Chiffrement

DriveLock offre différentes possibilités de chiffrement des données, partielle (**Encryption To Go**, **File Protection** et **BitLocker To Go**) ou complète (**Disk Protection**), qui ont chacune leurs avantages, et qui peuvent être mises à disposition des utilisateurs ou être appliquées de façon forcée.

L'accès peut être possible sans avoir DriveLock d'installé, et un système de récupération en ligne / hors ligne est également disponible.

Enfin le chiffrement n'est pas lié au matériel, ce qui signifie que n'importe quel support de stockage amovible pourra bénéficier d'une protection efficace.

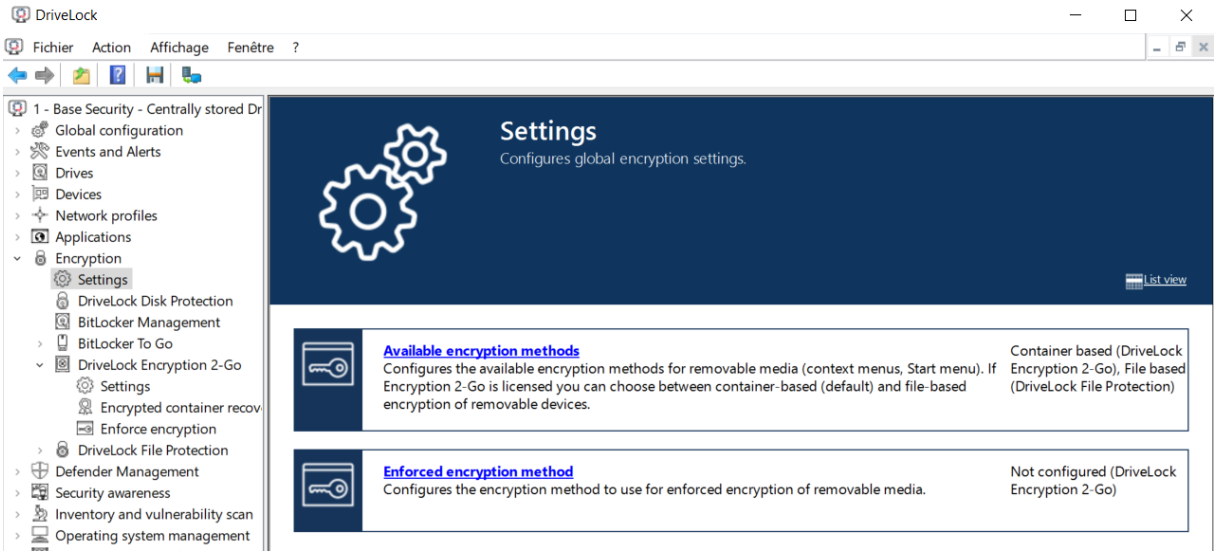
Méthodes de chiffrement prises en charge : AES (256 bits) avec en option le mode FIPS (recommandé), Blowfish, Twofish, CAST5, Serpent et Triple DES.

Le mot de passe pour chiffrer les lecteurs est lui-même chiffré à l'aide d'un algorithme de hachage ; les procédures de hachage prises en charge sont : SHA-512 FIPS-mode, SHA-256 FIPS-mode, SHA-1, RIPEMD-160 et Whirlpool.

Comparaison des méthodes de chiffrement

	Container (Enc2Go)	File & Folder (FP)	BitLocker To Go (BL2Go)
Prise en charge des lecteurs amovibles	X	X	X
Prise en charge des lecteurs / dossiers locaux	X	X	-
Prise en charge des lecteurs / dossiers réseau	X	X	-
Prise en charge multi-utilisateurs	-	X	-
Prise en charge des certificats utilisateur	-	X	-
Prise en charge du mot de passe administrateur/central	X	-	X
Noms de fichiers chiffrés / non visibles	X	-	X
Application de chiffrement mobile	X	X	-
Accéder aux données chiffrées sur un ordinateur externe	-	-	X
Prise en charge jusqu'à l'algorithme de chiffrement AES 256	X	X	X

Cela nécessite dans tous les cas de choisir et de paramétrer la ou les méthode(s) utilisée(s) à partir de la configuration (*policy*) à appliquer aux agents, mais aussi en cas de chiffrement forcé sur un périphérique (*enforce encryption*) ou de récupération (*recovery*) avec un mot de passe administratif et un certificat à configurer.



