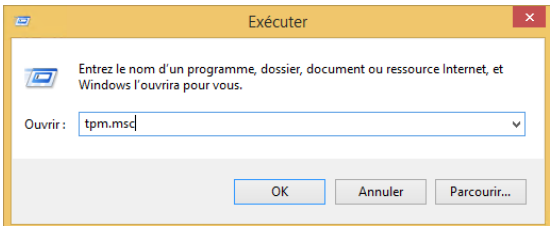
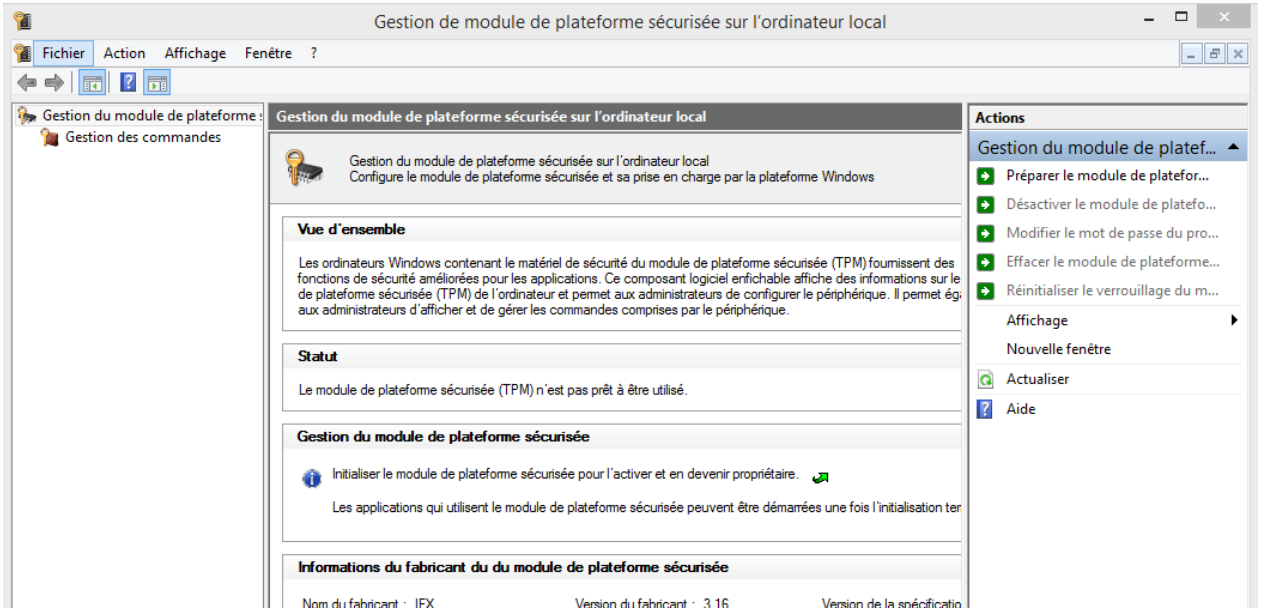
Utilisation de Bitlocker avec TPM avec Windows 8.1 Pro /Enterprise

Janvier 2014

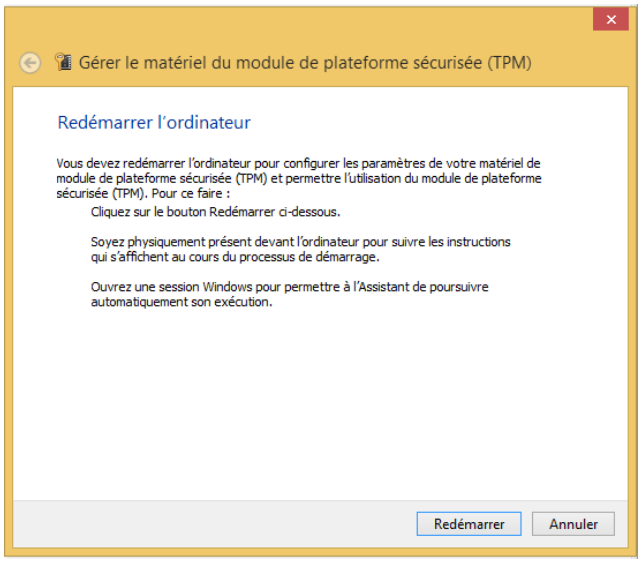
La machine dispose d'un disque avec 2 partitions

La machine étant équipée d'une puce TPM (Trusted Plateform Module), il faut commencer par l'activer en exécutant la commande tpm.msc

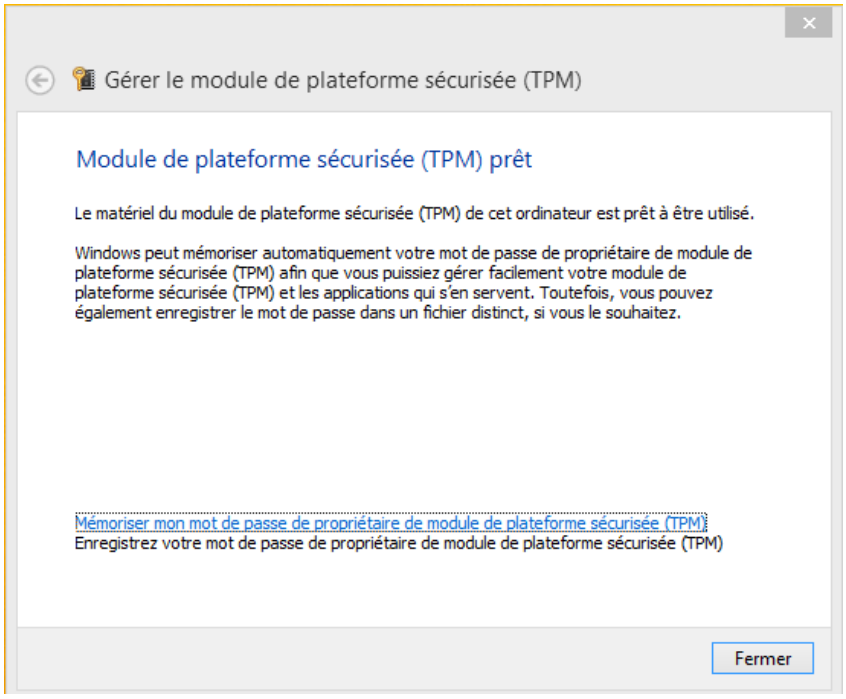




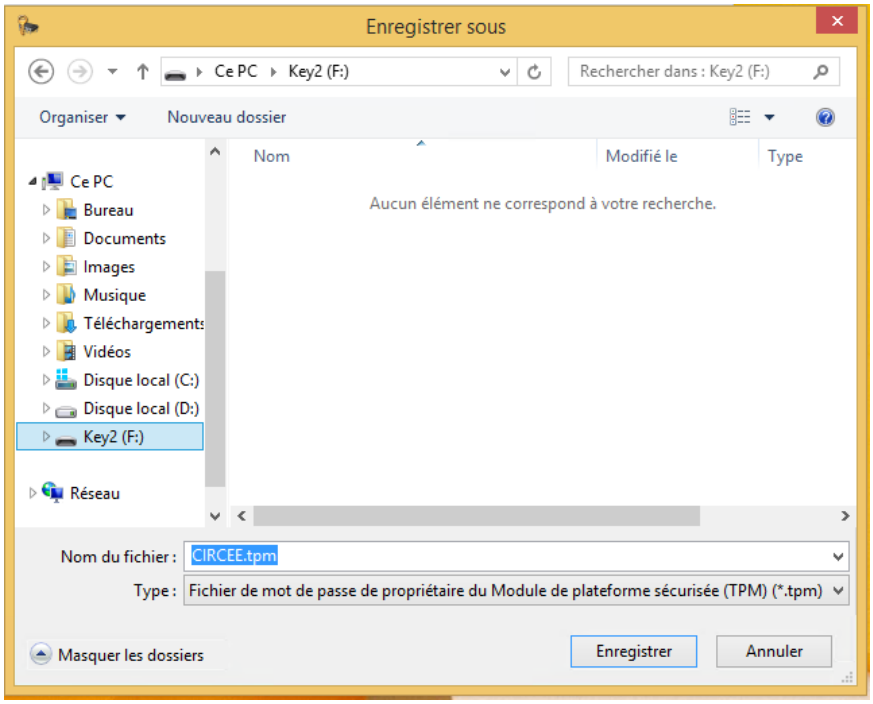
Il faut cliquer sur « Préparer le module de plateforme sécurisé »



Lors du redémarrage, il faut valider les changements en appuyant sur la touche de fonction indiquée



