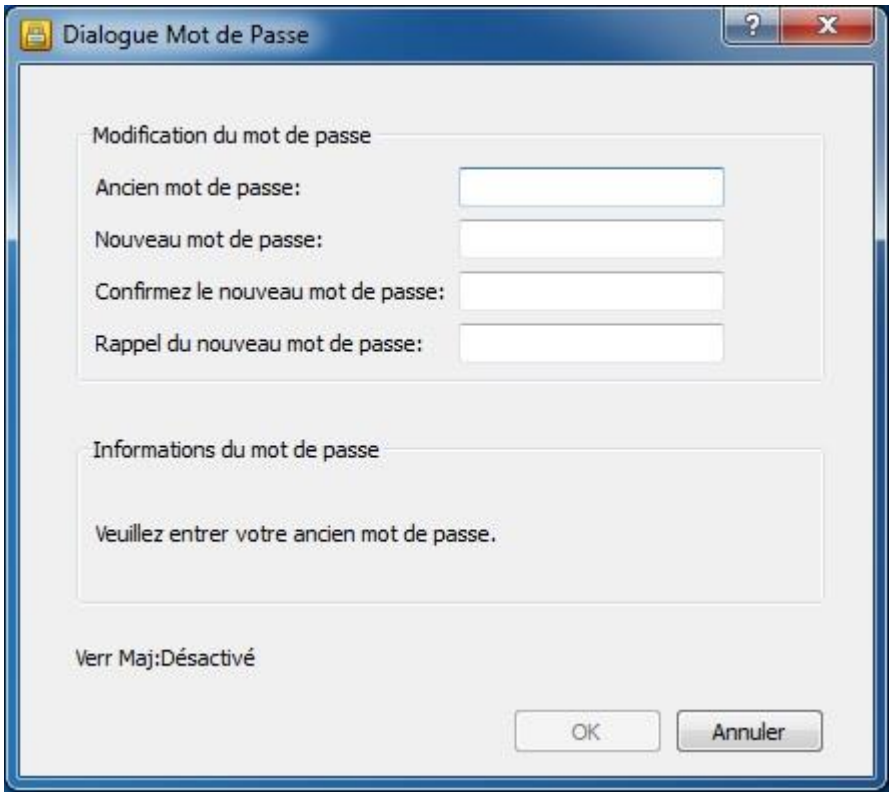
Les données copiées sur le dispositif peuvent être visualisées et modifiées directement dans EasyLock. Cette fonctionnalité est accessible par la commande "Ouvrir" ou double-cliquant sur le fichier désiré.

L'utilisateur doit ouvrir les documents sur le dispositif avec l'application associée. EasyLock essayera de fermer ces documents une fois l'application fermée. Si un document est modifié (sauvegardé avec le même nom ou dans le même répertoire), il sera crypté et stocké sur le dispositif. Si un document est modifié et sauvegardé mais il ne parvient pas à être crypté, lorsque le dispositif est retiré à l'improviste par exemple, il sera crypté au prochain démarrage d'EasyLock.

Attention! Lorsque EasyLock est démarré par Endpoint Protector comme une application securisée, l'option d'ouvrir des documents par le dispositif est désactivée car l'application associée n'a pas d'accès aux fichiers.

3.7. Paramètres de sécurité

Les paramètres de sécurité peuvent être modifiés dans EasyLock. Une fois connecté, on peut modifier son mot de passe. Pour faire cela, on doit dérouler le menu des paramètres de sécurité. Cela peut être fait soit en sélectionnant Options->Paramètres de Sécurité de la barre d'outils, soit en appuyant le raccourci Ctrl+O.



4. Comment fonctionne EasyLock avec EPP ou MyEPP

Quand on utilise EasyLock sur un dispositif portable de stockage comme un TrustedDevice de 1er Niveau, en combinaison avec Endpoint Protector (ou My Endpoint Protector, la solution hébergée SaaS), il s'assurera que toutes les données copiées d'un ordinateur client sécurisé par Endpoint Protector sur le dispositif soient cryptées.

En bas on trouve le scénario habituel pour l'utilisation d'un TrustedDevice de 1er Niveau:

1. L'utilisateur connecte le dispositif à l'ordinateur client protégé par Endpoint Protector.
2. Le dispositif est vérifié à l'égard de l'autorisation (si l'ordinateur client communique avec le serveur Endpoint Protector pour vérifier l'autorisation).
3. Si le dispositif est un TrustedDevice de 1er Niveau et l'Utilisateur ou l'Appareil est autorisé à utiliser le TrustedDevice de 1er Niveau, le logiciel EasyLock sur l'appareil sera automatiquement ouvert.
4. L'utilisateur peut transférer des fichiers par glisser-déposer dans EasyLock.
5. Les données transférées sur le dispositif sont cryptées par AES 256 bits.
6. L'utilisateur ne peut pas demarrer le dispositif directement en utilisant Windows Explorer ou des applications similaires (Total Commander par

exemple) pour s'assurer qu'aucune donnée ne soit copiée sur le dispositif portable sans être correctement cryptée.

