

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.

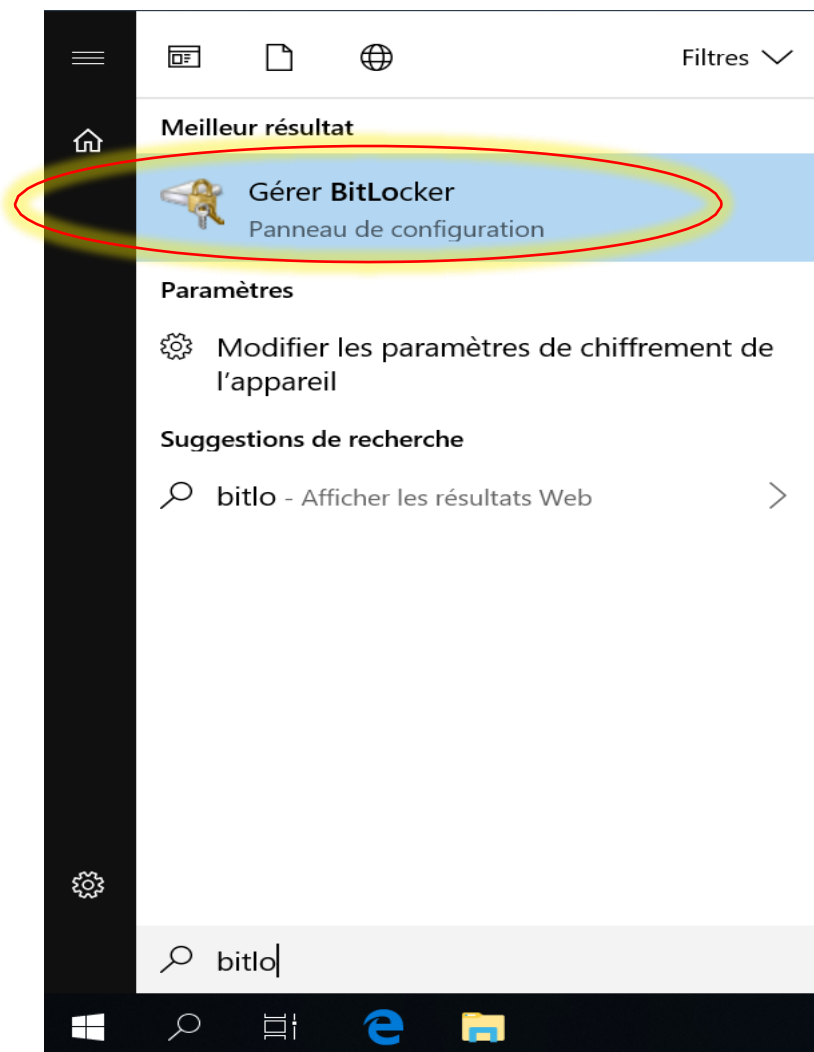
Chiffrement avec puce TPM.

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

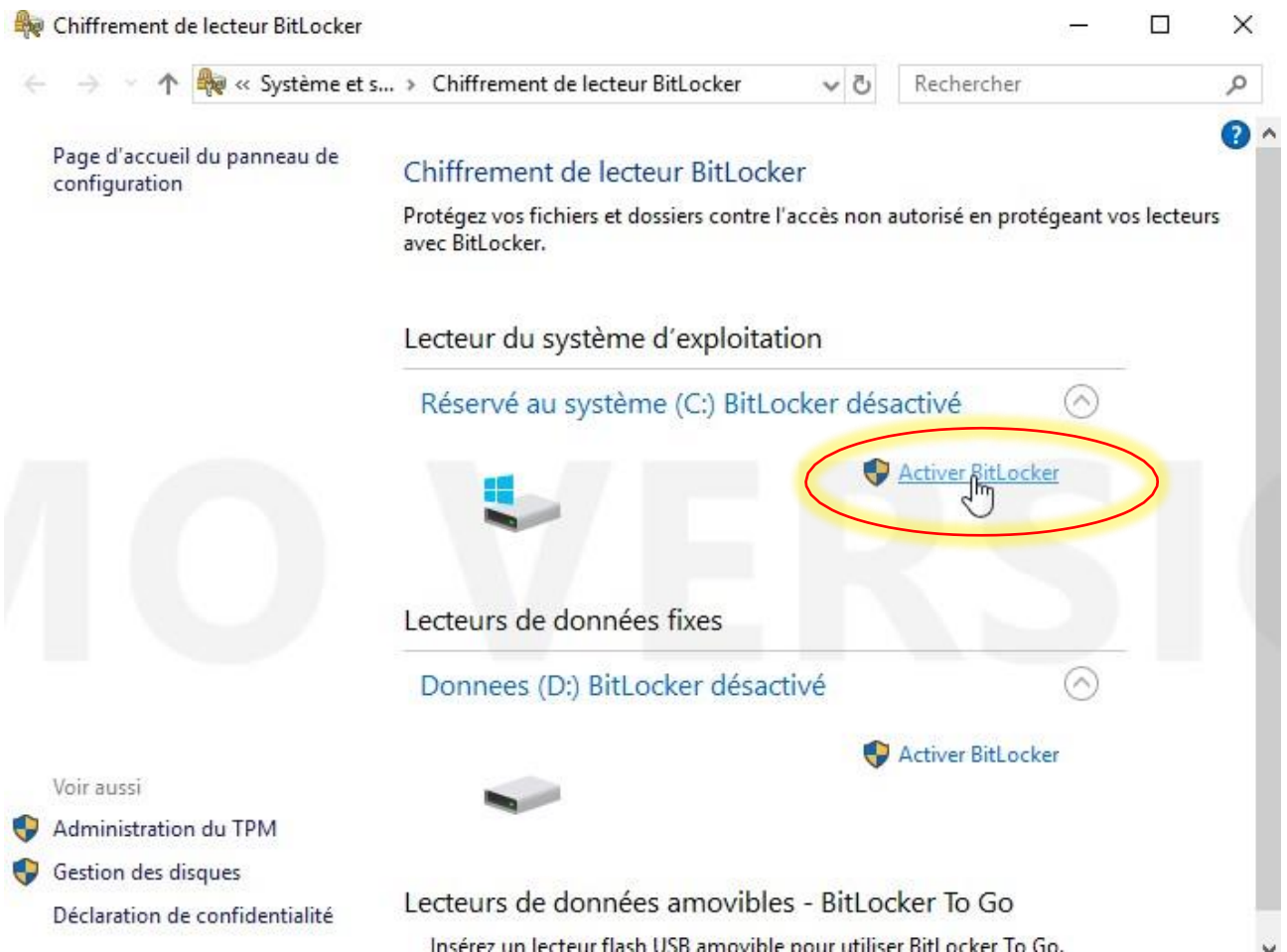
Par défaut, Bitlocker est désactivé.

Il faut l'activer afin de pouvoir lancer le chiffrement de la machine.

1. Lancez l'outil de gestion de Bitlocker



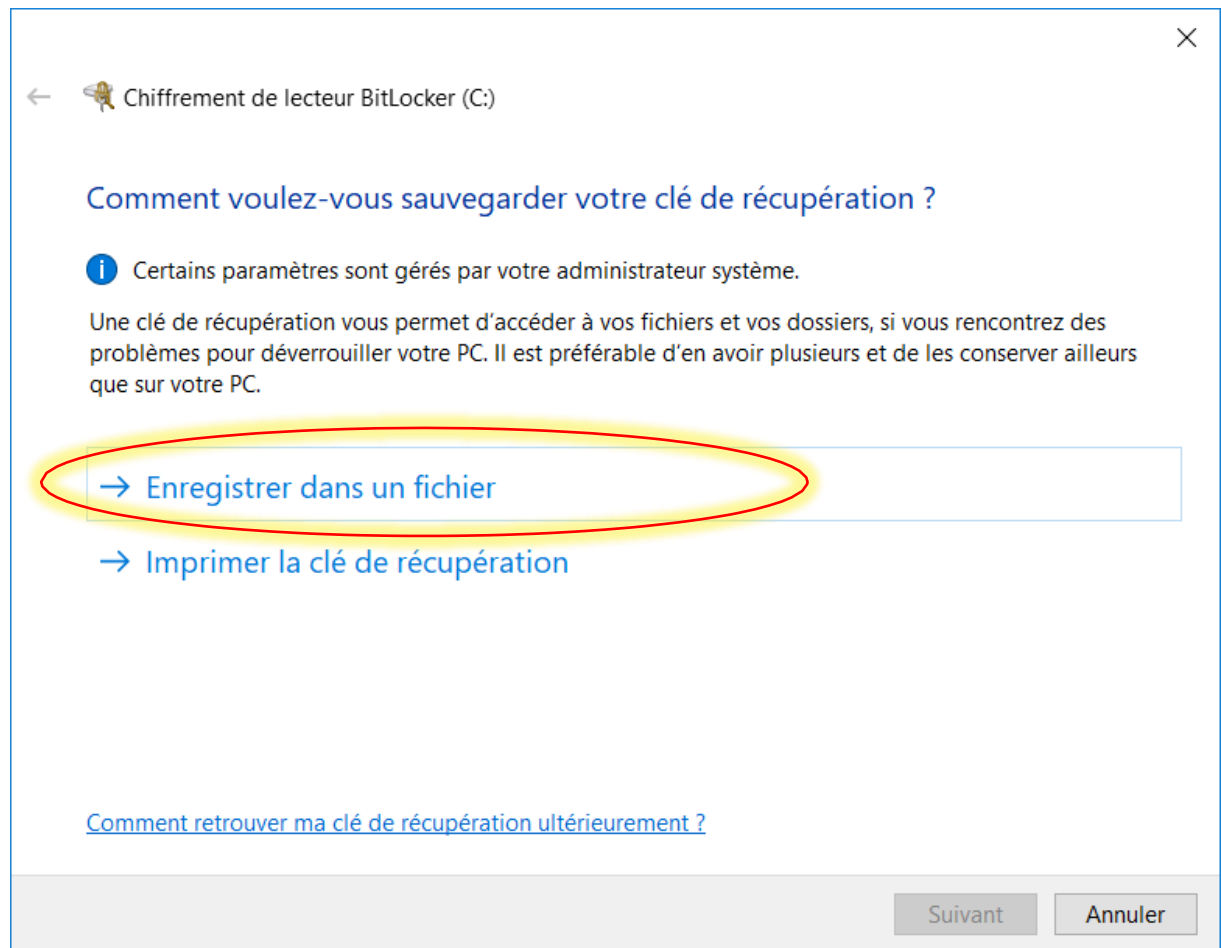
2. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer BitLocker ».



