Disques SSD chiffrés de Kingston

Activer et désactiver BitLocker eDrive pour utiliser le chiffrement matériel

Introduction

Ce document explique comment activer et désactiver la fonction BitLocker eDrive de Microsoft pour utiliser le chiffrement matériel sur un disque SSD Kingston. Cette procédure peut être appliquée sur les SSD Kingston qui supportent les normes TCG OPAL 2.0 et IEEE1667. Cette procédure fonctionne uniquement avec les disques SSD Kingston supportant les normes TCG OPAL 2.0 et IEEE1667. En cas de doute, veuillez contacter l'assistance technique Kingston : www.kingston.com/support

Dans ce document, eDrive signifie BitLocker eDrive. La procédure indiquée peut varier selon les versions et les mises à jour de Windows.

Configuration requise

- SSD Kingston avec les fonctions de sécurité TCG Opal 2.0 et IEEE1667
- Logiciel Kingston SSD Manager https://www.kingston.com/ssdmanager
- Équipement système et BIOS supportant les fonctions de sécurité TCG Opal 2.0 et IEEE1667

Configuration requise SE / BIOS

- Windows 8 et 8.1 (Pro/Enterprise)
- Windows 10 (Pro, Enterprise et Education)
- Windows Server 2012

Remarque : Tous les disques SSD chiffrés doivent être connectés à des contrôleurs non-RAID pour fonctionner normalement sous Windows 8, 10 et/ou Server 2012

Pour utiliser un disque SSD chiffré sous Windows 8, 10 ou Windows Server 2012 comme **disque de données** :

- Le disque ne doit pas être initialisé.
- La sécurité du disque doit être désactivée.

Pour les disques SSD chiffrés utilisés comme **disques de démarrage** :

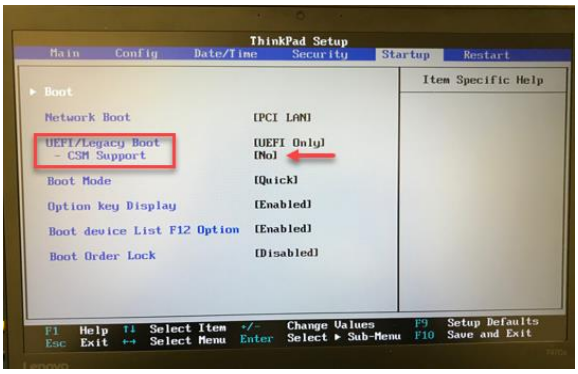
- Le disque ne doit pas être initialisé.
- La sécurité du disque doit être désactivée.
- L'ordinateur doit être basé sur la norme UEFI 2.3.1 et le protocole EFI_STORAGE_SECURITY_COMMAND_PROTOCOL doit être défini. (Ce protocole permet aux programmes exécutés par les services de démarrage EFI d'envoyer des commandes de protocole au disque).
- Sur l'ordinateur, le CSM (Compatibility Support Module ou module de support de compatibilité) doit être désactivé dans l'UEFI.
- L'ordinateur doit être configuré pour lancer systématiquement le démarrage natif dans l'UEFI.

Pour en savoir plus, veuillez lire l'article de Microsoft :
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Activez eDrive sur le disque SSD de démarrage.

