Chiffrement Windows8 avec BitLocker

(P. Mora de Freitas – RSSI Paris B – 11/06/2013)

Introduction

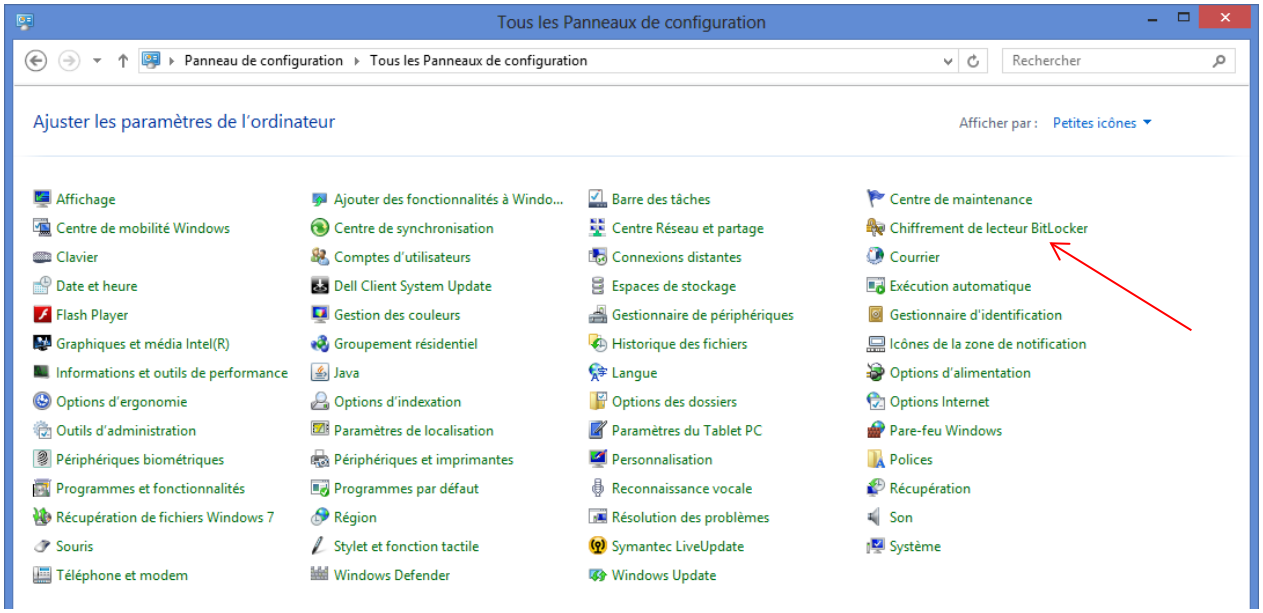
Ce document a été produit à l'occasion de l'atelier « Chiffrement » organisé le 25/06/2013 à Paris B, conjointement avec l'ENS et l'UPMC. Il décrit le chiffrement d'un disque système sous Windows8 à l'aide de BitLocker, outil inclus dans l'OS, qui permet de chiffrer l'ensemble du disque système et des lecteurs amovibles.

Le chiffrement de lecteur BitLocker est disponible uniquement dans les éditions Windows 8 Pro, Windows 8 Enterprise, Windows 7 Ultimate, Windows 7 Enterprise ou Windows Server 2008 R2. Pour le moment BitLocker reste l'unique moyen de chiffrement gratuit pour Windows8 (inclus dans l'OS), en attendant une version compatible de TrueCrypt.

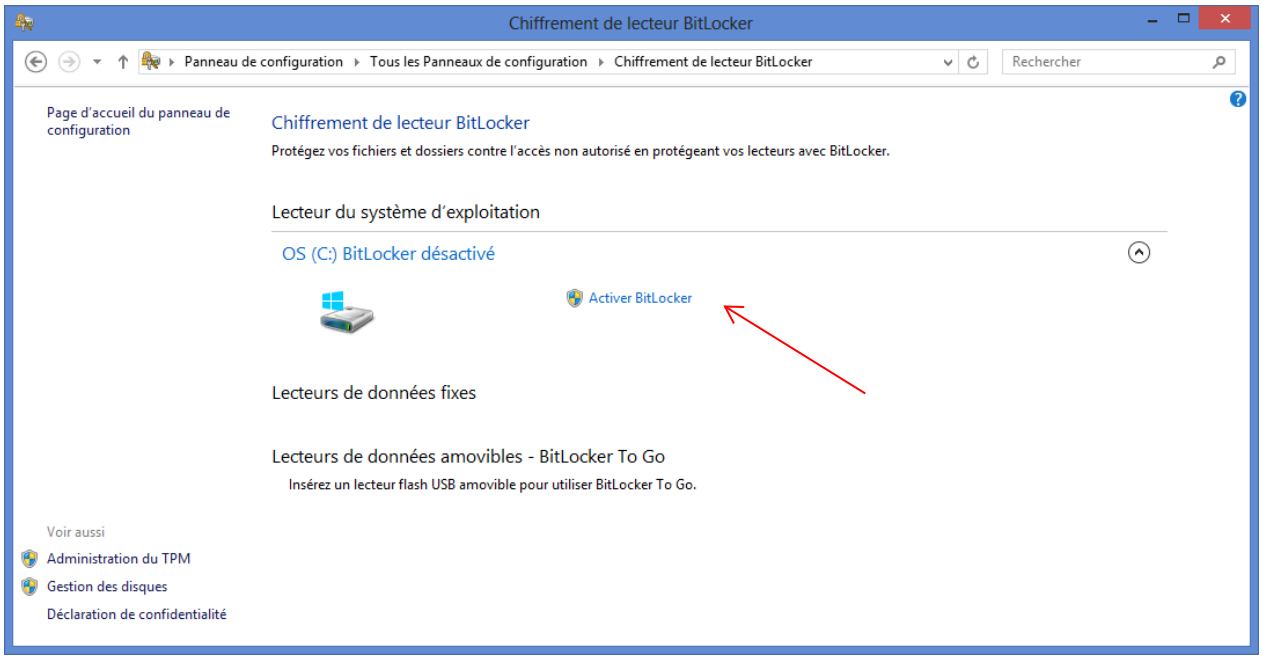
Nous recommandons au préalable la lecture des recommandations disponibles à l'adresse https://aresu.dsi.cnrs.fr/spip.php?rubrique99 concernant le chiffrement des postes de travail.

Activation de BitLocker

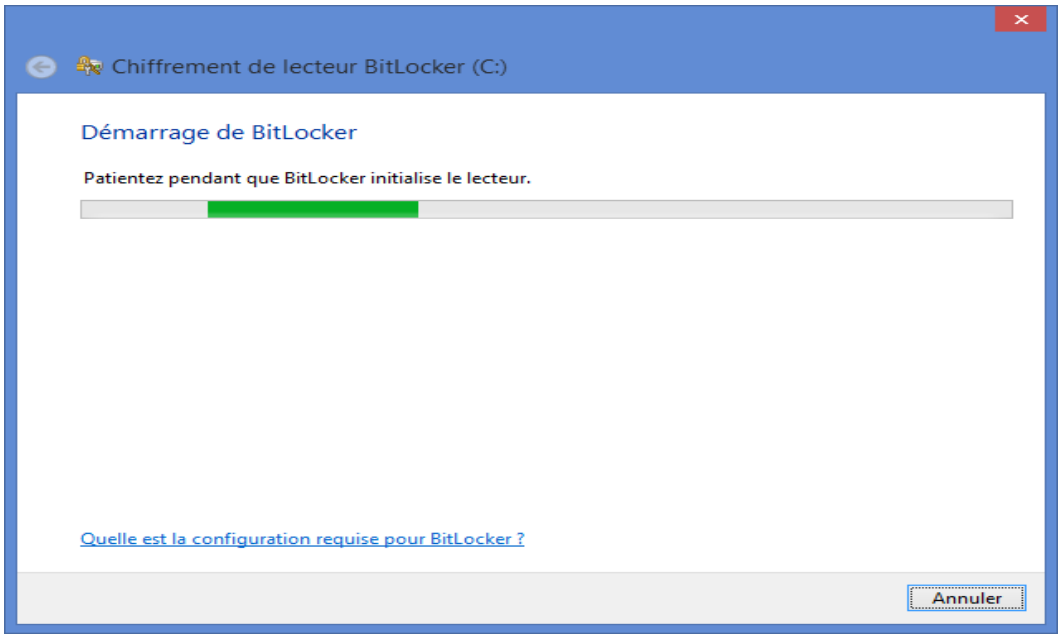
Dans le panneau de configuration , cliquez sur « Chiffrement de lecteur BitLocker » :



Cliquez sur « Activer BitLocker ». Autorisation de l'administrateur nécessaire, il peut vous être demandé de fournir un mot de passe d'administrateur ou de confirmer votre choix.