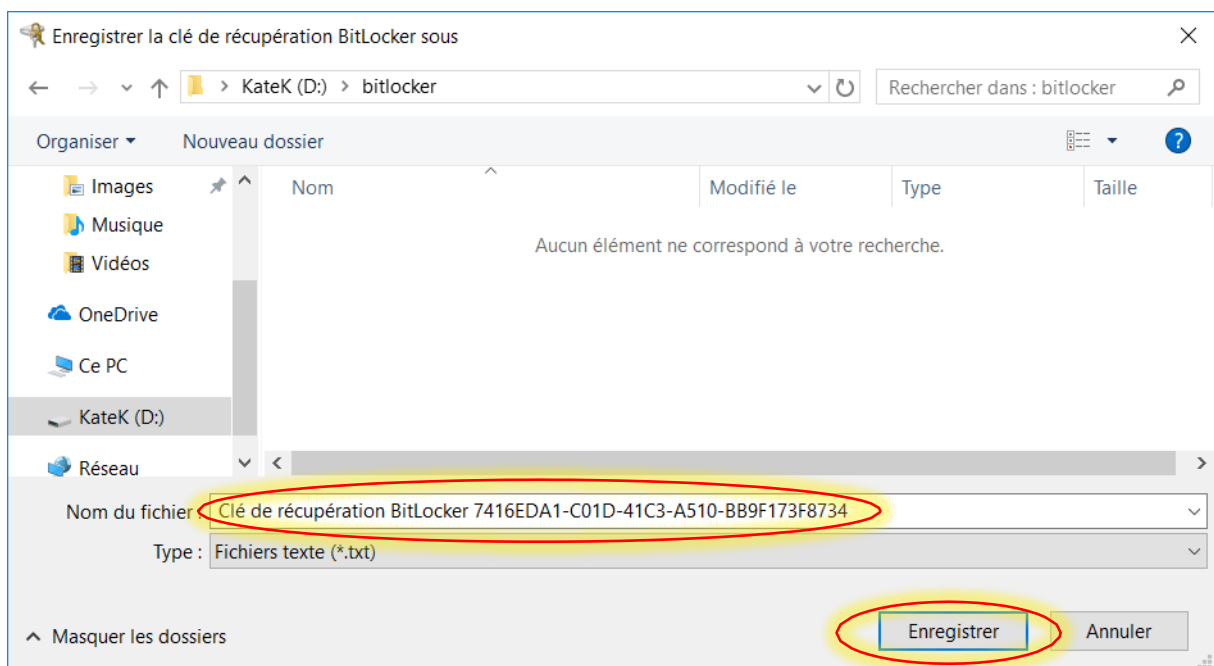
ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

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

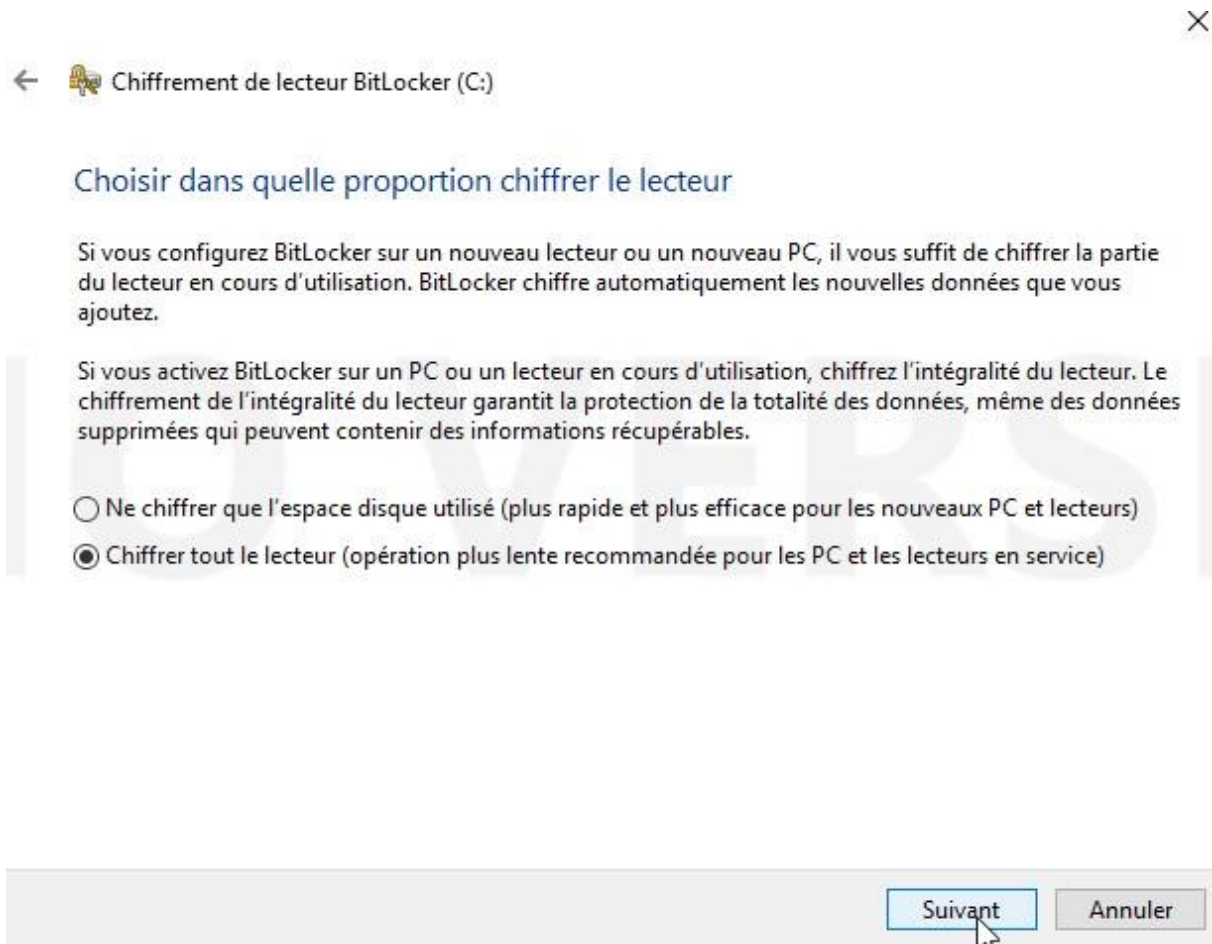
3. Cliquez sur « Enregistrer dans un fichier ».



