Chiffrement du disque système Windows à l'aide de Bitlocker.

L'objectif de ce document est de décrire étape par étape la méthode de chiffrement d'un système d'exploitation Windows 10 à l'aide du logiciel BITLOCKER

Postulat de départ : le chiffrement du disque système doit être réalisé uniquement par l'administrateur système et réseau du laboratoire, ceci dans un objectif de gestion pertinente des clefs de recouvrement.

Installez le logiciel ou demandez à l'administrateur de votre machine de le faire.

TPM ou pas ?

La plupart des machines récentes sont équipées d'une puce TPM (Trusted Platform Module). Celle-ci prend en charge le stockage de la clef de chiffrement du disque.

Par défaut, sous Windows 10, Bitlocker est configuré pour utiliser la puce TPM.

Or, vous pouvez être amené à intervenir sur des machines non munies de cette puce ou sur lesquelles elle a été désactivée.

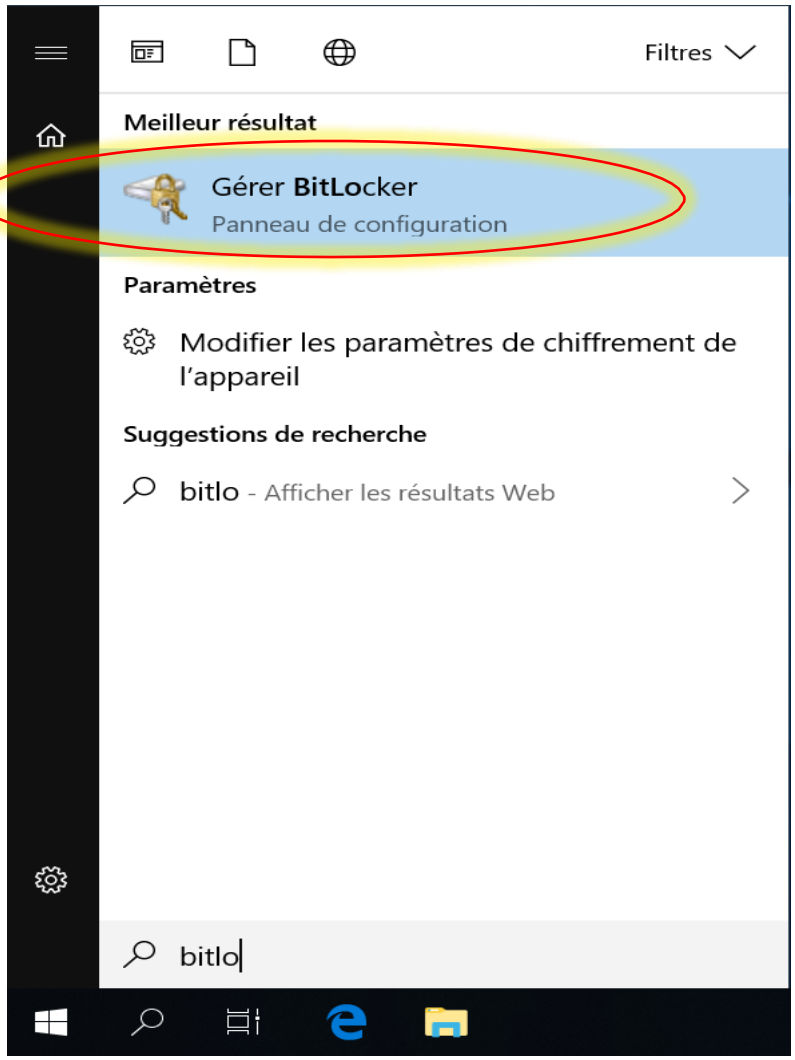
Les étapes ci-dessous décrivent la configuration d'une machine avec et sans TPM.

Chiffrement avec puce TPM.

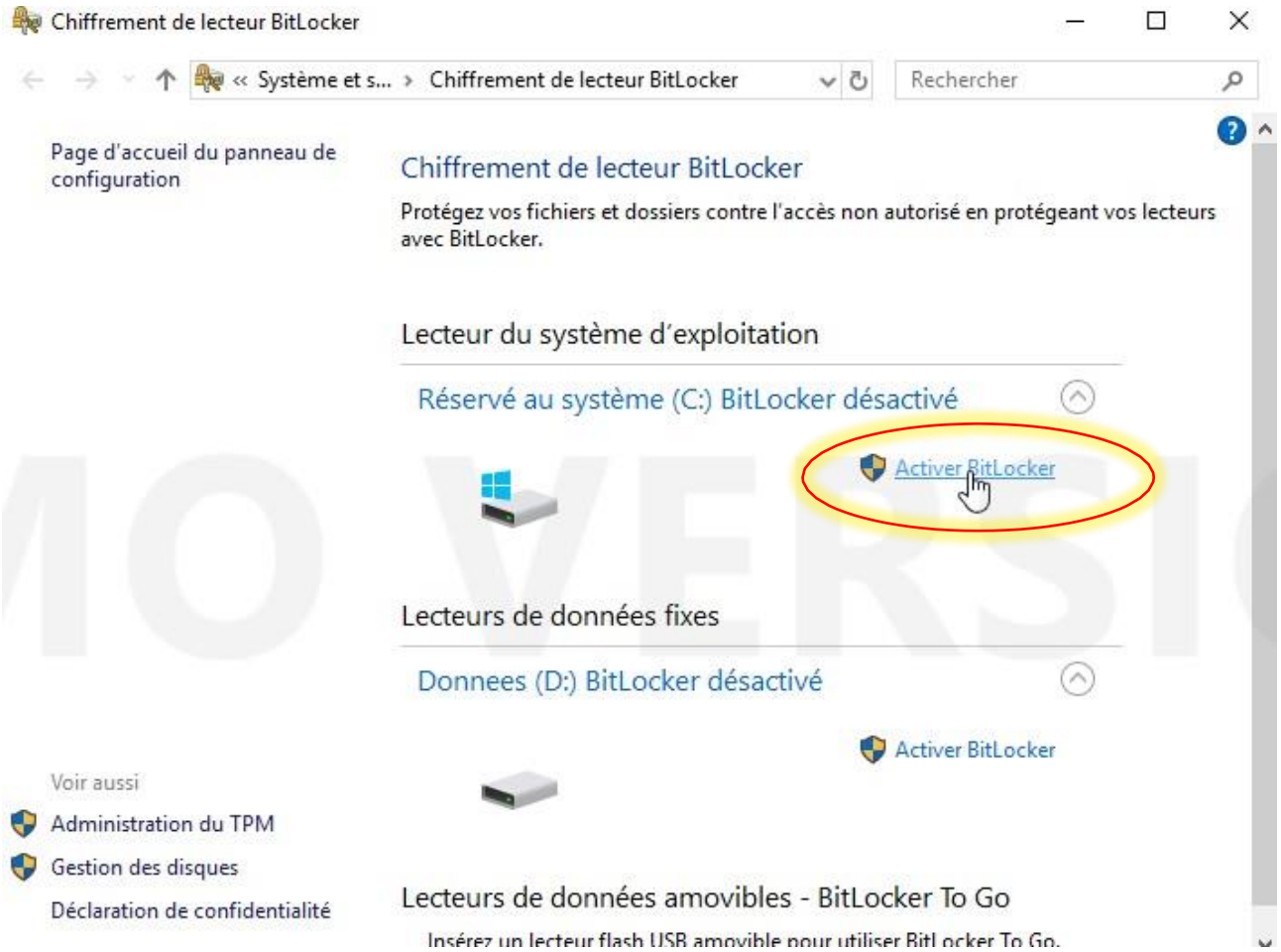
Etape 1 : Activation de Bitlocker et chiffrement du système d'exploitation.

Par défaut, Bitlocker est désactivé.
Il faut l'activer afin de pouvoir lancer le chiffrement de la machine.

1. Lancez l'outil de gestion de Bitlocker



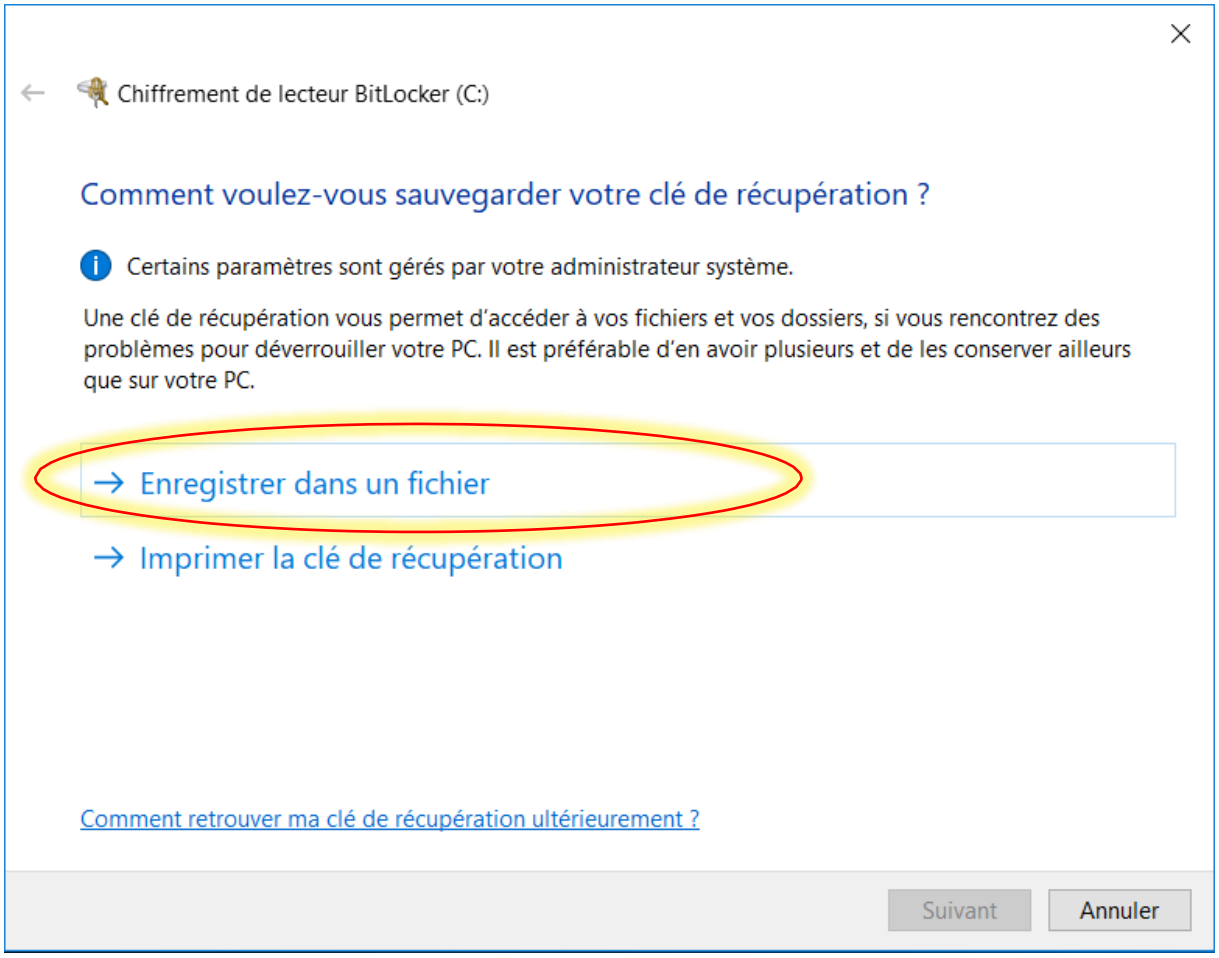
2. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer Bitlocker ».



ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

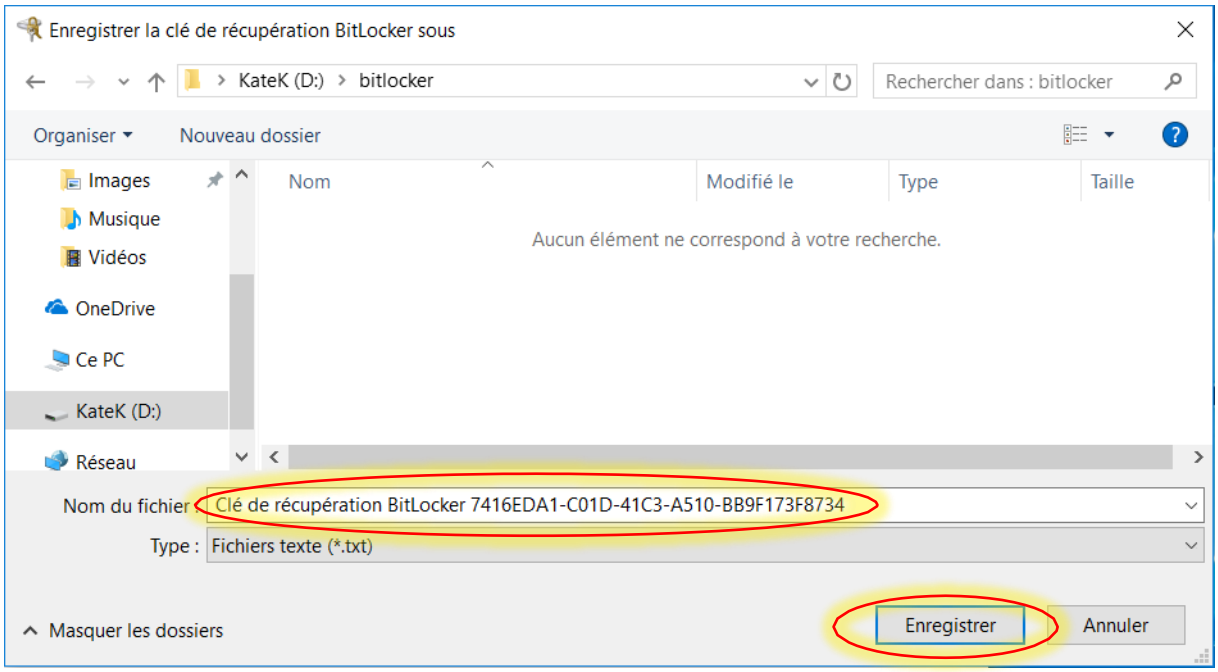
Concernant le chiffrement des périphériques de stockage « mobiles », un autre document décrit la marche à suivre.

3. Cliquez sur « Enregistrer dans un fichier ».

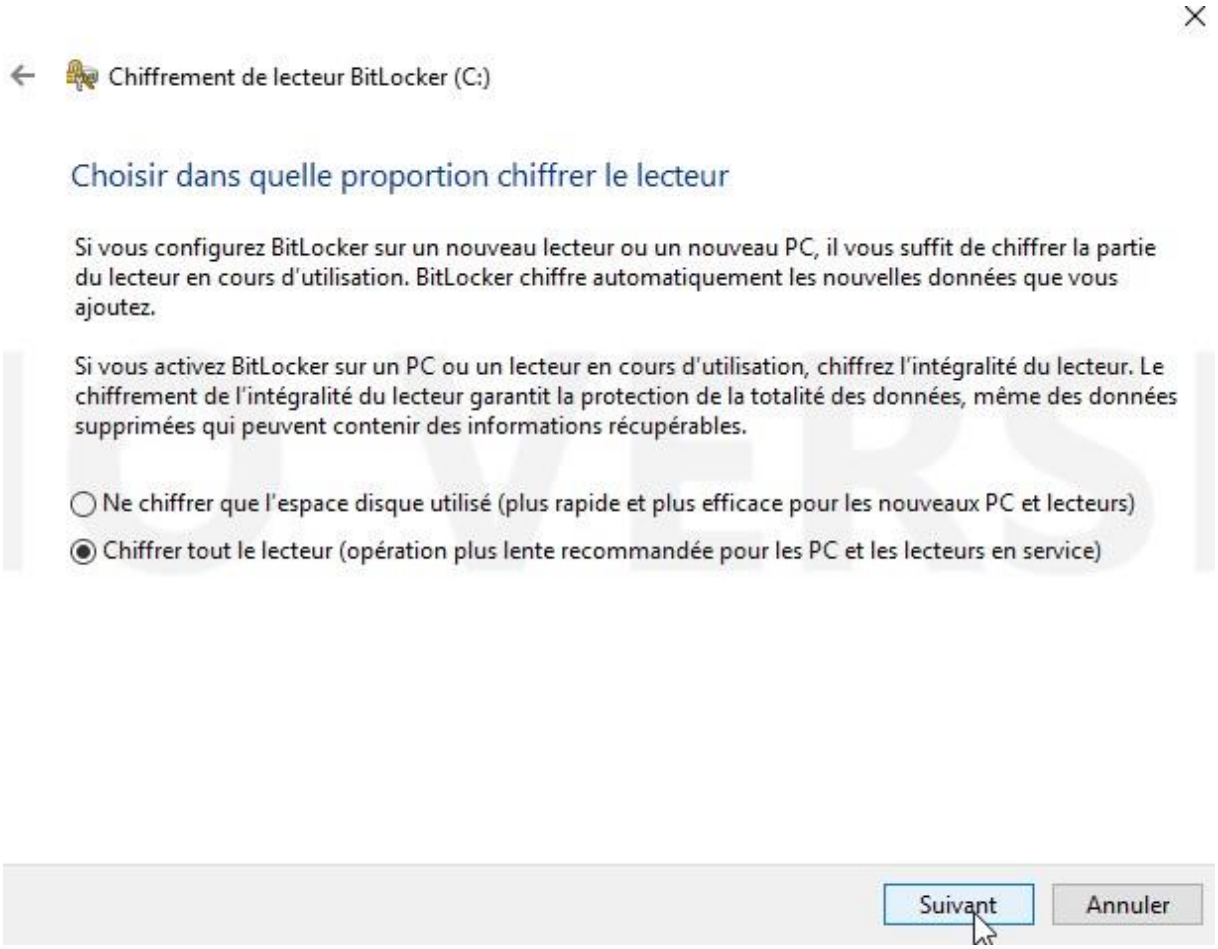


4. La mise en place de la clef de recouvrement est une étape importante. Cette clef doit être stockée dans un endroit sûr et accessible uniquement aux personnes autorisées.

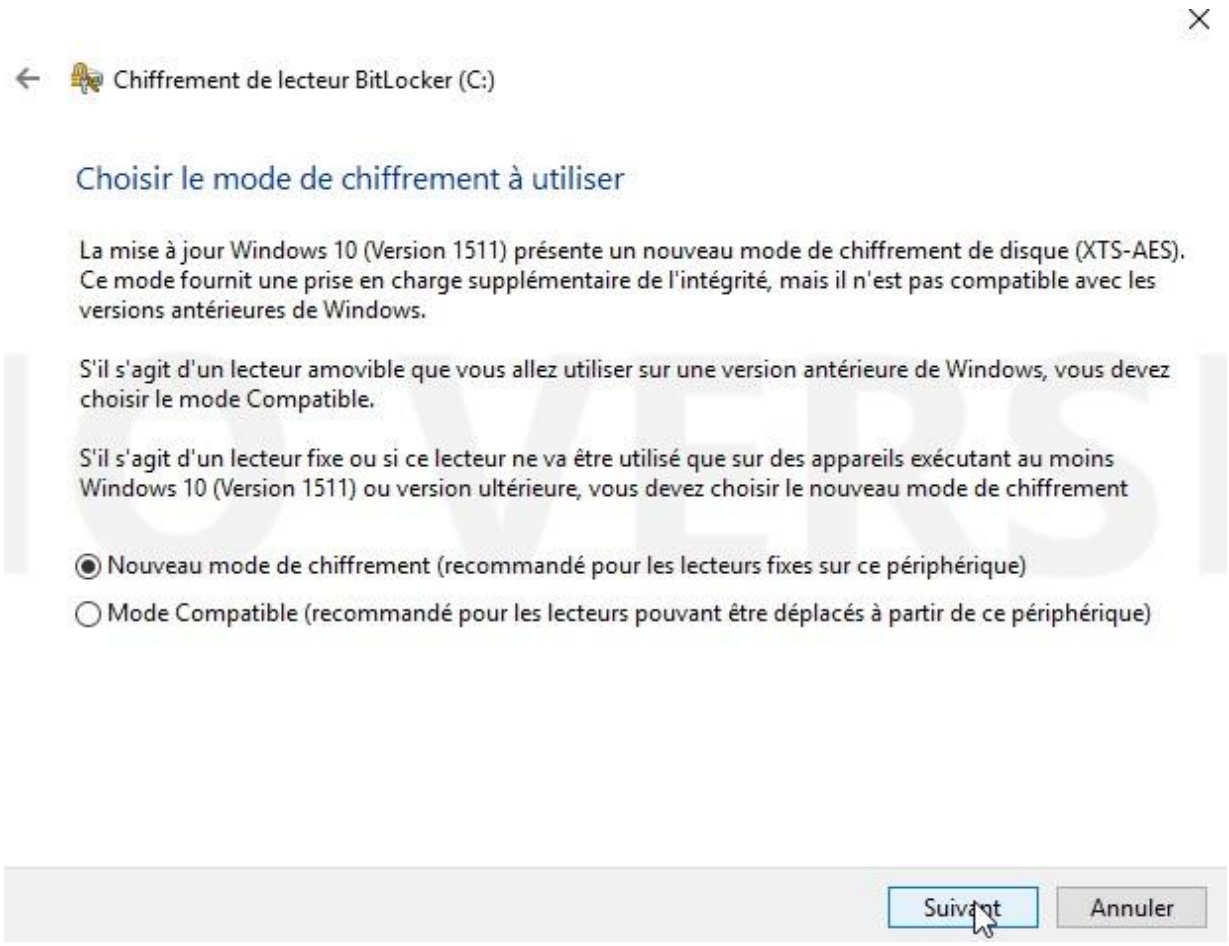
5. Bitlocker vous propose d'enregistrer cette clef au format « .txt ». Vous pouvez la stocker sur un périphérique de stockage mobile, mais il est recommandé de la stocker dans un gestionnaire de mot de passe, un logiciel type « coffre fort numérique » ou tout système de gestion de secret vous paraissant adapté à la protection de cette clef.



