

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.

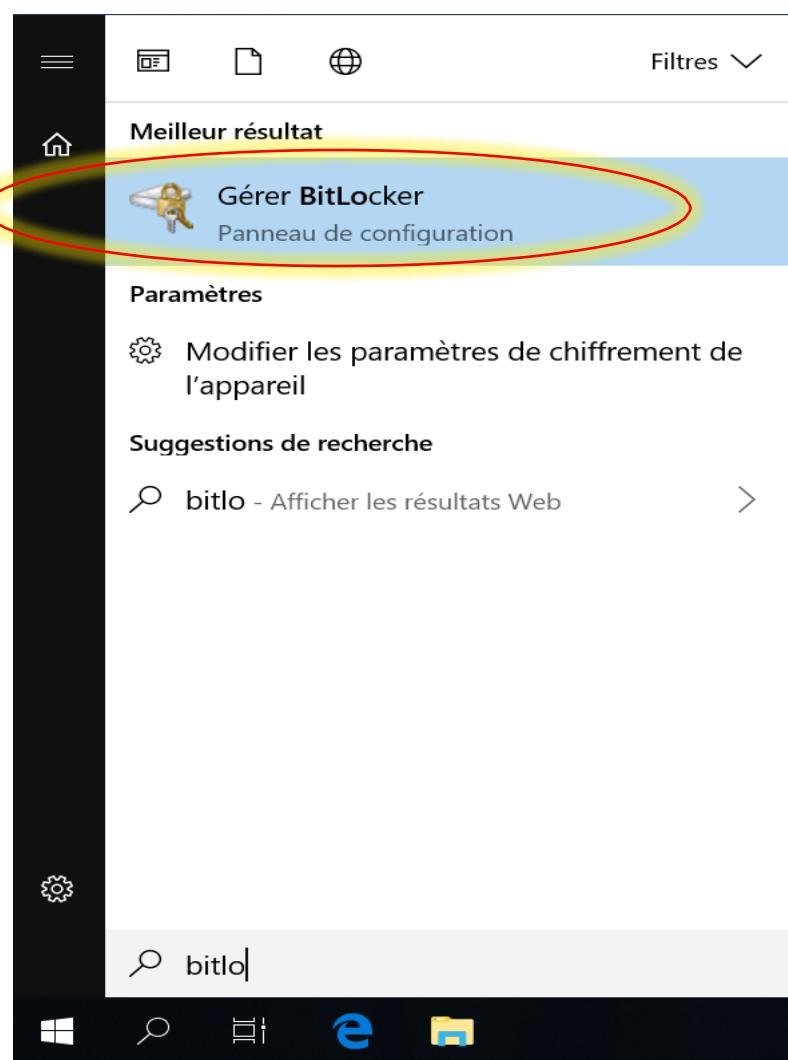
Chiffrement avec puce TPM.

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

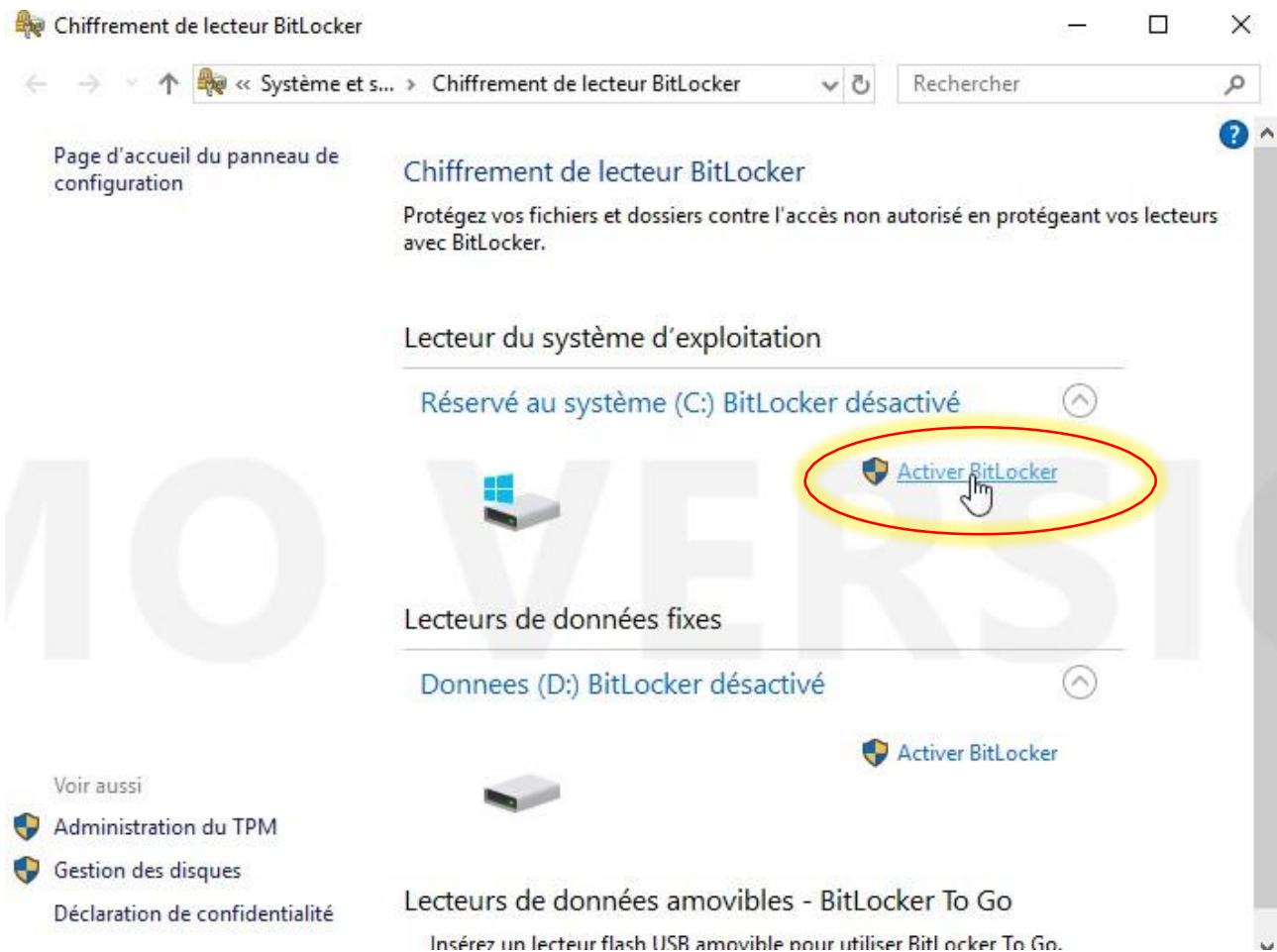
Par défaut, Bitlocker est désactivé.