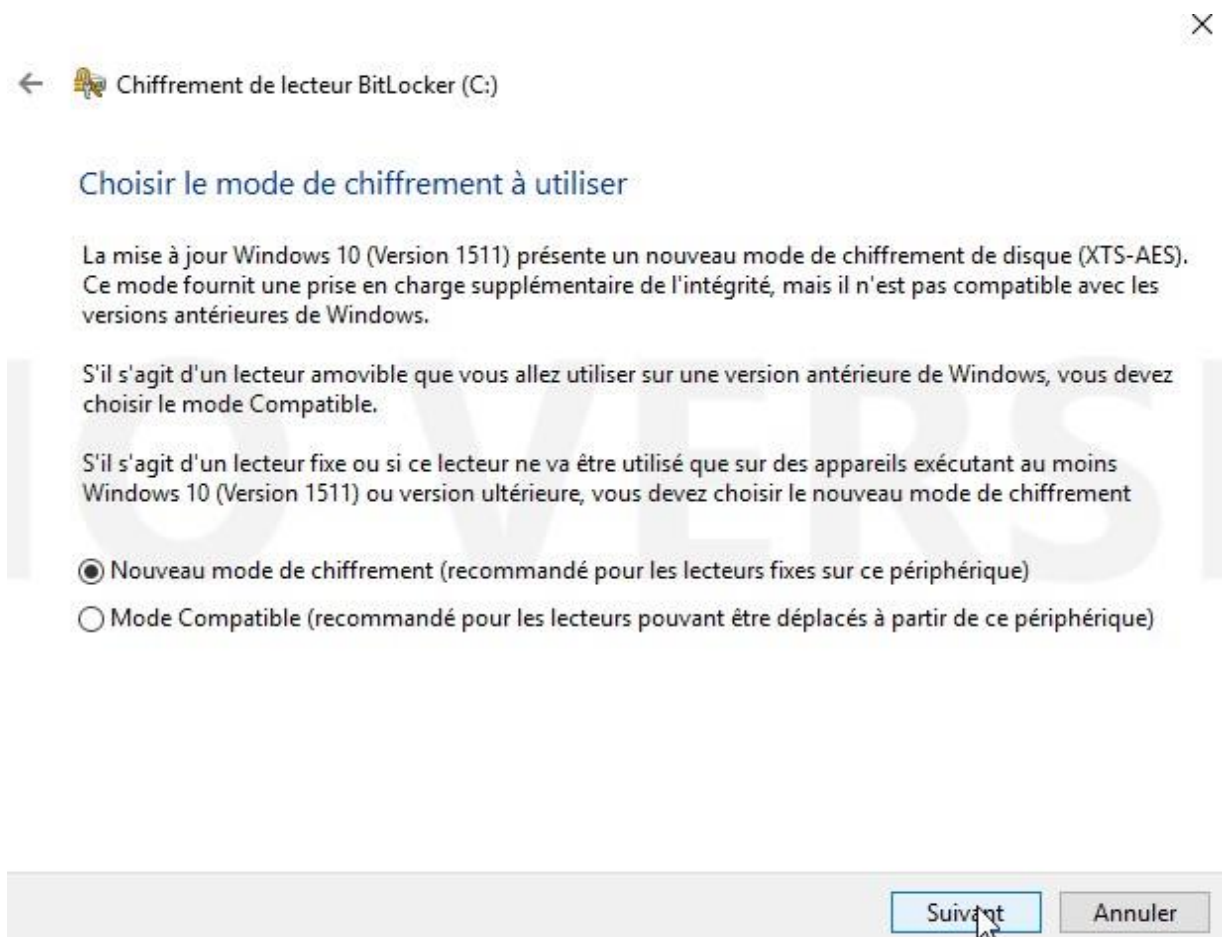
4. La mise en place de la clef de recouvrement est une étape importante. Cette clef doit être stockée dans un endroit sûr et accessible uniquement aux personnes autorisées.
5. Bitlocker vous propose d'enregistrer cette clef au format « .txt ». Vous pouvez la stocker sur un périphérique de stockage mobile, 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.



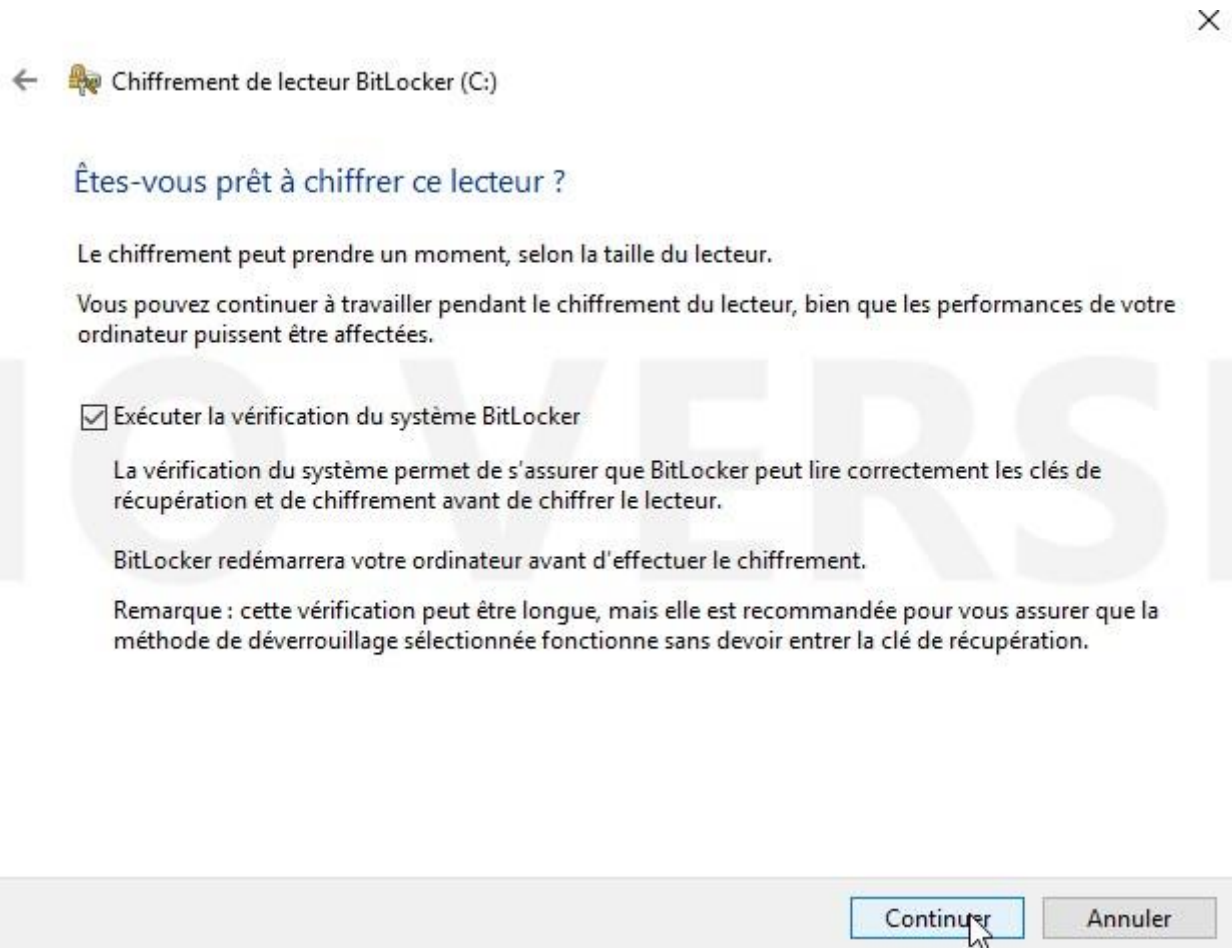
6. Cochez « chiffrer tout le lecteur » puis cliquez sur suivant



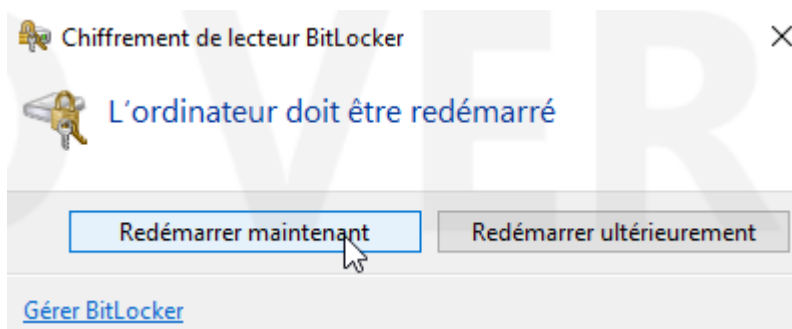
7. Cochez « nouveau mode de chiffrement » puis cliquez sur suivant



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

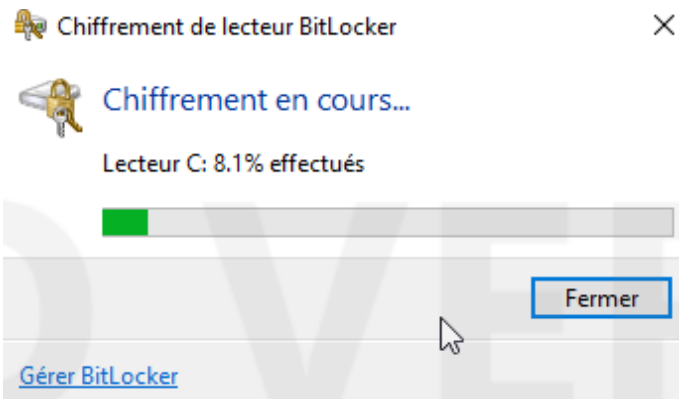


9. Redémarrez l'ordinateur



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.