Encryption To Go

Un conteneur sous forme de fichier .dlv est créé, et les données qui y sont placées sont automatiquement chiffrées. Il peut être créé n'importe où, que ce soit dans le système de fichiers, sur un partage ou un lecteur. Le conteneur est monté en tant que nouveau lecteur, et demande de s'authentifier pour pouvoir y accéder.

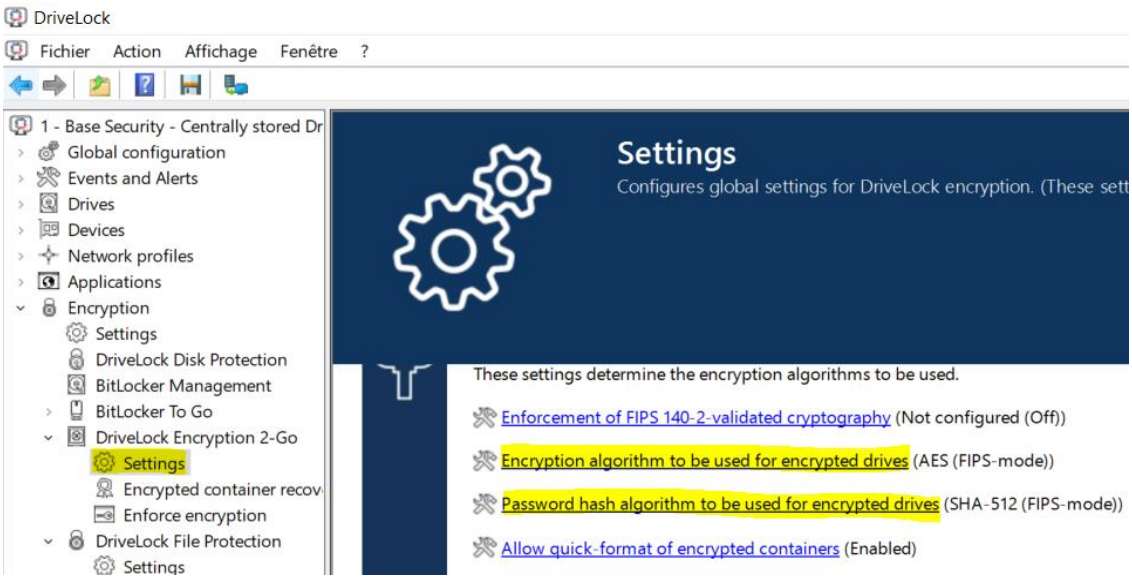
Configuration

Dans **Encryption** > **DriveLock Encryption 2-Go** > **Settings**, choisissez :

- l'algorithme de chiffrement (par exemple AES FIPS-Mode),

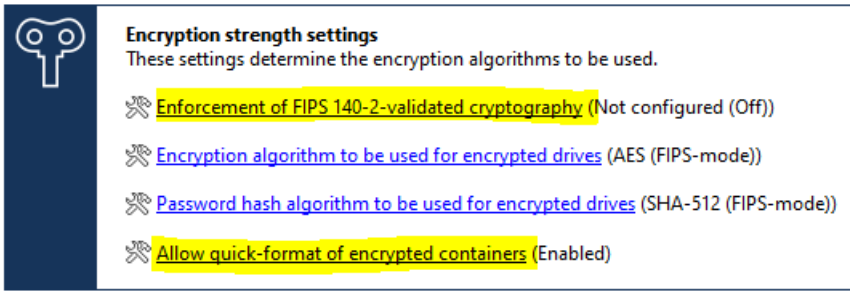
- l'algorithme de hachage du mot de passe (par exemple SHA-512),

- la méthode pour sécuriser la suppression des fichiers (par exemple Random data).