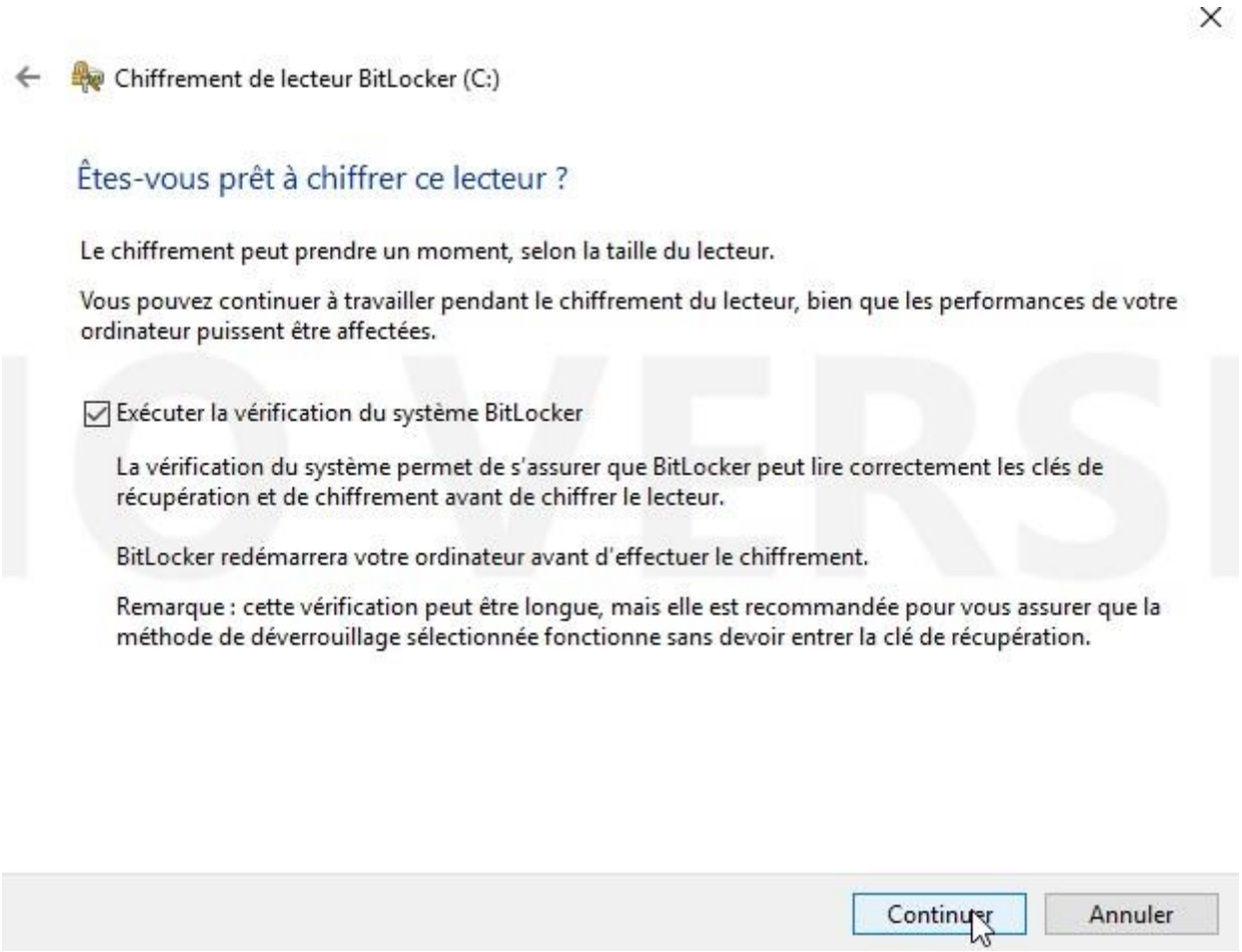
6. Cochez « chiffrer tout le lecteur » puis cliquez sur suivant



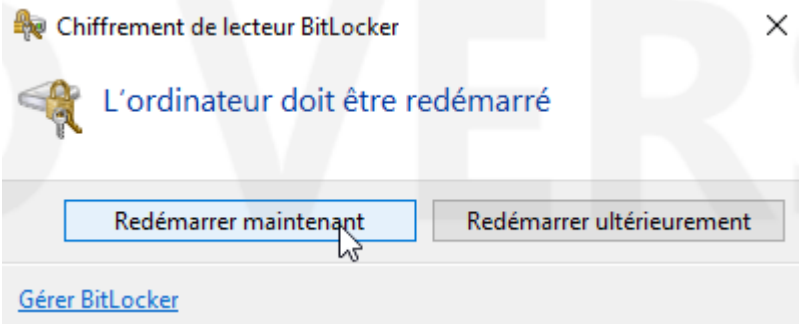
7. Cochez « nouveau mode de chiffrement » puis cliquez sur suivant



8. Cochez « Exécuter la vérification du système », puis cliquez sur « continuer »

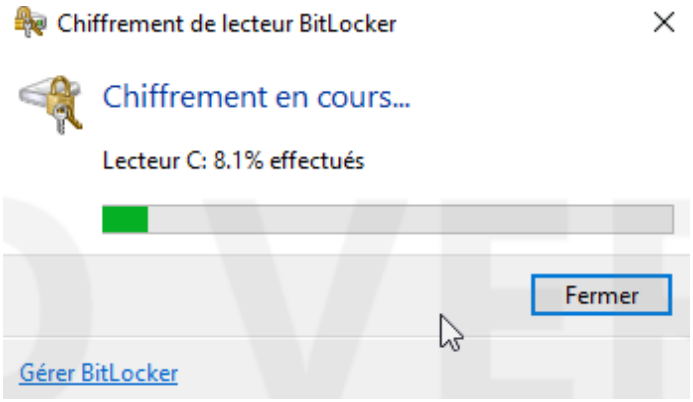


9. Redémarrez l'ordinateur



10. Au démarrage de la machine vous serez invité à saisir le code PIN que vous avez défini plus haut. Attention : à la saisie du code PIN, le clavier sera en QWERTY.

11. Pour connaitre l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icone cachée à droite de la barre des tâches.

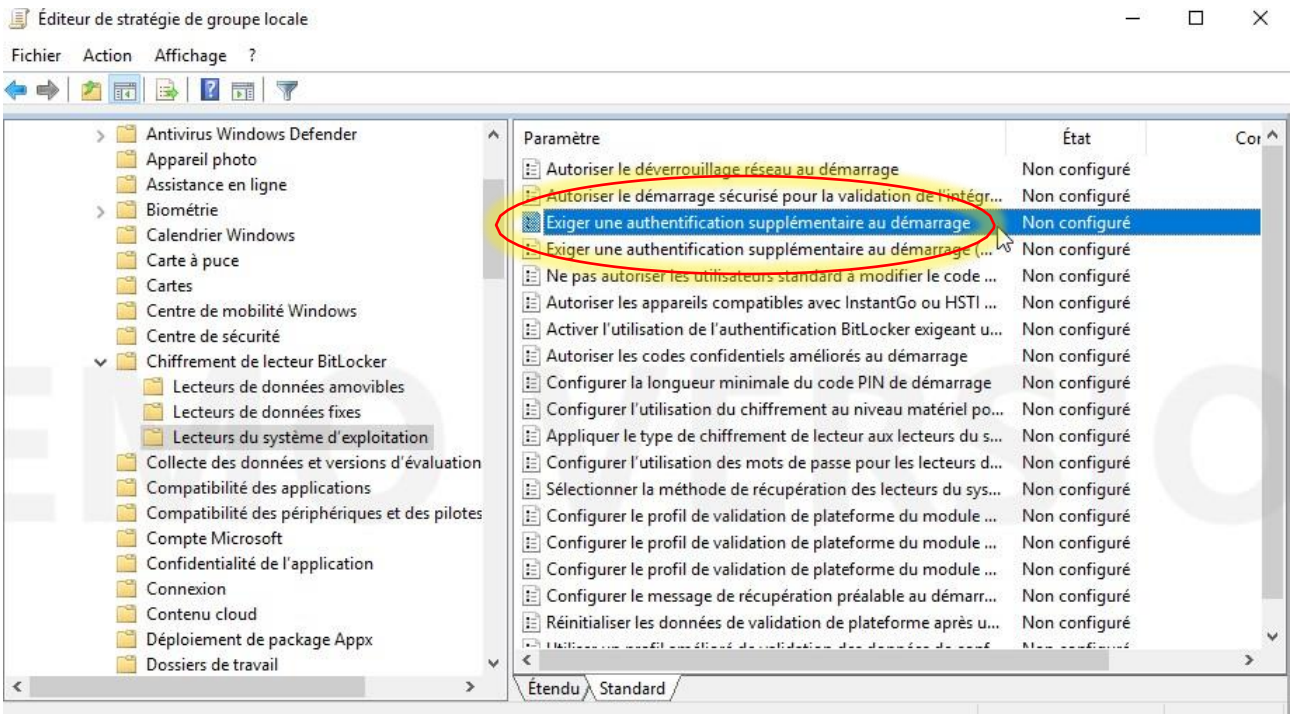


Chiffrement sans puce TPM ou puce TPM désactivée.