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

1. Lancez l'outil de gestion de Bitlocker



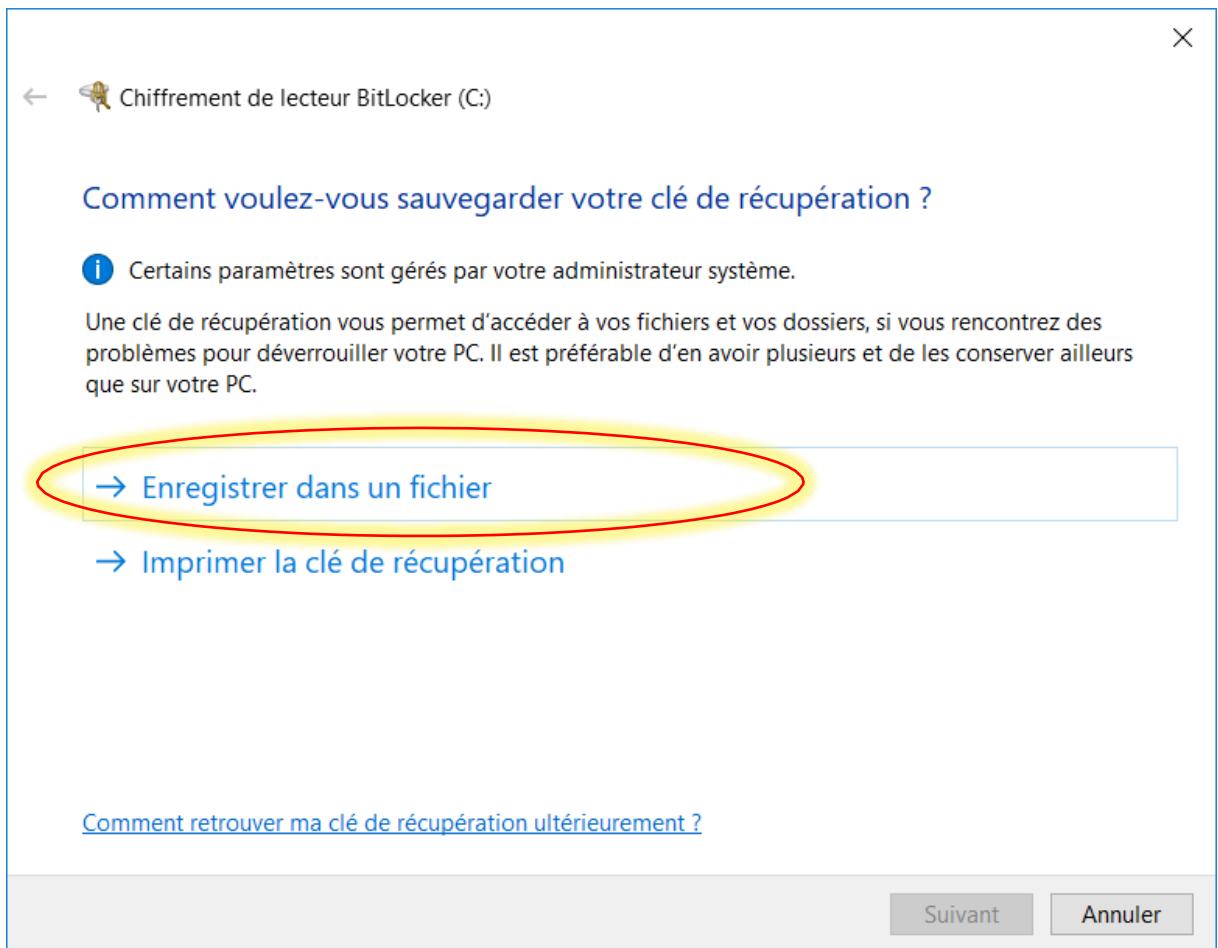
2. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer Bitlocker ».



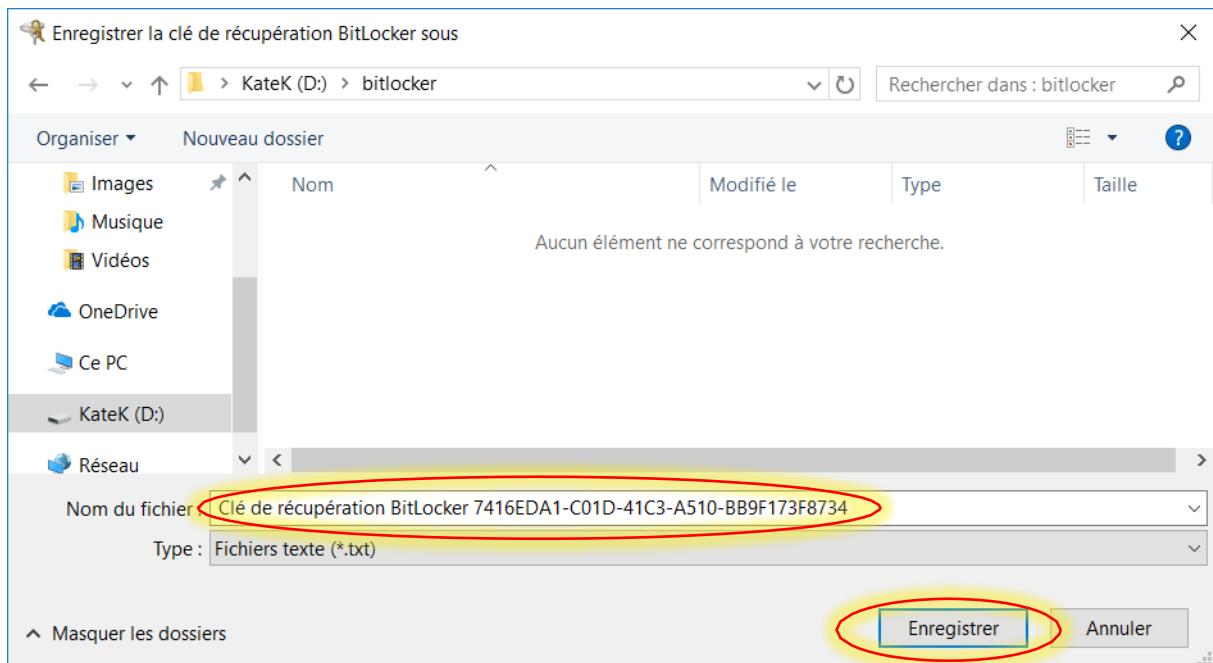
ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

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

The screenshot shows a Windows-style dialog box for BitLocker setup. At the top right is a close button (X). Below it, a back arrow points left, followed by the text "Chiffrement de lecteur BitLocker (C:)". A large blue header reads "Choisir dans quelle proportion chiffrer le lecteur". Underneath, a descriptive text states: "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." Another text block explains: "Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrerez 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." At the bottom, there are two radio buttons: one for "Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)" and one for "Chiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)". The "Chiffrer tout le lecteur" option is selected. At the very bottom right are two buttons: "Suivant" with a mouse cursor pointing to it, and "Annuler".

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

X

←  Chiffrement de lecteur BitLocker (C:)

Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

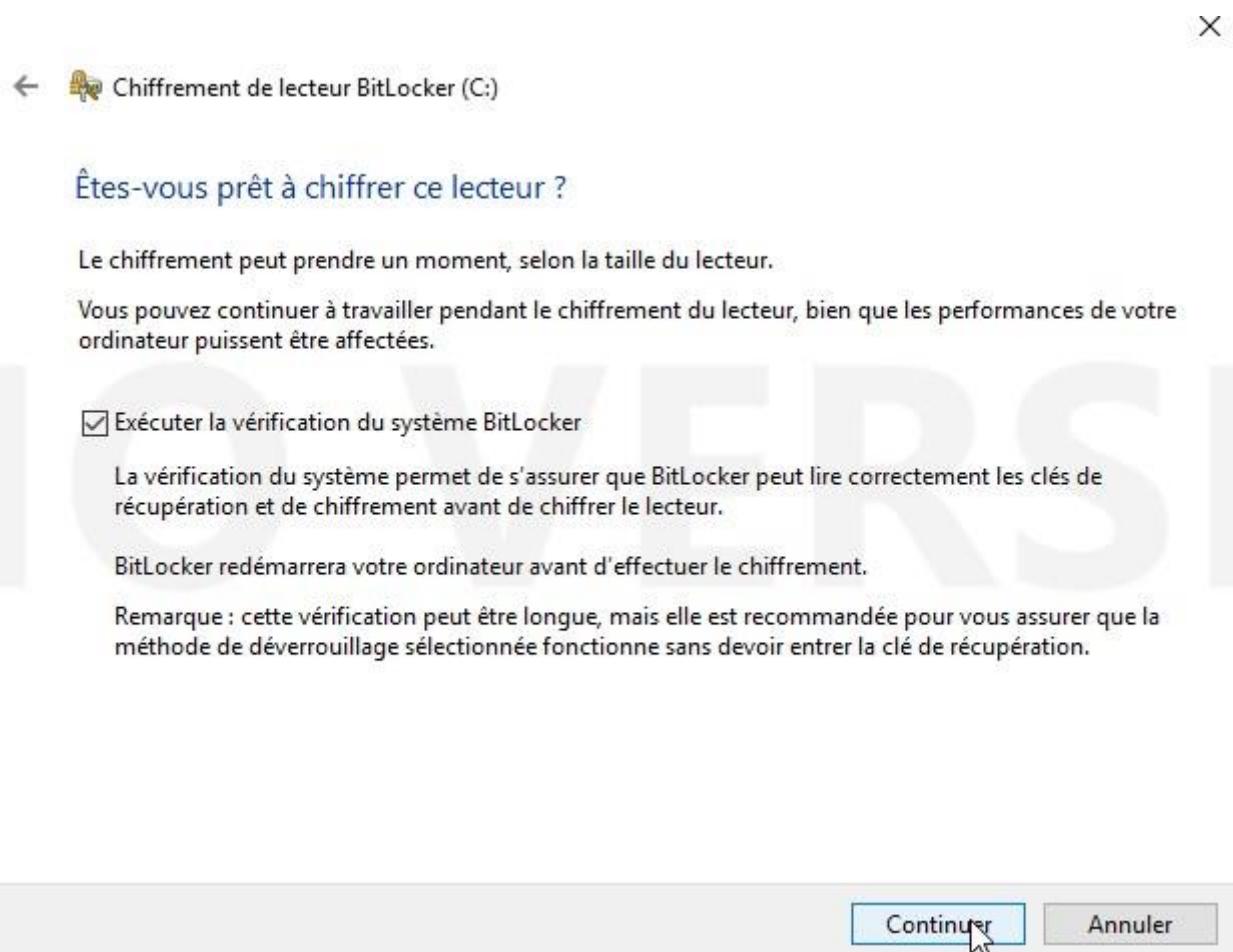
S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

