



<http://WWW.CABARE.NET> ©

Sécurisation Bitlocker Windows – sys 30 – Cours T.P. -

Cryptage Bitlocker et AxCrypt Windows

Michel Cabaré – Ver 1.0 – Juillet 2015-

Sécurisation Bitlocker Windows

Cours et T.P.

Michel Cabaré – Ver 1.0 – Juillet 2015

www.cabare.net ©



Sécuriser Windows Bitlocker

– SYS 30 Cours et T.P. - ver 1.0

TABLE DES MATIERES

BITLOCKER VS EFS	3
CRYPTAGE LOGICIEL	3
BITLOCKER	4
PREREQUIS HARD	4
PREREQUIS WINDOWS	4
CRYPTAGE D'UN VOLUME.....	5
LANCEMENT DE BITLOCKER	5
1° ACTIVATION DE BITLOCKER SUR UN VOLUME	6
ACCES A UN VOLUME CRYPTÉ	8
ACCES INTERDIT	8
ACCES AUTORISÉ	9
CLE DE RECUPERATION ET GESTION BITLOCKER	9
BITLOCKER TO GO.....	10
CRYPTAGE LECTEUR USB	10
LECTURE LECTEUR USB.....	11
BITLOCKER SANS TPM	12
PARAMETRAGE VIA GPEDIT.MSC	12

BITLOCKER VS EFS

Cryptage Logiciel

BitLocker est conçu pour protéger la totalité des fichiers personnels et des fichiers système d'un lecteur logique. Vous pouvez utiliser **BitLocker** pour chiffrer tous les fichiers sur des lecteurs de données fixes (tels que des disques durs internes) et utiliser **BitLocker To Go** pour chiffrer les fichiers sur des lecteurs de données amovibles (disques durs externes ou disques flash ou USB).

Le **système de fichiers EFS** permet de protéger des fichiers individuels sur tout lecteur, en fonction du login de l'utilisateur.

N.B: Le chiffrement est perdu en cas de transmission par mail ou via le réseau.

BitLocker (logiciel et matériel)

- BitLocker chiffre tous les fichiers personnels et système sur un lecteur de données fixe et sur des lecteurs de données amovibles.
- BitLocker ne dépend pas des comptes d'utilisateurs individuels associés aux fichiers. BitLocker est activé ou désactivé, pour tous les utilisateurs ou groupes.
- BitLocker peut utiliser le module de plateforme sécurisée (TPM), une puce spéciale présente sur de nombreux ordinateurs et qui prend en charge des fonctionnalités de stockage et de chiffrement.
- Vous devez être un administrateur pour activer ou désactiver le chiffrement BitLocker

EFS, Système de fichiers EFS (logiciel)

- EFS chiffre les fichiers personnels et système un par un et ne chiffre pas le contenu complet d'un lecteur.
- Le système de fichiers EFS chiffre des fichiers en fonction du compte d'utilisateur associé. Si un ordinateur comporte plusieurs utilisateurs ou groupes, chacun peut chiffrer ses propres fichiers individuellement.
- Le système de fichiers EFS ne requiert ou n'utilise pas de matériel spécial.
- Il n'est pas nécessaire que vous soyez un administrateur pour pouvoir utiliser le système de fichiers EFS.

Prérequis Hard

Au niveau du matériel un microprocesseur de module de plateforme sécurisée version 1.2 dit TPM est recommandé. Un BIOS compatible TCG (Trusted Computing Group) pour l'utilisation de BitLocker si on l'utilise sur des lecteurs du système d'exploitation

N.B: Si l'ordinateur ne dispose pas d'un module TPM, un lecteur flash USB peut être utilisé pour stocker la clé de récupération BitLocker

Récapitulatif des types de protection selon le type de lecteur

Système d'exploitation

- TPM
- TPM + code confidentiel
- Clé de démarrage (pour les systèmes sans TPM)
- Mot de passe (pour les systèmes sans TPM)

Lecteur de données fixe

- Déverrouillage automatique
- Mot de passe / Carte à puce

Lecteur de données amovible

- Mot de passe / Carte à puce

Prérequis Windows

Au niveau Windows, **Bitlocker** est disponible sous les versions suivantes :