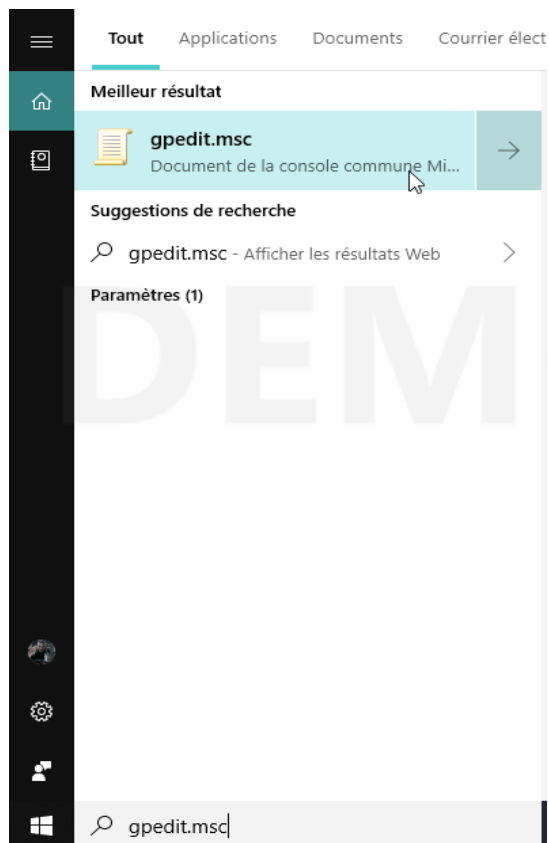
11. Pour connaître l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icône cachée à droite de la barre des tâches.



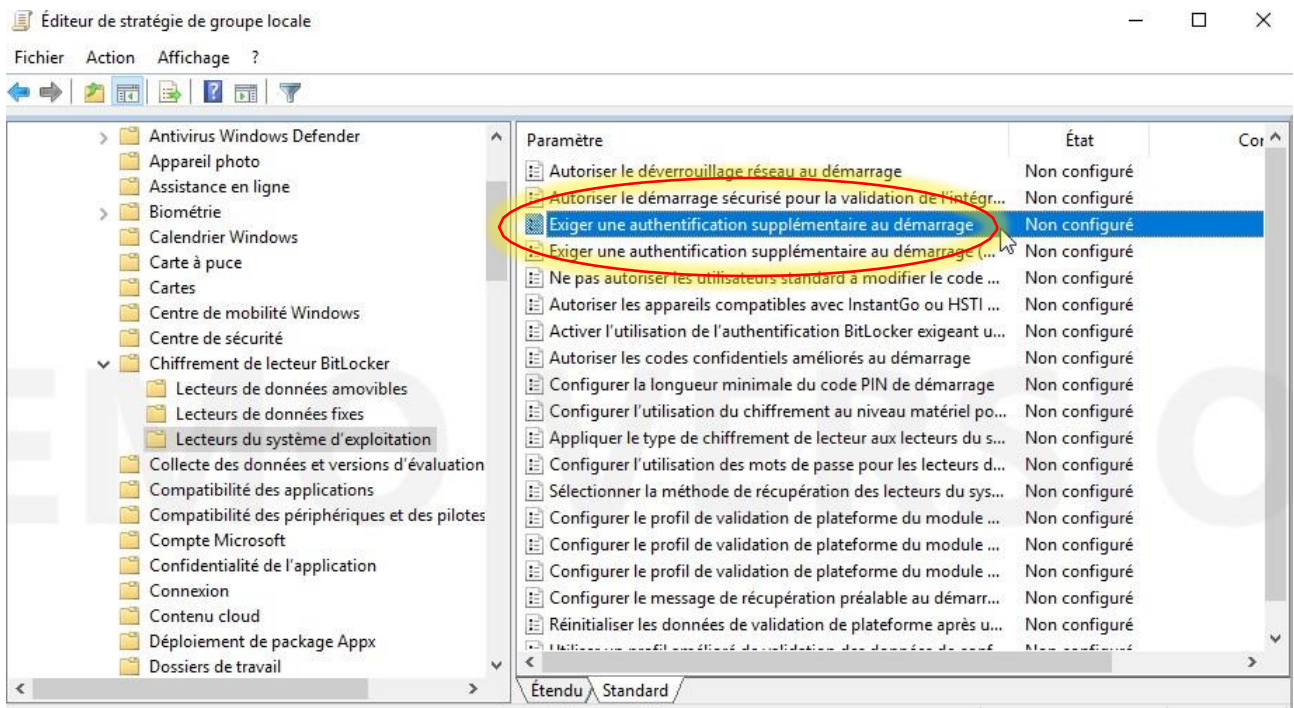
Chiffrement sans puce TPM ou puce TPM désactivée.

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 ».

Exiger une authentification supplémentaire au démarrage

Exiger une authentification supplémentaire au démarrage Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :
☒ **Activé**
☐ Désactivé

Pris en charge sur : Au minimum Windows Server 2008 R2 ou Windows 7

Options : Aide :

☒ **Autoriser BitLocker sans un module de plateforme sécurisée compatible**
mot de passe ou une clé de démarrage sur un disque

Paramètres pour les ordinateurs avec un module de plateforme sécurisée compatible

Configurer le démarrage du module de plateforme sécurisée

Autoriser le module de plateforme sécurisée

Configurer le code PIN de démarrage de module de plateforme sécurisée

Autoriser un code PIN de démarrage avec le module de plateforme sécurisée

Configurer la clé de démarrage de module de plateforme sécurisée

Autoriser une clé de démarrage avec le module de plateforme sécurisée

Configurer le code PIN et la clé de démarrage de module de plateforme sécurisée

Autoriser une clé et un code PIN de démarrage avec le module de plateforme sécurisée

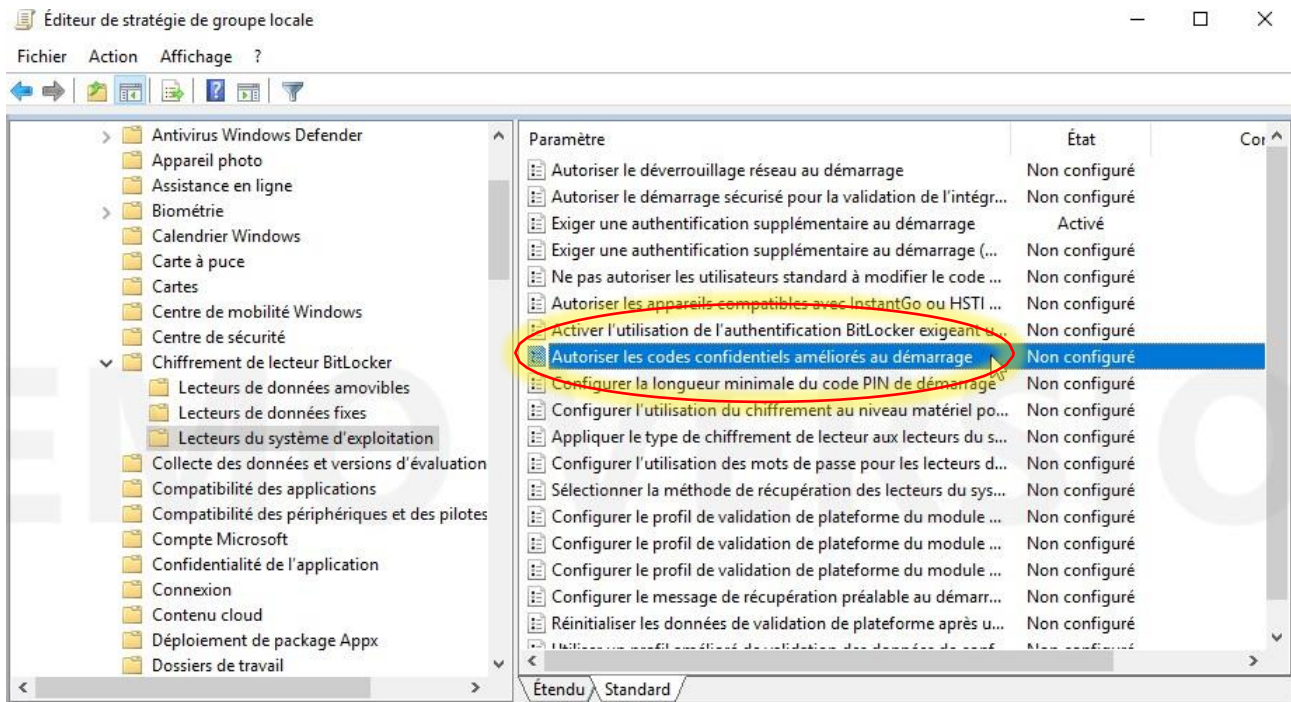
Ce paramètre de stratégie vous permet de configurer si BitLocker exige une authentification supplémentaire à chaque démarrage de l'ordinateur et si vous utilisez BitLocker avec ou sans module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker.