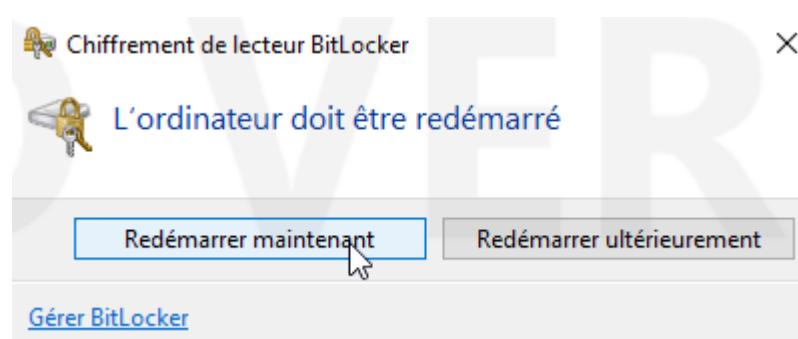
Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)
 Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

[Suivant](#) [Annuler](#)

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

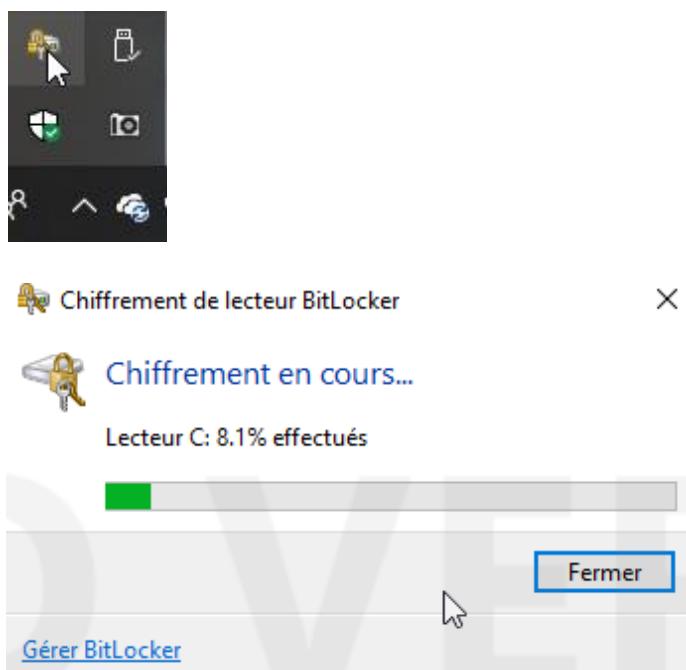


9. Redémarrez l'ordinateur



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.

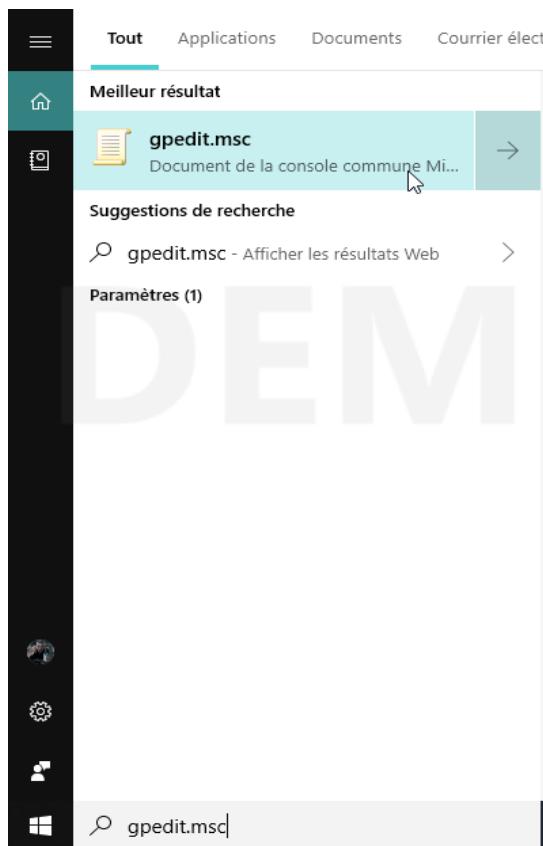
11. Pour connaître l'état d'avancement de la procédure de chiffrement du disque, cliquez sur l'icone cachée à droite de la barre des tâches.



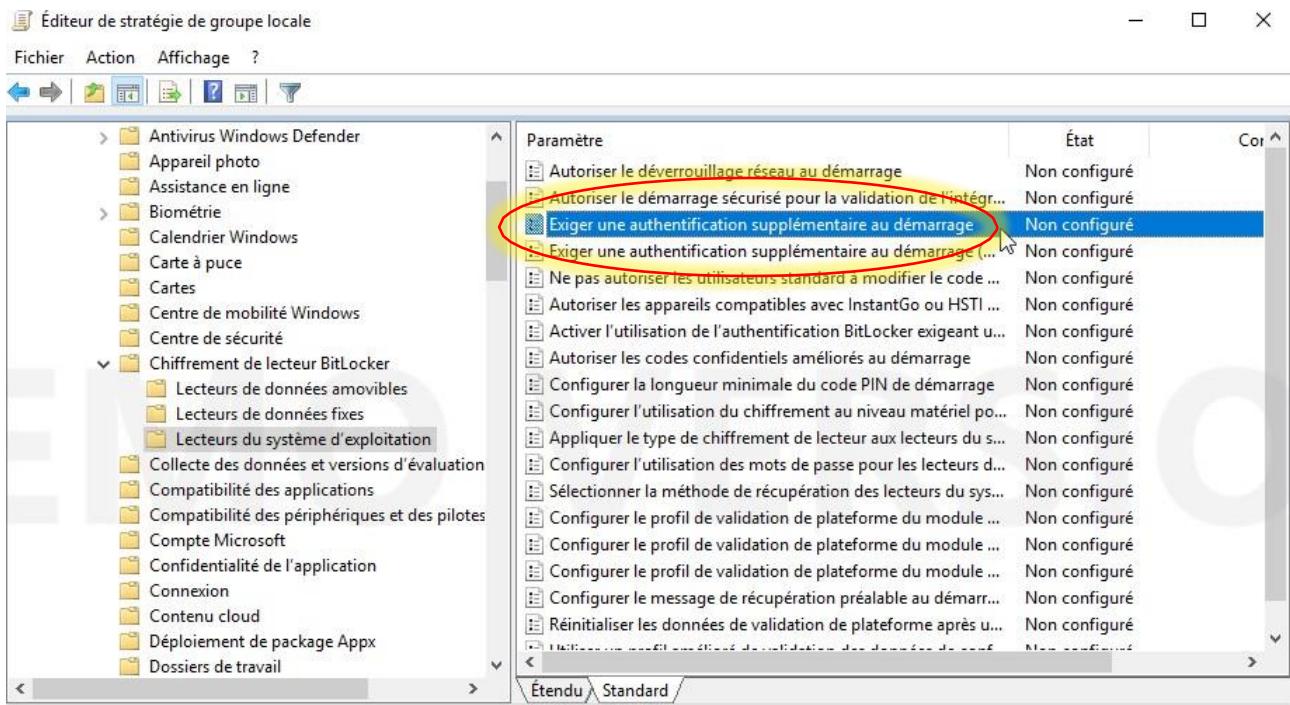
Chiffrement sans puce TPM ou puce TPM désactivée.