Windows Seven: entreprise – intégrale

Windows 8-8.1: professionnel - entreprise

Windows 10: professionnel - entreprise

Au niveau Windows, **Bitlocker to go** est disponible sous les mêmes versions et en plus en version Lecture seule sur :

Windows Seven: pro

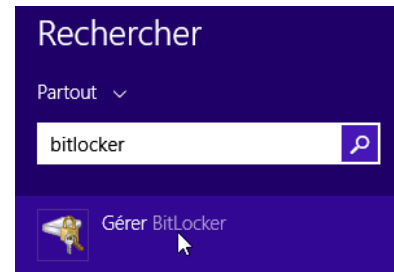
Windows XP: pro (en téléchargement)

CRYPTAGE D'UN VOLUME

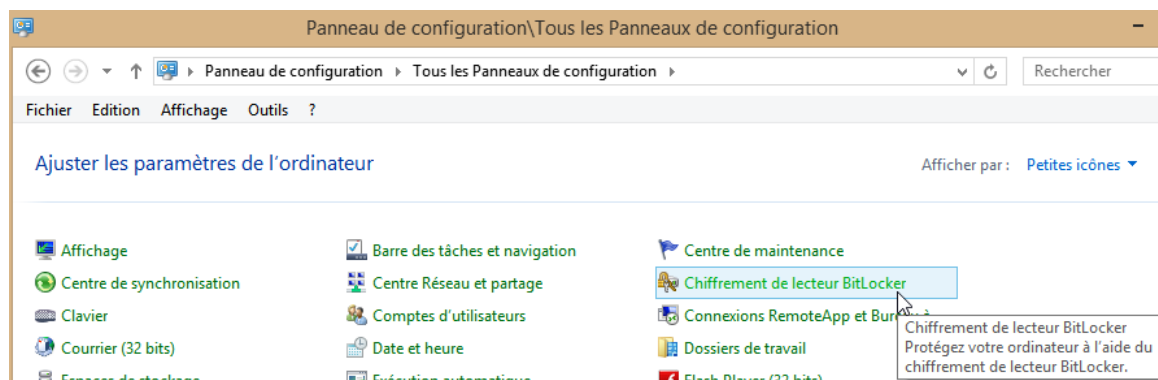
Lancement de Bitlocker

Un recherche sous Windows 8 ou

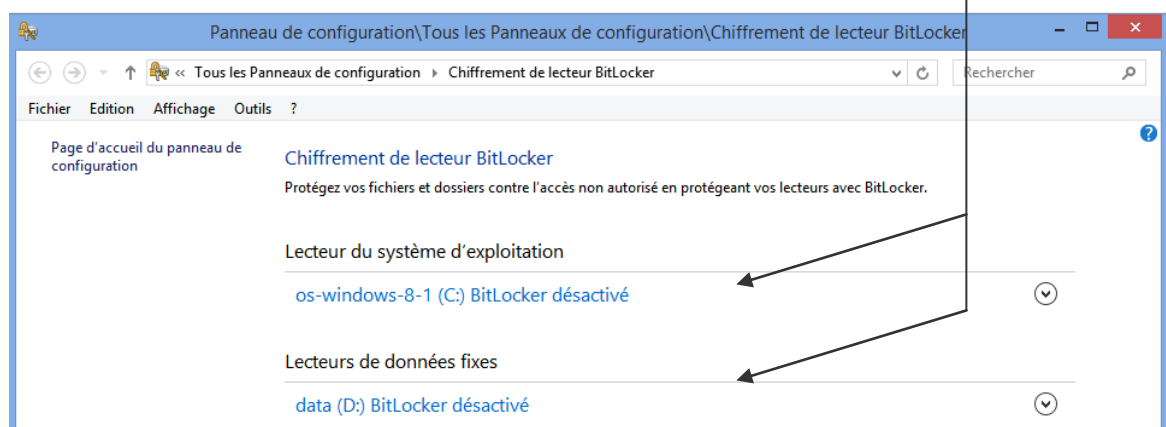
Le raccourci **Chiffrement de Lecteur BitLocker**