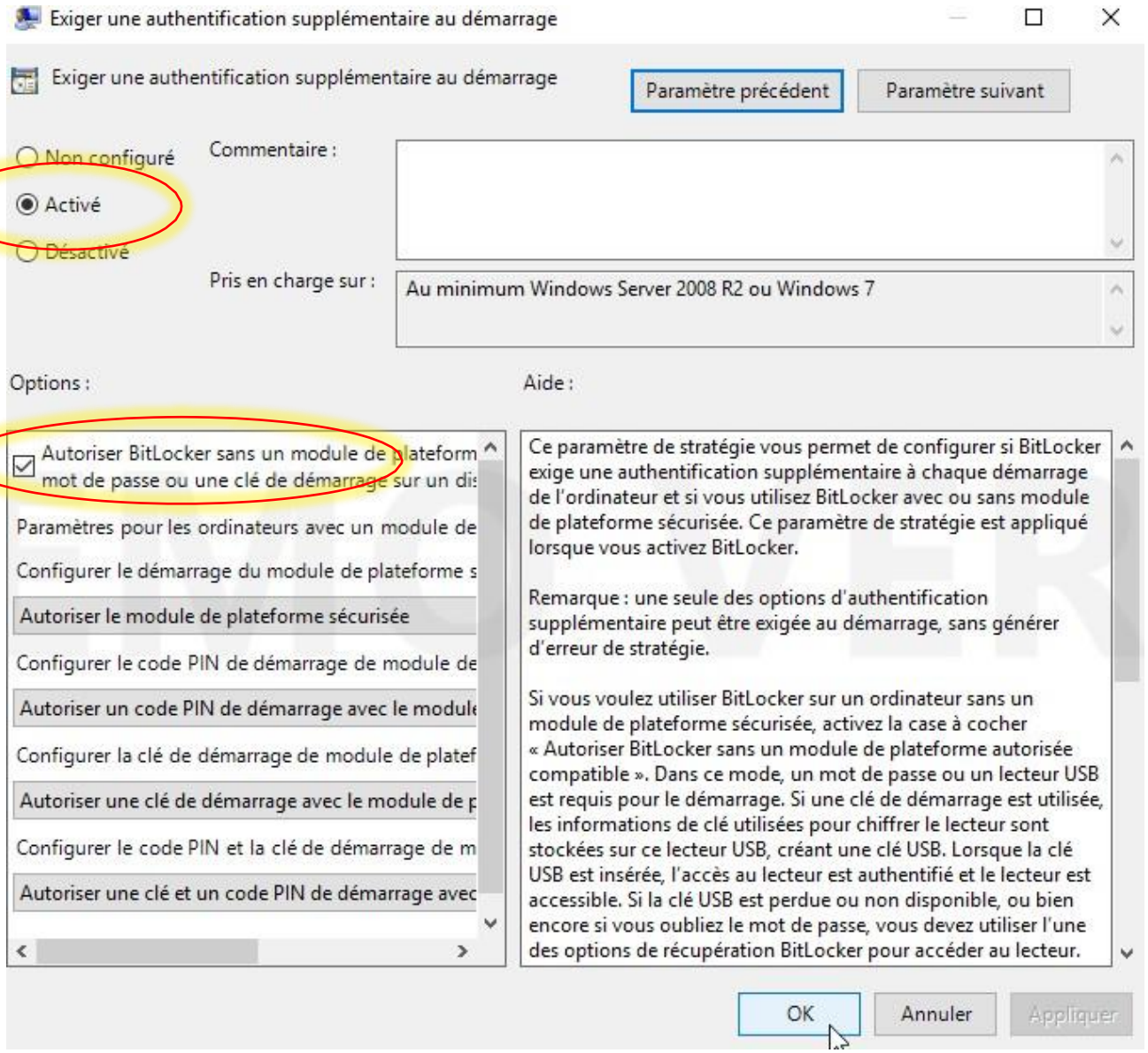
Etape 1 : autoriser Bitlocker à ne pas utiliser TPM

1. Lancez l'éditeur de stratégie de groupe « gpedit.msc »

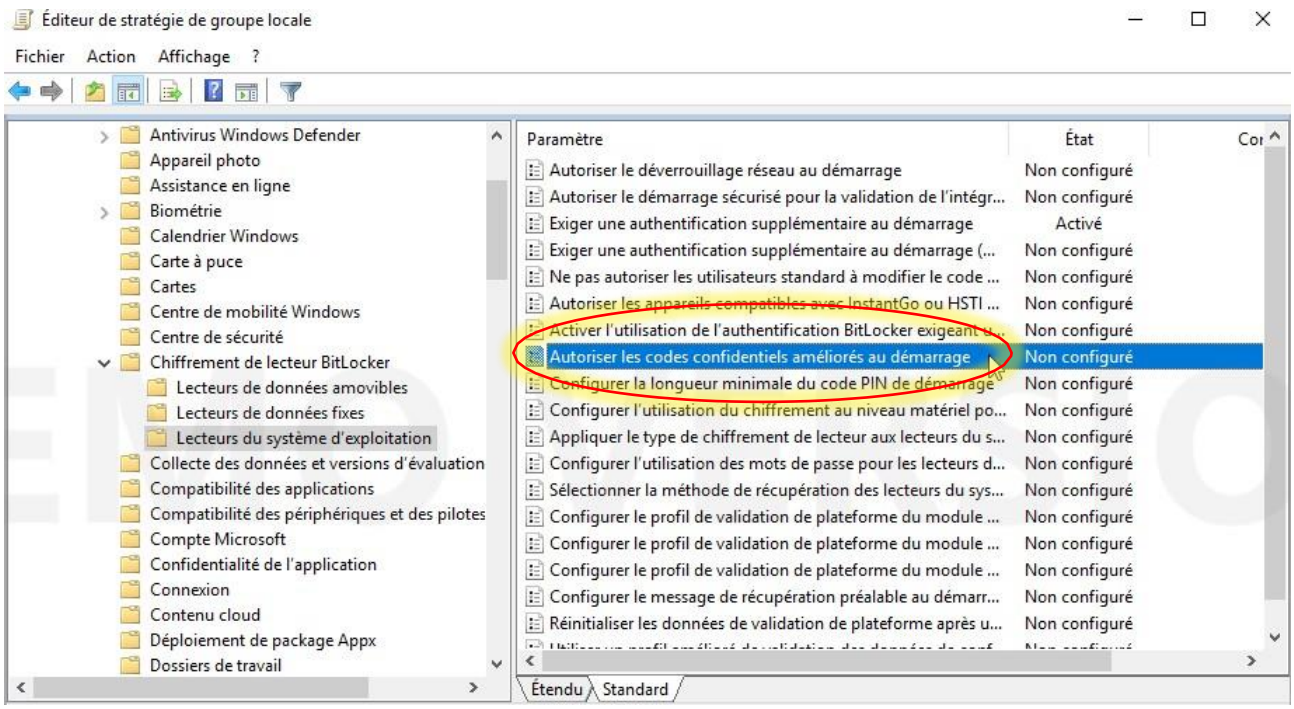
2. Placez-vous dans « Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs du système d'information », double-cliquez sur « **Exiger une authentification supplémentaire au démarrage** ».



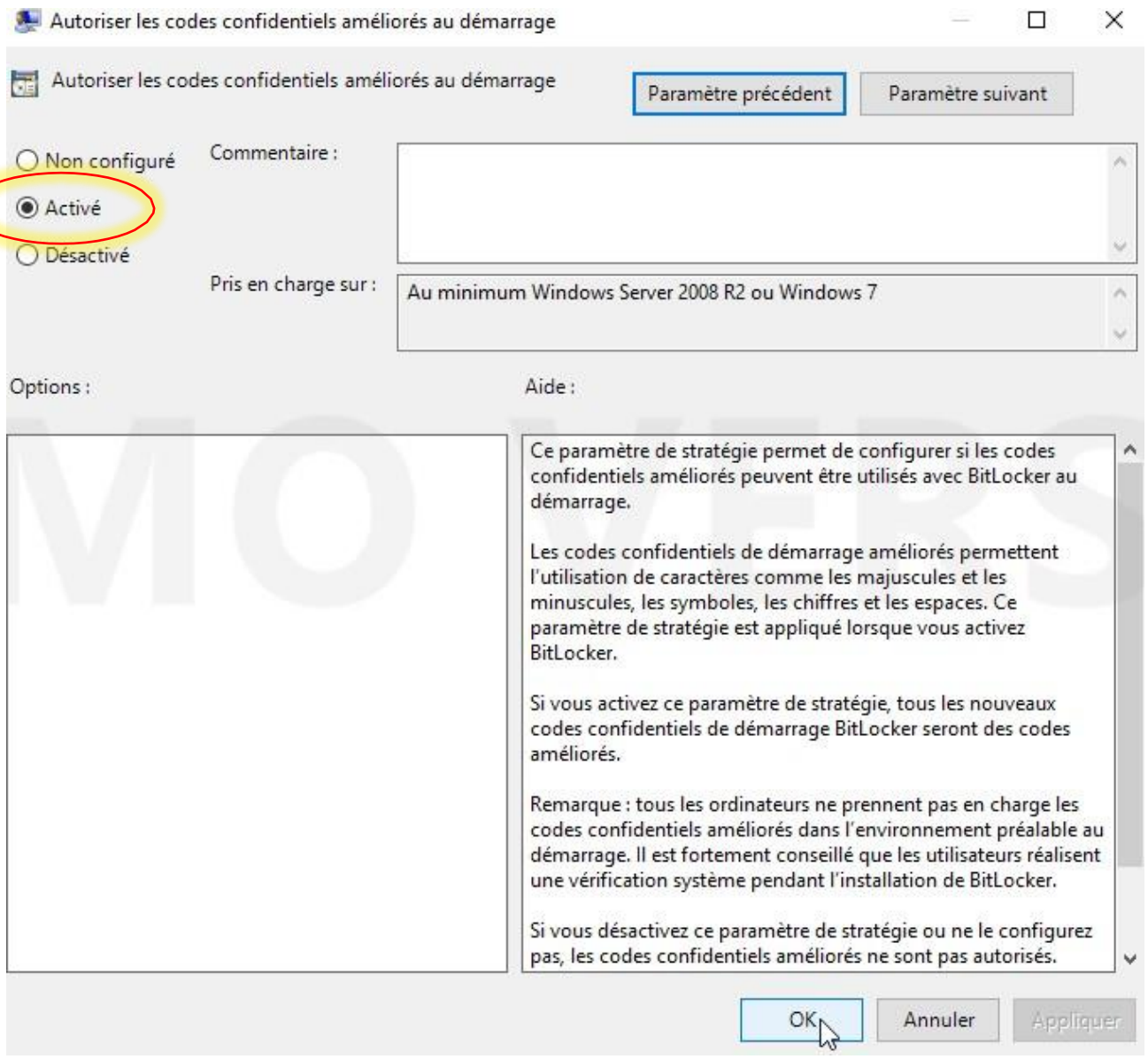
3. Cochez « Activé ».
4. Cochez la case « Autoriser Bitlocker sans un module de plateforme sécurisée compatible ».