L'Assistant Installation du chiffrement de lecteur BitLocker s'ouvre :



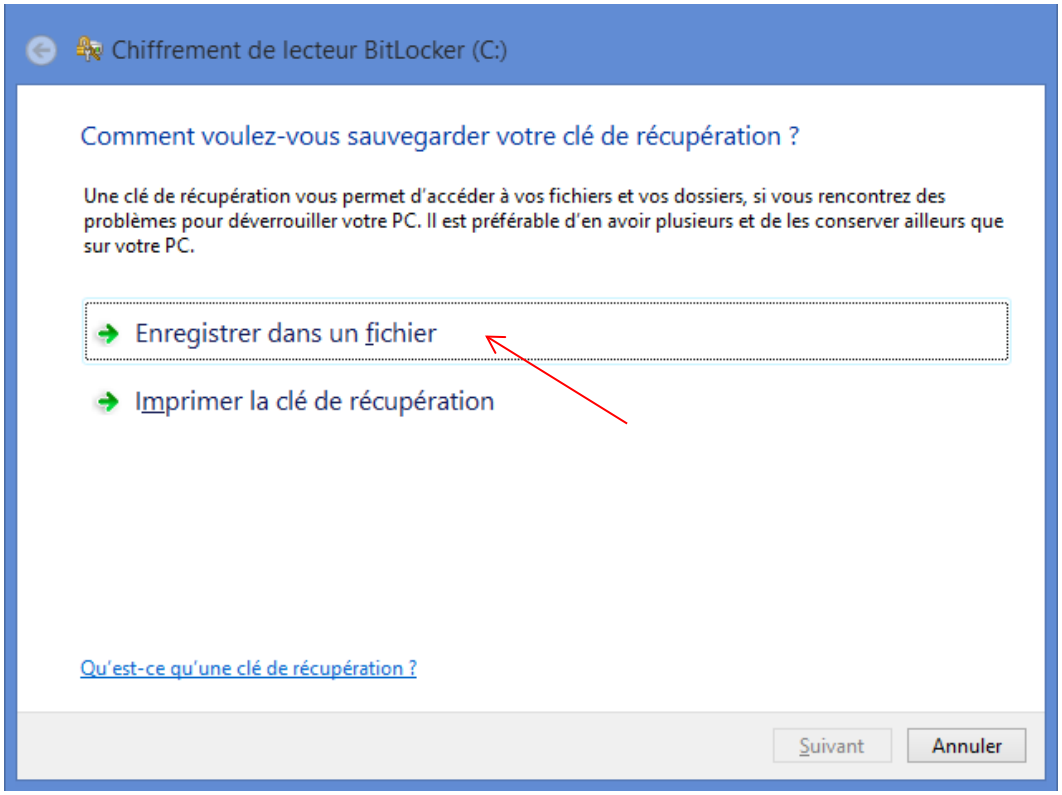
Le premier écran vous permet de sauver la clé de récupération en cas de problèmes avec le disque plus tard. **Il faut absolument garder une ou plusieurs copies de cette clé**, dans le cas contraire il se peut que vous perdiez définitivement l'accès à vos fichiers.

Vous pouvez sauver la clé dans un fichier, pourvu que le fichier ne soit pas dans le lecteur en train d'être chiffré, et/ou l'imprimer.

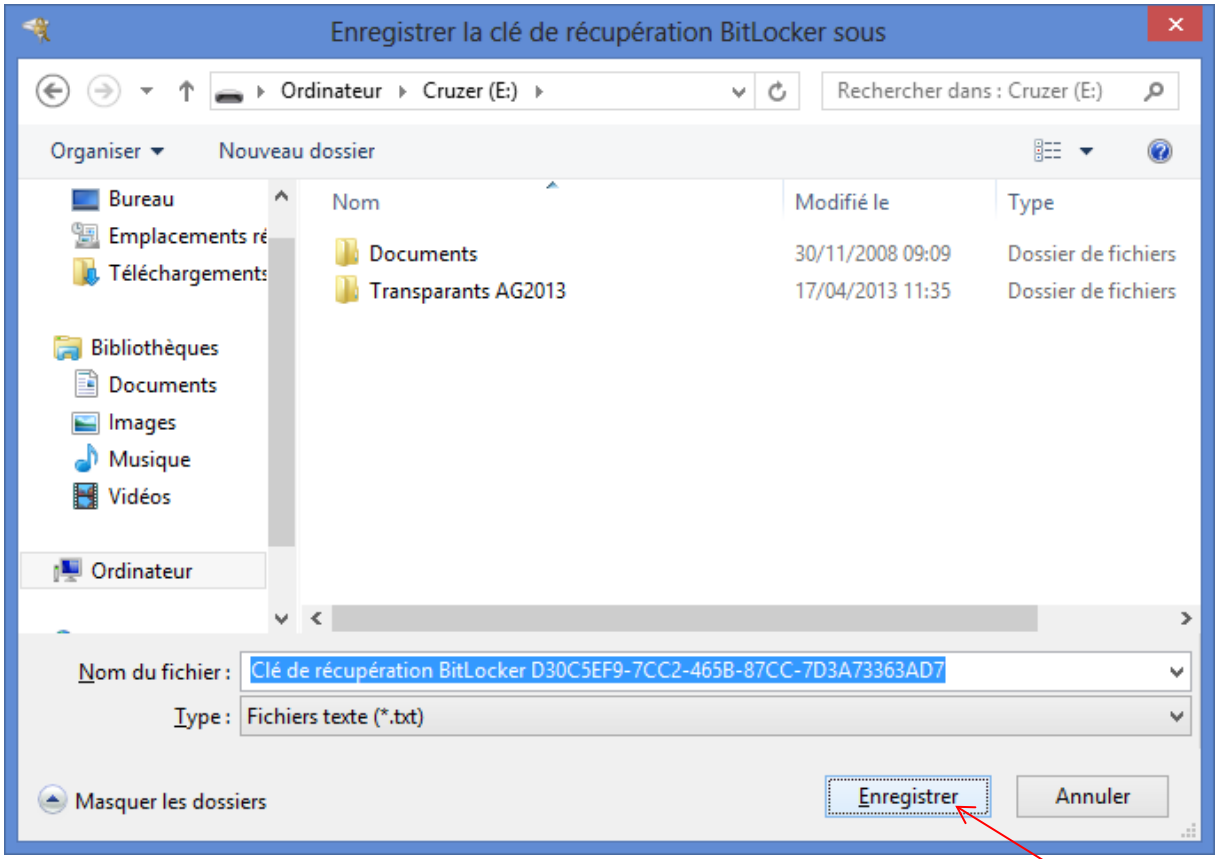
Si vous décidez de sauver les clé en format papier, il faut absolument les stocker dans un coffre.Si vous décidez de les sauver dans un fichier, il faudra les stocker dans un endroit sûr. Vous pouvez par exemple les stocker dans un cointaner chiffré avec TrueCrypt, lequel peut résider dans un de vos serveurs de fichiers dûment sécurisés selon les bonnes pratiques d'administration système et réseau.

Si votre instalation est géré par un AD, vous pouvez aussi déployer la GPO « BitLocker Group Policy settings » pour configurer le comportement de BitLocker dans les ordinnateurs de la fôret. En particulier, vous pouvez faire de la sorte que les clés de récupération de chaque ordinateur soient stockées dans l'AD, ce qui vous épargnera la gestion des copies des clés dans un endroit sûr.