Remarque : une seule des options d'authentification supplémentaire peut être exigée au démarrage, sans générer d'erreur de stratégie.

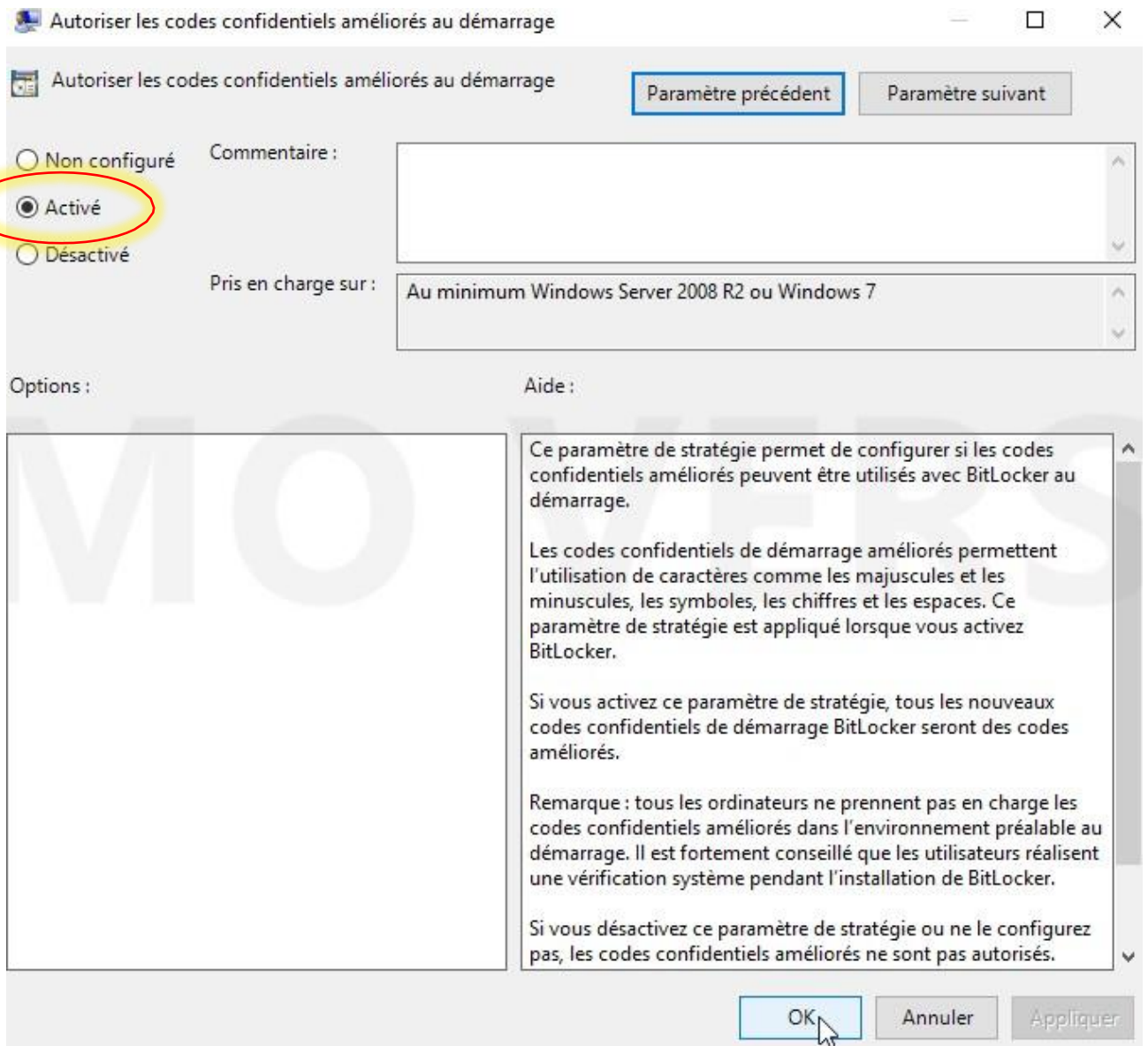
Si vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisée, activez la case à cocher « Autoriser BitLocker sans un module de plateforme autorisée compatible ». Dans ce mode, un mot de passe ou un lecteur USB est requis pour le démarrage. Si une clé de démarrage est utilisée, les informations de clé utilisées pour chiffrer le lecteur sont stockées sur ce lecteur USB, créant une clé USB. Lorsque la clé USB est insérée, l'accès au lecteur est authentifié et le lecteur est accessible. Si la clé USB est perdue ou non disponible, ou bien encore si vous oubliez le mot de passe, vous devez utiliser l'une des options de récupération BitLocker pour accéder au lecteur.

OK Annuler Appliquer

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



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



Autoriser les codes confidentiels améliorés au démarrage

Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :

☒ **Activé**

☐ Désactivé

Pris en charge sur : Au minimum Windows Server 2008 R2 ou Windows 7

Options :

Aide :

Ce paramètre de stratégie permet de configurer si les codes confidentiels améliorés peuvent être utilisés avec BitLocker au démarrage.

Les codes confidentiels de démarrage améliorés permettent l'utilisation de caractères comme les majuscules et les minuscules, les symboles, les chiffres et les espaces. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker.

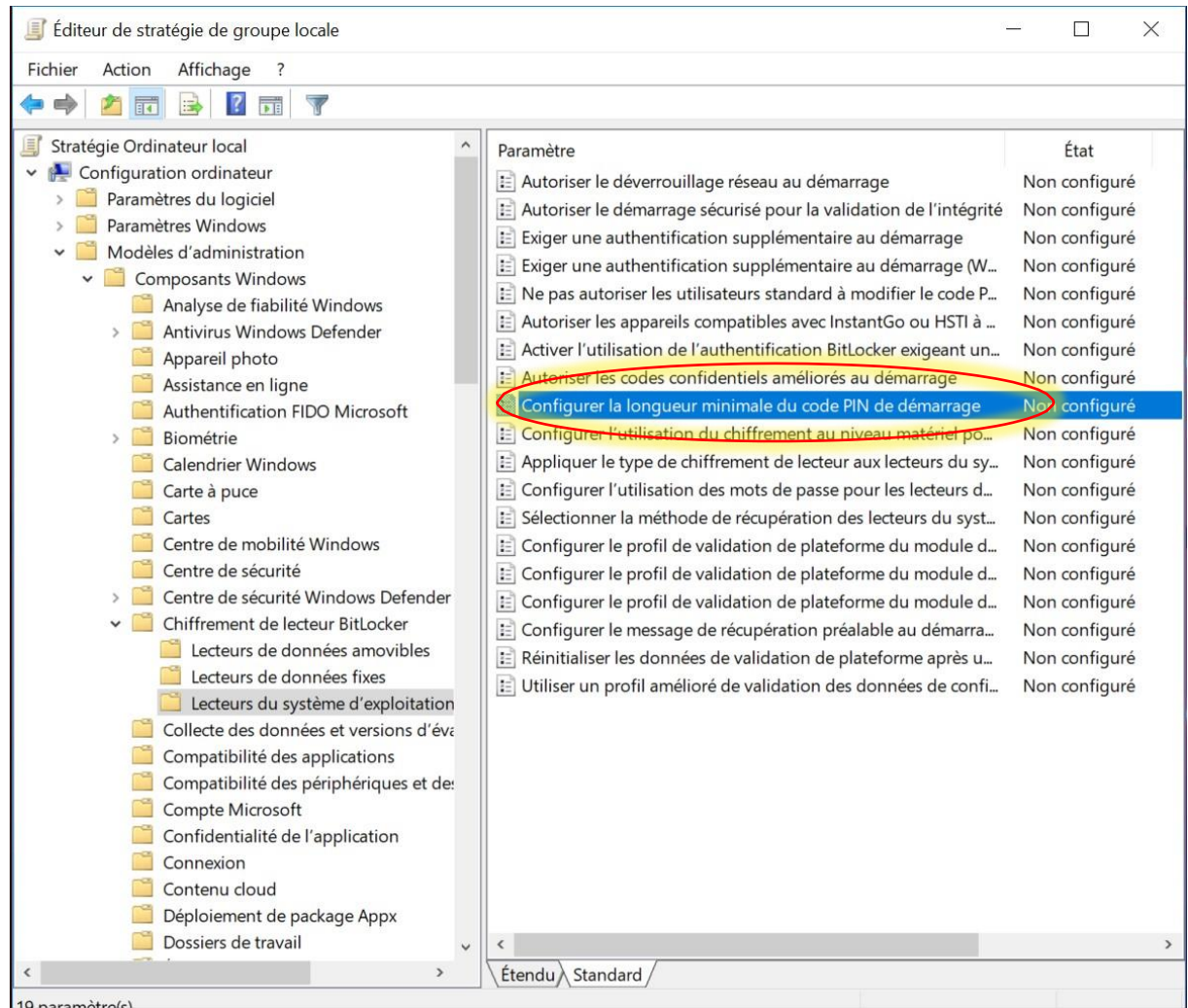
Si vous activez ce paramètre de stratégie, tous les nouveaux codes confidentiels de démarrage BitLocker seront des codes améliorés.