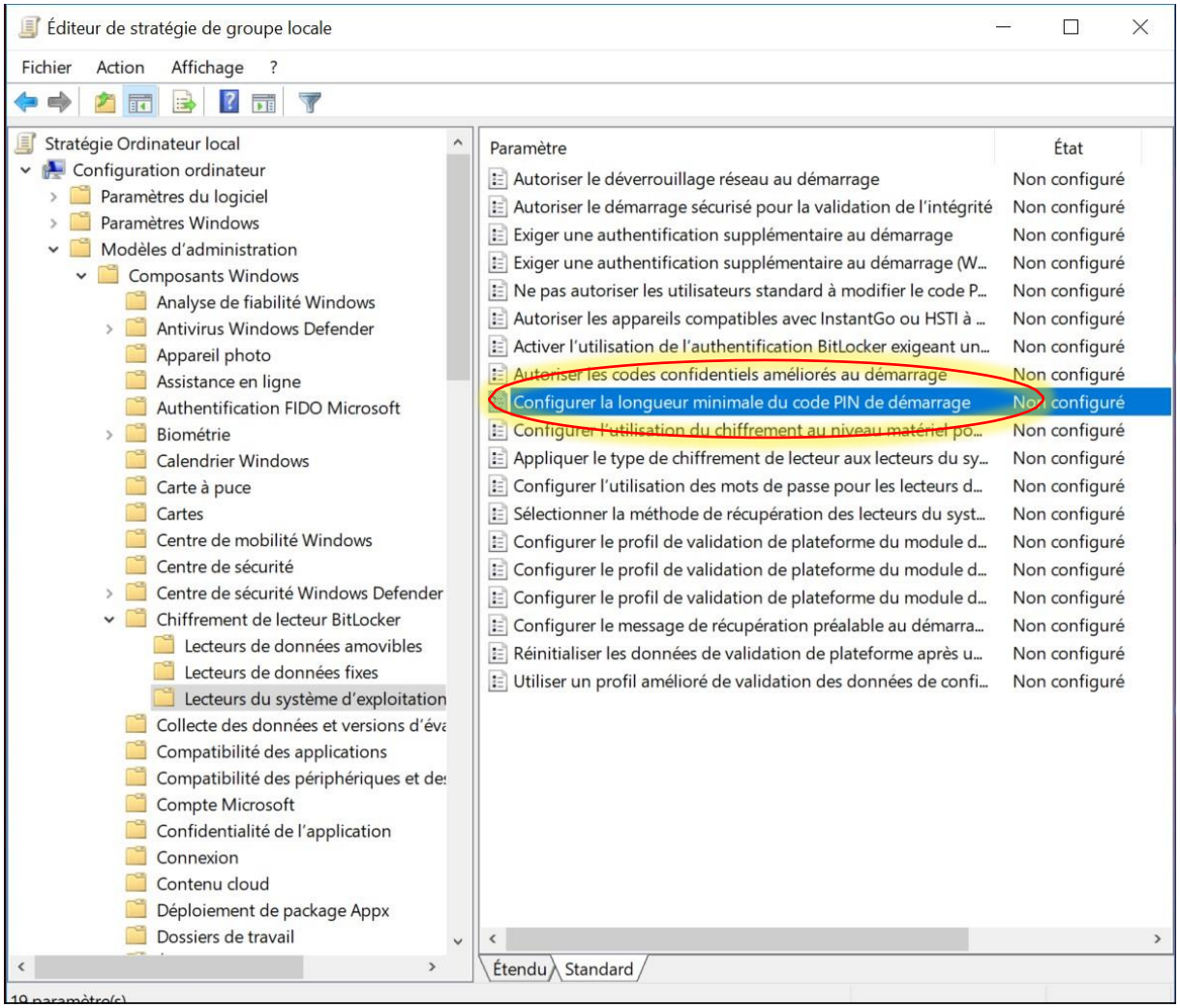
5. Double-cliquez sur « Autoriser les codes confidentiels améliorés au démarrage »



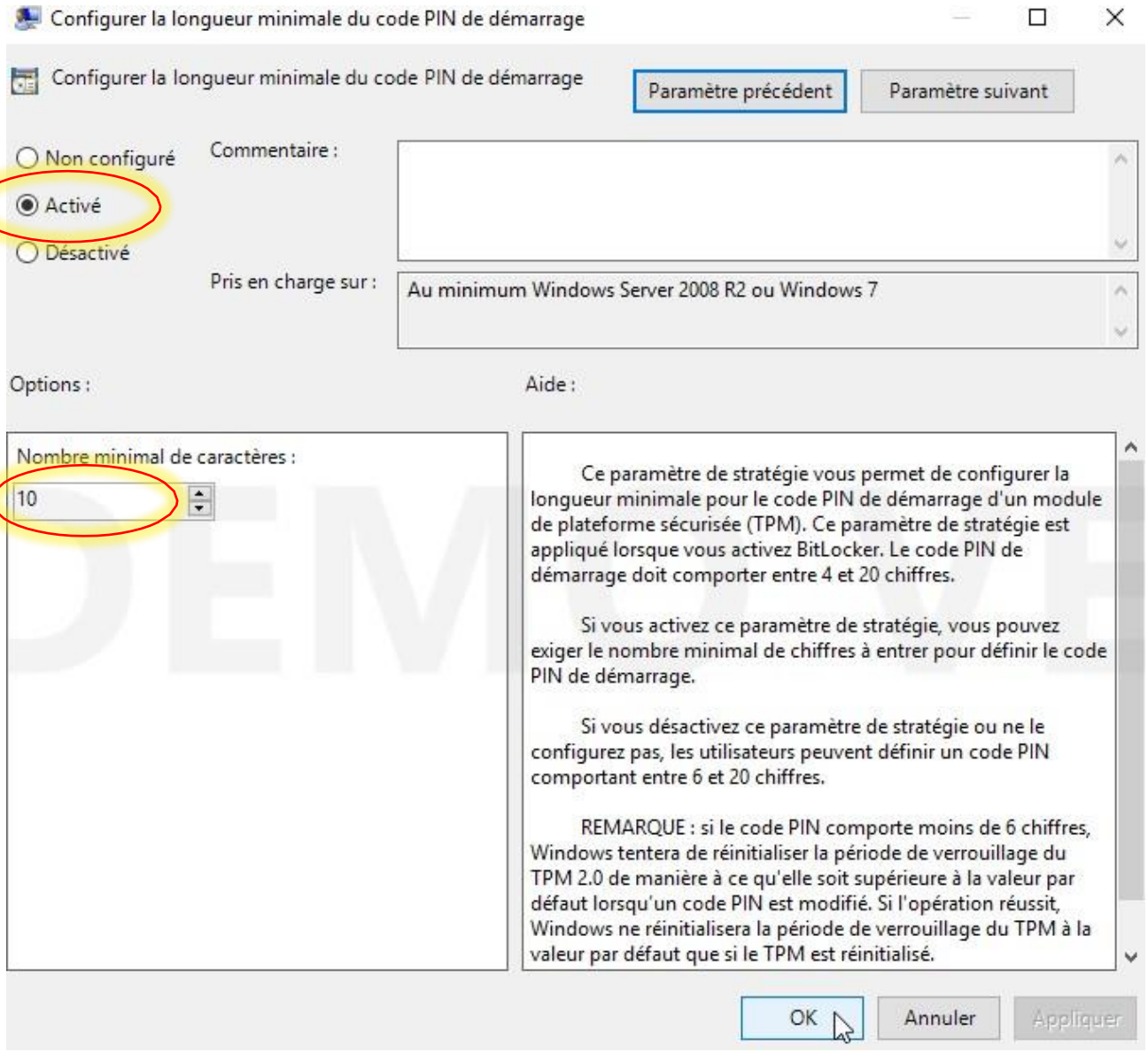
6. Cochez « Activé » puis validez en cliquant sur « OK »