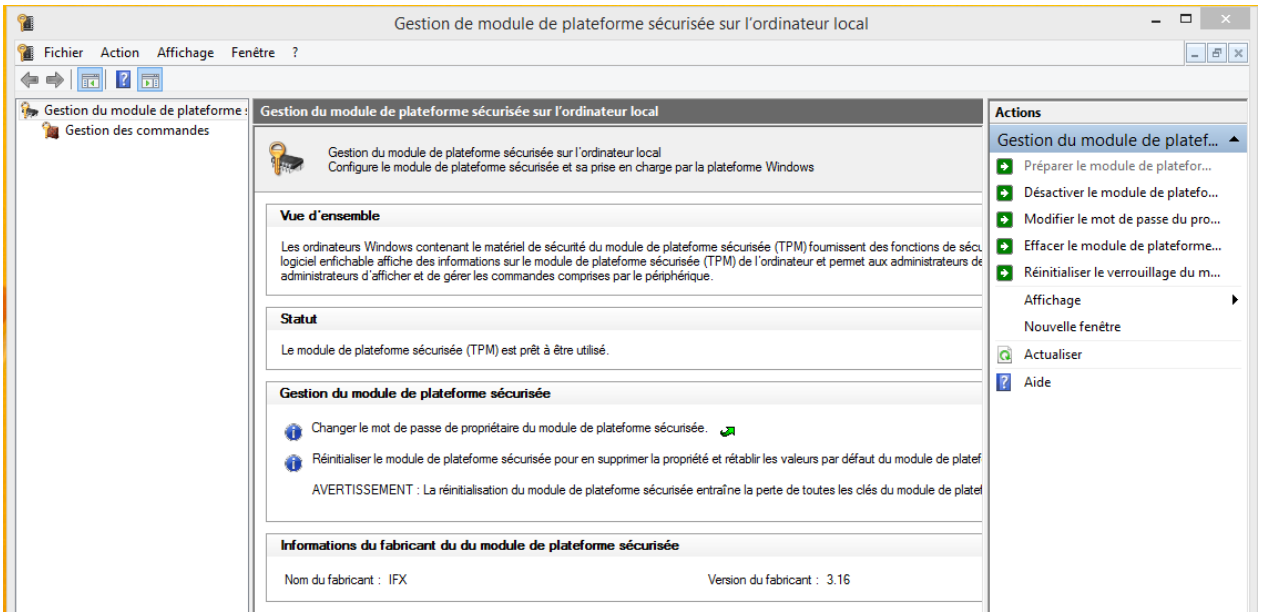
Il faut ensuite cliquer sur « Mémoriser mon mot de passe …. ». Cela sauvegarde un fichier « NomPC.tpm », qu'il faut stocker pour le recouvrement (?). Le fichier ne peut être stocké sur le disque local.



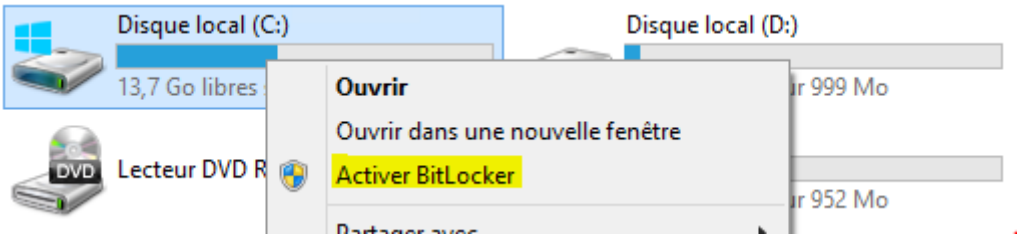
Voici un exemple du contenu de ce fichier

<?xml version="1.0" encoding="UTF-8"?>
<!--Cette page est une sauvegarde des informations d'autorisation du
propriétaire du module de plateforme sécurisée (TPM). Lorsque vous y
êtes invité, utilisez les informations d'autorisation pour prouver
que vous possédez le module de plateforme sécurisée (TPM) de l'ordinateur.
IMPORTANT : conservez ce fichier en lieu sûr, hors du disque dur local de l'ordinateur.
-->
<tpmOwnerData version="1.0" softwareAuthor="Microsoft Windows [Version 6.3.9600]" creationDate="2014-01-09T14:36:52+01:00" creationUser="Circee\stagiaire" machineName="CIRCEE">
    <tpmInfo manufacturerId="1229346816"/>
    <ownerAuth>ptR7DPeHp2mOgjVi0eREmyqRpF8=</ownerAuth>
</tpmOwnerData>

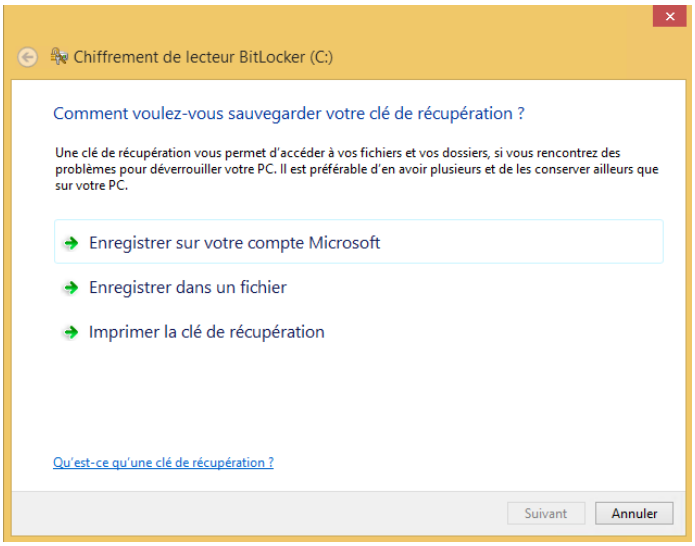
On retournant sur le gestionnaire TPM, d'autres actions sont maintenant disponibles

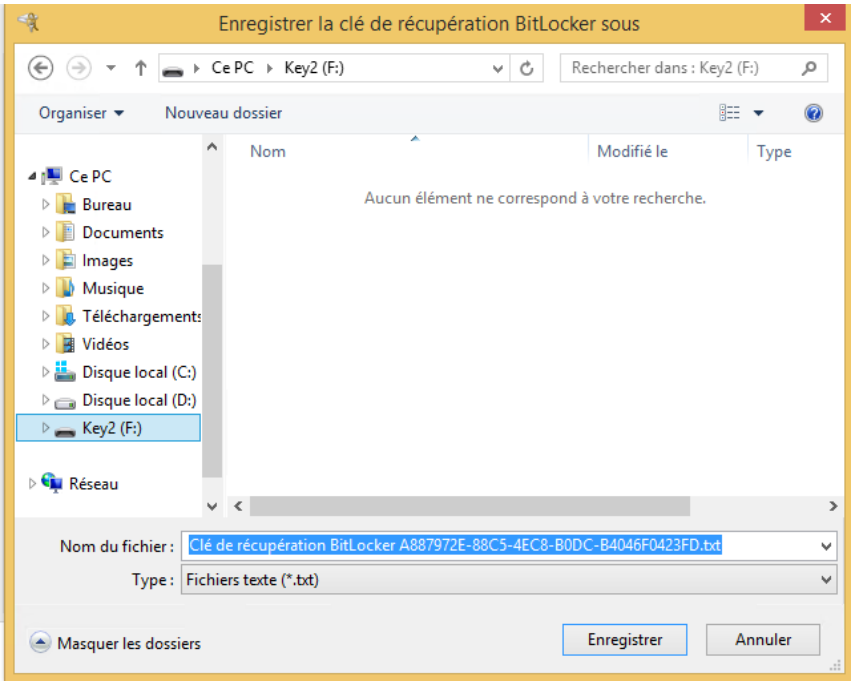


Activons Bitlocker sur le lecteur du système d'exploitation

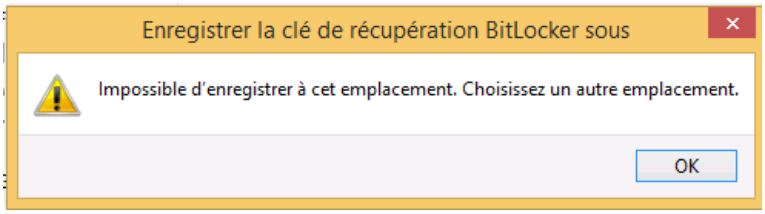


Nous enregistrons la clé de récupération dans un fichier





La clé de récupération ne peut pas être enregistrée sur le lecteur en cours de chiffrement



Voici un exemple du contenu du fichier

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 :