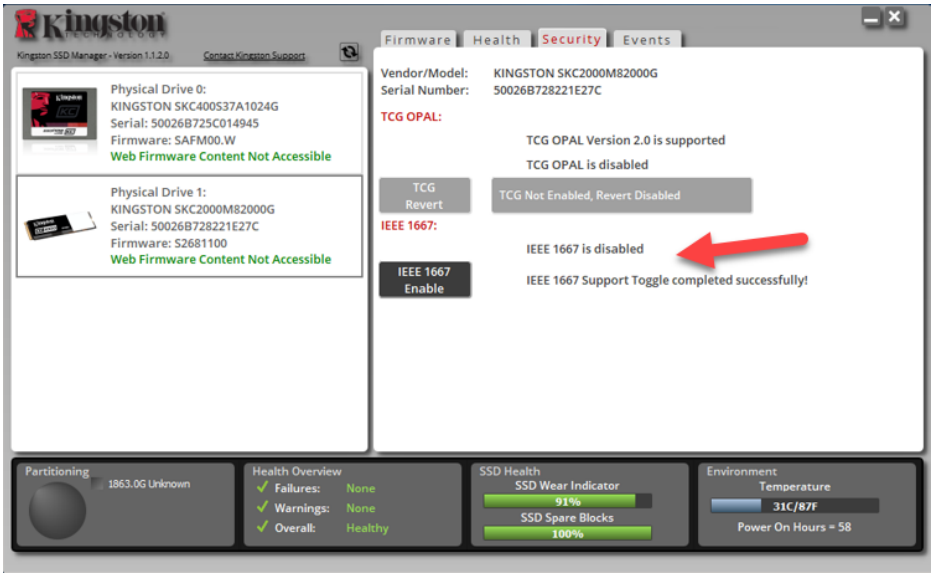
Configuration du BIOS

1. Consultez la documentation du fabricant de votre ordinateur pour confirmer que le BIOS est basé sur UEFI 2.3.1. Le protocole EFI_STORAGE_SECURITY_COMMAND_PROTOCOL doit être défini.
2. Ouvrez le BIOS et désactivez le CSM (Compatibility Support Module ou module de support de compatibilité).

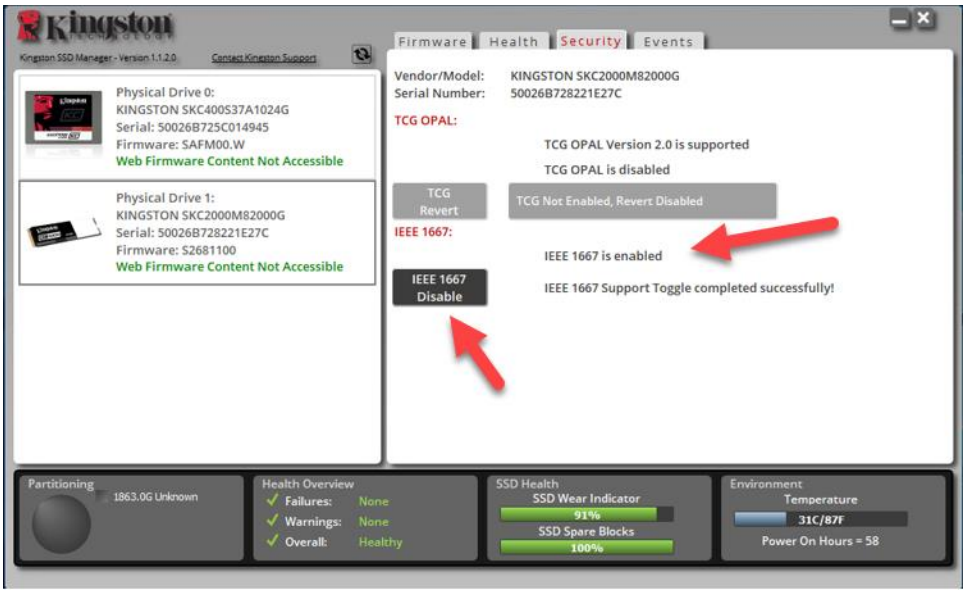


Préparation du disque

1. Si vous n'avez pas déjà téléchargé le logiciel SSD Manager (KSM) de Kingston, veuillez le faire maintenant. https://www.kingston.com/ssdmanager
2. Dans le logiciel KSM, utilisez la fonction d'effacement sécurisé "Secure Erase" pour supprimer toutes les données sur le disque SSD cible. Vous pouvez choisir une autre méthode standard pour effectuer cette procédure d'effacement.
3. Montez le SSD cible comme disque secondaire pour confirmer le statut IEEE1667. Le disque doit être en mode **Désactivé**.



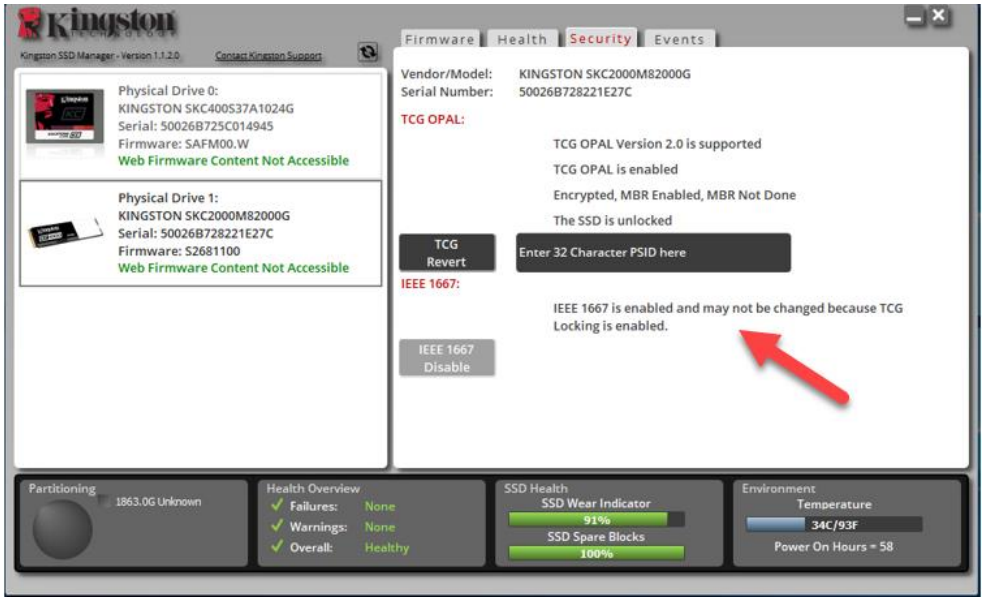
4. Cliquez sur le bouton IEEE1667 et **Activer** cette fonction. Confirmez que la fonction est correctement activée.