Dans notre exemple nous allons sauver sur une clé USB. Pour cela, cliquez dans « Enregistrer dans un fichier » :



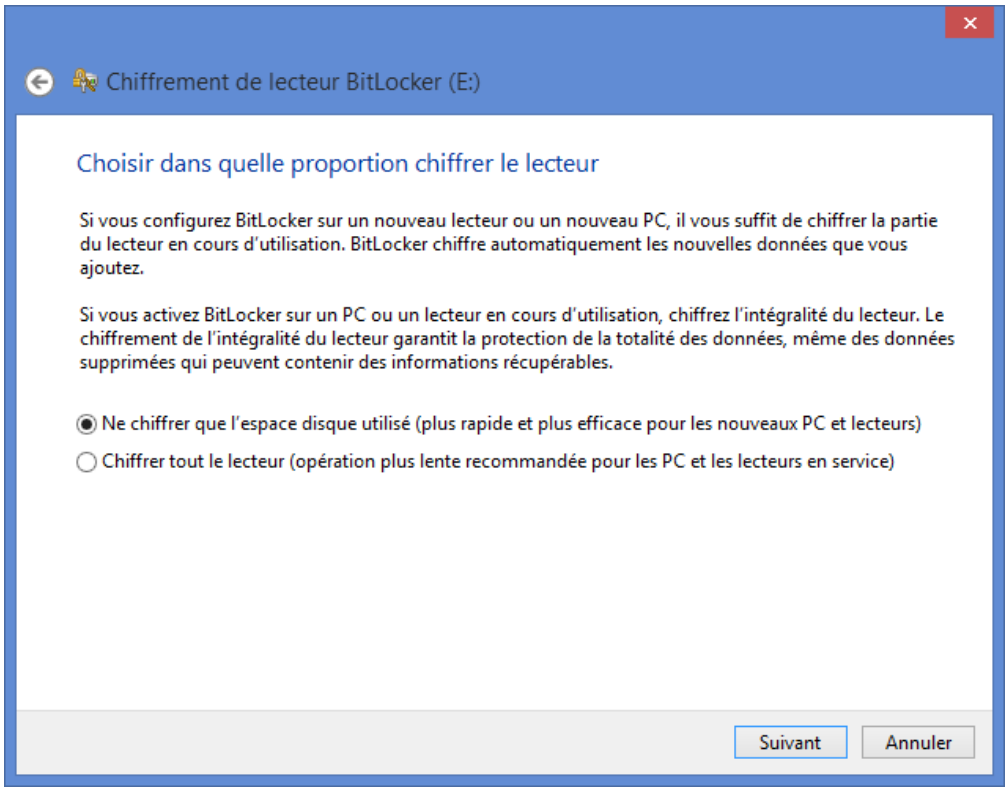
Clique dans Ordinateur, ensuite dans la clé USB, ensuite dans « Enregistrer » :



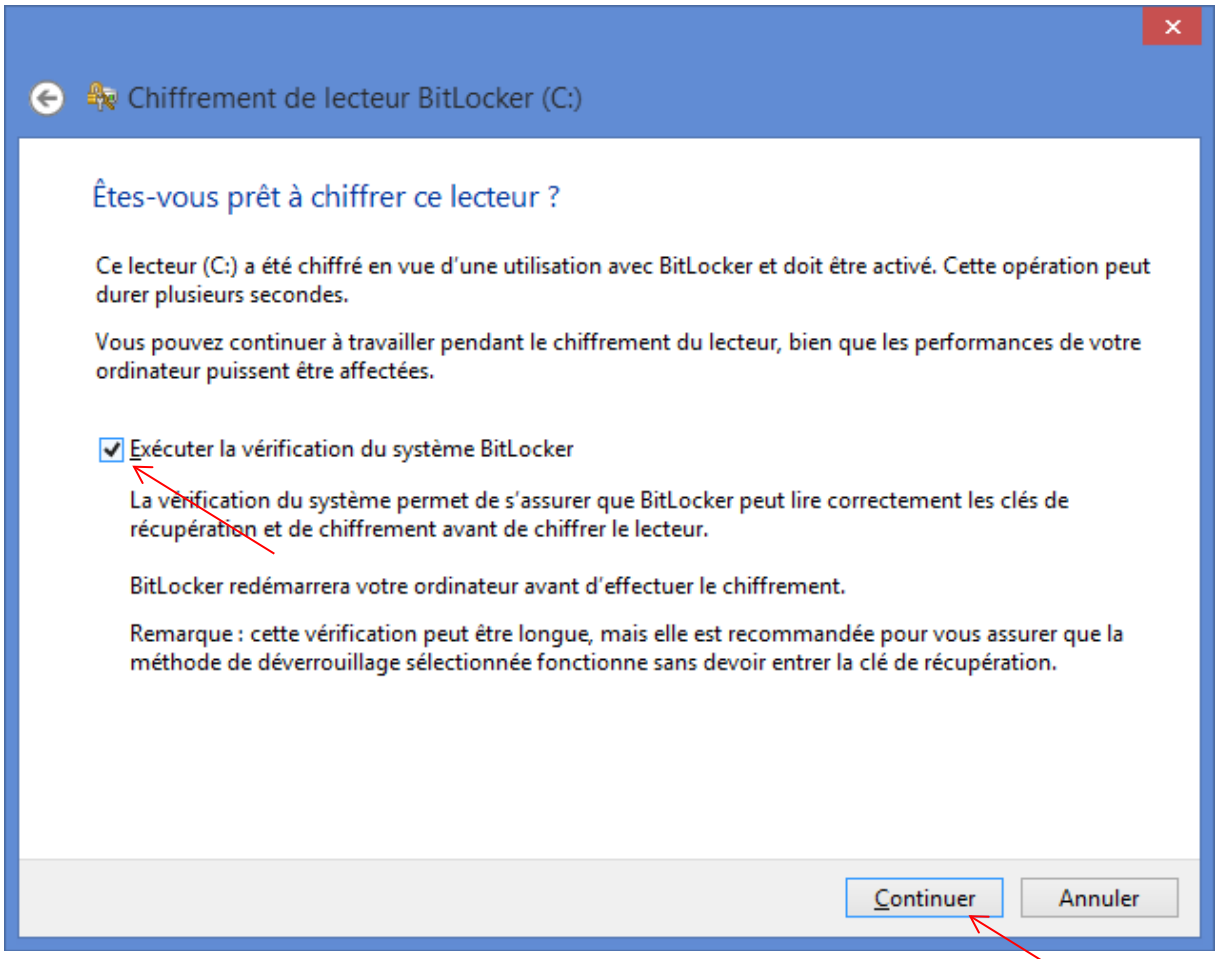
La clé est sauvée dans un fichier .txt en format ASCII, donc lisible. Voici un exemple où nous avons masqué le valeur de la clé :

```
Clé de récupération du chiffrement de lecteur BitLocker_

Pour vérifier qu'il s'agit de la clé de récupération appropriée,
comparez le début de l'identificateur suivant avec la valeur
d'identification affichée sur l'ordinateur.

Identificateur :

     D30C5EF9-7CC2-465B-87CC-7D3A73363AD7

Si l'identificateur ci-dessus correspond à celui affiché sur
l'ordinateur, utilisez la clé suivante pour déverrouiller le
lecteur.

Clé de récupération :

     XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX

Si l'identificateur ci-dessus ne correspond pas à celui affiché sur
l'ordinateur, cette clé ne permet pas de déverrouiller le lecteur.
Essayez une autre clé de récupération ou contactez votre
administrateur ou le support technique pour obtenir de l'aide.
```

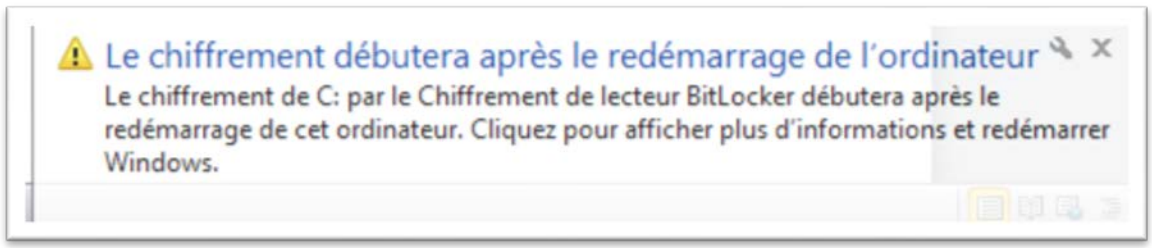
Une fois que vous avez fait une copie de la clé dans un endroit sûr, vous devez décider de chiffrer l'intégralité du disque ou seulement l'espace disque utilisé. Suivez les recommandations de l'écran ci-dessous, en sachant que le chiffrement de l'intégralité du disque prendra beaucoup plus de temps, et cliquez dans « Suivant » :