A887972E-88C5-4EC8-B0DC-B4046F0423FD

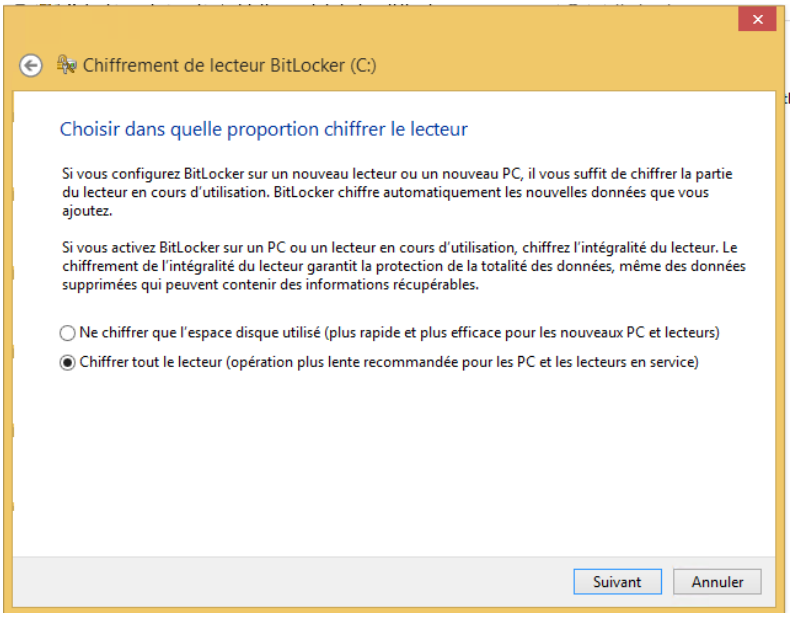
Si l'identificateur ci-dessus correspond à celui affiché sur l'ordinateur, utilisez la clé suivante pour déverrouiller le lecteur.
Clé de récupération :

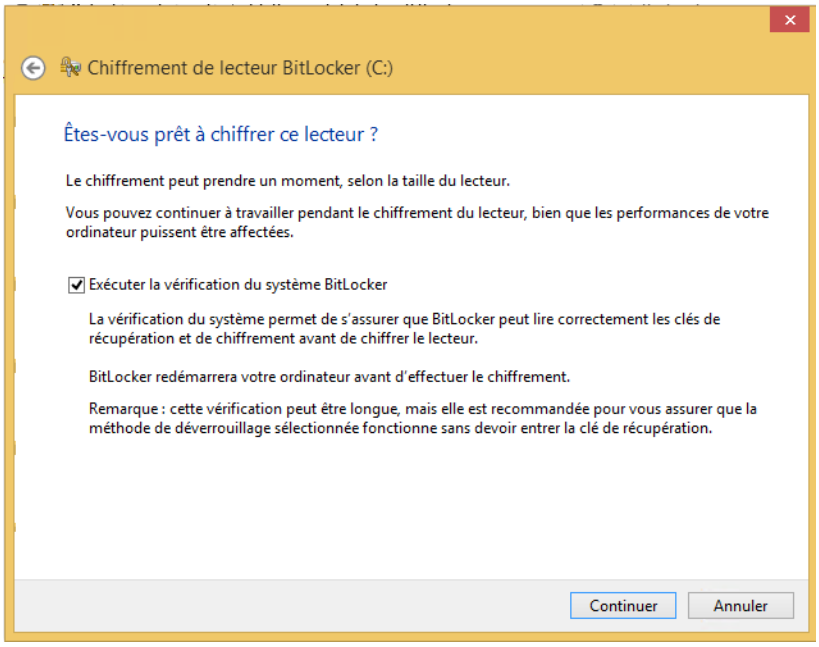
536195-058553-270358-127248-125587-515361-309639-108416

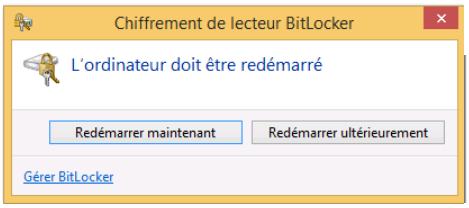
Si l'identificateur ci-dessus ne correspond pas à celui affiché sur l'ordinateur, cette clé ne permet pas de déverrouiller le lecteur.
Essayez une autre clé de récupération ou accédez à http://go.microsoft.com/fwlink/?LinkID=260589 pour obtenir une aide supplémentaire.

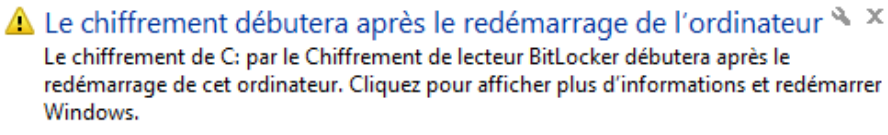
IL faut ensuite cliquer sur « Suivant »

Choisir de chiffrer tout le lecteur (dans le cadre de l'exercice on peut choisir de prendre la première option pour gagner du temps)

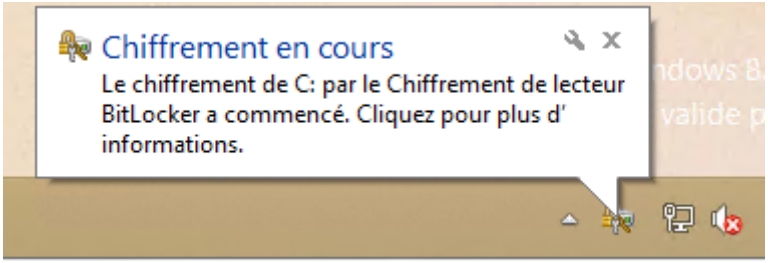


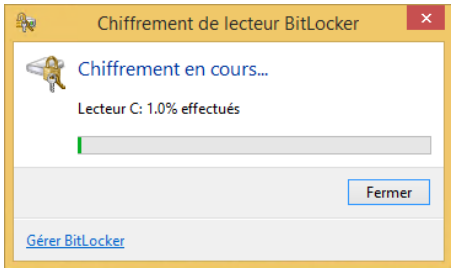


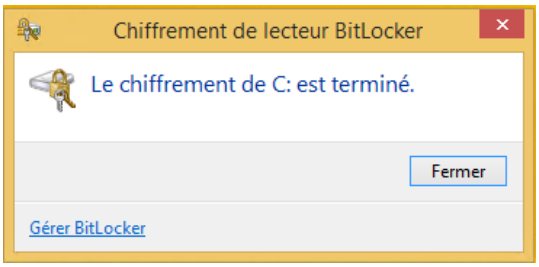




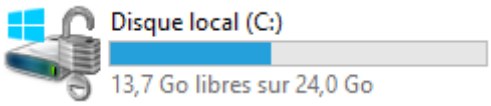
Au redémarrage, le chiffrement commence



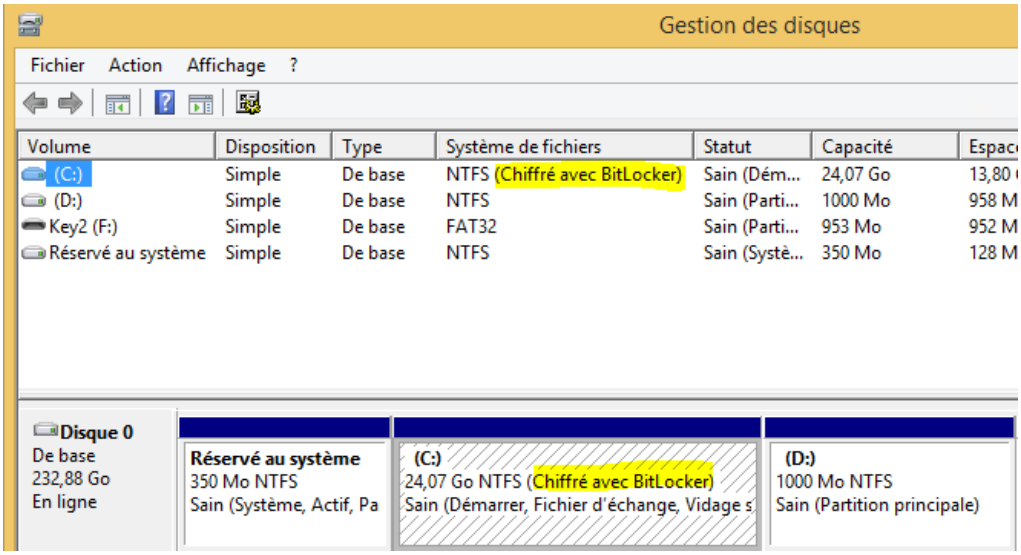




L'icône du lecteur a changé



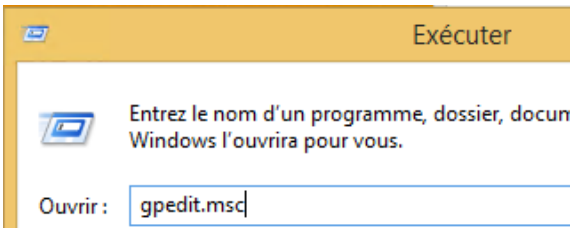
En utilisant le gestionnaire de disque, on retrouve l'information que le lecteur est chiffré