7. L'utilisateur n'a pas la possibilité de copier des données dans un état non crypté sur le TrustedDevice (sur un ordinateur client Endpoint Protector).

8. Tous les transferts de fichiers à partir de l'ordinateur client Endpoint Protector vers le dispositif peuvent être enregistrés si le traçage des fichiers et la duplication des fichiers sont activés dans Endpoint Protector. Des actions telles que la suppression des fichiers ou le renommage des fichiers sont également enregistrées.

9. Les administrateurs peuvent vérifier plus tard l'identités de l'utilisateur, du dispositif, de l'ordinateur et des fichiers impliquées dans le transfert.

Si un TrustedDevice ne parvient pas à obtenir l'autorisation d'Endpoint Protector, il ne sera pas employable par l'utilisateur. Le dispositif sera bloqué et l'utilisateur ne sera pas en mesure de demarrer le dispositif.

4.1. Le traçage des fichiers sur TrustedDevices EasyLock

Le Traçage des Fichiers sur TrustedDevices EasyLock est une nouvelle fonctionnalité d'Endpoint Protector 4, utilisée en combinaison avec EasyLock, qui permet de surveiller les fichiers copiés de manière cryptée sur des dispositifs portables.

En activant l'option Traçage des Fichiers, toutes les données transférées vers et à partir des dispositifs utilisant EasyLock sont enregistrées et sauvegardées pour une vérification ultérieure. Les informations enregistrées sont automatiquement envoyées au serveur Endpoint Protector si un client Endpoint Protector est présent sur l'ordinateur et il y a une connexion Internet active.

Dans le cas où le client Endpoint Protector n'est pas présent, l'information est stockée sur le dispositif dans un format crypté et elle sera envoyée ultérieurement de tout ordinateur ayant un client Endpoint Protector installé.

Pour un plus de détails sur l'activation et l'utilisation du Traçage des Fichiers sur les TrustedDevices EasyLock, veuillez consulter le Manuel de l'Utilisateur Endpoint Protector 4.

5. Configurer l’emploi de TrustedDevice dans EPP ou MyEPP

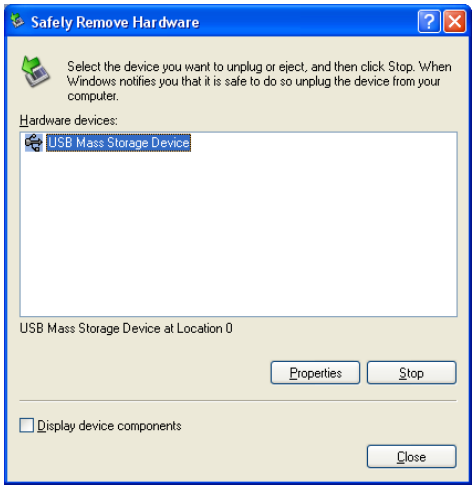
Pour savoir comment configurer l’utilisation de TrustedDevice en combinaison avec Endpoint Protector veuillez consulter le Manuel de l’utilisateur Endpoint Protector.

Pour savoir plus sur Endpoint Protector, merci bien de visitez: www.EndpointProtector.com

6. Détacher un dispositif en sécurité

Afin de débrancher votre dispositif portable de stockage du port USB de l'ordinateur, on doit utiliser la commande "Retirer le périphérique en toute sécurité" de la barre d'état, sinon on risque de corrompre les données de la clé USB (surtout si on utilise Windows 2000).

Pour retirer le périphérique en toute sécurité, double-cliquez sur l'icône de la barre d'état, puis sélectionnez le lecteur USB que vous voulez supprimer de la liste et cliquez sur le bouton "Arrêter".



Un message apparaîtra en indiquant que le dispositif de stockage peut être maintenant retiré en toute sécurité. Si un message en disant «Le dispositif '…' ne peut pas être arrêté maintenant» apparaît, on doit fermer l'Explorateur Windows, EasyLock ou toute autre application qui accède encore les données de la clé USB.

7. Assistance technique

Au cas où on a besoin de l'aide supplémentaire, des FAQs ou de l'assistance par mail, on peut visiter le site web d' assistance directement à http://www.cososys.com/help.html

8. Note importante / Avertissement

Les mesures de sécurité, par leur nature, peuvent être contournées. CoSoSys ne peut pas et ne garantit pas que les données ou les dispositifs ne seront pas accédés par des personnes non autorisées, et CoSoSys décline toute garantie à cet effet dans toute la mesure permise par la loi.