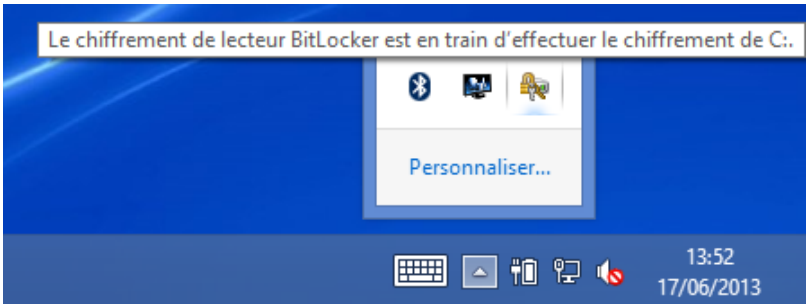
Avant de lancer le chiffrement, coucher la case « Exécuter la vérification du système BitLocker » pour plus de sécurité, avant de cliquer dans « Continuer » :



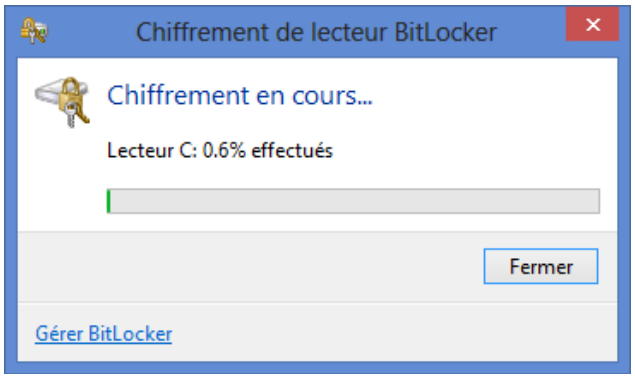
L'assistant BitLocker se ferme et une alerte vous informe que **le chiffrement débutera lors du prochain redémarrage** :



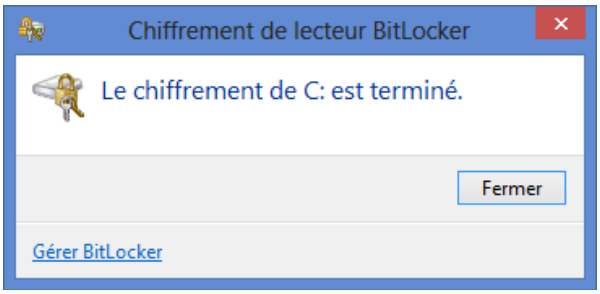
Une fois redémarré, un petit icone vous informe que le chiffrement est en cours. Vous pouvez travailler normalement pendant le chiffrement :



Si vous cliquez dans le petit icone, vous aurez l'état d'avancement du chiffrement du disque :



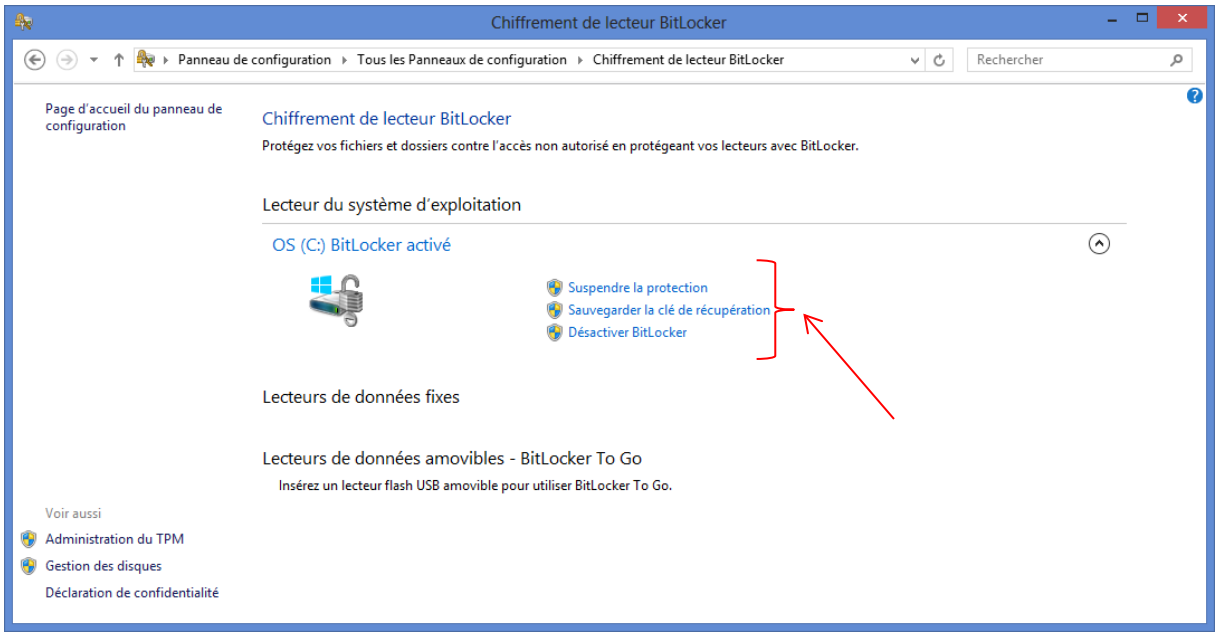
Et à la fin :



Les perfomances de BitLocker en vitesse de chiffrement sont comparables à celles de TrueCrypt.

Gestion de BitLocker

Une fois BitLocker activé, à partir de« Chiffrement de lecteur BitLocker » dans le panneau de configuration, vous pouvez :



Suspendre : cela permet de suspendre temporairement BitLocker (par exemple, pour installer un nouveau logiciel que BitLocker serait susceptible de bloquer), puis le reprendre.

Sauvegarder la clé : de créer d'autres copies de la clé sur un fichier ou de les imprimer.

Désactiver : désactive BitLocker et déchiffre le lecteur. Après cela, appuyez ou cliquez sur le bouton Désactiver BitLocker.

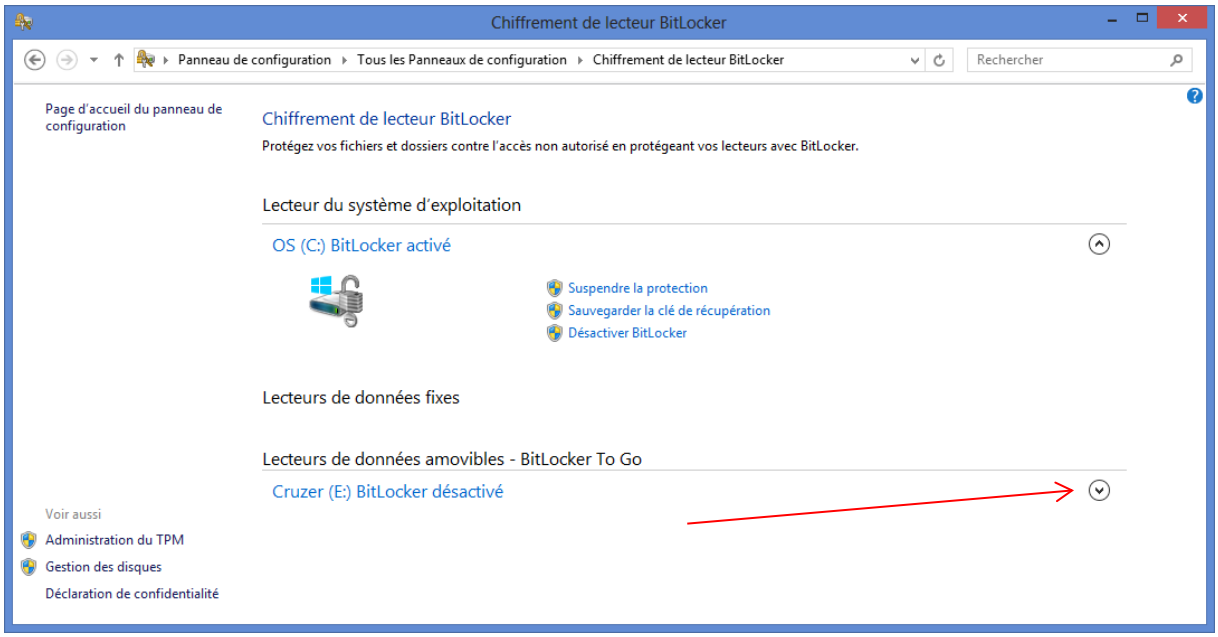
Obs : autorisation de l'administrateur nécessaire pour ces opérations. Il peut vous être demandé de fournir un mot de passe d'administrateur ou de confirmer votre choix.