Ou via le Panneau de configuration



Amène l'interface de gestion de Bitlocker



On y trouvera tous les volumes existants sur la machine, avec la possibilité de décider quoi y faire

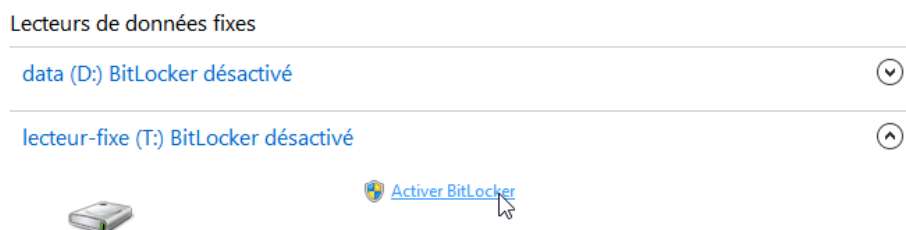
1° Activation de Bitlocker sur un volume

Il est plus compliqué et délicat d'activer un cryptage sur la partition système, et dans ce cas la présence d'une "puce" sur la carte mère de la machine est grandement souhaitée

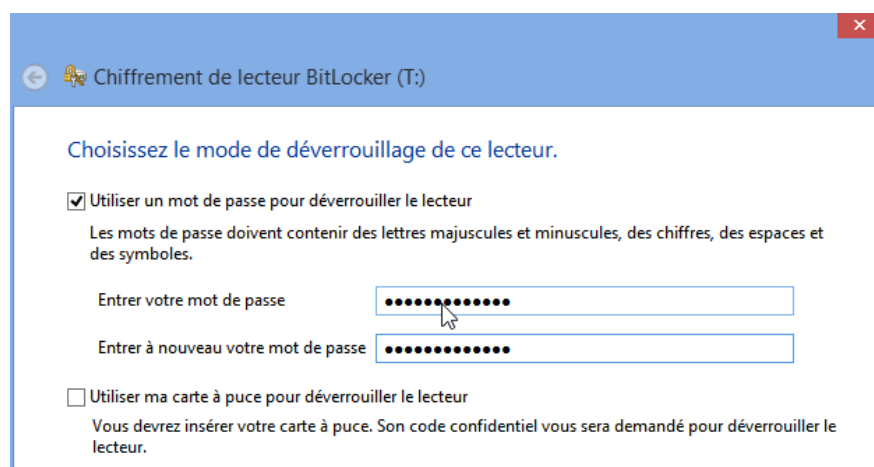


Par contre on peut sans hésiter décider d'utiliser Bitlocker sur une partition de données.

Lorsque l'on utilise BitLocker pour la première fois, il faut s'assurer du stockage de la clé de récupération. Dans le cas contraire, il se peut que vous perdiez définitivement l'accès aux fichiers !



cliquez sur **Activer BitLocker**. La boîte de dialogue d'installation du Chiffrement de lecteur BitLocker s'ouvre. On choisit un mot e passe...



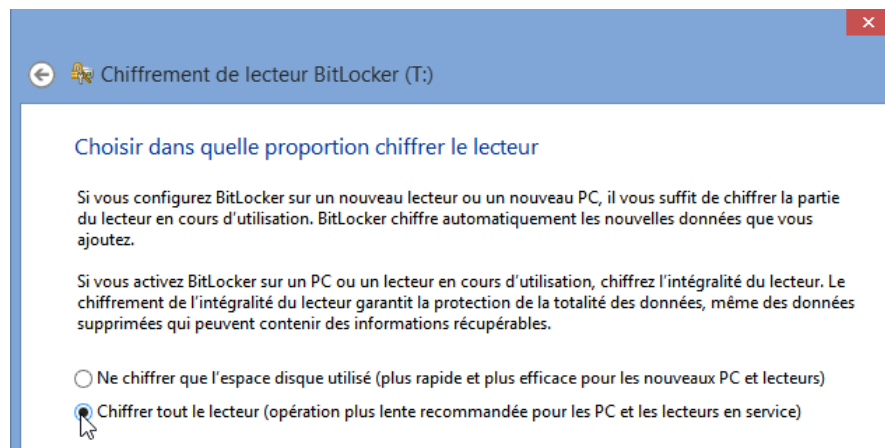
Et il faut choisir l'endroit de stockage du fichier qui contient la clé de récupération du cryptage (en cas de perte du mot de passe)