Etape 1 : autoriser Bitlocker à ne pas utiliser TPM

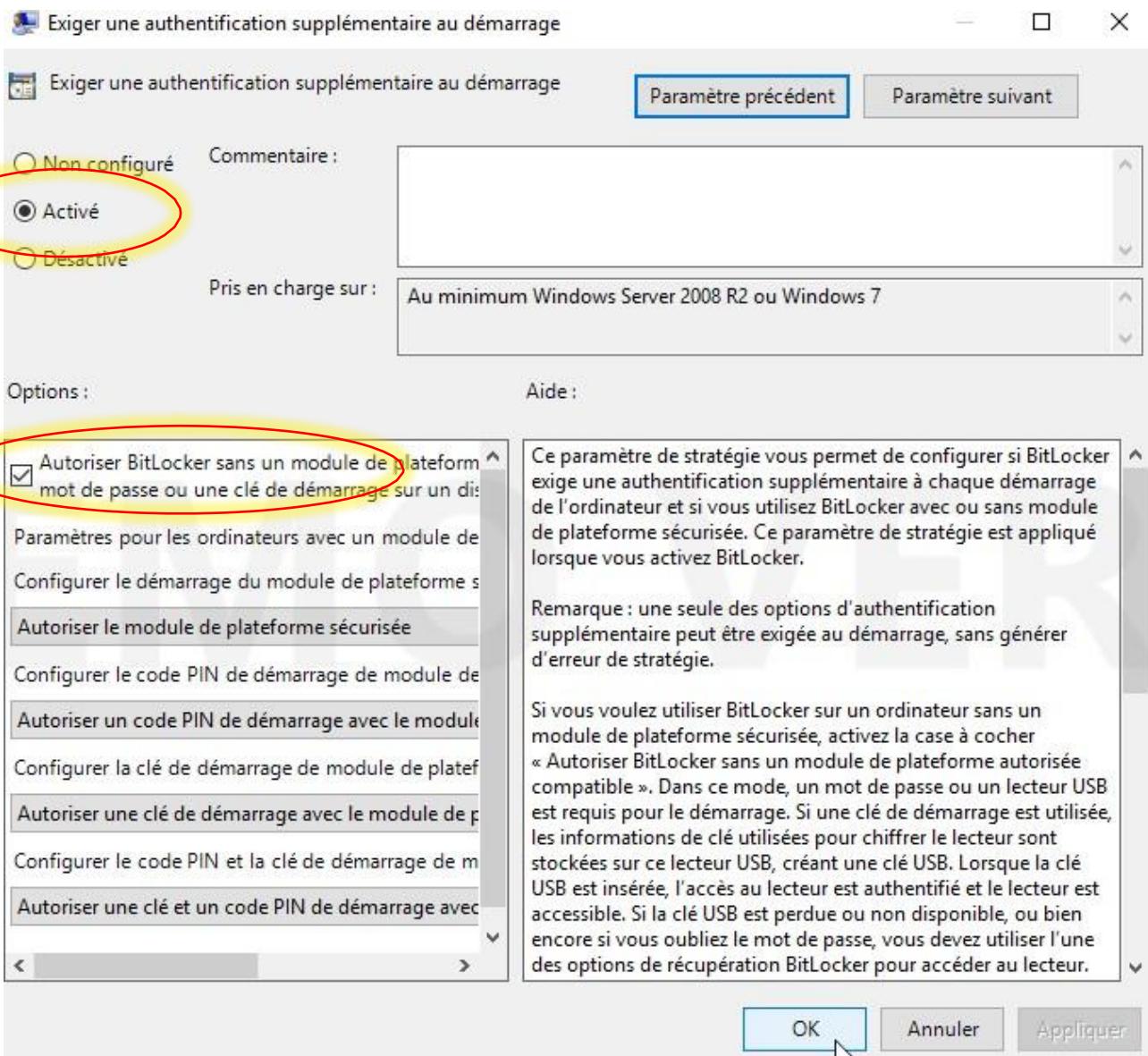
1. Lancez l'éditeur de stratégie de groupe « gpedit.msc »



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 »

Éditeur de stratégie de groupe locale

Fichier Action Affichage ?

Antivirus Windows Defender

Appareil photo

Assistance en ligne

Biométrie

Calendrier Windows

Carte à puce

Cartes

Centre de mobilité Windows

Centre de sécurité

Chiffrement de lecteur BitLocker

- Lecteurs de données amovibles
- Lecteurs de données fixes
- Lecteurs du système d'exploitation