Lecteurs de données amovibles

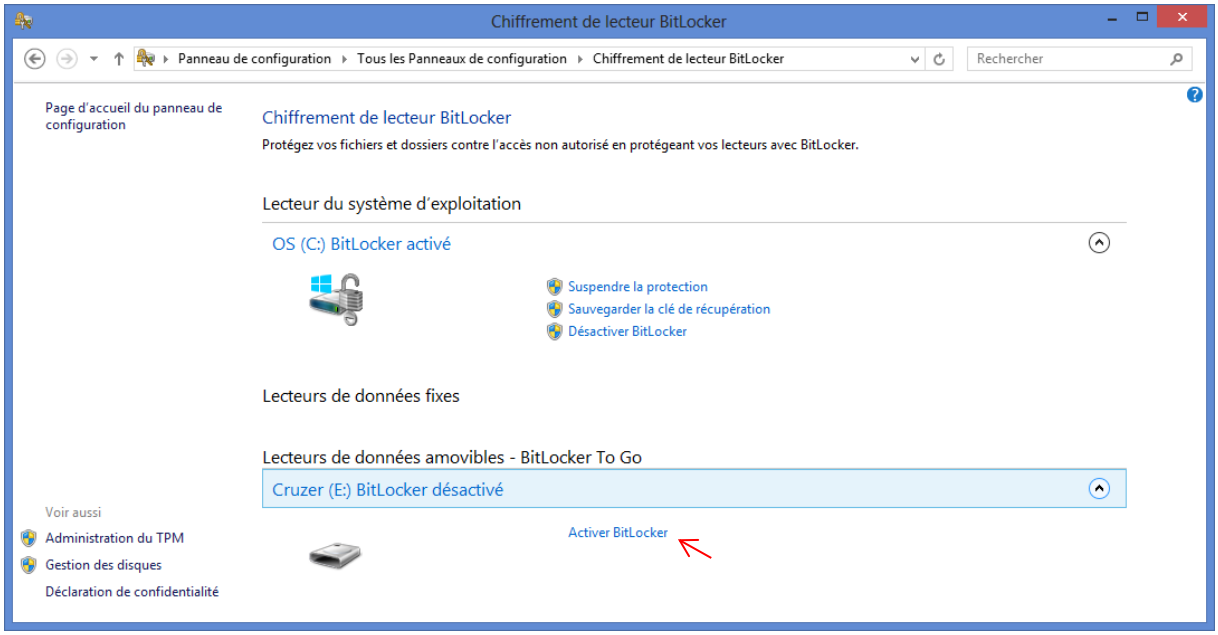
BitLocker permet également de chiffrer des supports tels qu'un disque dur externe ou une clé USB. Les supports ainsi chiffrés sont autonomes : vous n'avez pas besoin d'installer BitLocker pour pouvoir les lire sur un autre ordinateur sous Windows 2008, Windows XP, Windows7 ou Windows8. C'est la solution la plus simple dans les cas où vous êtes sûr que les données seront lues avec un ordinateur sous Windows. TrueCrypt permet une portabilité entre Windows, Mac et Linux, néanmoins il nécessite une installation de cet outil au préalable dans la machine cible.

Exemple avec une clé USB

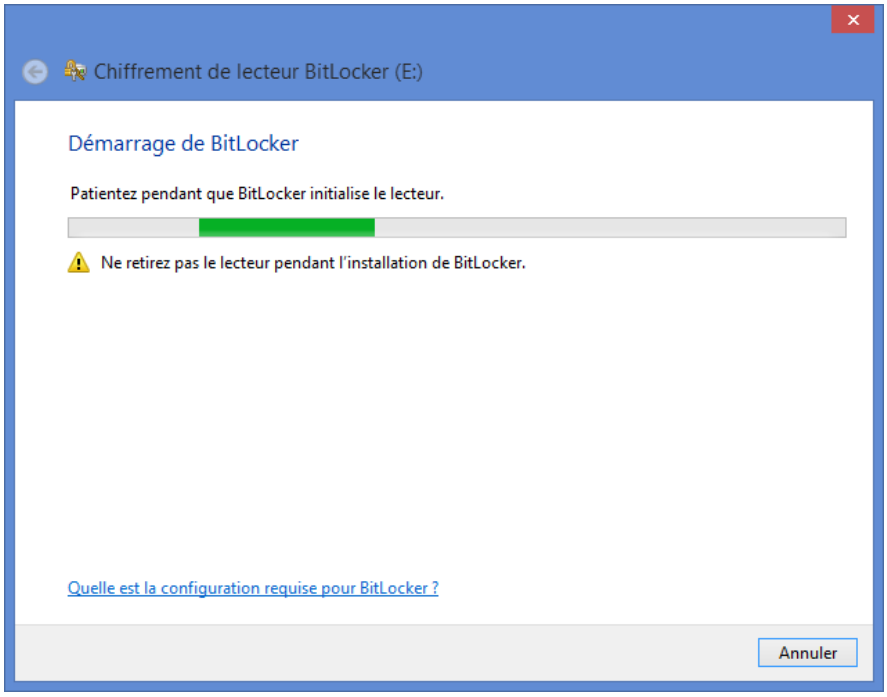
Lorsque vous insérez une clé USB dans votre ordinateur, elle s'affiche dans le panneau « Chiffrement de lecteur BitLocker ». Cliquer sur le lecteur choisi :



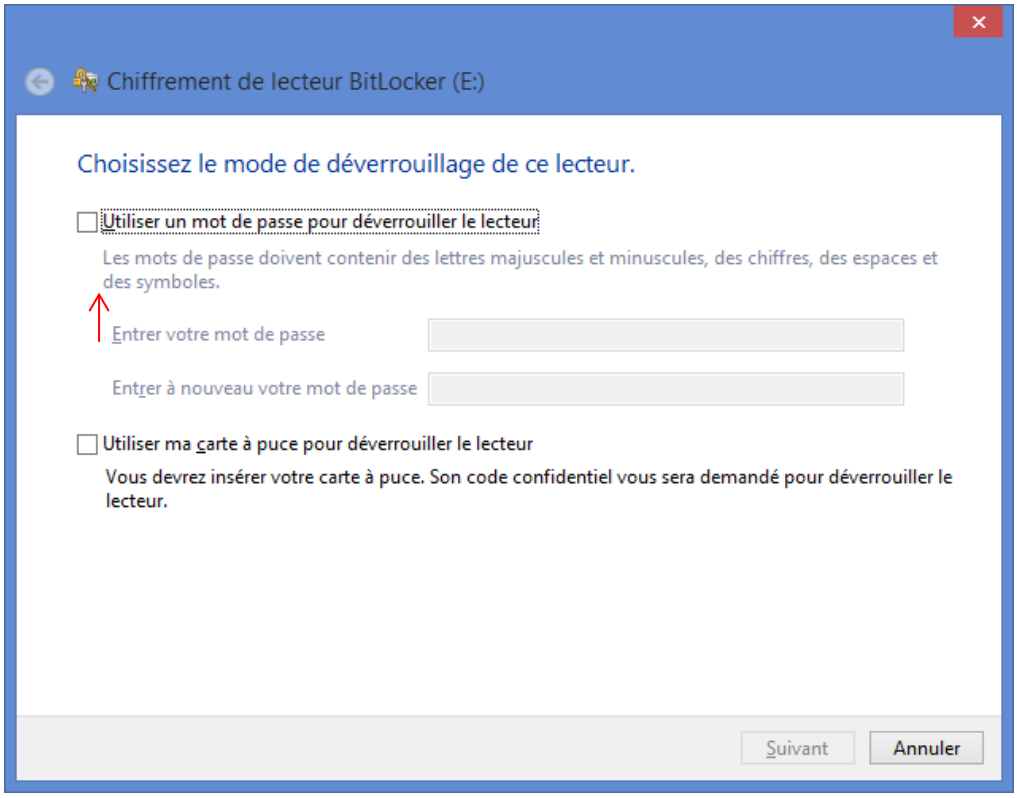
Et dans « Activer BitLocker » :