Remarque : tous les ordinateurs ne prennent pas en charge les codes confidentiels améliorés dans l'environnement préalable au démarrage. Il est fortement conseillé que les utilisateurs réalisent une vérification système pendant l'installation de BitLocker.

Si vous désactivez ce paramètre de stratégie ou ne le configurez pas, les codes confidentiels améliorés ne sont pas autorisés.

OK Annuler Appliquer

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 »

Configurer la longueur minimale du code PIN de démarrage

Configurer la longueur minimale du code PIN de démarrage Paramètre précédent Paramètre suivant

☐ Non configuré Commentaire :

☒ Activé

☐ Désactivé Pris en charge sur : Au minimum Windows Server 2008 R2 ou Windows 7

Options : Aide :

Nombre minimal de caractères : 10

Ce paramètre de stratégie vous permet de configurer la longueur minimale pour le code PIN de démarrage d'un module de plateforme sécurisée (TPM). Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker. Le code PIN de démarrage doit comporter entre 4 et 20 chiffres.

Si vous activez ce paramètre de stratégie, vous pouvez exiger le nombre minimal de chiffres à entrer pour définir le code PIN de démarrage.

Si vous désactivez ce paramètre de stratégie ou ne le configurez pas, les utilisateurs peuvent définir un code PIN comportant entre 6 et 20 chiffres.

REMARQUE : si le code PIN comporte moins de 6 chiffres, Windows tentera de réinitialiser la période de verrouillage du TPM 2.0 de manière à ce qu'elle soit supérieure à la valeur par défaut lorsqu'un code PIN est modifié. Si l'opération réussit, Windows ne réinitialisera la période de verrouillage du TPM à la valeur par défaut que si le TPM est réinitialisé.

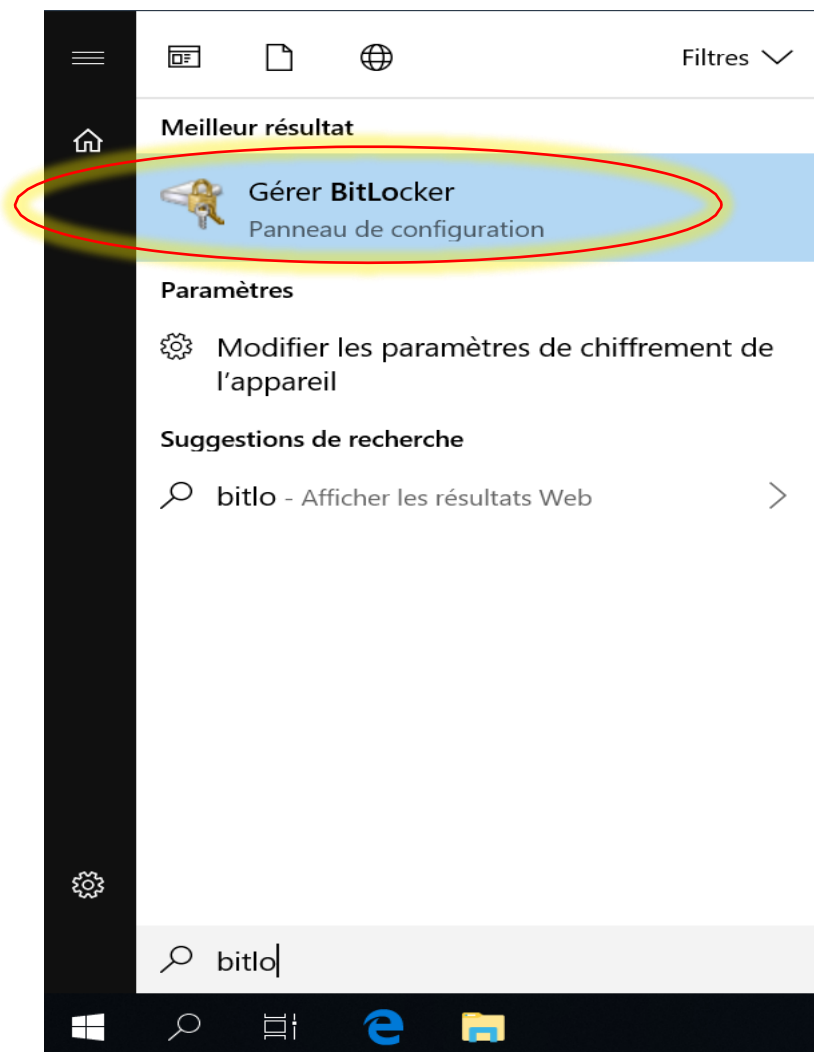
OK Annuler Appliquer

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

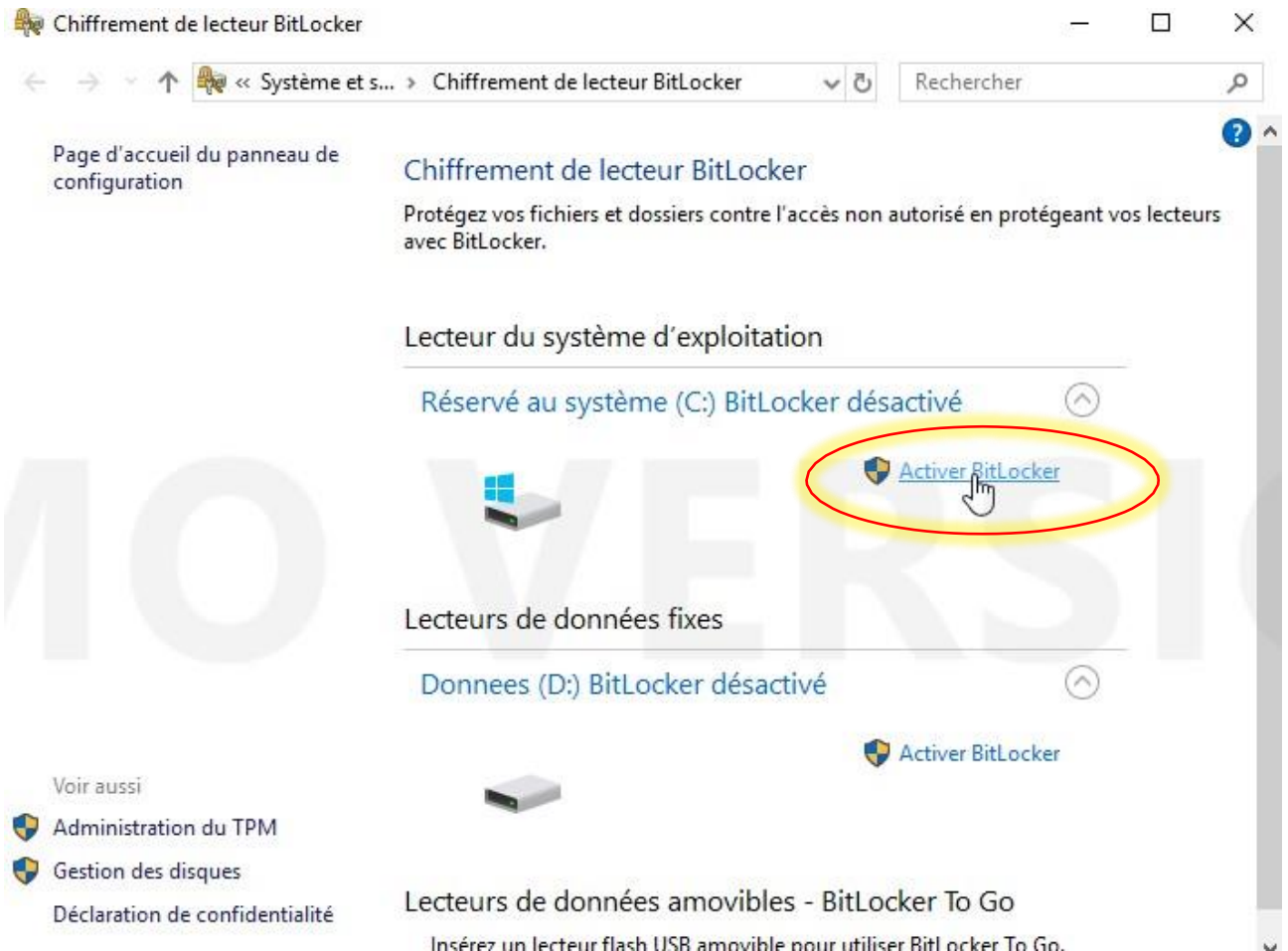
Par défaut, Bitlocker est désactivé.