Collecte des données et versions d'évaluation

Compatibilité des applications

Compatibilité des périphériques et des pilotes

Compte Microsoft

Confidentialité de l'application

Connexion

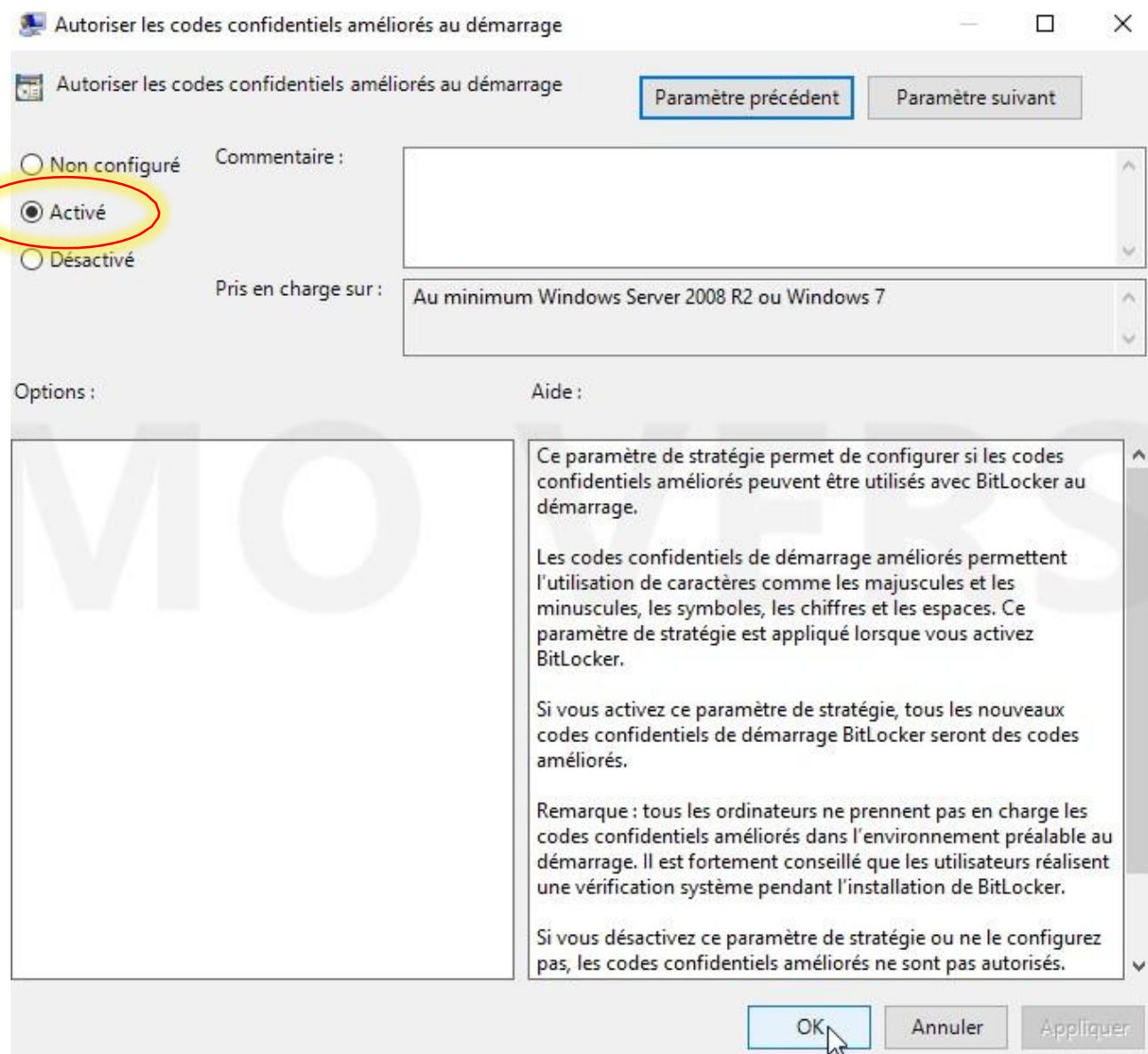
Contenu cloud

Déploiement de package Appx

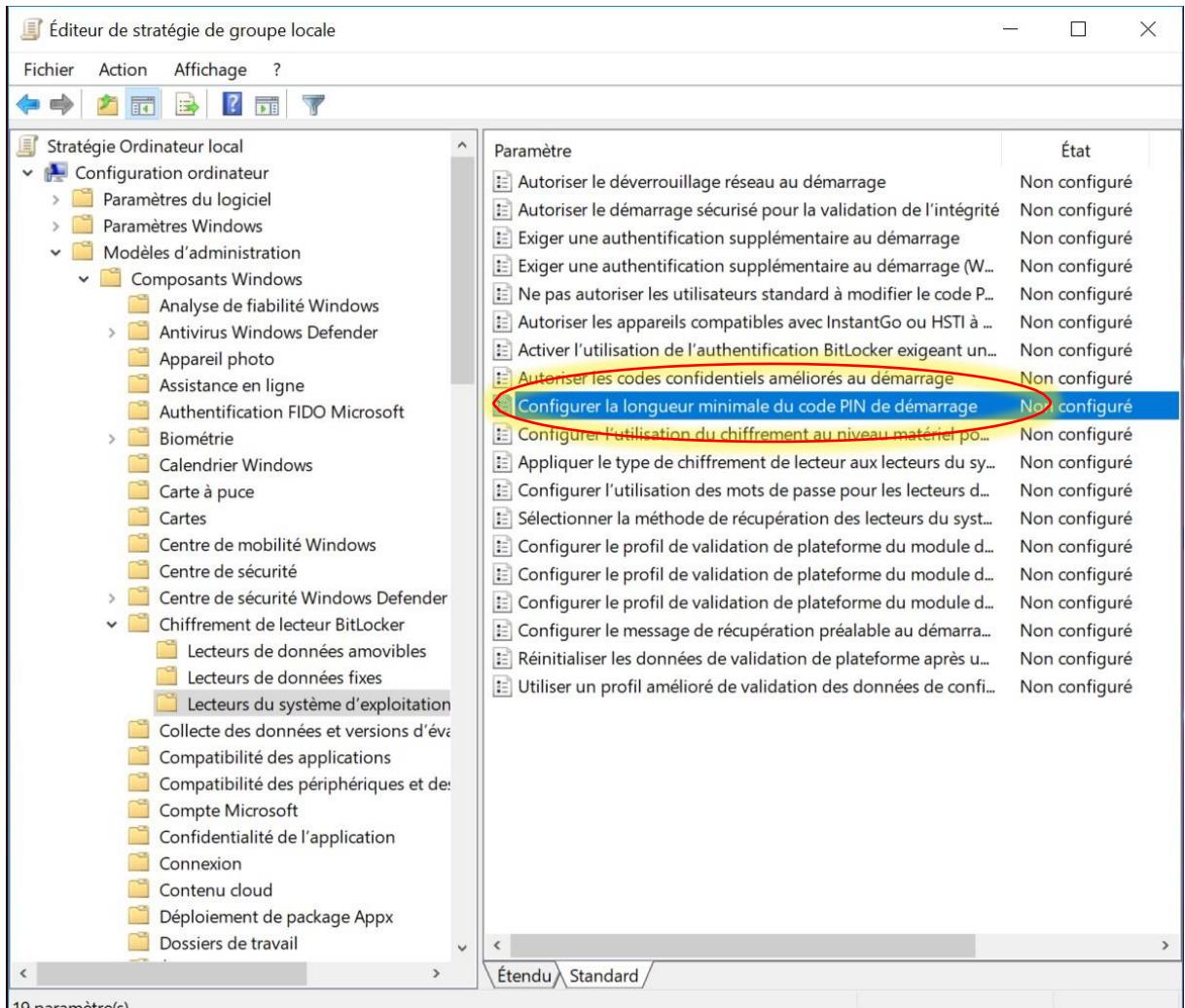
Dossiers de travail

Paramètre	État
Autoriser le déverrouillage réseau au démarrage	Non configuré
Autoriser le démarrage sécurisé pour la validation de l'intégr...	Non configuré
Exiger une authentification supplémentaire au démarrage	Activé
Exiger une authentification supplémentaire au démarrage (...)	Non configuré
Ne pas autoriser les utilisateurs standard à modifier le code ...	Non configuré
Autoriser les appareils compatibles avec InstantGo ou HSTI ...	Non configuré
Activer l'utilisation de l'authentification BitLocker exigeant u...	Non configuré
Autoriser les codes confidentiels améliorés au démarrage	Non configuré
Configurer la longueur minimale du code PIN de démarrage	Non configuré
Configurer l'utilisation du chiffrement au niveau matériel po...	Non configuré
Appliquer le type de chiffrement de lecteur aux lecteurs du s...	Non configuré
Configurer l'utilisation des mots de passe pour les lecteurs d...	Non configuré
Sélectionner la méthode de récupération des lecteurs du sys...	Non configuré
Configurer le profil de validation de plateforme du module ...	Non configuré
Configurer le profil de validation de plateforme du module ...	Non configuré
Configurer le profil de validation de plateforme du module ...	Non configuré
Configurer le message de récupération préalable au démarr...	Non configuré
Réinitialiser les données de validation de plateforme après u...	Non configuré

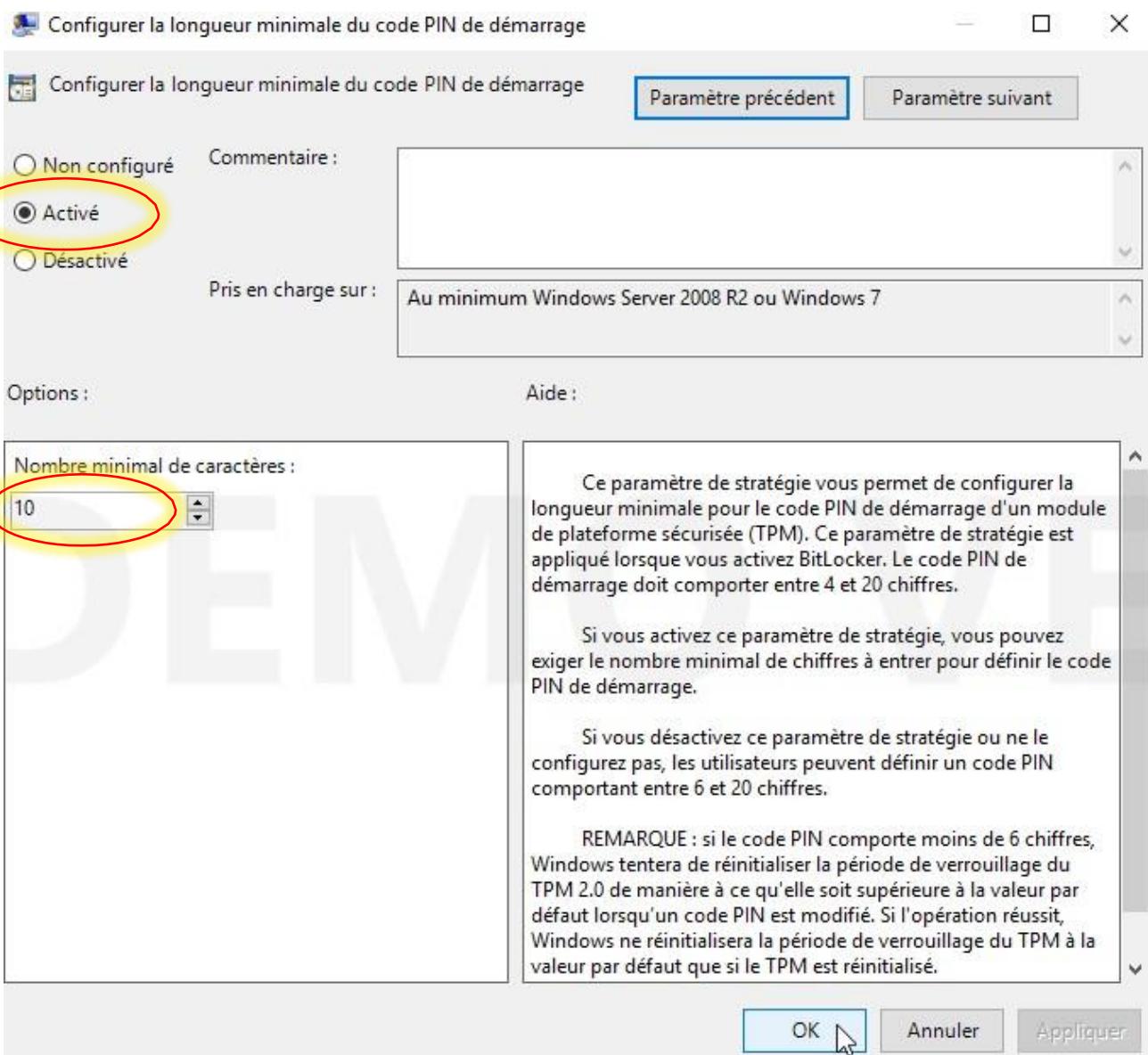
6. Cochez « Activé » puis validez en cliquant sur « OK »