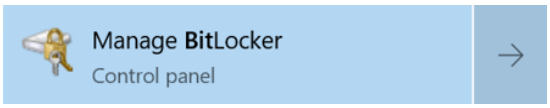
Installation du système d'exploitation (SE)

Remarque : Ne pas cloner le système d'exploitation sur votre SSD cible*. Le clonage du SE sur le disque cible empêche d'activer le chiffrement matériel en utilisant eDrive. Le SE doit être installé comme une première installation sur le disque cible pour autoriser l'utilisation du chiffrement matériel avec eDrive.*

1. Installez le SE requis sur le SSD cible.
2. Après l'installation du SE, installez le logiciel Kingston SSD manager (KSM) et lancez-le. Confirmez que le message suivant est affiché dans l'onglet Sécurité de l'application :
   "IEEE 1667 est activé et ne peut pas être modifié parce que TCG Locking est activé."

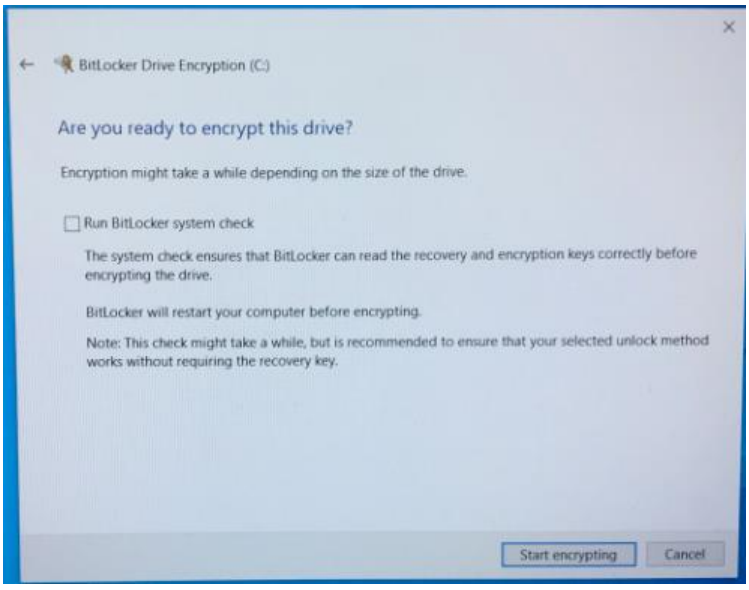