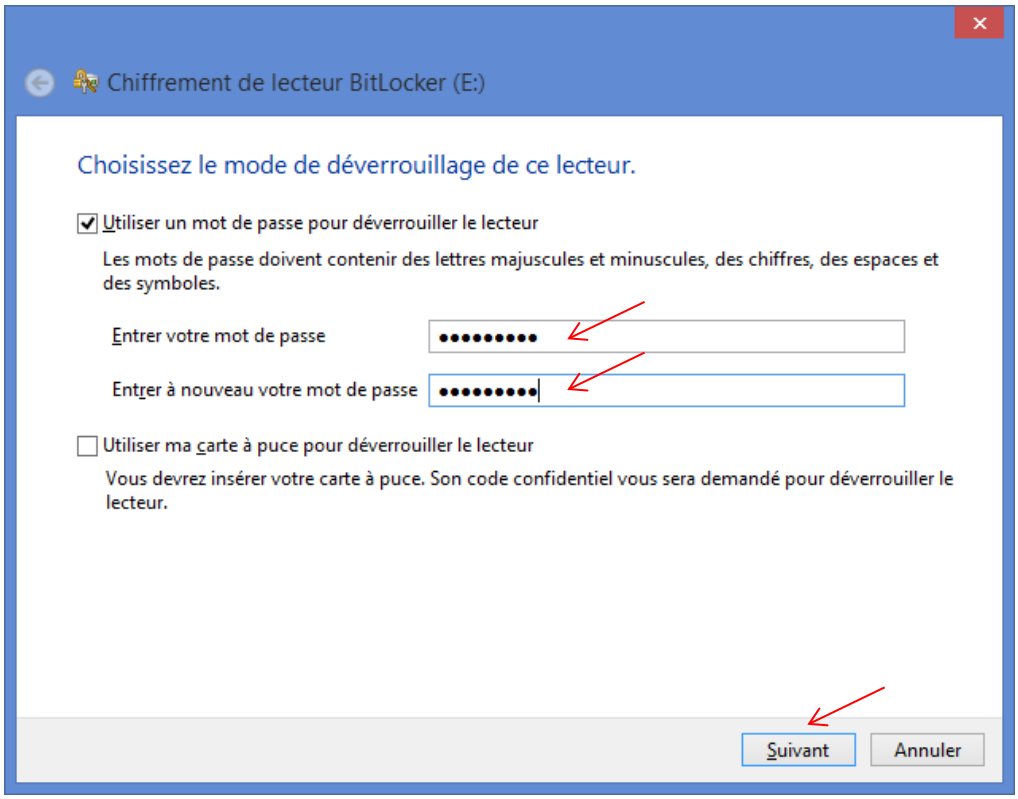


Ne pas retirer le lecteur pendant l'installation de BitLocker :

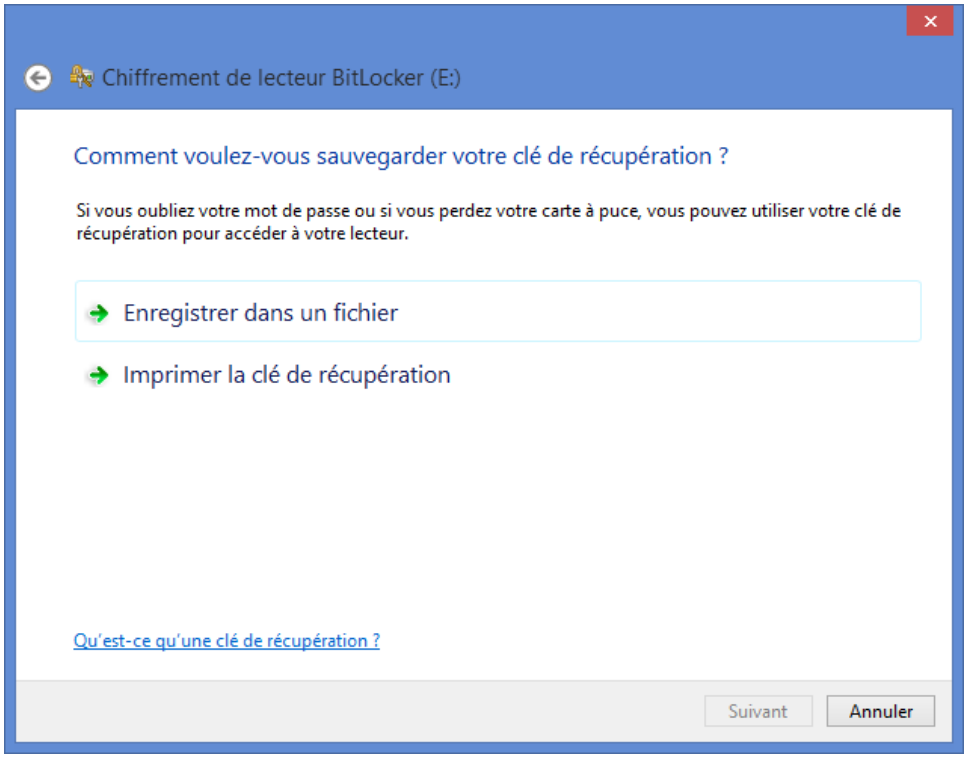


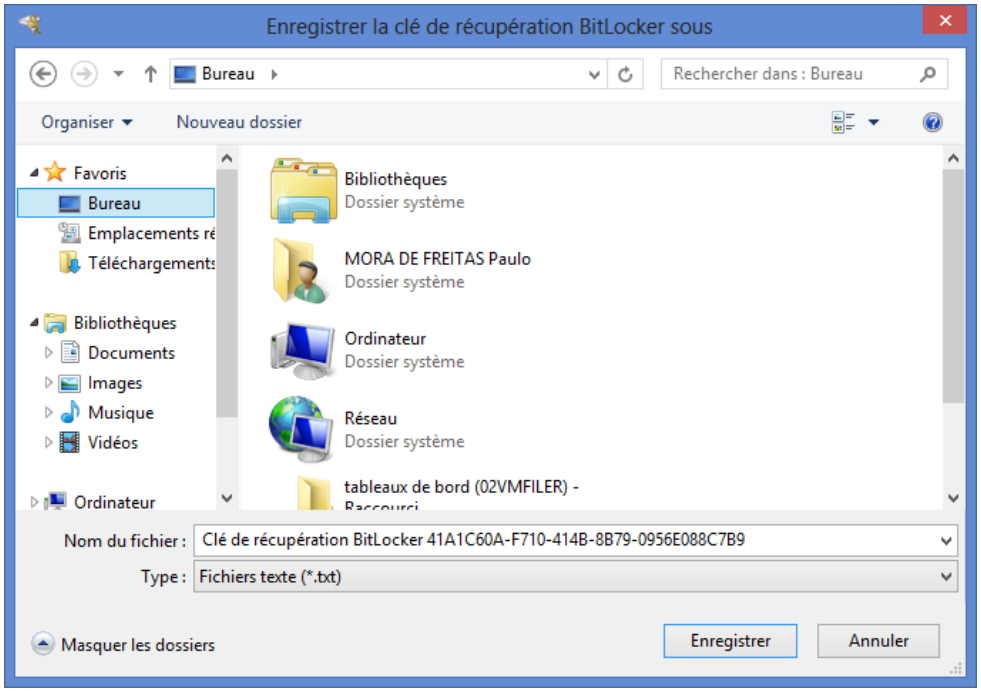
Pour des supports amovibles, il est à vous de définir le mot de passe :