7. Double-cliquez sur « Configurer la longueur minimale du code PIN de démarrage »



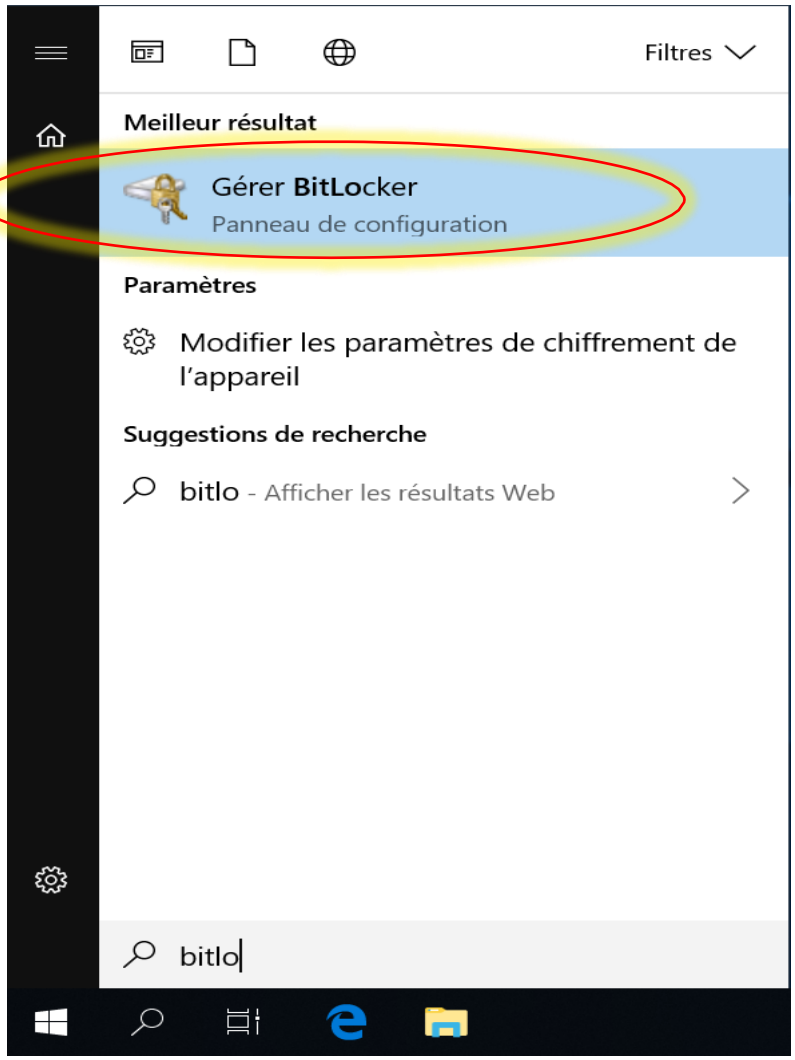
8. Cochez « Activé », fixez le nombre minimal de caractères à 10 puis validez en cliquant sur « OK »



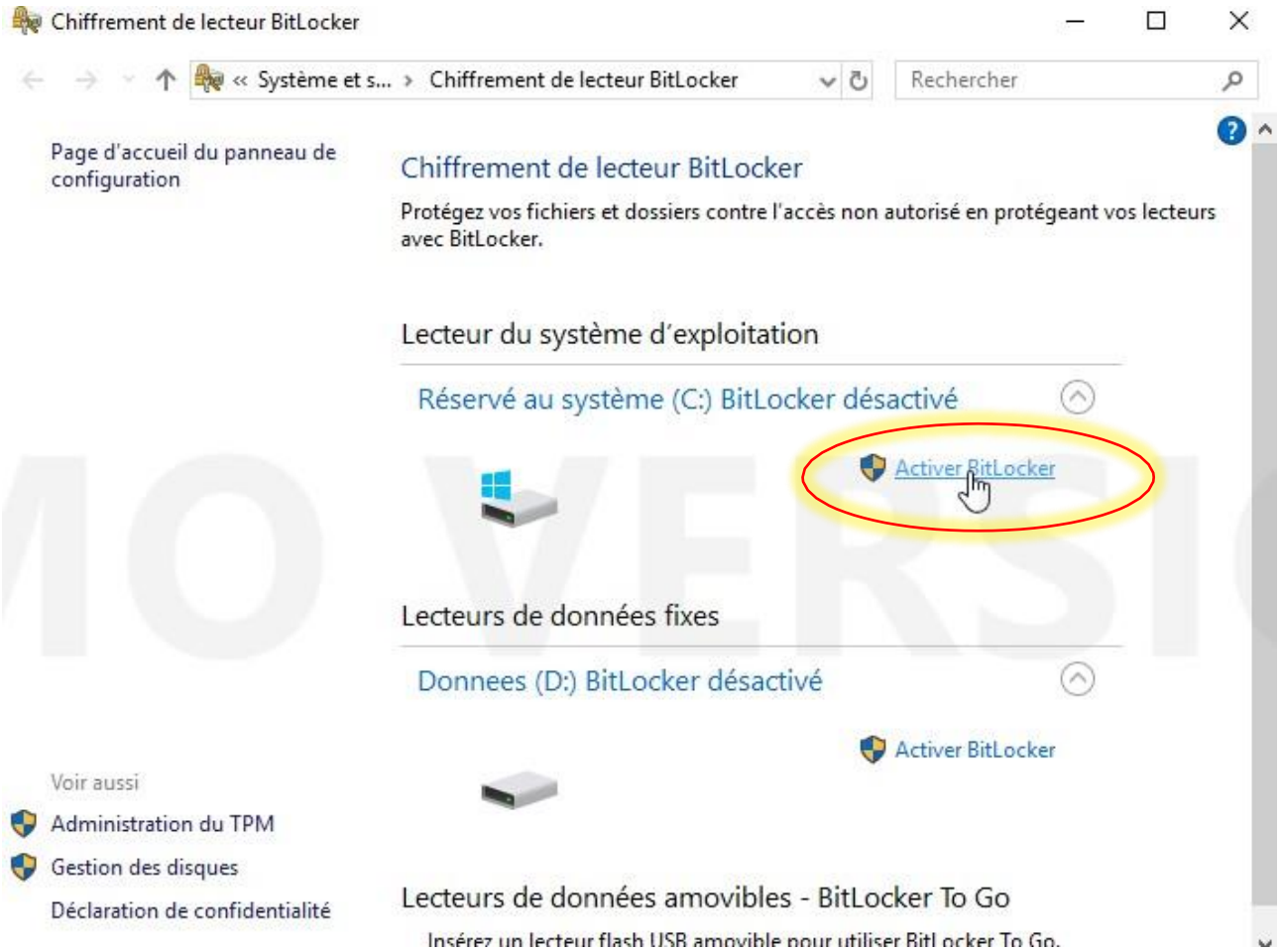
Etape 2 : Activation de Bitlocker et chiffrement du système d'exploitation.

Par défaut, Bitlocker est désactivé.
Il faut l'activer afin de pouvoir lancer le chiffrement de la machine.

12. Lancez l'outil de gestion de Bitlocker



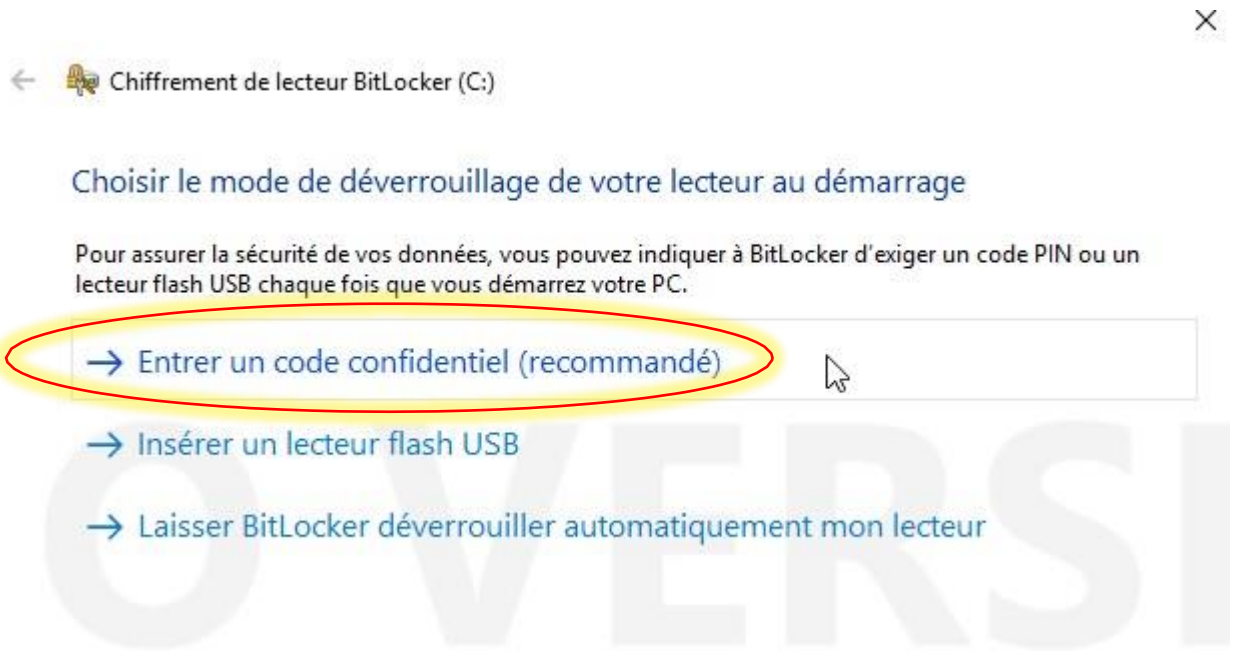
13. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer Bitlocker ».



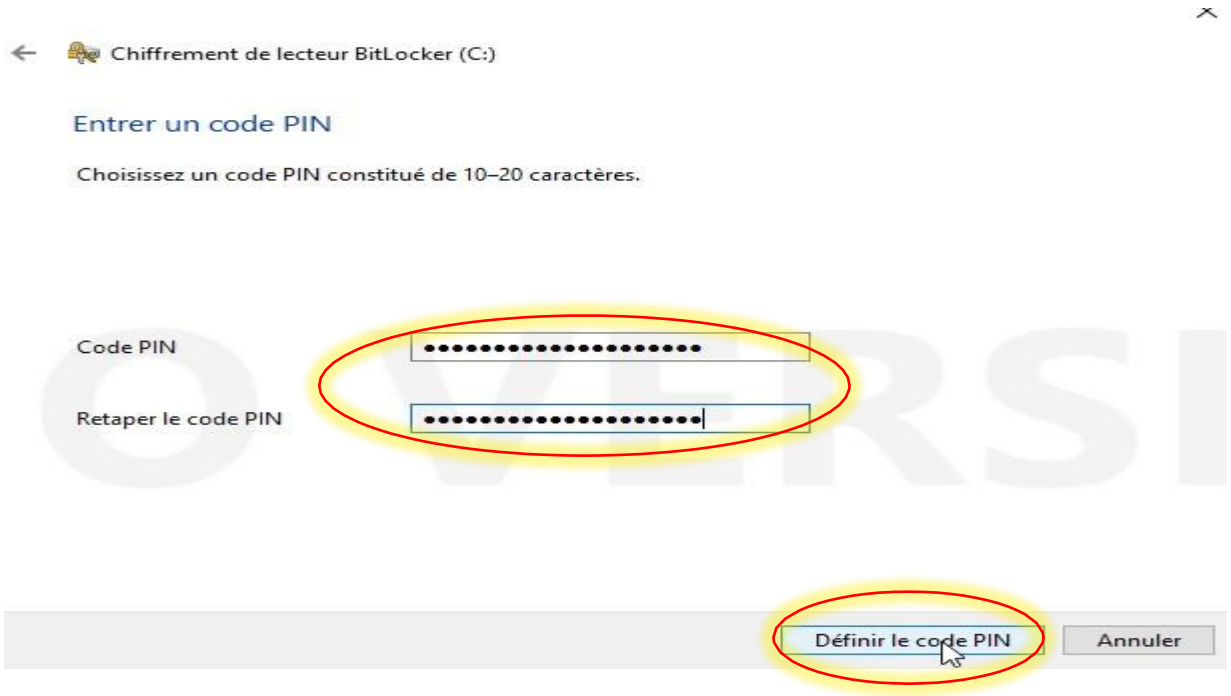
ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

Concernant le chiffrement des périphériques de stockage « mobiles », un autre document décrit la marche à suivre.