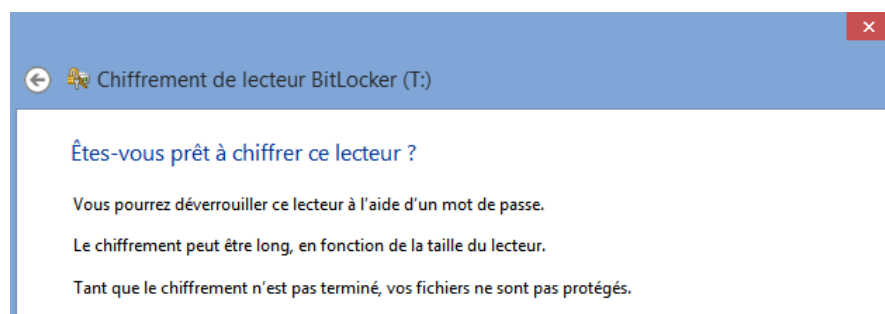
Dans un fichier du genre

Nom du fichier :	Clé de récupération BitLocker 1B693FE8-6B89-4F14-B8B4-F1C2130D5FCC.txt
Type :	Fichiers texte (*.txt)

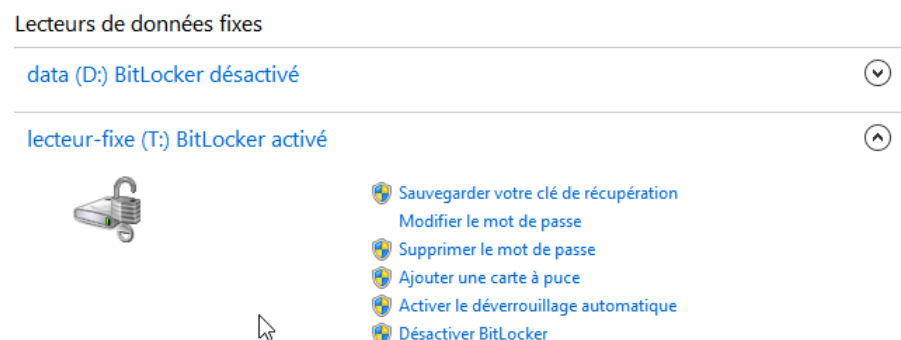
On demande de **Chiffrer tout le lecteur**