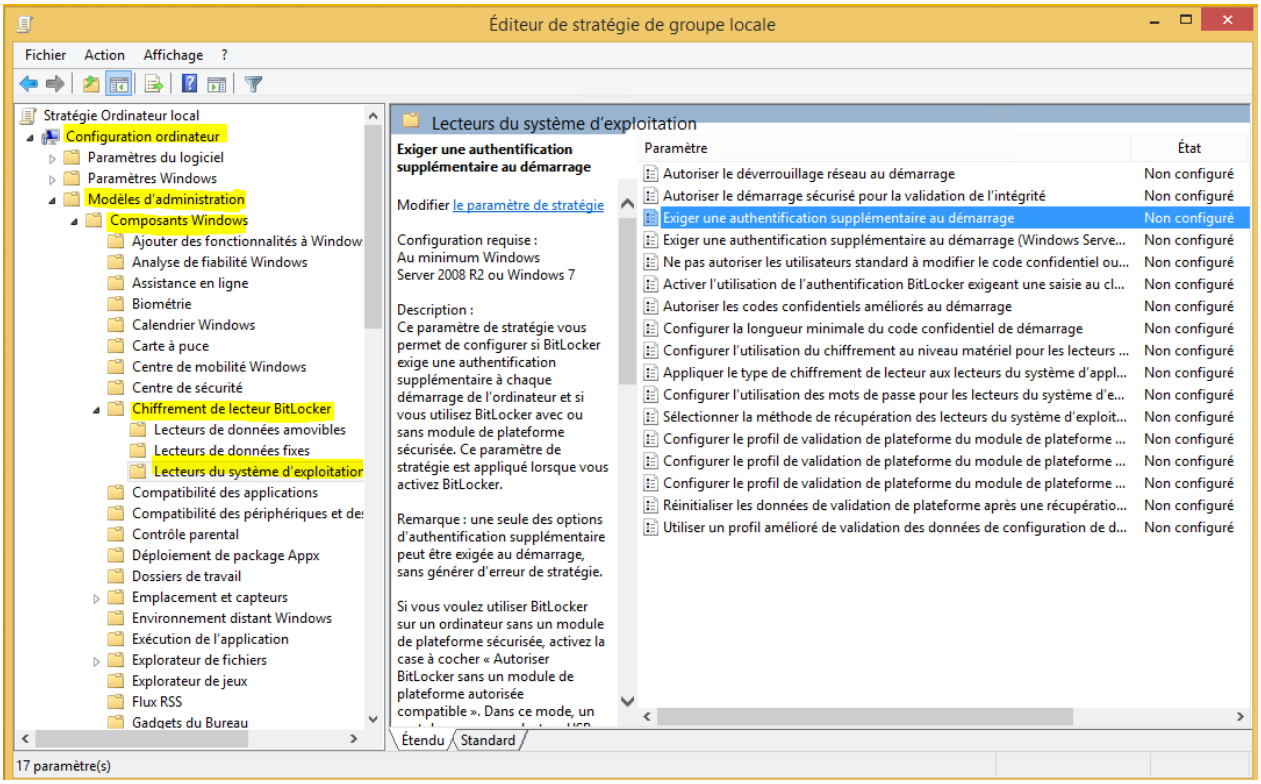
Le problème à ce niveau, c'est que le système se déchiffre automatiquement au démarrage de la machine via la puce TPM.

Il faut donc augmenter la sécurité en demandant à l'utilisateur de saisir un code PIN au démarrage du PC

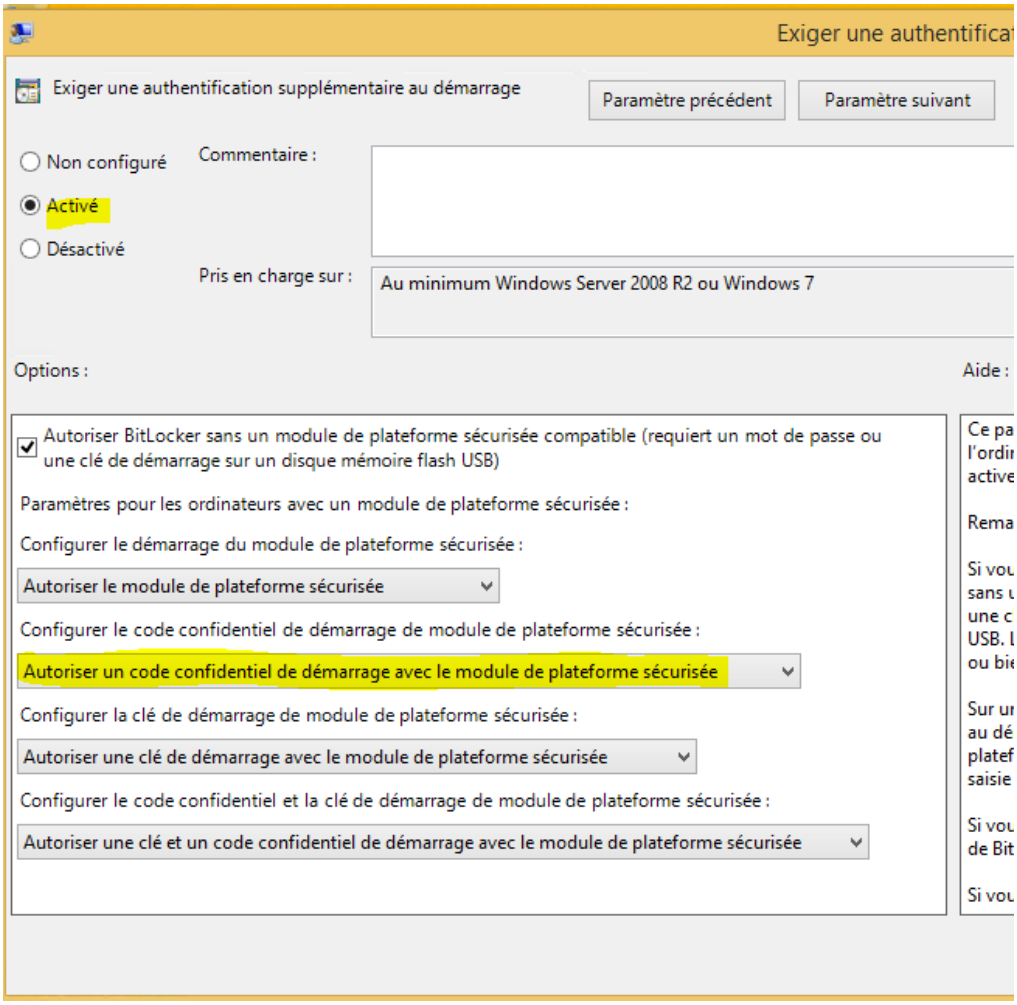
Exécutons la commande gpedit.msc

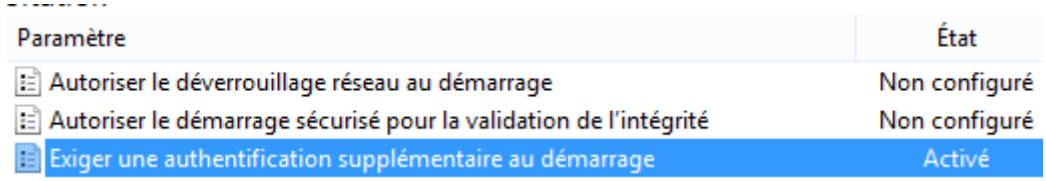


Il faut changer la stratégie « Exiger une authentification supplémentaire au démarrage » située dans « Configuration ordinateur/Modèles d'administration/Composants Windows/Chiffrement de lecteur Bitlocker/ Lecteurs du système d'exploitation »



Il faut activer cette stratégie et autoriser un code confidentiel de démarrage avec TPM