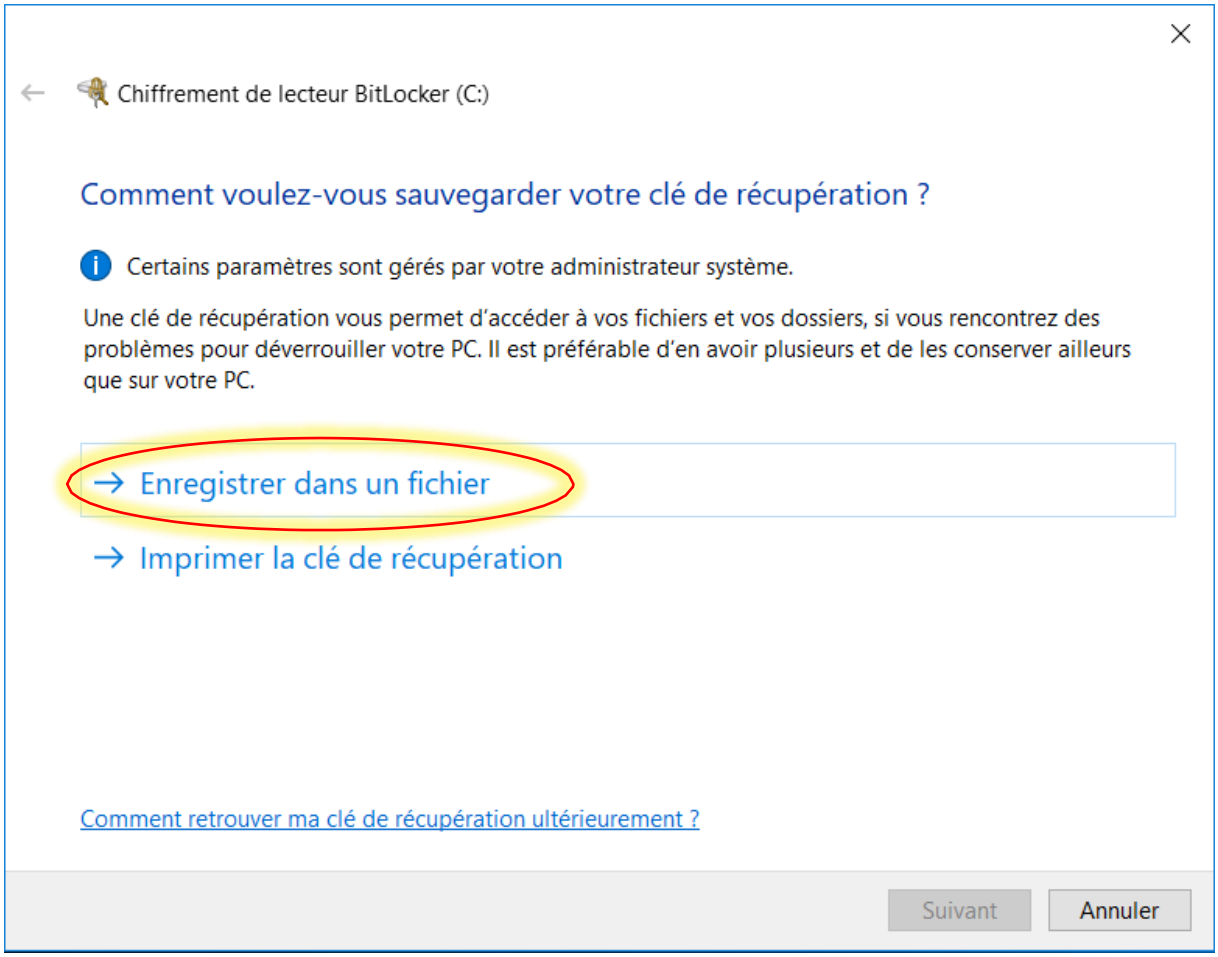
14. Cliquez sur « Entrer un code confidentiel »



15. Saisissez le code PIN que vous souhaitez utiliser. Validez en cliquant sur « définir le code PIN »

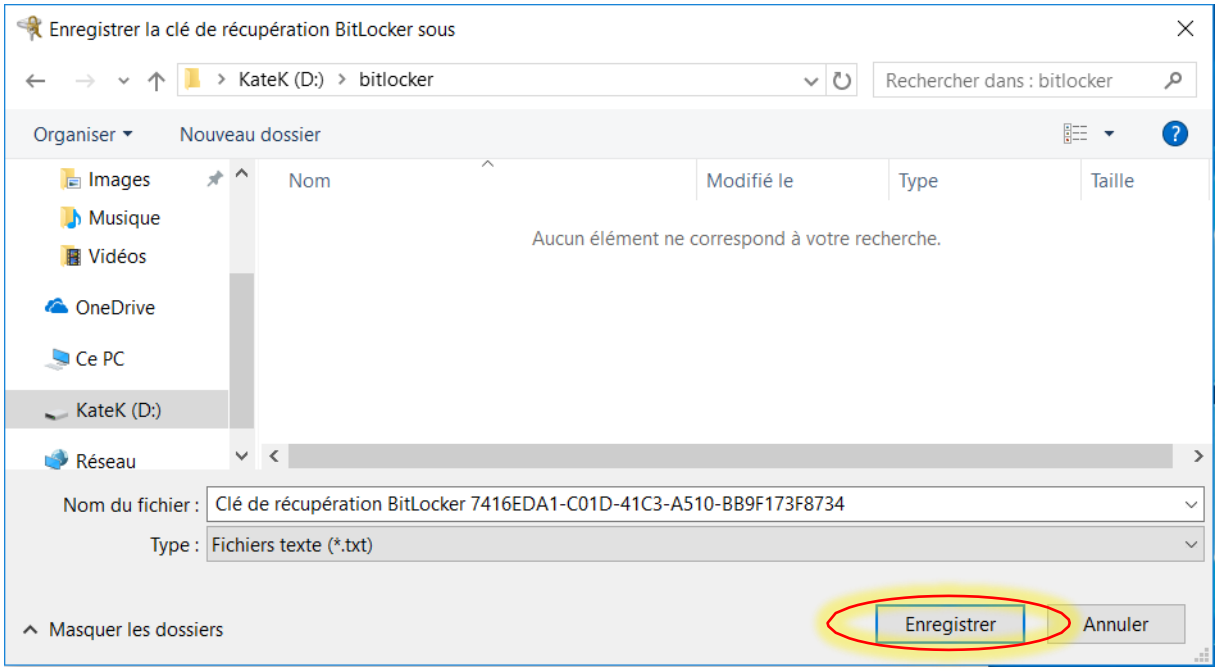


16. Cliquez sur « Enregistrer » dans un fichier.

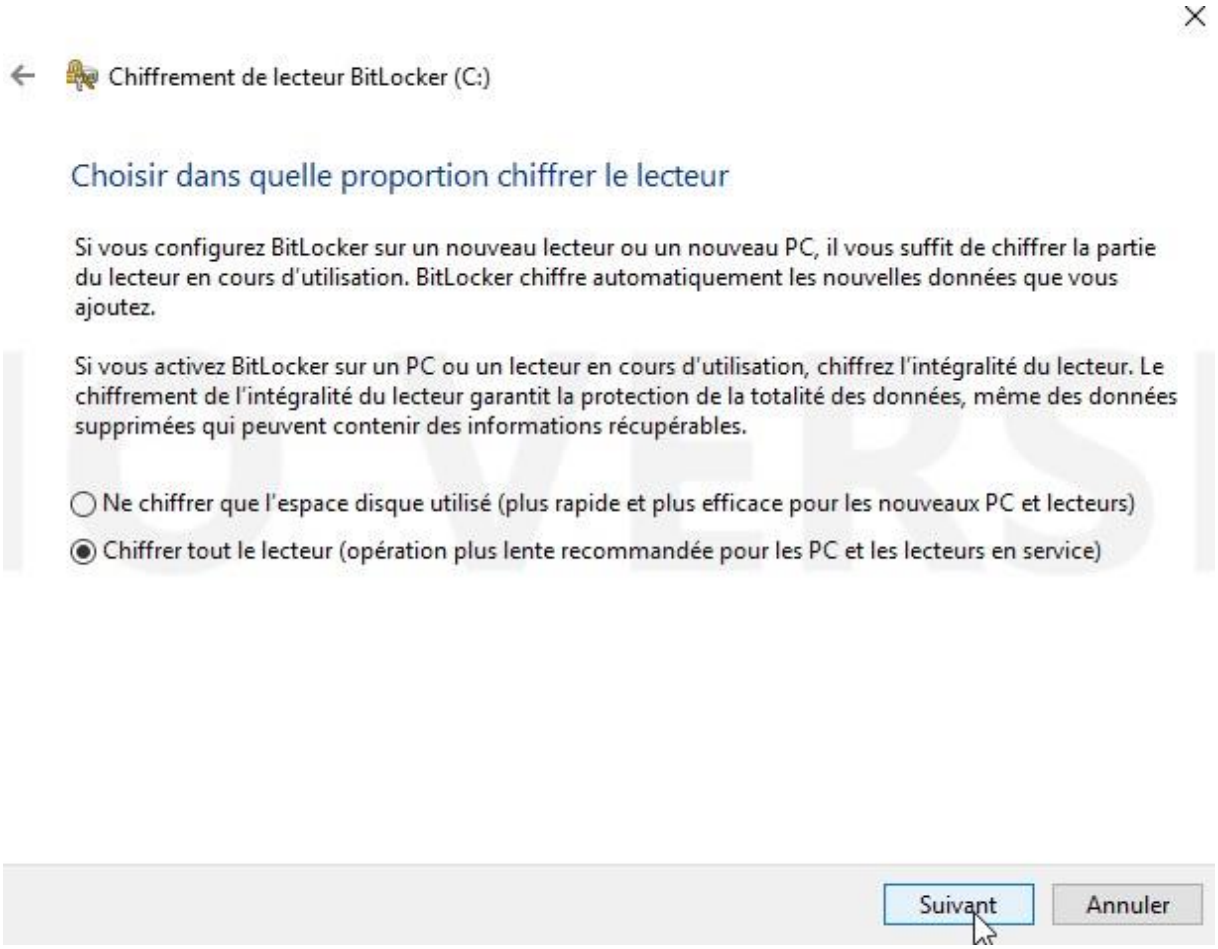


17. La mise en place de la clef de recouvrement est une étape importante. Cette clef doit être stockée dans un endroit sûr et accessible uniquement aux personnes autorisées.