Puis on confirme



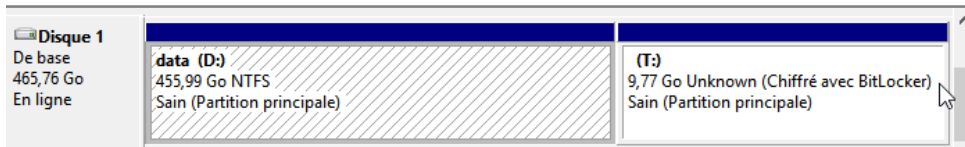
Et on obtient



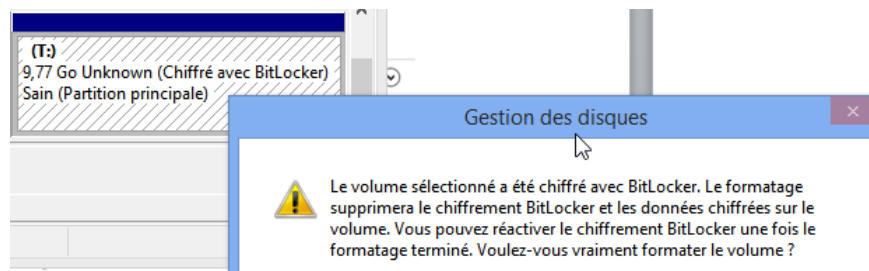
ACCES A UN VOLUME CRYPTÉ

Accès interdit

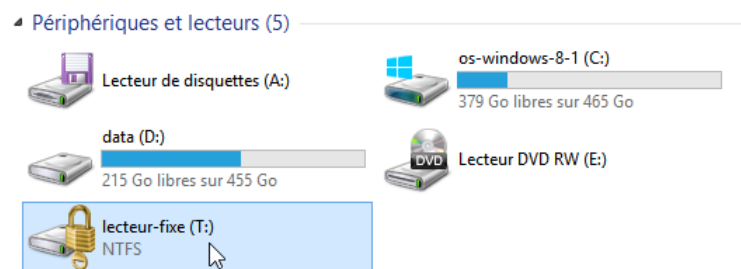
Dans le **gestionnaire de disque**



le formatage du disque restera possible...



Mais dans le gestionnaire de fichier



Une tentative d'accès demande une authentification, soit par

le **mot de passe**

BitLocker (T:)

Entrez le mot de passe pour déverrouiller ce lecteur.

[Plus d'options](#)

Déverrouiller

ou la **clé de récupération**

BitLocker (T:)

Entrez le mot de passe pour déverrouiller ce lecteur.

[Moins d'options](#)

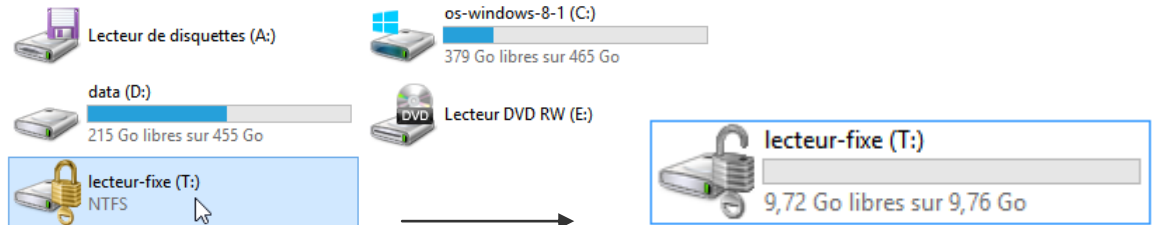
[Entrer la clé de récupération](#)

Déverrouiller

Accès autorisé

Une fois le mot de passe saisi, (ou la clé..) le lecteur restera accessible pour toute les sessions en cours... tant que le poste ne sera pas re-démarré !
donc aucun problème de compatibilité applicative, et confort maximal

▀ Périphériques et lecteurs (5)



Clé de récupération et gestion bitlocker

via le gestionnaire bitlocker

lecteur-fixe (T:) BitLocker activé



- Sauvegarder votre clé de récupération
- Modifier le mot de passe
- Supprimer le mot de passe
- Ajouter une carte à puce
- Activer le déverrouillage automatique
- Désactiver BitLocker

Les options intéressantes sont bien sur

- **Sauvegarder votre clé de récupération**
- **Modifier le mot de passe**
- **Désactiver Bitlocker**

N.B: Pour vérifier qu'il s'agit de la bonne clé de récupération il faut comparer le début de l'identificateur du volume crypté.

BitLocker (T:)

Entrez le mot de passe pour déverrouiller ce lecteur.

Moins d'options

Entrer la clé de récupération

Déverrouiller

↶ BitLocker (T:)

Entrez la clé de récupération de 48 chiffres pour déverrouiller ce lecteur.
(ID de clé : 1B693FE8)

Charger une clé à partir d'un lecteur USB

Avec celui de la clé...qui est d'ailleurs dans le nom defichier...