On initialise le code PIN en utilisant la commande suivante

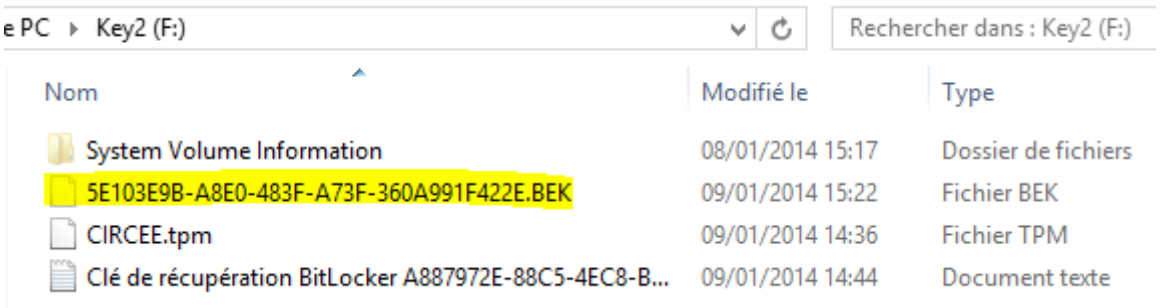
```
Microsoft Windows [version 6.3.9600]
(c) 2013 Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>manage-bde -protectors -add c: -TPMAndPIN 1234567890
Chiffrement de lecteur BitLocker : outil de configuration version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Protecteurs de clés ajoutés :

    TPM And PIN :
      ID : {2C9068E8-73CD-49C4-BA7B-BF8342039ADC}
      Profil de validation PCR :
        0, 2, 4, 8, 9, 10, 11

Le protecteur de clé avec l'ID "{14625799-58A7-4B14-8DEA-2DF0D3CFDA2E}" a été su
pprimé.

C:\Windows\system32>_
```

Le code PIN doit contenir entre 4 et 20 chiffres

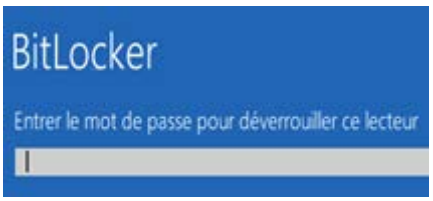
On génère ensuite un fichier de recouvrement sur une clé USB (lecteur F :)

```
C:\Windows\system32>manage-bde -protectors -add c: -RecoveryKey F:
Chiffrement de lecteur BitLocker : outil de configuration version 6.3.9600
Copyright (C) 2013 Microsoft Corporation. Tous droits réservés.

Protecteurs de clés ajoutés :

    Enregistré dans le répertoire F:

    Clé externe :
      ID : {5E103E9B-A8E0-483F-A73F-360A991F422E}
      Nom de fichier de clé externe :
        5E103E9B-A8E0-483F-A73F-360A991F422E.BEK
```

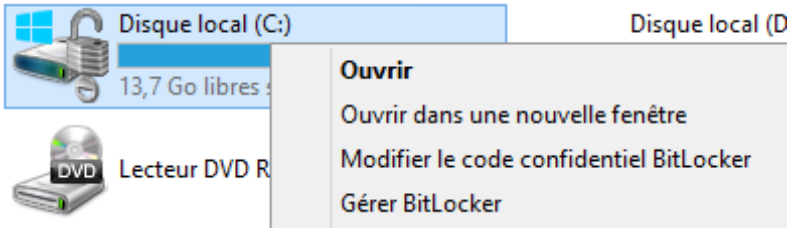
Pour voir ce fichier (extension .BEK), il faut afficher les fichiers caché du système. Il ne faut pas renommer ce fichier.

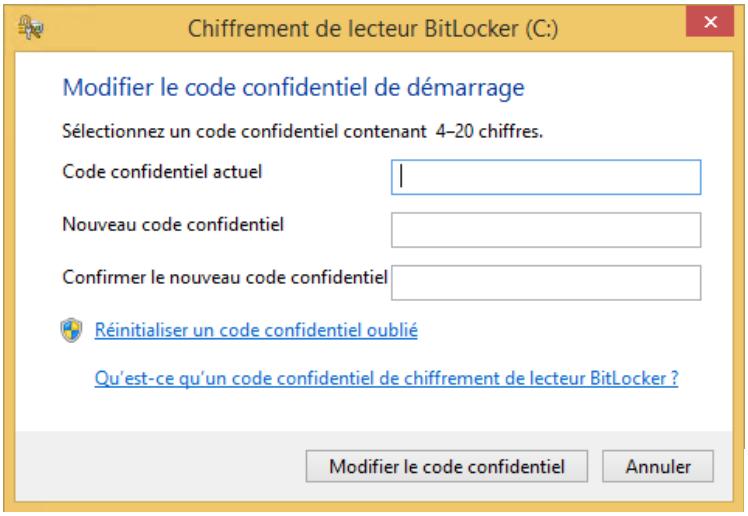


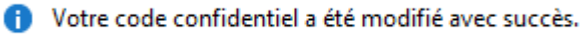
A chaque démarrage/redémarrage du PC, il faut saisir le code PIN



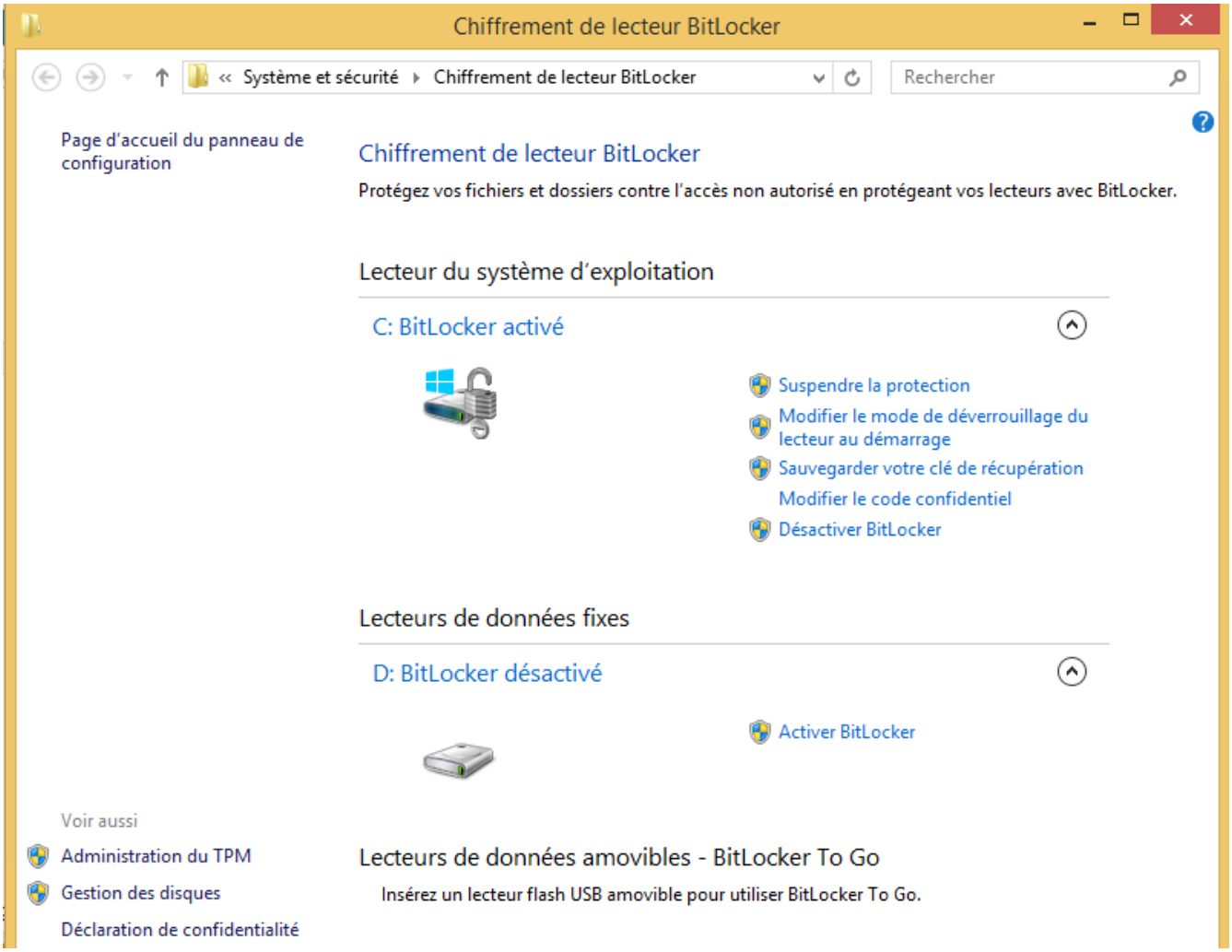
Voyons les options de gestion de bitlocker



