

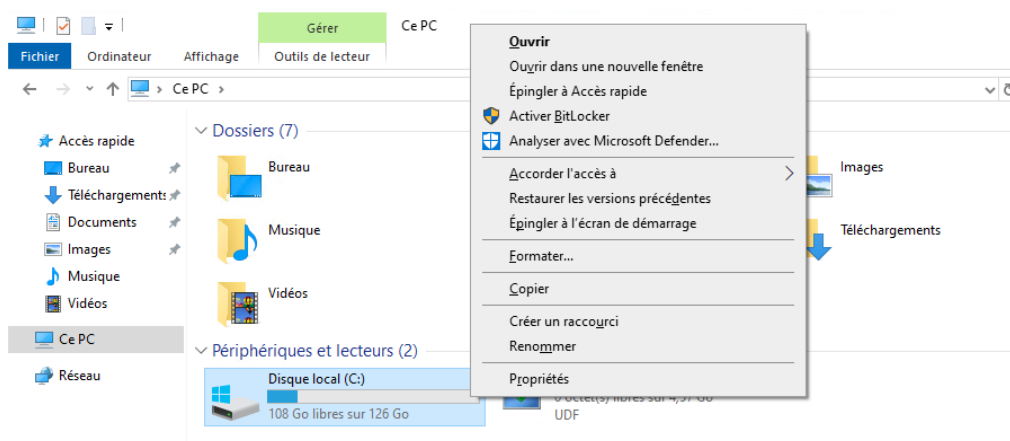
Solution de chiffrement avec Bitlocker

BitLocker est un outil de chiffrement intégré dans les versions professionnelles et supérieures de Windows. Il permet de chiffrer les données sur un disque dur, un lecteur USB ou une partition, afin de protéger ces données contre tout accès non autorisé, même si le périphérique est perdu ou volé.

Chiffrement manuel d'un lecteur avec BitLocker :

Comme nous utilisons uniquement Windows Professionnelle, BitLocker y est directement intégré il suffit donc l'activer et de le configurer.

Pour commencer, nous devons **ouvrir BitLocker** en effectuant un clic droit sur le lecteur que nous souhaitons chiffrer dans l'Explorateur Windows. Dans notre cas, il s'agit du disque **C:** qui contient le système d'exploitation. Ensuite, nous sélectionnons **"Activer BitLocker"**.



Il est essentiel de sauvegarder la clé de récupération. Nous avons la possibilité de l'enregistrer sur un compte Microsoft, dans un fichier ou de l'imprimer. Dans notre cas, nous choisirons **"Imprimer la clé de récupération"** au format PDF.

←

Chiffrement de lecteur BitLocker (C:)

×

Comment voulez-vous sauvegarder votre clé de récupération ?

Une clé de récupération vous permet d'accéder à vos fichiers et vos dossiers, si vous rencontrez des problèmes pour déverrouiller votre PC. Il est préférable d'en avoir plusieurs et de les conserver ailleurs que sur votre PC.