Clé de récupération BitLocker 1B693FE8-6B89-4F14-B8B4-F1C2130D5FCC.txt

BITLOCKER TO GO

Cryptage lecteur USB

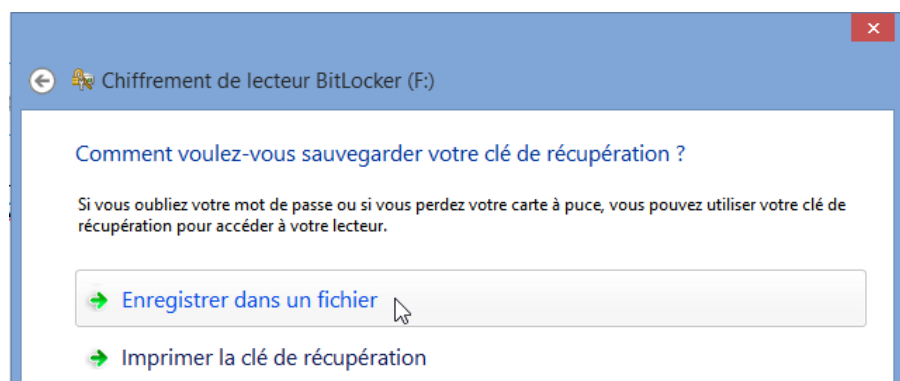
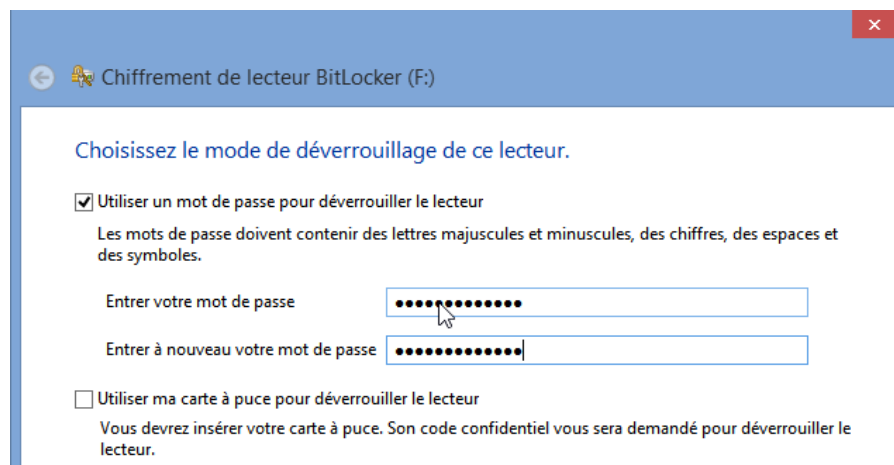
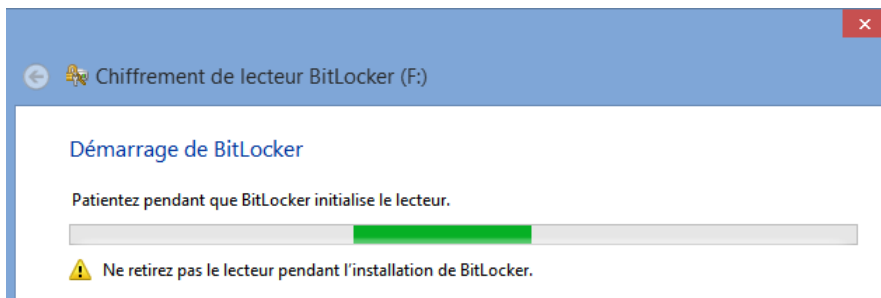
De manière quasi identique, le cryptage se fera via le **gestionnaire Bitlocker**