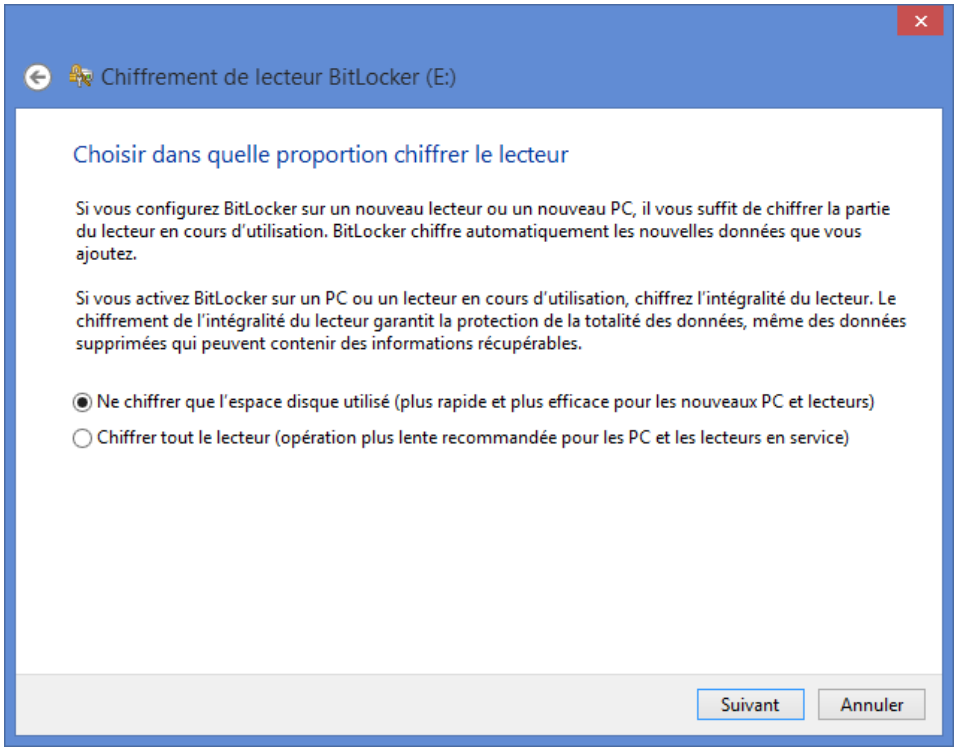


Comme dans le cas d'un disque système, BitLocker vous propose de sauvegarder une clé de récupération le cas où le mécanisme de déchiffrement embarqué dans le lecteur pose problème. La procédure est identique. Dans cet exemple nous savons sur le disque dur de la machine :

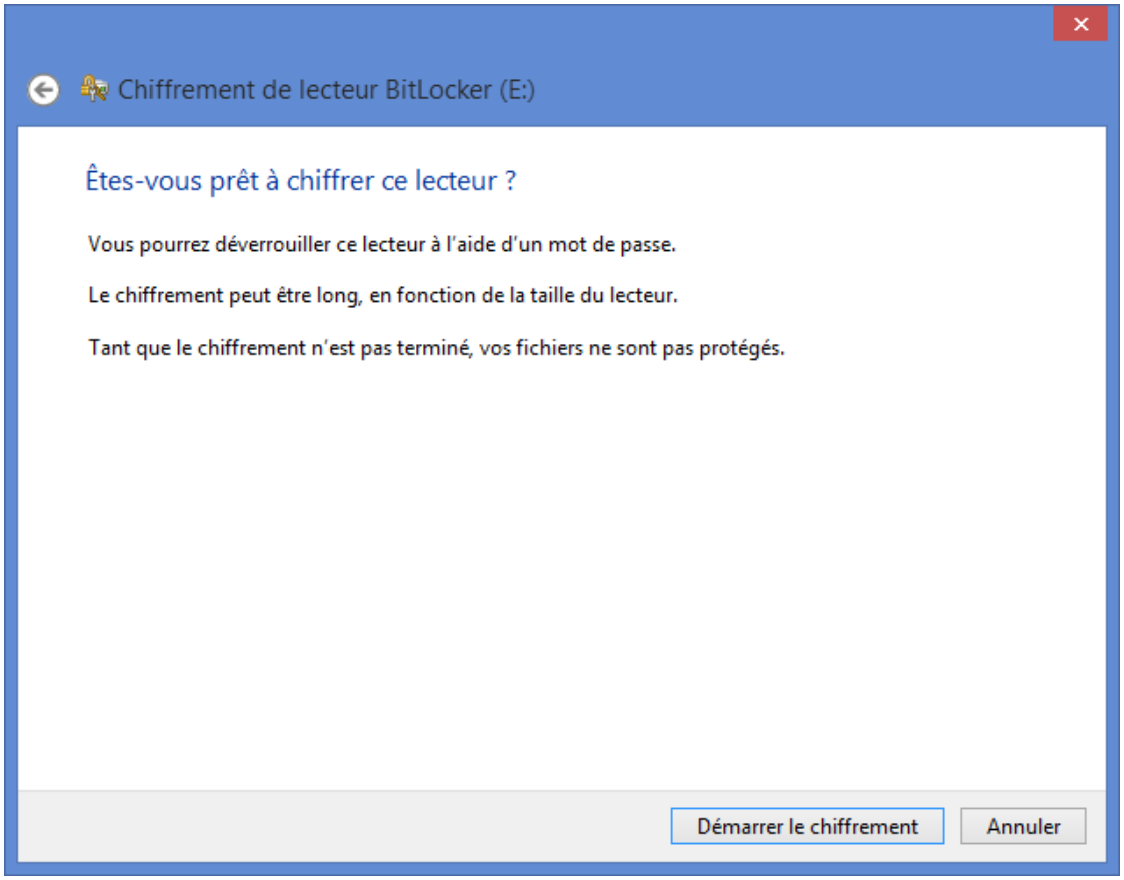




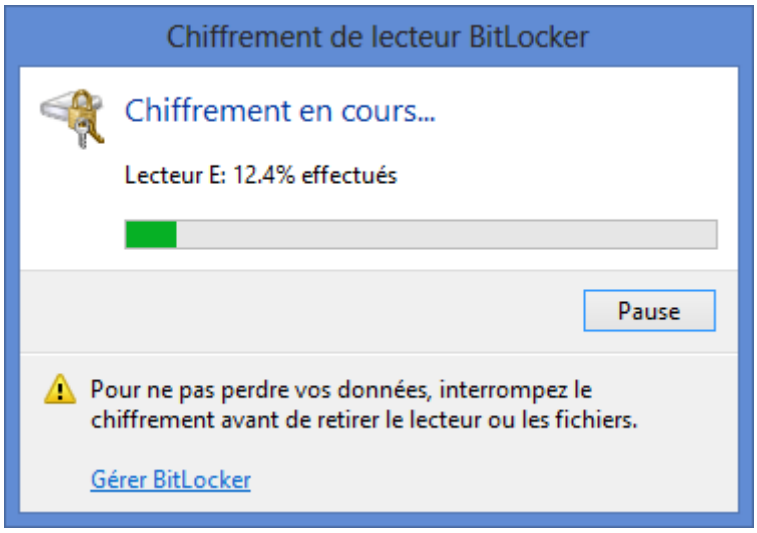
Vous pouvez choisir de chiffrer tout le support ou seulement l'espace utilisé, en fonction de de la sensibilité des données qui y ont été enregistrés et effacés auparavant :



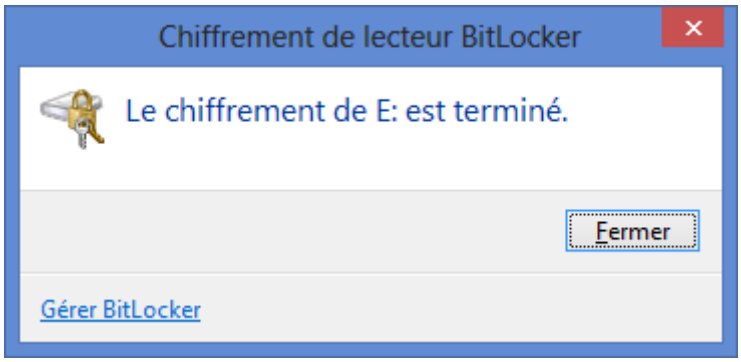
Un dernier avertissement avant de lancer le chiffrement :