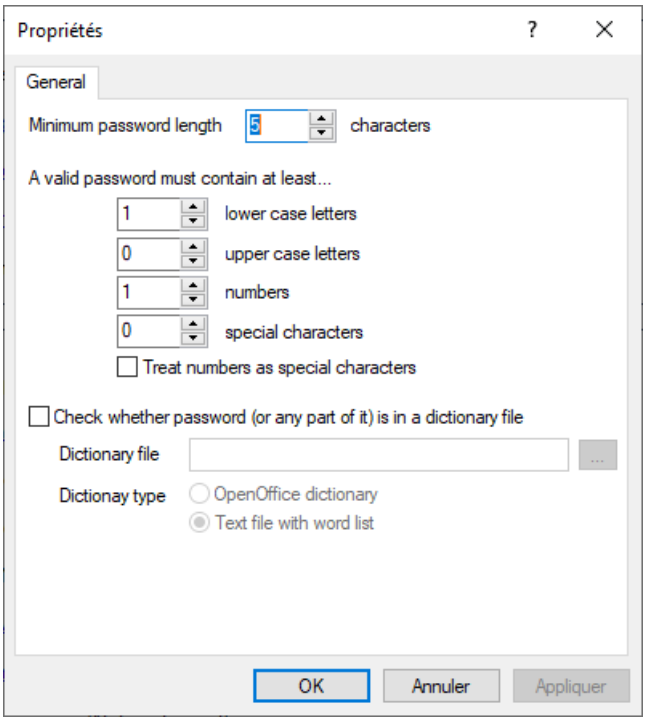
Options de chiffrement

Il est conseillé de laisser la cryptographie validée FIPS 140-2 sur "Off" (*Enforcement of FIPS 140-2 validated cryptography*), et le formatage rapide des conteneurs chiffrés sur "Enabled" (*Allow quick-format of encrypted containers*) pour accélérer le formatage.



Complexité du mot de passe

Utilisez les paramètres concernant le mot de passe (*Password strength settings*) pour l'adapter à vos exigences, en particulier sa complexité (*Password complexity policy*) pour définir sa longueur, l'utilisation de majuscules, de minuscules, de chiffres et/ou de caractères spéciaux.



Récupération

Pour récupérer l'accès à un conteneur chiffré (par exemple si un utilisateur a oublié son mot de passe), il est possible d'utiliser un mot de passe administratif ou un certificat. Le mot de passe administratif permet d'accéder à chaque conteneur chiffré, tandis que la récupération

basée sur un certificat a une option de récupération en ligne et une option de récupération hors ligne.

En ligne

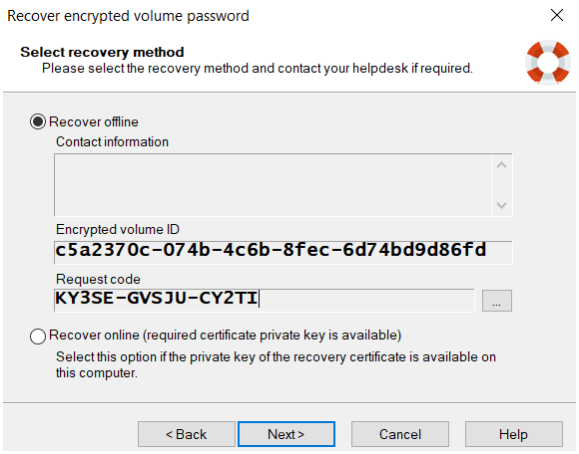
S'il existe un accès direct au conteneur (par exemple via le réseau ou un accès direct au support de données), le mot de passe de l'utilisateur peut être réinitialisé avec la méthode de récupération basée sur un certificat créé précédemment, y compris la clé privée.

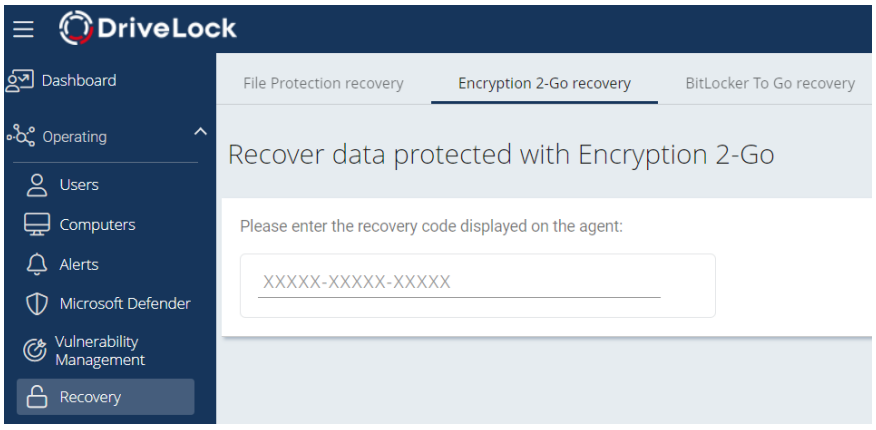
Si l'utilisateur doit être en mesure de réinitialiser le mot de passe par lui-même, le certificat de récupération peut être importé dans le stockage de certificats de Windows à un moment antérieur (avec l'option que la clé privée ne soit pas exportable, ce qui empêchera le certificat d'être volé). Le processus lui-même peut être exécuté directement à partir du menu Démarrer ou du menu contextuel dans la zone de notification.