→ Enregistrer sur votre compte Microsoft

→ Enregistrer dans un fichier

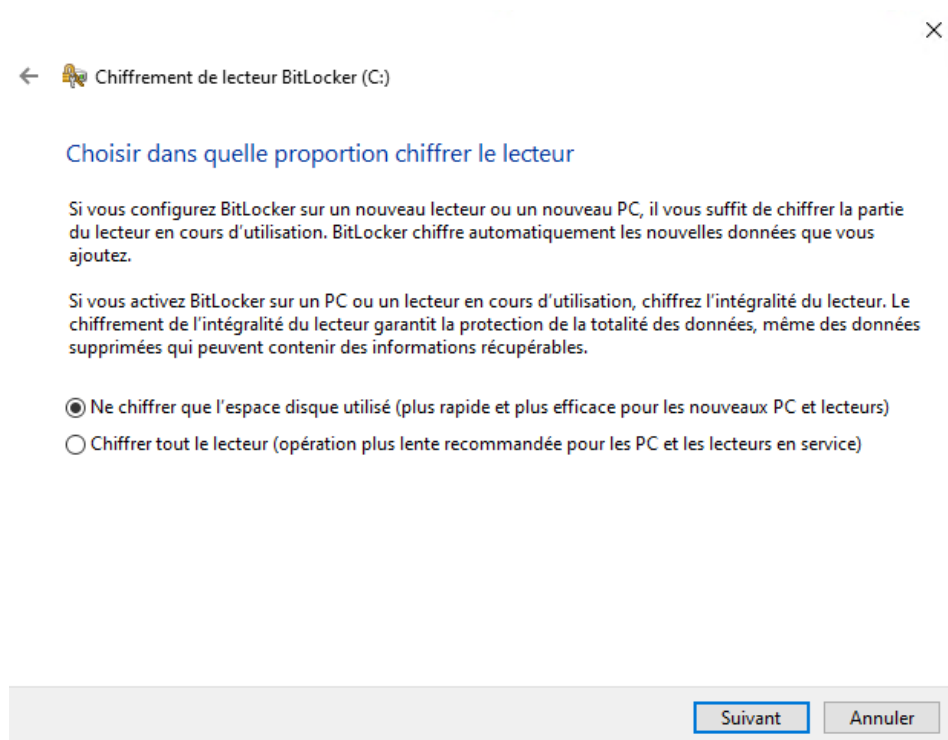
→ Imprimer la clé de récupération

Comment retrouver ma clé de récupération ultérieurement ?

Suivant

Annuler

Il nous est ensuite demandé de choisir dans quelle proportion on veut chiffrer le lecteur. Ici nous choisirons **"Ne chiffrer que l'espace disque utilisé"**.



← 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.

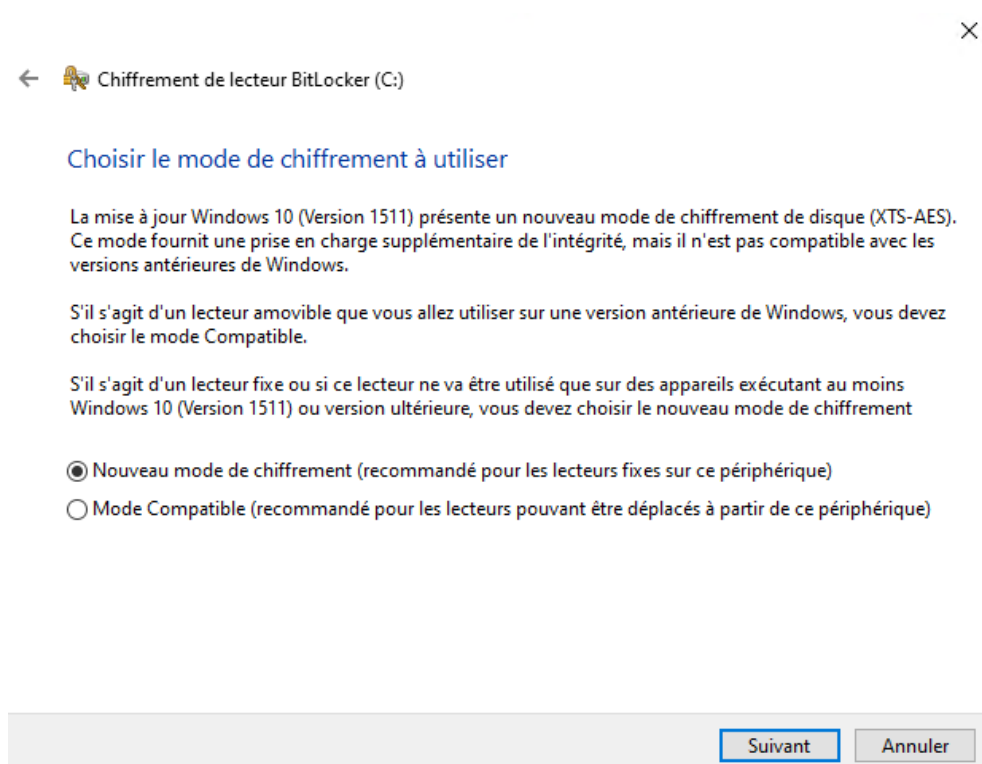
Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

☒ 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

Pour le mode de chiffrement à utiliser on choisit **"Nouveau mode de chiffrement"** car on chiffre le lecteur C: qui est un lecteur fixe.