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 »

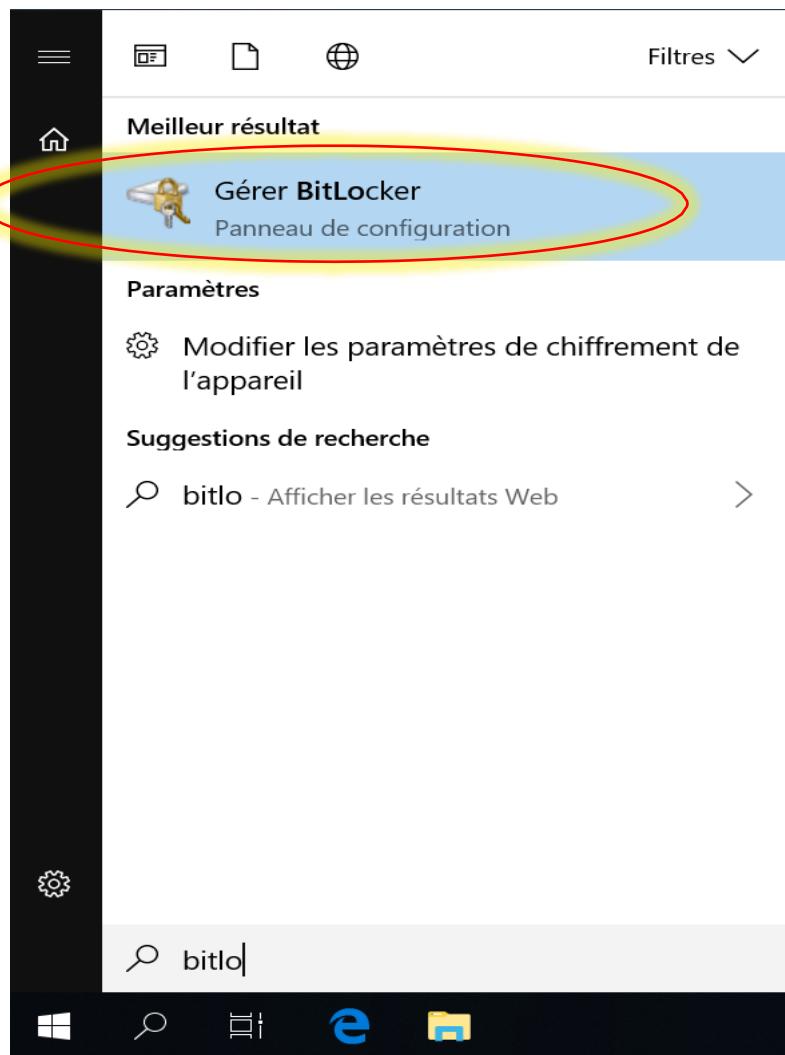


Etape 2 : Activation de Bitlocker et chiffrement du système d'exploitation.

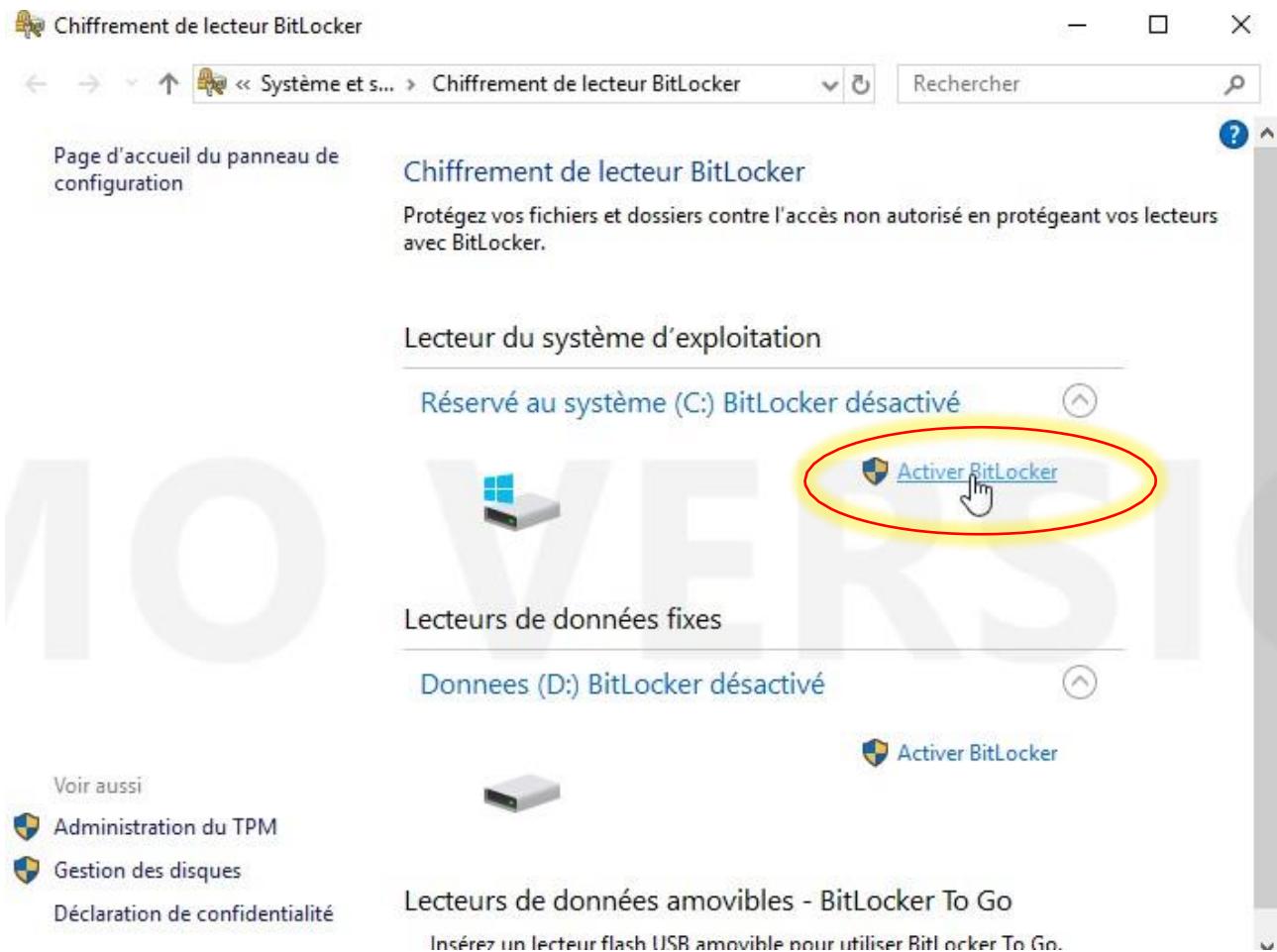
Par défaut, Bitlocker est désactivé.