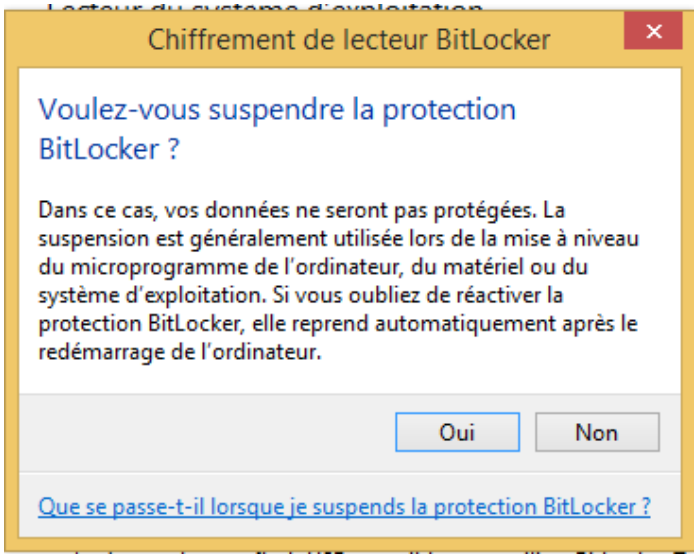




Voici les informations que l'on trouve dans le gestionnaire Bitlocker



Suspendre la protection

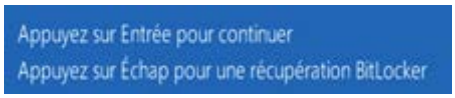


Sauvegarder la clé de récupération

Permet d'enregistrer à nouveau le fichier créé lors de l'activation de bitlocker pour ce lecteur

Recouvrement

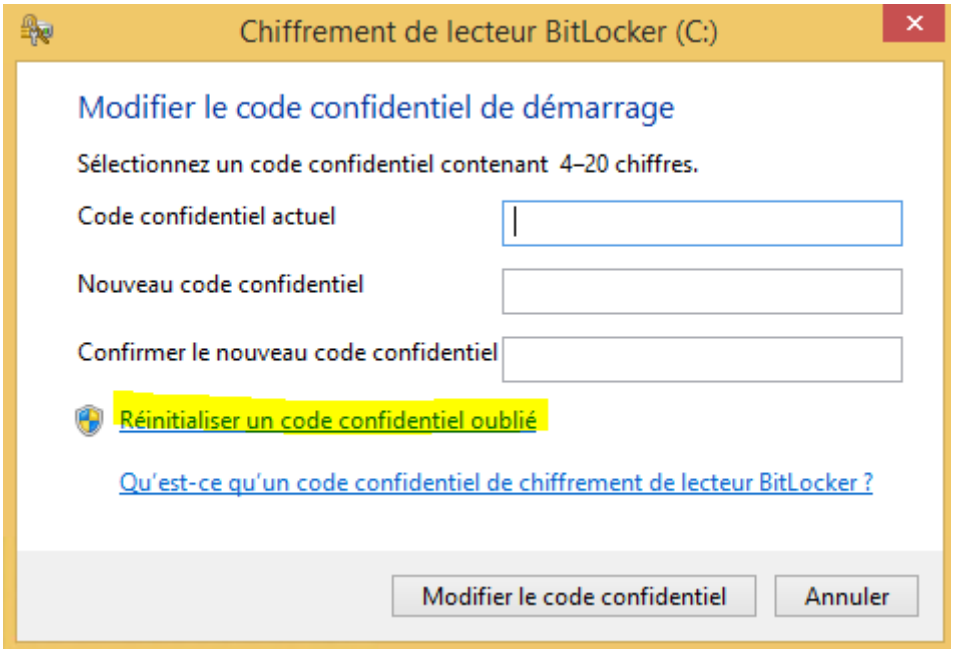
En cas de perte du code PIN, il faut appuyer sur la touche Echap

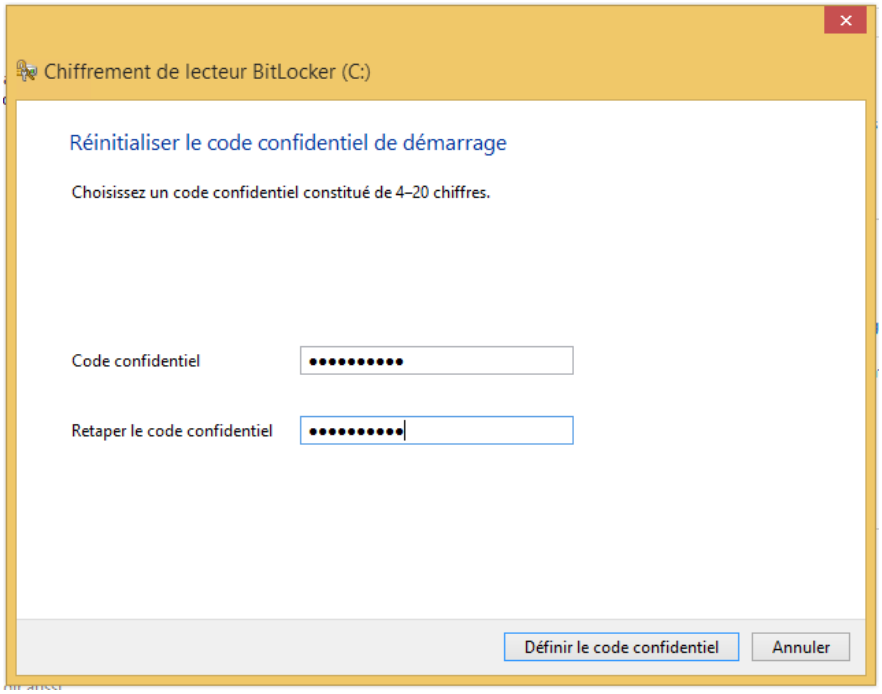


Il faut alors mettre la clé USB contenant le fichier BEK (à sa racine) et appuyer sur la touche « Entrée »

Le système va démarrer. Cela ne réinitialise pas le code PIN mais donne accès à la machine

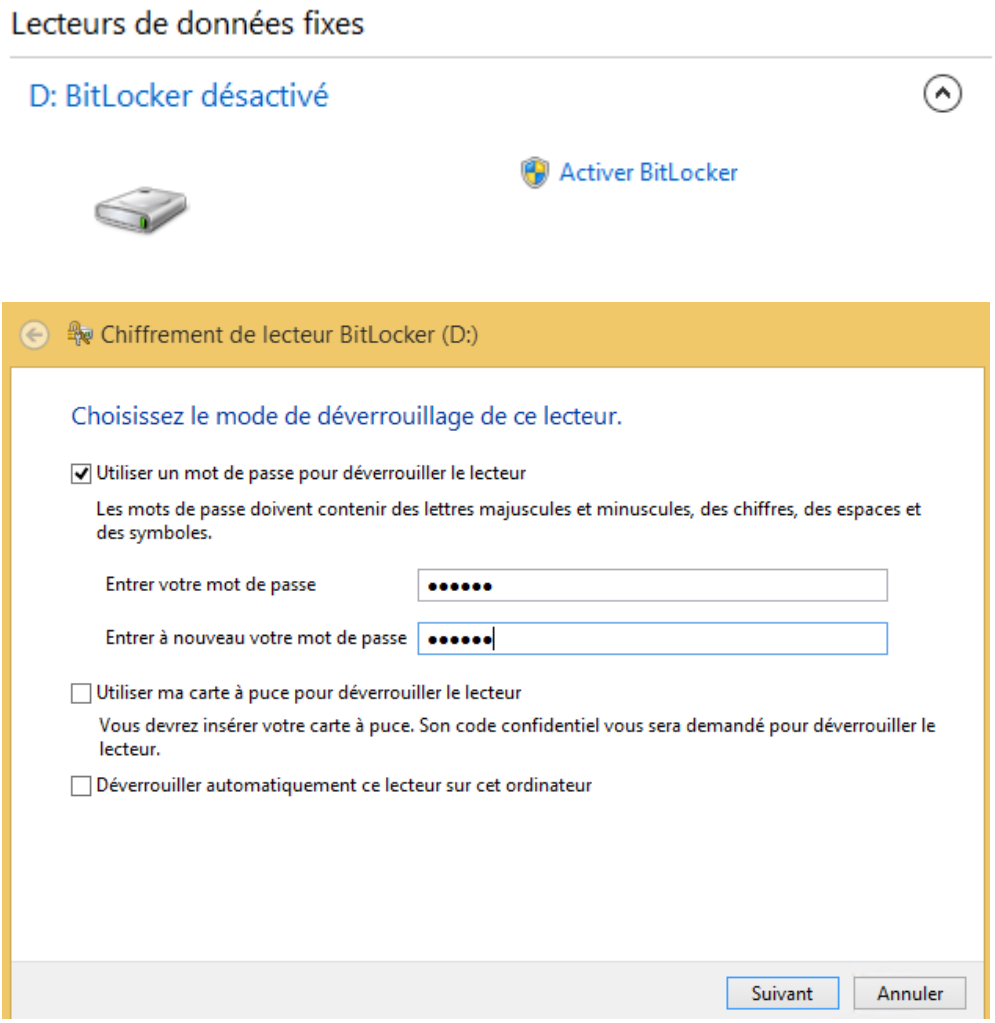
Il est alors possible de réinitialiser le code PIN