← 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.

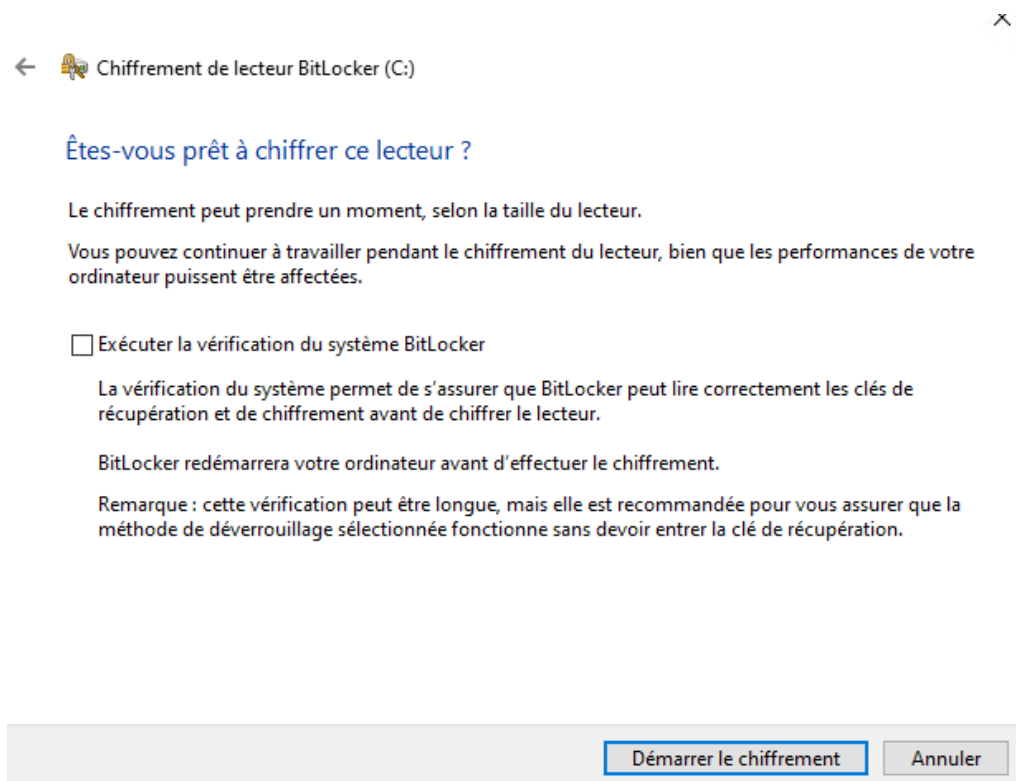
S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

☒ 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

On peut exécuter la vérification du système BitLocker, ceci redémarrera le PC. Dans notre cas nous ne l'avons pas faite et avons fait démarrer le chiffrement.





BitLocker entame alors le processus de chiffrement du lecteur. La durée de cette opération peut varier en fonction de la taille du lecteur et de la puissance de l'ordinateur. Il faudra maintenant la clé disponible dans le PDF crée précédemment pour désactiver le chiffrement.

Lecteur du système d'exploitation

C: Chiffrement BitLocker en cours



-  [Sauvegarder votre clé de récupération](#)
-  [Désactiver BitLocker](#)

Lecteurs de données fixes

Lecteurs de données amovibles - BitLocker To Go

Insérez un lecteur flash USB amovible pour utiliser BitLocker To Go.