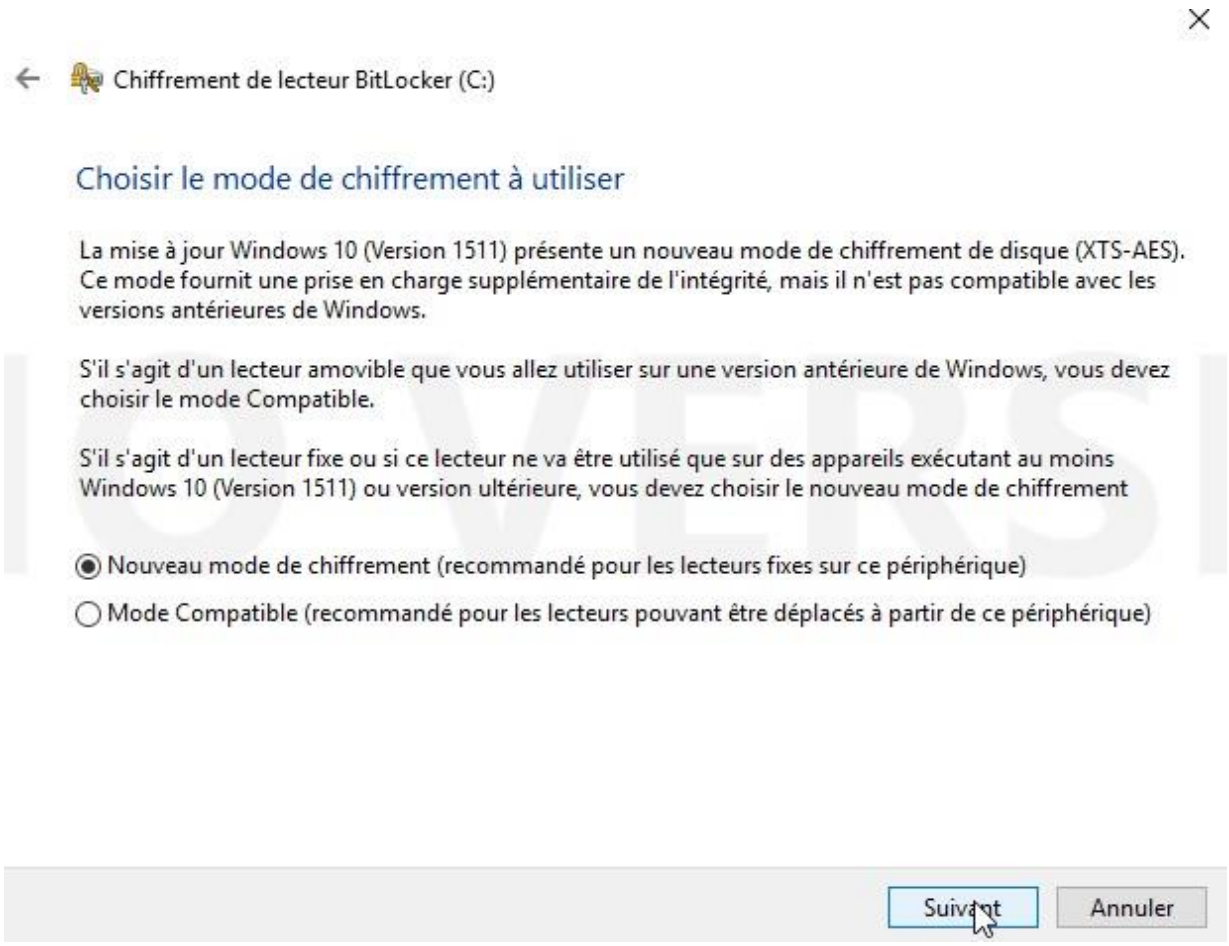
18. Bitlocker vous propose d'enregistrer cette clef au format « .txt ». Vous pouvez la stocker sur un périphérique de stockage mobile, mais il est recommandé de la stocker dans un gestionnaire de mot de passe, un logiciel type « coffre fort numérique » ou tout système de gestion de secret vous paraissant adapté à la protection de cette clef.



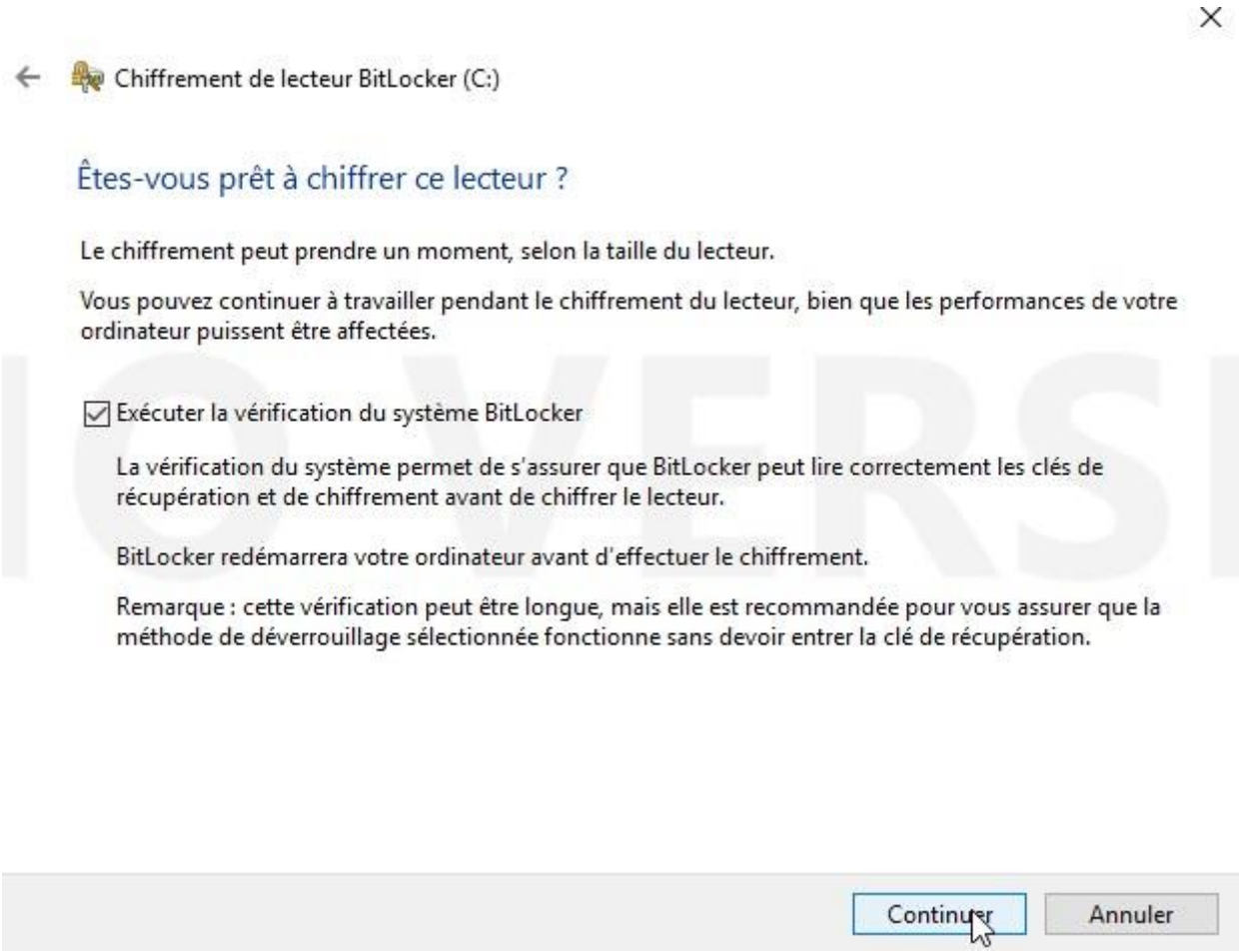
19. Cochez « chiffrer tout le lecteur » puis cliquez sur suivant



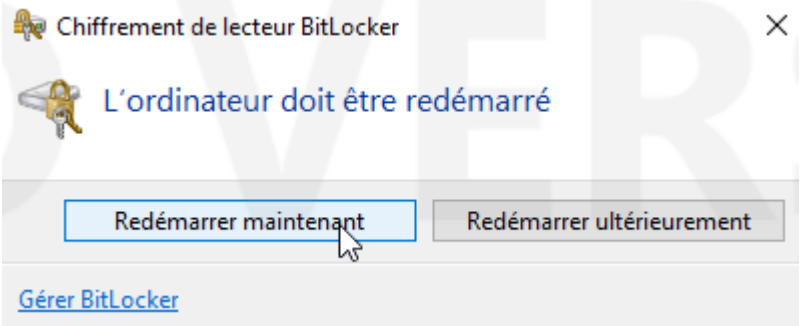
20. Cochez « nouveau mode de chiffrement » puis cliquez sur suivant



21. Cochez « Exécuter la vérification du système », puis cliquez sur « continuer »



22. Redémarrez l'ordinateur



23. Au démarrage de la machine vous serez invité à saisir le code PIN que vous avez défini plus haut. Attention : à la saisie du code PIN, le clavier sera en QWERTY.

24. Pour connaitre l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icone cachée à droite de la barre des tâches.