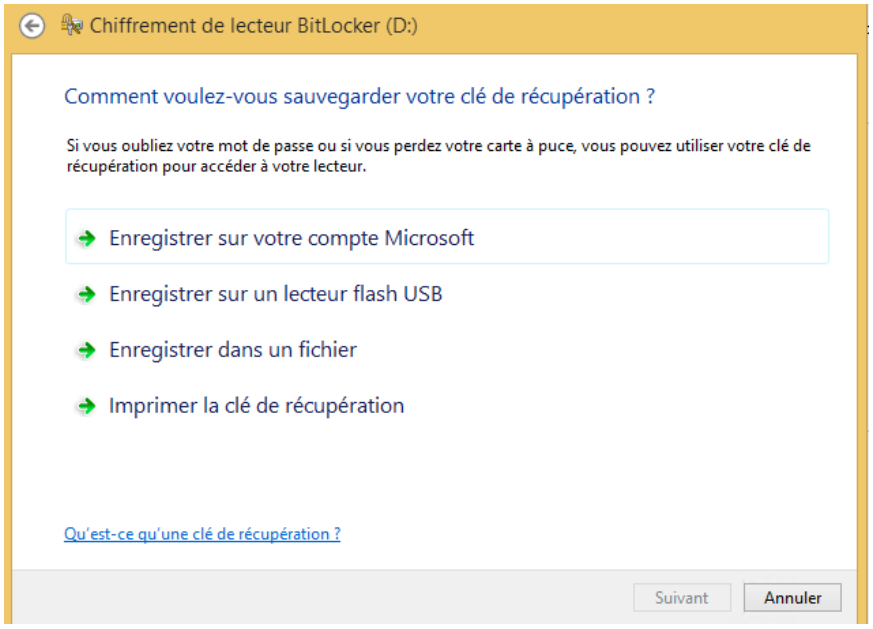


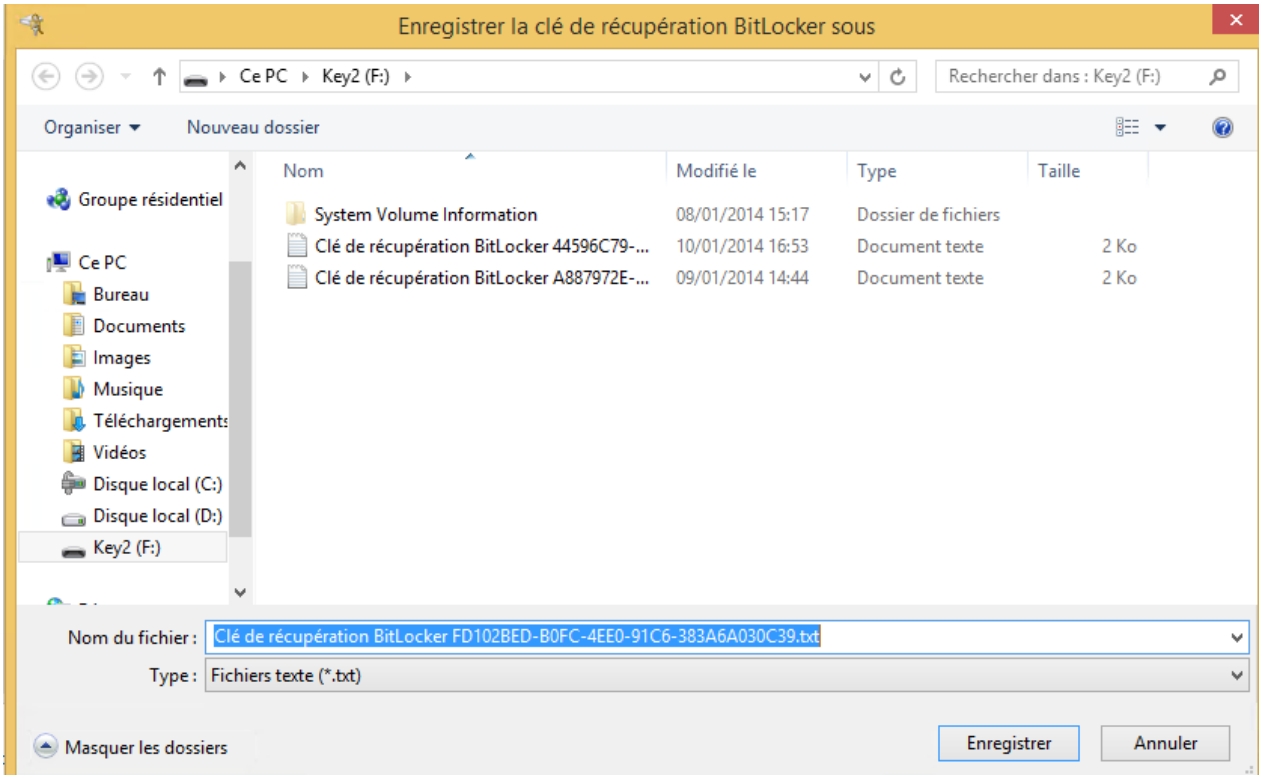


Activer bitlocker sur le lecteur D

La procédure est assez similaire à celle du lecteur système







Voici un exemple de ce type de fichier

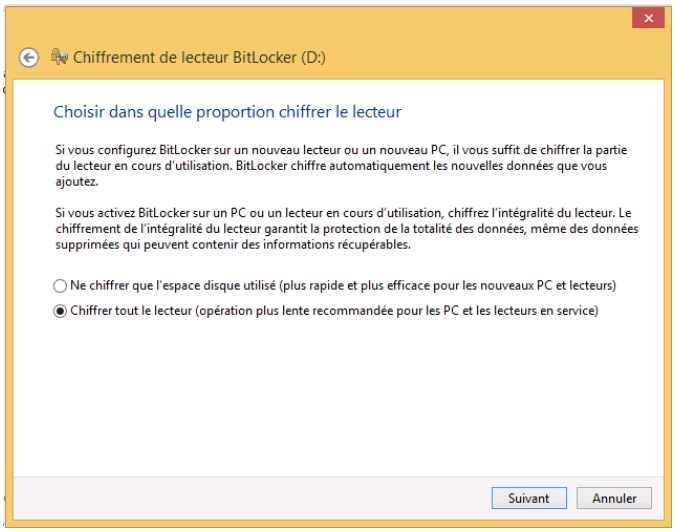
Clé de récupération du chiffrement de lecteur BitLocker
Pour vérifier qu'il s'agit de la clé de récupération appropriée, comparez le début de l'identificateur suivant avec la valeur d'identification affichée sur l'ordinateur.
Identificateur :

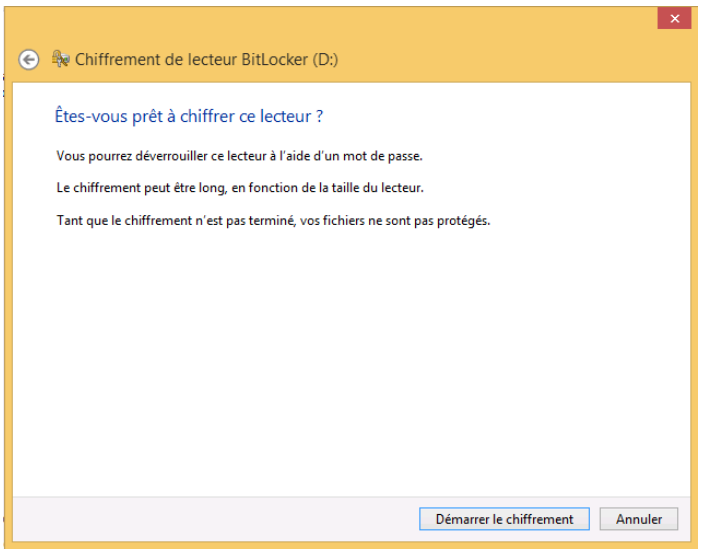
FD102BED-B0FC-4EE0-91C6-383A6A030C39

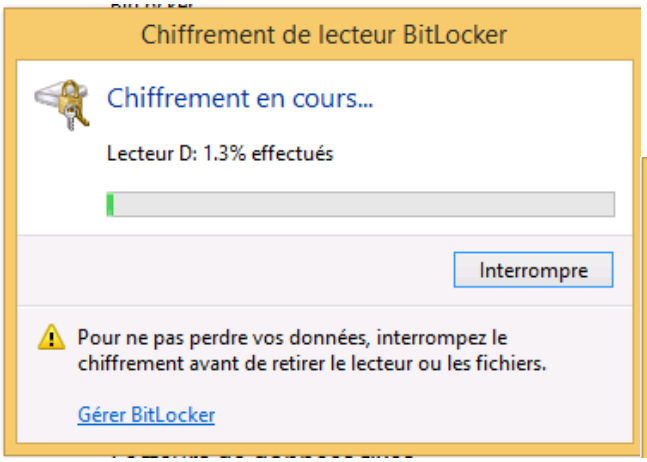
Si l'identificateur ci-dessus correspond à celui affiché sur l'ordinateur, utilisez la clé suivante pour déverrouiller le lecteur.
Clé de récupération :

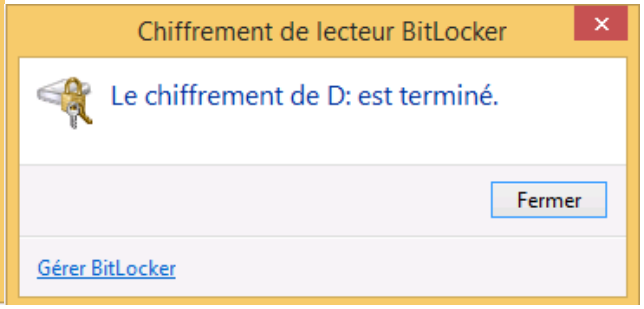
167497-397859-091300-409299-030217-489379-104544-467324

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 accédez à http://go.microsoft.com/fwlink/?LinkID=260589 pour obtenir une aide supplémentaire.