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

12. Lancez l'outil de gestion de Bitlocker



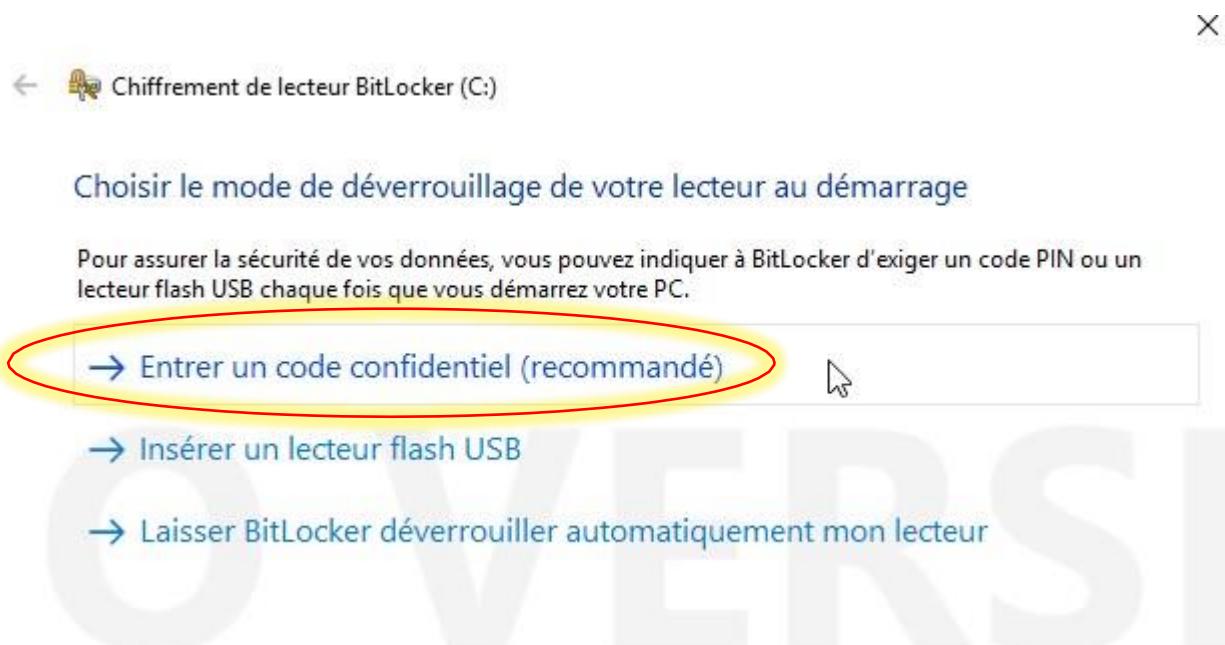
13. Dans la partie « Lecteur du système d'exploitation », cliquez sur « Activer Bitlocker ».



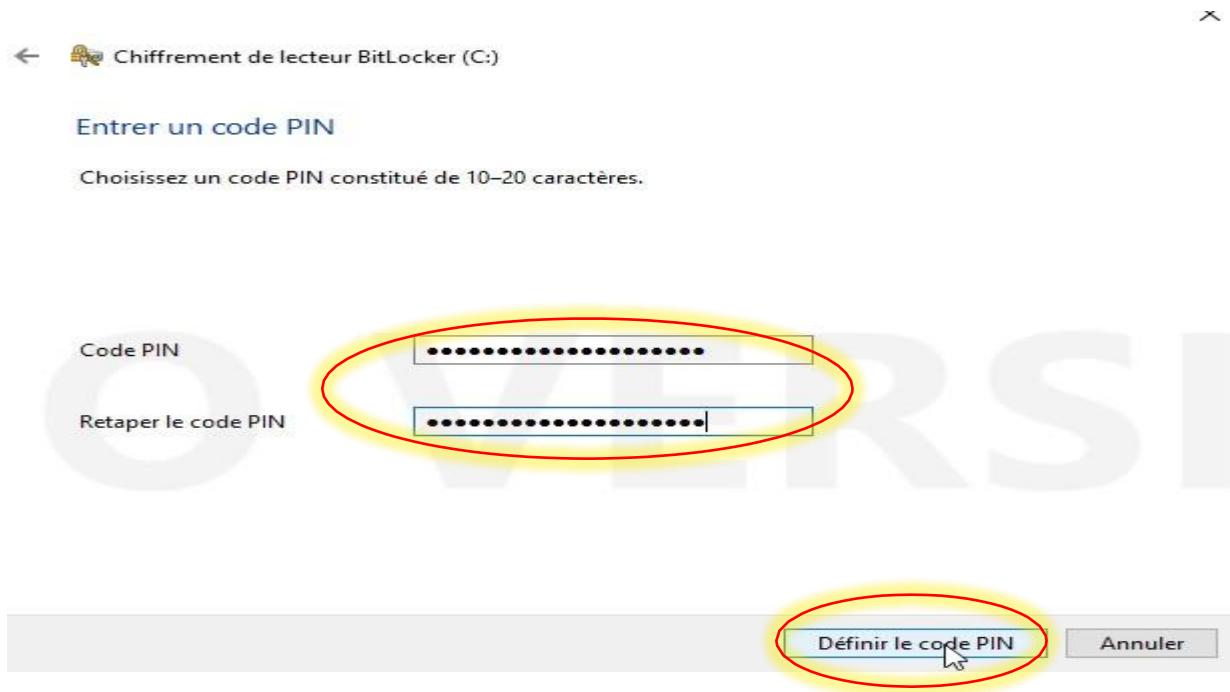
ATTENTION : l'objet de ce document est de chiffrer le lecteur du système d'exploitation. Il est possible de chiffrer un autre disque dur « interne » en utilisant la même méthode.

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

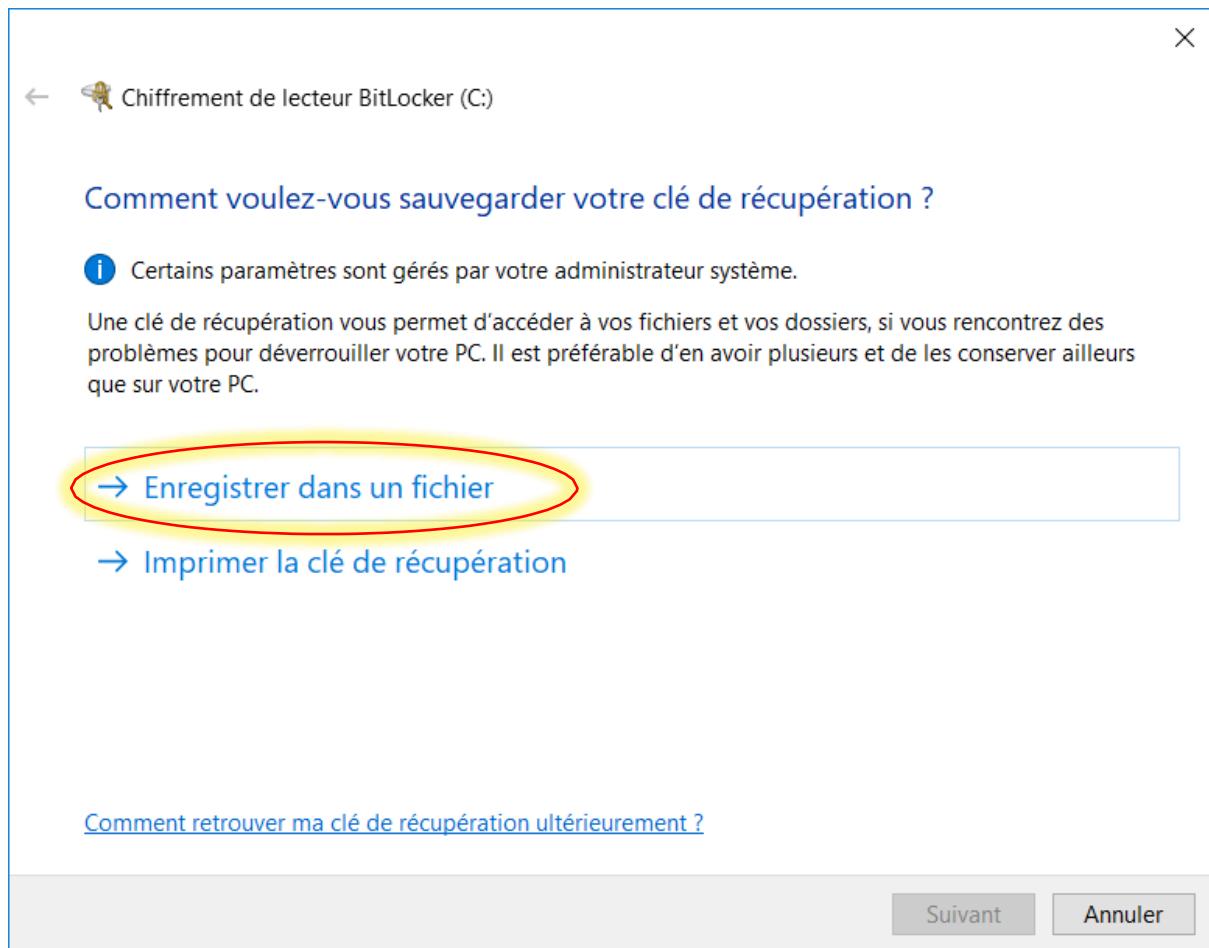
14. Cliquez sur « Entrer un code confidentiel »