Si aucun certificat n'est utilisé, un accès alternatif est possible en utilisant le mot de passe administrateur.

Hors ligne

Lorsque l'administrateur n'a pas accès au conteneur chiffré et que l'utilisateur n'est pas en possession du certificat et de la clé privée (c'est le cas s'il n'est pas sur le réseau de l'entreprise et a oublié son mot de passe), il y a un procédé de défi-réponse, avec un code généré par l'utilisateur et un code réponse donné par l'administrateur au téléphone à partir du DriveLock Operations Center (vue **Recovery** du menu **Operating**).





NB : Ces paramètres de récupération sont facultatifs, et DriveLock ne vous rappellera pas de les créer, alors assurez-vous qu'ils ont été correctement paramétrés dans **Encrypted container recovery**.

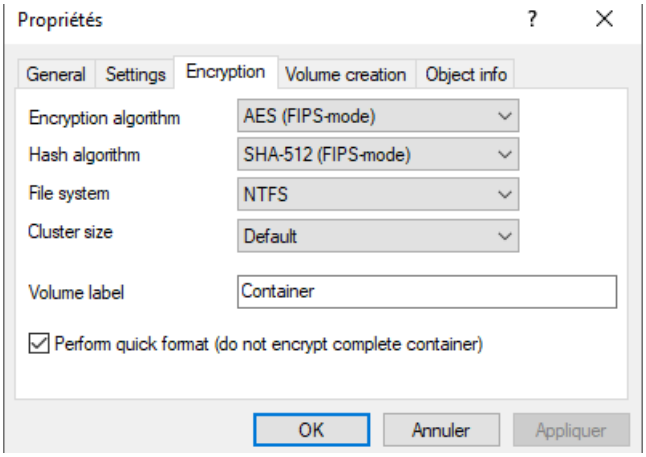
Chiffrement forcé

Il faut tout d'abord configurer les paramètres dans **Encryption** > **DriveLock Encryption 2-Go** > **Enforce encryption** :

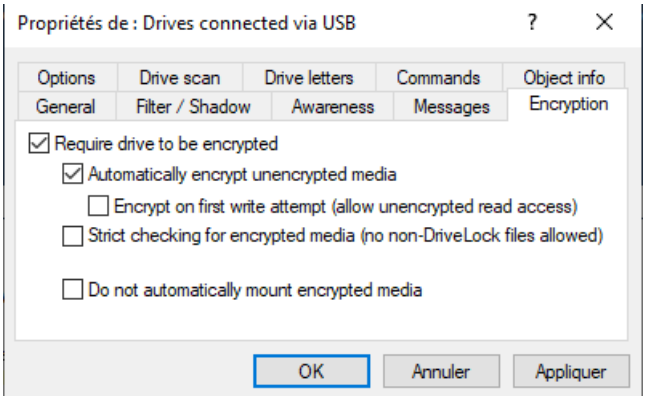
- dans l'onglet **Settings**, choisissez si vous souhaitez chiffrer tout ou une partie de l'espace de stockage,

- dans l'onglet **Encryption**, sélectionnez l'algorithme de chiffrement et de hachage, et cochez la case pour le formatage rapide,

- dans l'onglet **Volume creation**, indiquez si vous souhaitez conserver ou non les données existantes, et si vous voulez copier l'application mobile (**Mobile Encryption Application**) pour pouvoir accéder au conteneur chiffré même s'il n'y a pas d'agent DriveLock.