Il est possible de retirer la clé avant la fin du chiffrement, mais il est nécessaire d'interrompre le chiffrement pour ne pas perdre des données :

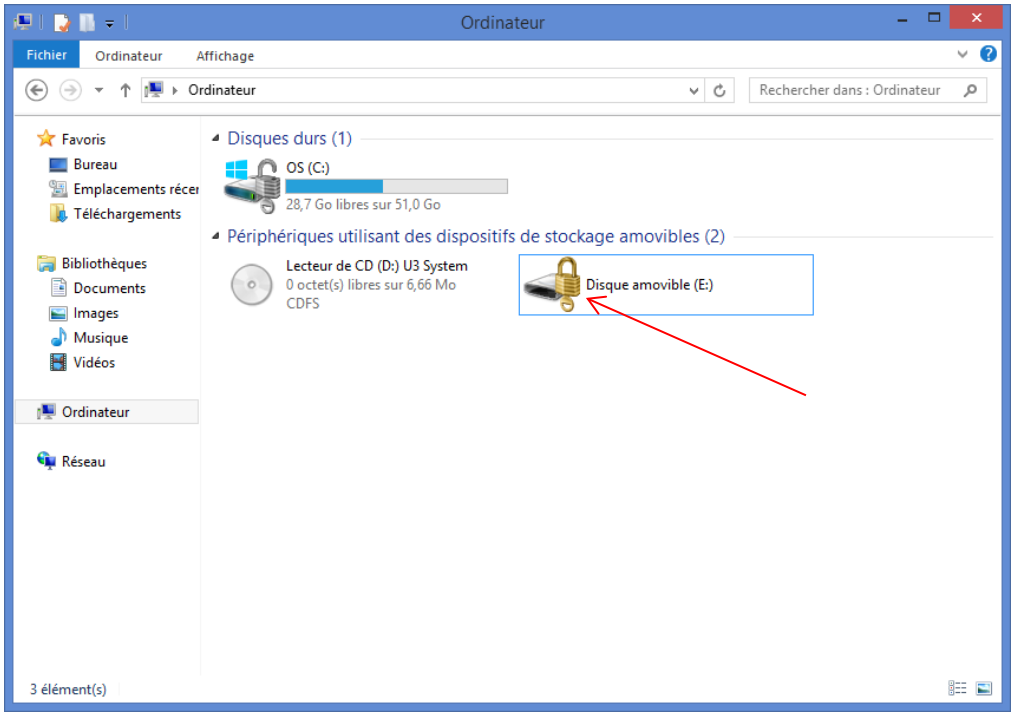


Au final, vous avez un message pour vous avertir de la fin du chiffrement :

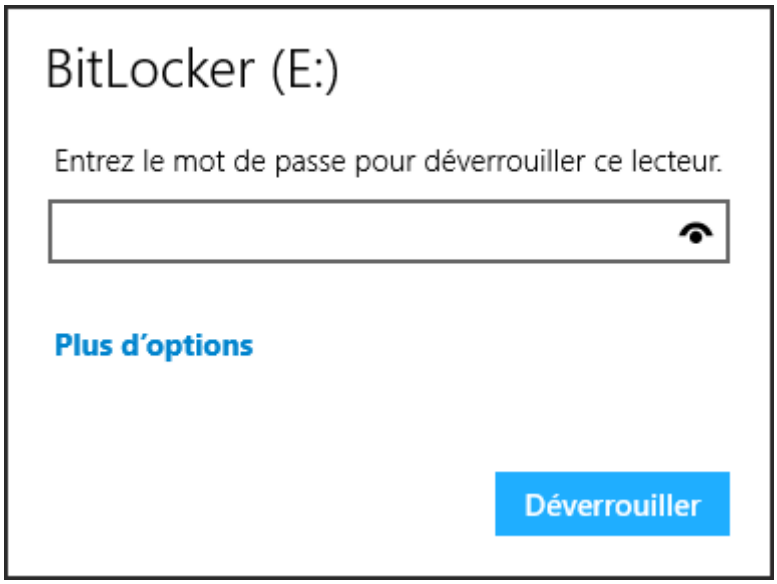


Utilisation d'un lecteur de données chiffré avec BitLocker

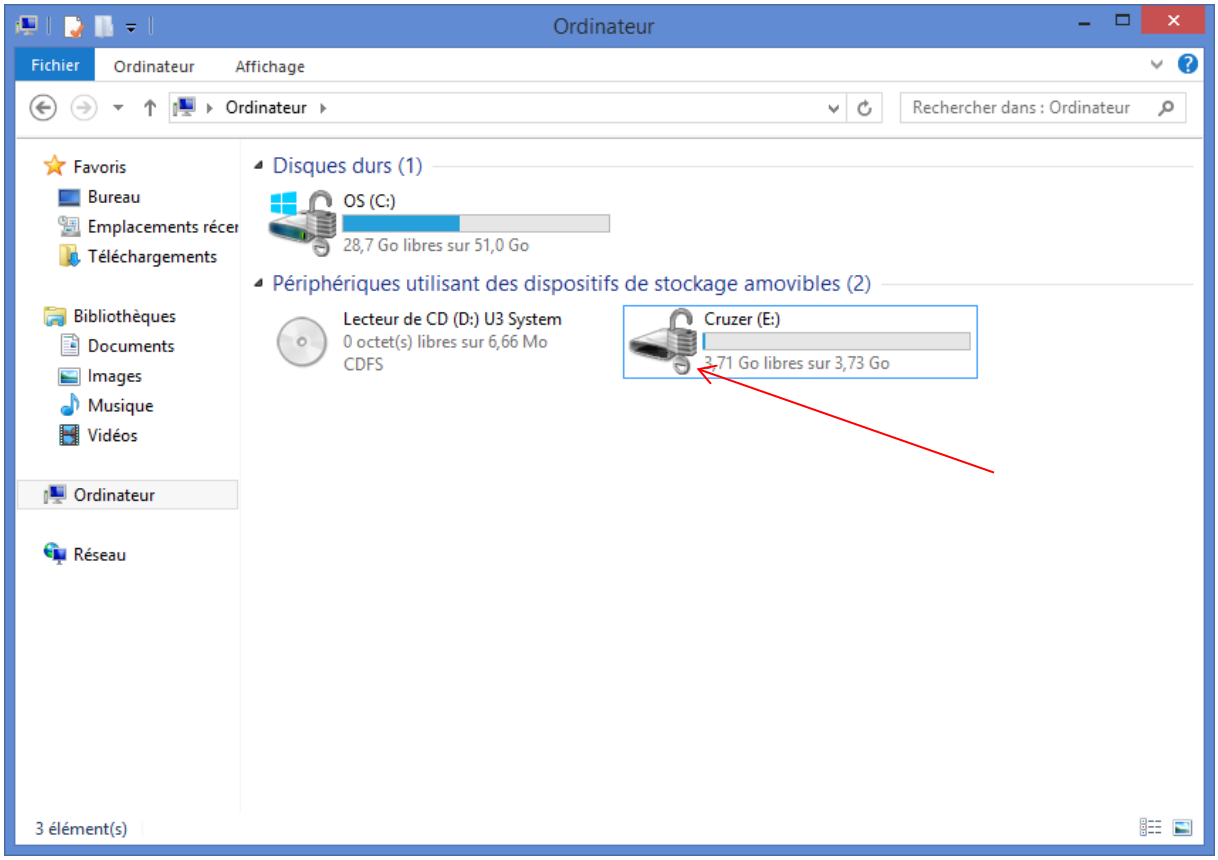
Lorsque vous insérer un lecteur amovible chiffré avec BitLocker, il apparaitra avec un cadenas fermé pendant que le bon mot de passe n'ait pas été saisi :



Lorsque vous cliquez sur le lecteur, le mot de passe est demandé (ici, écran Windows8) :



Une fois le bon mot de passe saisi, l'icône du lecteur apparaît avec un cadenas ouvert :



En revenant sur le panneau « Chiffrement de lecteur BitLocker » vous trouverez plusieurs options pour gérer un lecteur chiffré avec BitLocker :