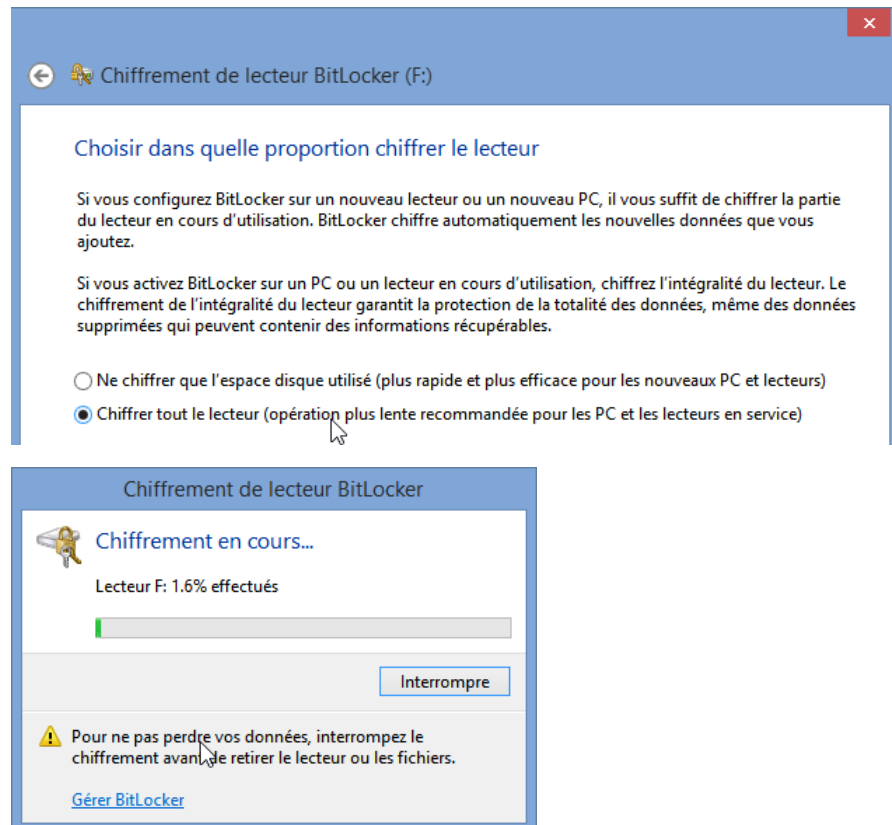
Lecteurs de données amovibles - BitLocker To Go

G: BitLocker désactivé



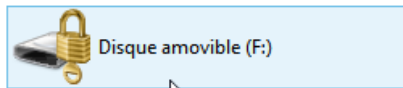
[Activer BitLocker](#)





Lecture lecteur USB

La mécanique est identique..



Lecteurs de données amovibles - BitLocker To Go

F: BitLocker activé (Verrouillé)



[Déverrouiller le lecteur](#)

N.B: la lecture de la clé USB est possible sur toutes les version de Windows 7 (pro-entreprise-intégrale) et sous XP moyennant le téléchargement du logiciel Bitlocker to Go en lecture...

BITLOCKER SANS TPM

Paramétrage via gpedit.msc

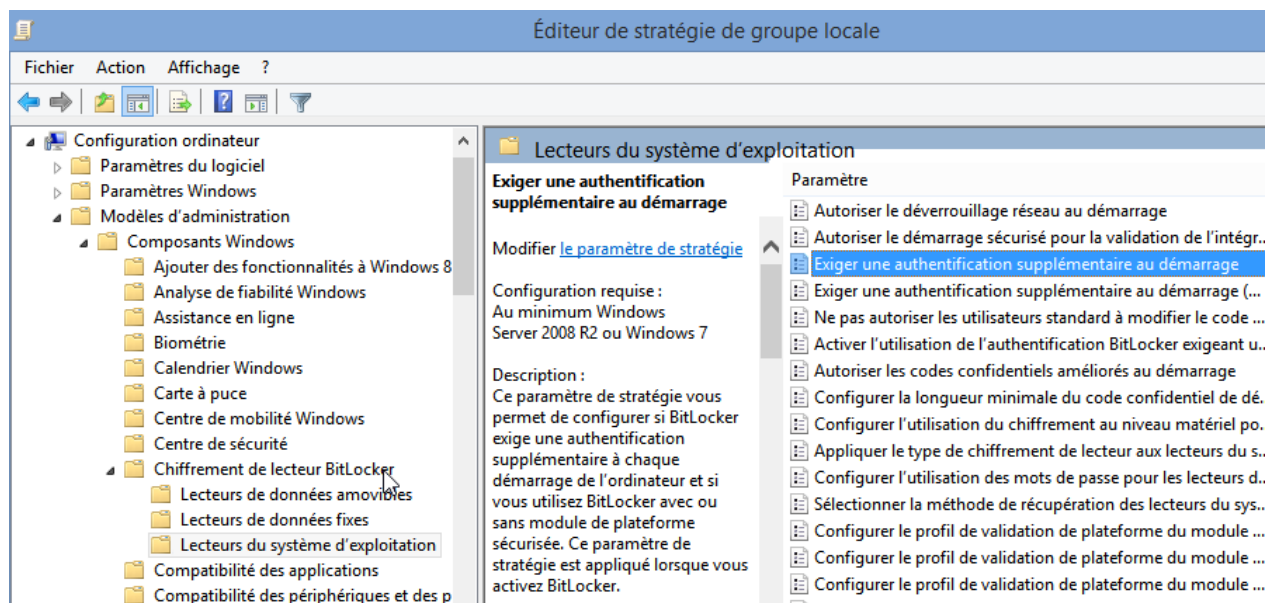
Selon les versions, Bitlocker ne voudra pas chiffrer la partition système sans présence de puce TPM...