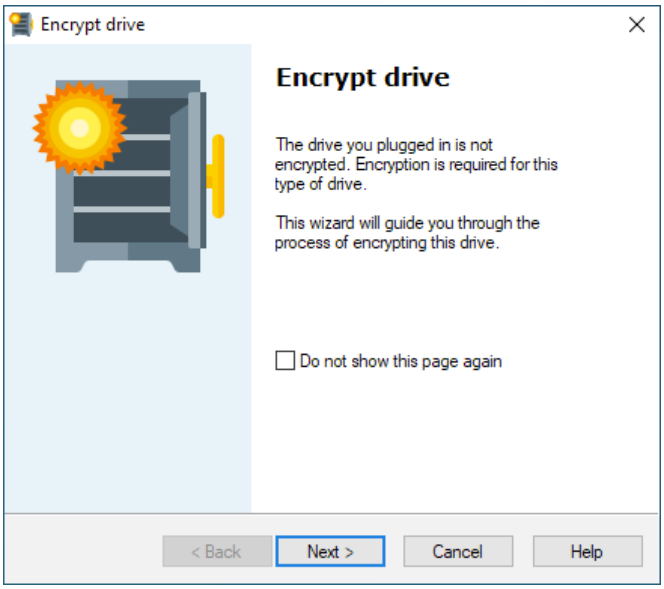
Une fois la configuration terminée, vous pouvez aller dans les options des périphériques pour forcer leur chiffrement :



Si par exemple une clé USB est branchée sur un ordinateur avec un agent DriveLock, un assistant va alors se lancer pour guider l'utilisateur dans le processus de chiffrement.

Le processus de chiffrement initial va se lancer, avec une durée variable en fonction de la vitesse du port USB, et de la vitesse et de la taille de la clé USB.

NB : Le déplacement de données existantes vers le conteneur chiffré en train d'être créé peut rallonger de façon considérable cette durée.



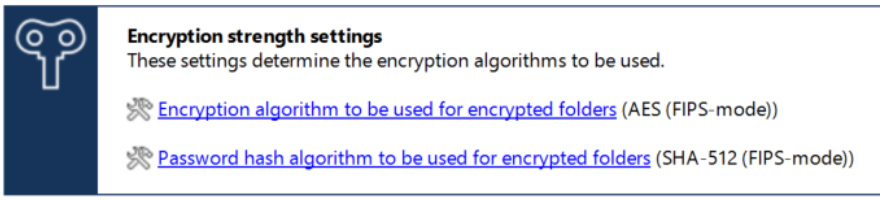
File Protection

Contrairement au chiffrement basé sur un conteneur (Encryption To Go), ici tout le contenu d'un fichier est chiffré alors que sa structure et son nom restent inchangés.

Cela garantit que les fichiers chiffrés apparaissent dans l'explorateur Windows de la même manière que des fichiers non chiffrés. Des programmes de sauvegarde ou de défragmentation les traiteront ainsi de la même façon que n'importe quel autre fichier.

Ce n'est que lorsque vous essayez d'afficher le contenu d'un tel fichier, par exemple si vous l'ouvrez dans Word, que le chiffrement devient alors apparent.

Cette méthode de chiffrement se configure de la même façon que Encryption To Go en allant à **Encryption** > **DriveLock File Protection** > **Settings**, avec une procédure de récupération, et peut être elle aussi utilisée pour du chiffrement forcé.



N'importe quel dossier peut être chiffré avec File Protection n'importe où, par exemple dans le système de fichiers local (C:\tmp), sur un partage (\\serveur\dossier) ou un lecteur.

BitLocker To Go

Cette méthode de chiffrement peut être utilisée pour les supports amovibles, comme une clé USB ou un disque dur externe, formatés à l'aide du système de fichiers NTFS, FAT16, FAT32 ou EXFAT.

Comme pour BitLocker, les lecteurs chiffrés à l'aide de BitLocker To Go peuvent être ouverts à l'aide d'un mot de passe ou d'une carte à puce sur un autre ordinateur à l'aide de BitLocker Drive Encryption.

Cette méthode de chiffrement se configure de la même façon que Encryption To Go en allant à **Encryption** > **BitLocker To Go** > **Settings**, avec une procédure de récupération, et peut être elle aussi utilisée pour du chiffrement forcé.