Il faut l'activer afin de pouvoir lancer le chiffrement de la machine.

12. Lancez l'outil de gestion de Bitlocker



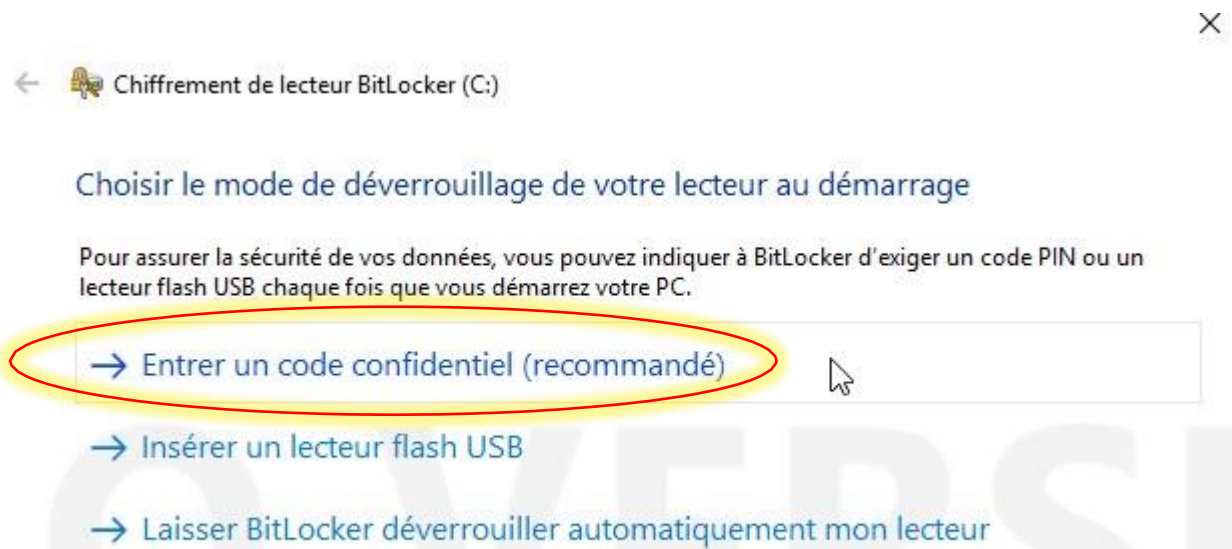
13. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer BitLocker ».




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 »

←  Chiffrement de lecteur BitLocker (C:) ✕

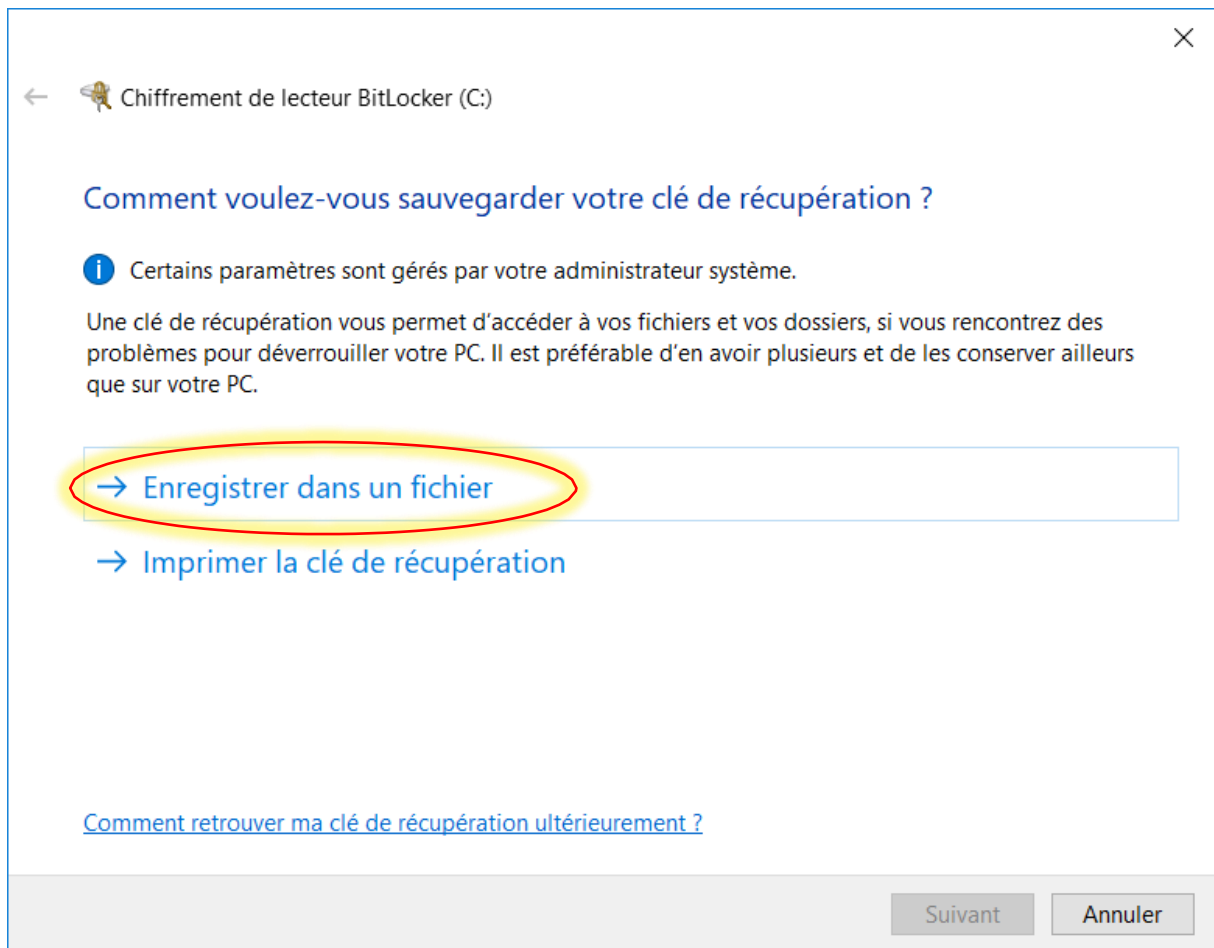
Entrer un code PIN

Choisissez un code PIN constitué de 10–20 caractères.

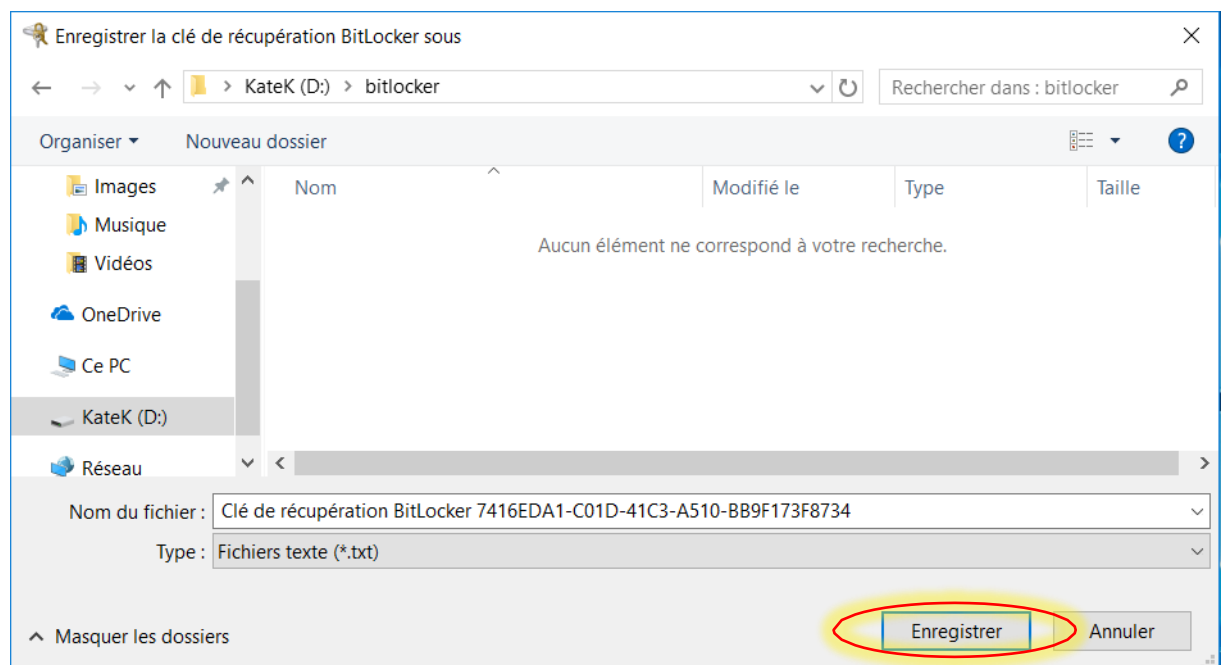
Code PIN

Retaper 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

✕

  Chiffrement de lecteur BitLocker (C:)

Choisir dans quelle proportion chiffrer le lecteur

Si vous configurez BitLocker sur un nouveau lecteur ou un nouveau PC, il vous suffit de chiffrer la partie du lecteur en cours d'utilisation. BitLocker chiffre automatiquement les nouvelles données que vous ajoutez.

Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

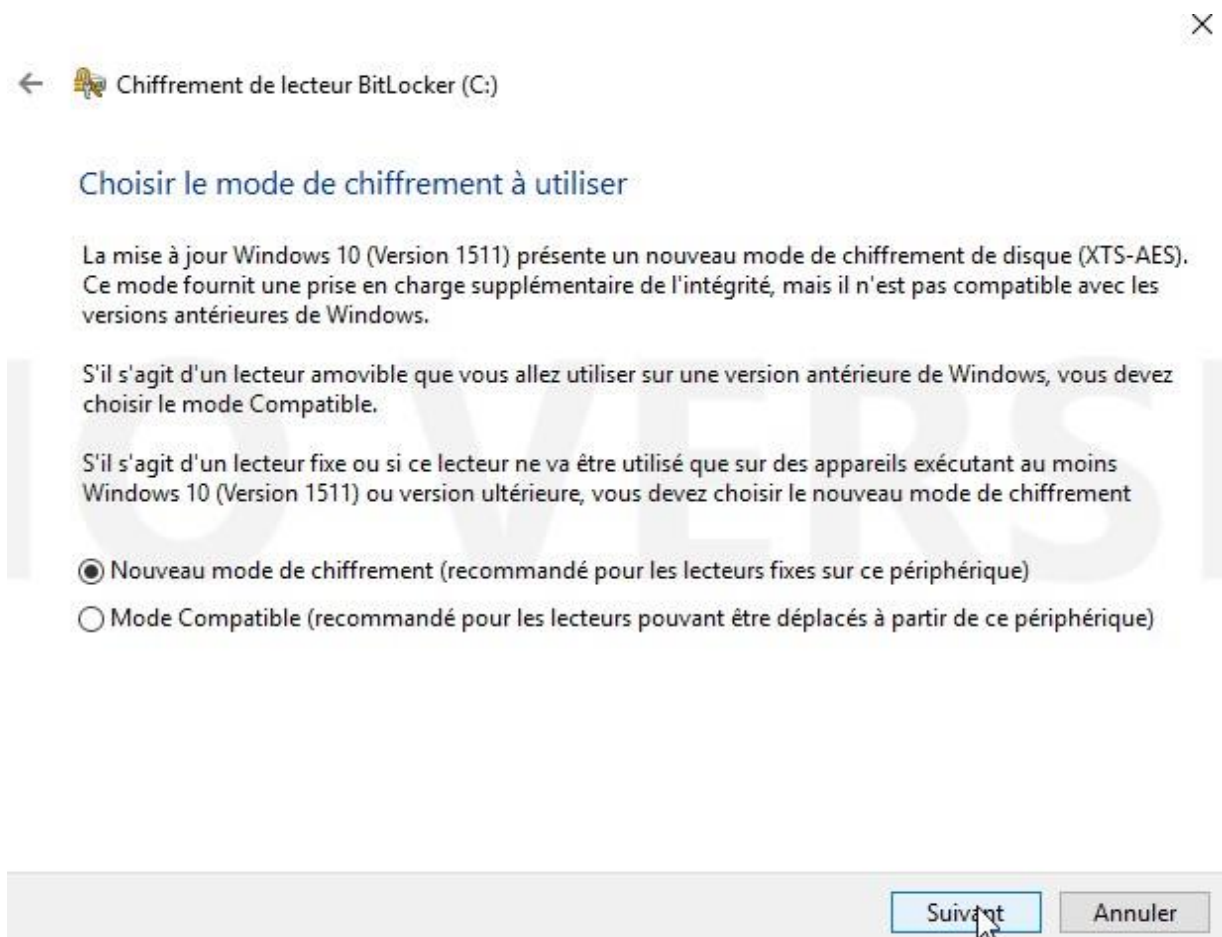
☐ Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)

☒ Chiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)

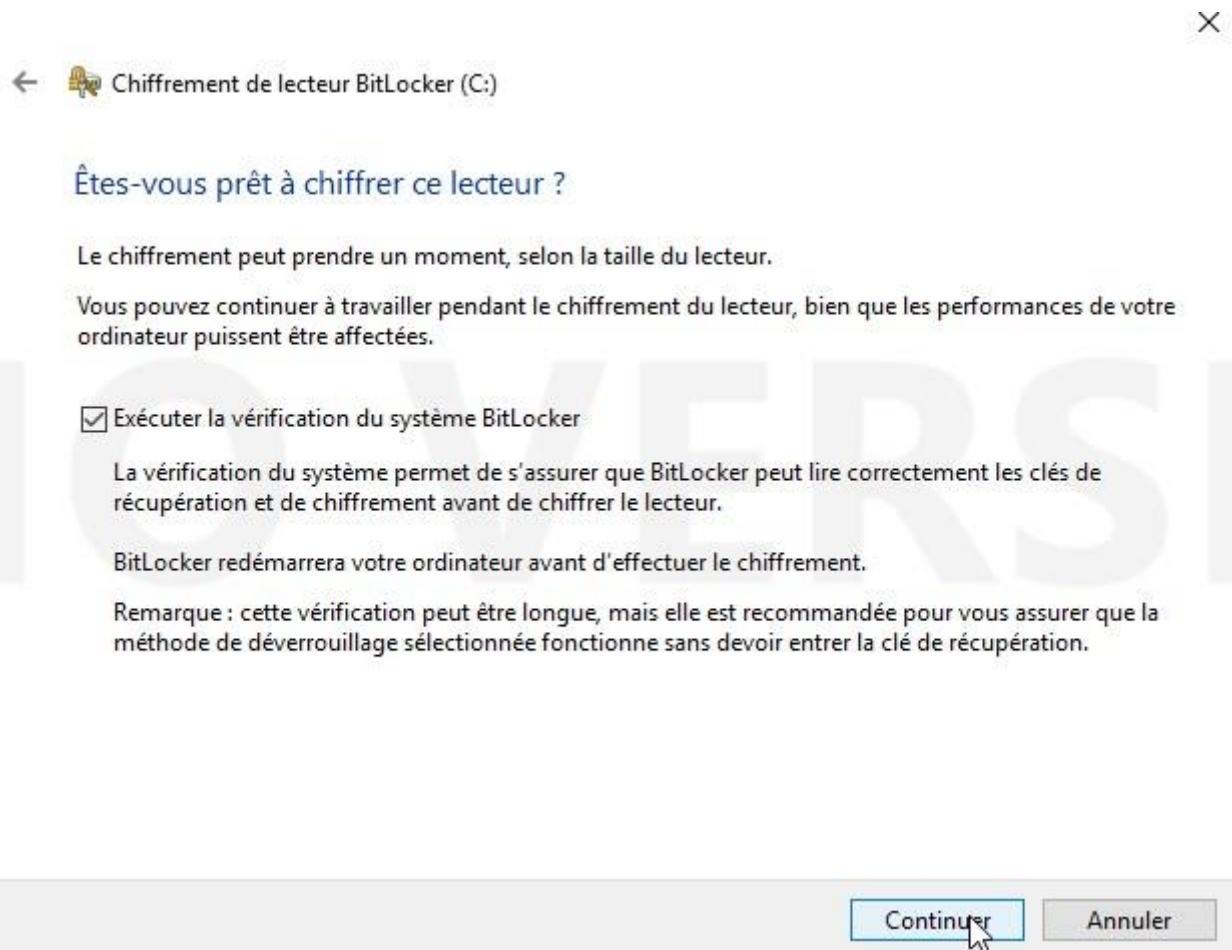
Suivant

Annuler

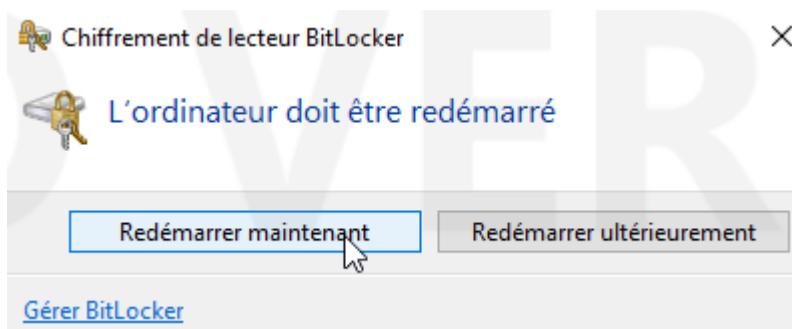
20. Cochez « nouveau mode de chiffrement » puis cliquez sur suivant



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 connaître l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icône cachée à droite de la barre des tâches.