via **gpedit.msc** dans Exécuter... du menu démarrer.

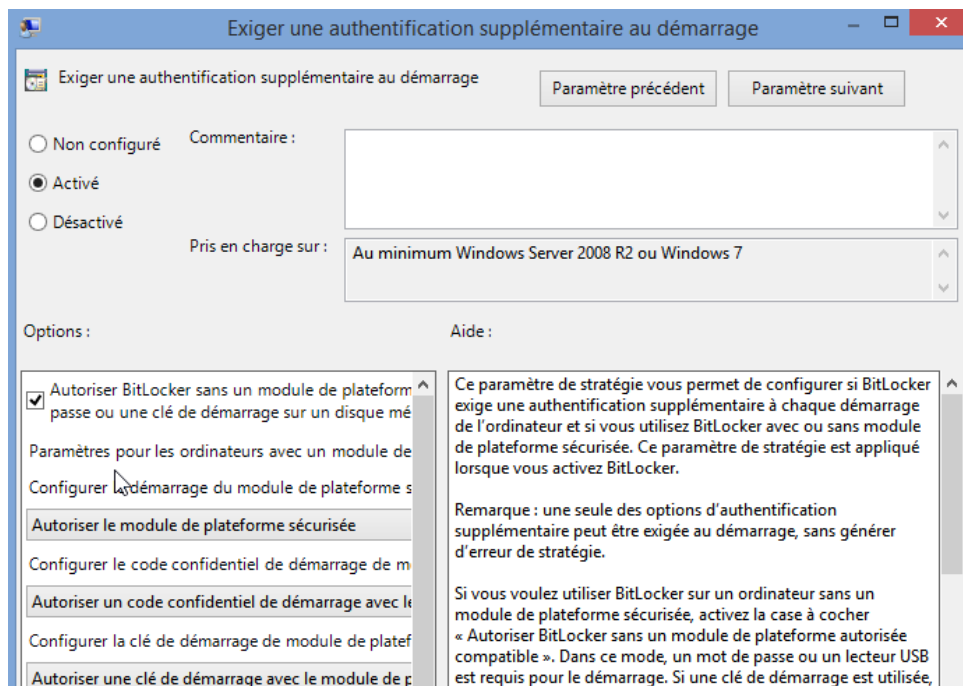
Configuration ordinateur + Modèles d'administration + Composants Windows + Chiffrement de lecteur Bitlocker + Lecteurs du système d'exploitation .

Le paramètre qui nous intéresse est:

Exiger une authentification supplémentaire au démarrage .



Une fois la fenêtre de propriétés ouverte, vous devez cocher **Activé** en haut, puis la case **Autoriser Bitlocker sans un module de plateforme compatible**.



C'est fait, maintenant lorsque vous tenterez d'activer Bitlocker sur votre disque C:\ , vous pouvez activer Bitlocker à l'aide d'une clef USB.

Cette clef USB sera la clef de votre ordinateur.

Si cette clef USB n'est pas présente dans un des ports USB de votre ordinateur, Windows ne démarrera pas, à moins que vous saissiez la clef de recouvrement Bitlocker(numéro super long de secours). La clef USB devient en quelque sorte votre puce TPM, mais avec moins de fonctionnalités. La puce TPM possède des fonctionnalités avancées permettant de ne pas démarrer Windows du tout, si le disque dur n'est pas dans le même ordinateur, que le BIOS, le MBR, ou le Gestionnaire de démarrage ont changés.