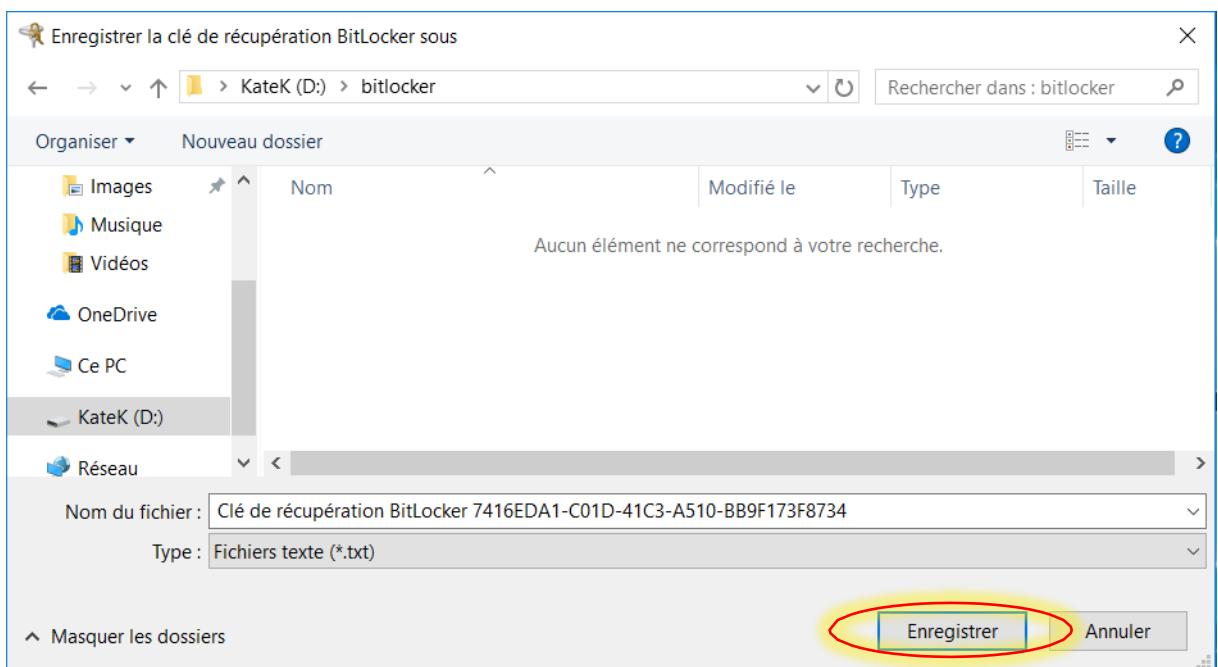
15. Saisissez le code PIN que vous souhaitez utiliser. Validez en cliquant sur « définir le code PIN »



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

The screenshot shows a Windows dialog box titled "Chiffrement de lecteur BitLocker (C:)". At the top right is a close button (X). Below the title, there's a back arrow icon and the text "← Chiffrement de lecteur BitLocker (C:)". The main content area has a blue header "Choisir dans quelle proportion chiffrer le lecteur". A descriptive text explains that BitLocker can encrypt the used disk space or the entire drive. Two radio buttons are shown: one for encrypting used space (unchecked) and one for encrypting the entire drive (checked). At the bottom are "Suivant" and "Annuler" buttons.

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, chiffrerez 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

X

←  Chiffrement de lecteur BitLocker (C:)

Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

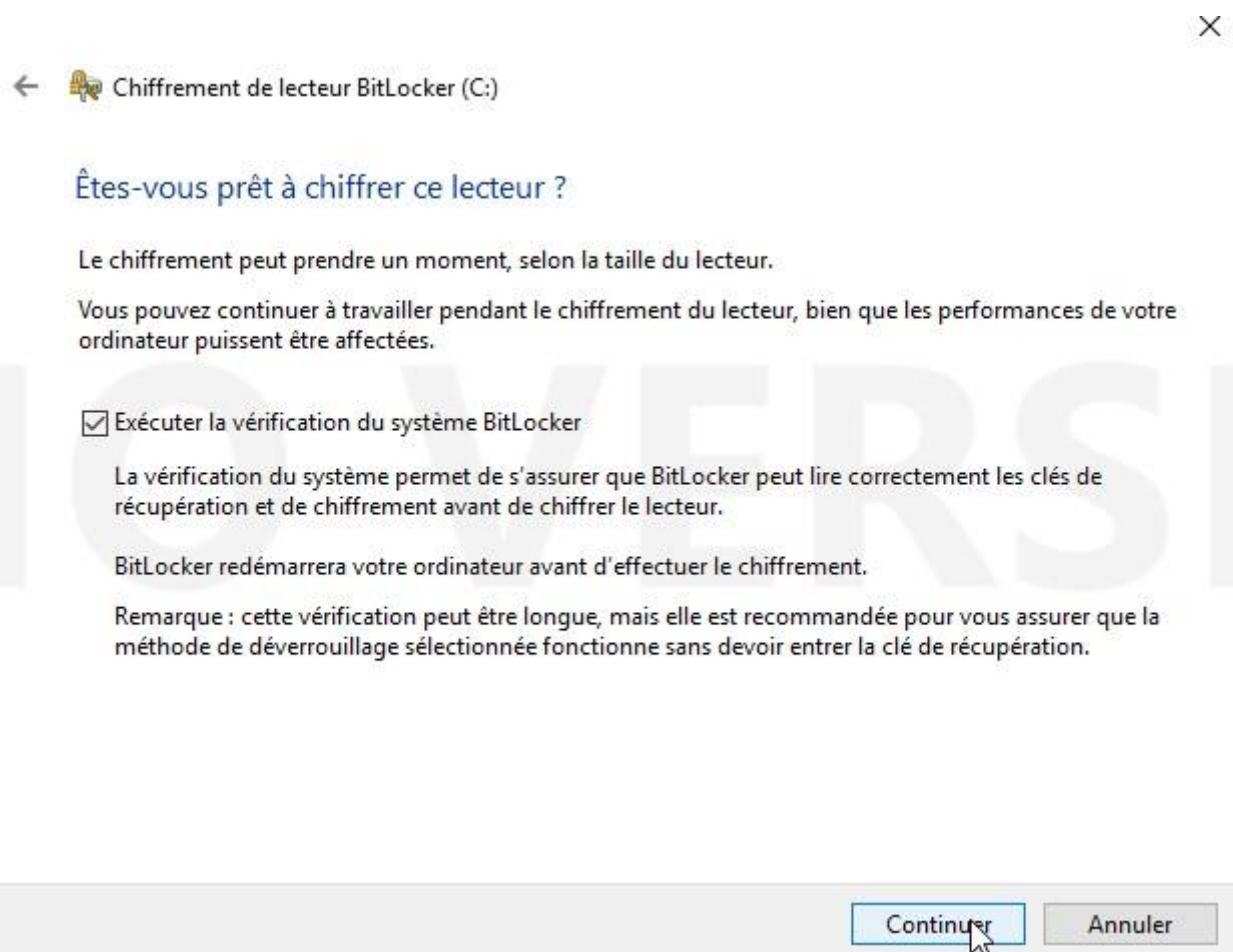
S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

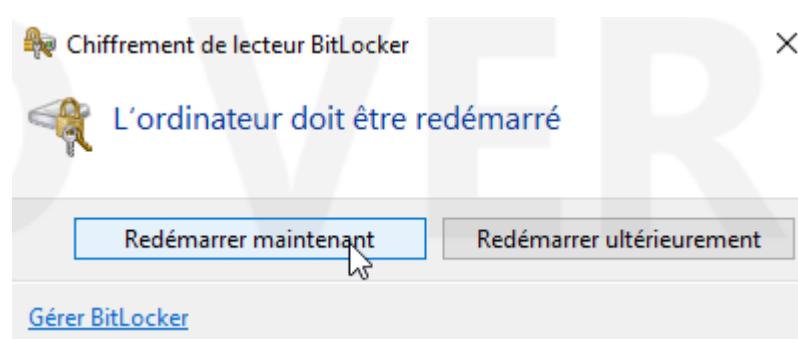
Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)
 Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

[Suivant](#) [Annuler](#)

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'icone cachée à droite de la barre des tâches.