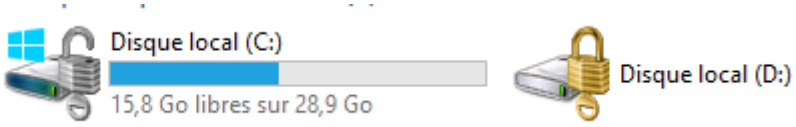




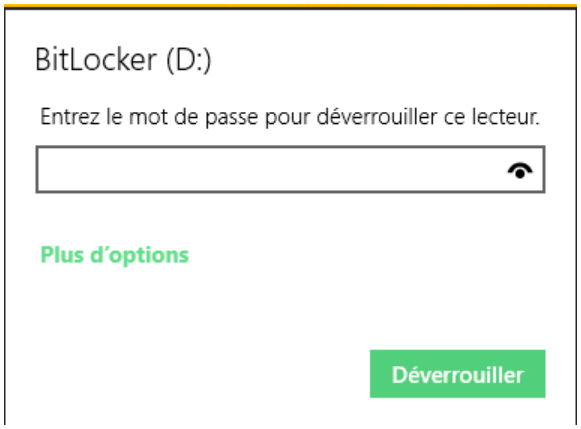


Au redémarrage du poste, il faut toujours saisir le mot de passe pour le lecteur système.

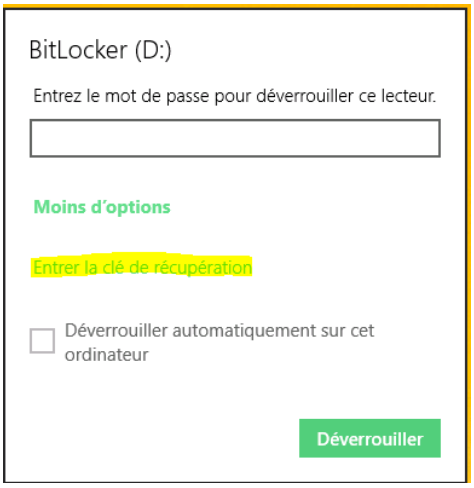
Le lecteur D reste chiffré

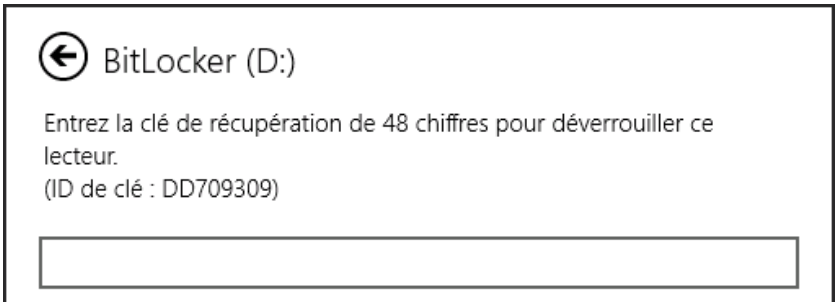


Quand on veut y accéder, il faut saisir le mot de passe



En affichant les options, on retrouve la possibilité de saisir la clé de récupération (il suffit de saisir le code de 48 chiffres pour acceder au lecteur et modifier le mot de passe)

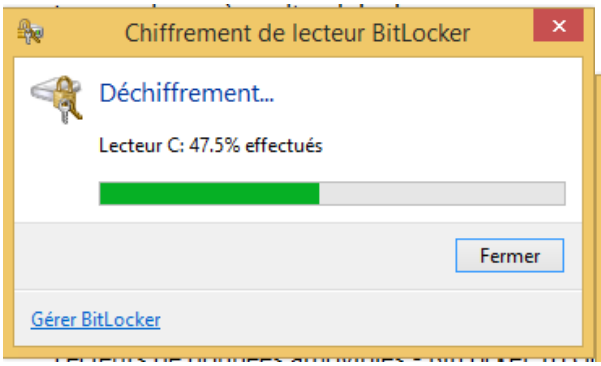


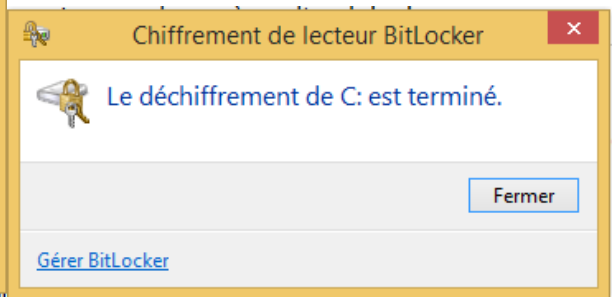


Dans le gestionnaire de bitlocker, on trouve une option « Activation du déverrouillage automatique »

Si on active cette option, le lecteur est automatiquement déverrouillé (sans mot de passe) lors du démarrage de la machine.

Désactivation de bitlocker :

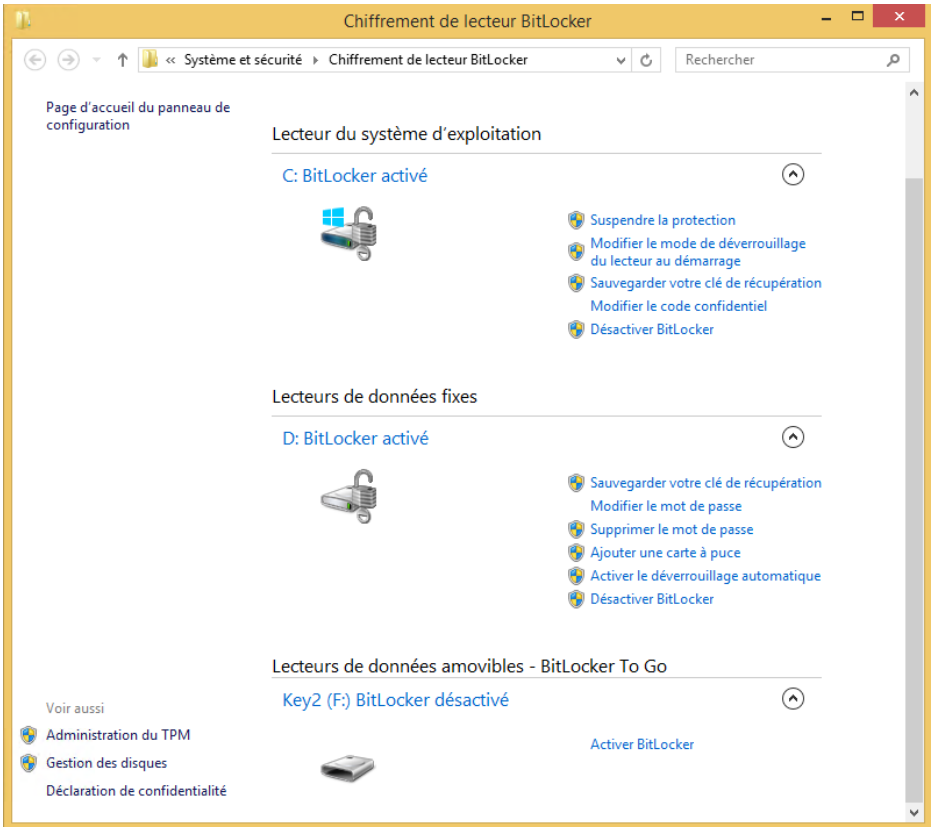




Tests avec un utilisateur non administrateur :

Par défaut, il peut modifier les mots de passe, mais ne peux pas désactiver bitlocker sur les lecteurs fixes.

Par contre, il peut faire ce qu'il veut sur les lecteurs amovibles



Tests non réalisés :

Intégration avec AD