3. Utilisez la clé Windows pour chercher **Manage BitLocker**, puis lancez cette application.

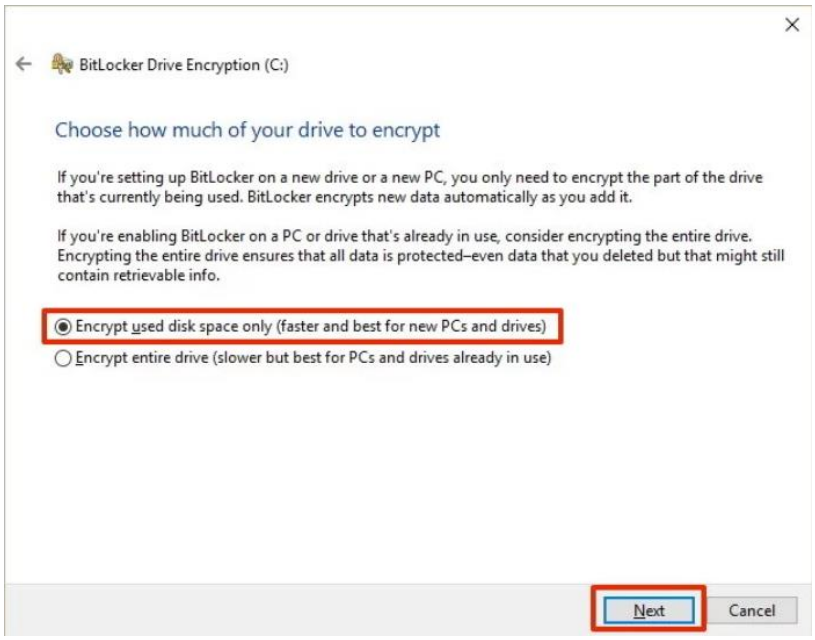


4. Sélectionnez **Activer BitLocker** dans la fenêtre de l'Explorateur.

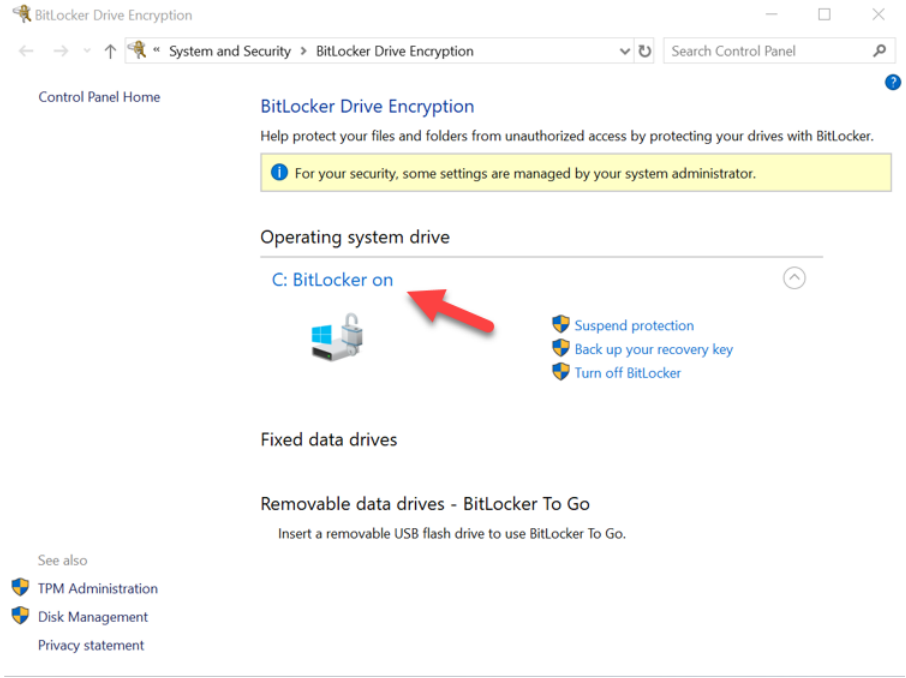
5. Continuez en suivant les instructions pour configurer le SSD cible. Lorsque le système vous le demande, sélectionnez la commande **Démarrer le chiffrement.** Par défaut, l'option **Lancer BitLocker Système** est activée. Nous recommandons de vérifier que ce paramètre est coché avant de continuer. Si ce paramètre n'est pas coché, vous pourrez vérifier si le chiffrement matériel est activé sans avoir à redémarrer le système.



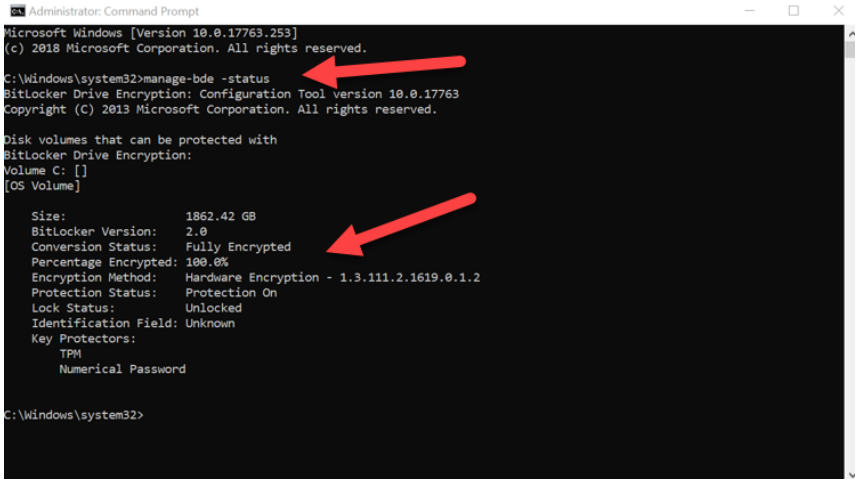
Remarque : Si un message vous demande de "Choisir le volume partiel du disque à chiffrer", cela signifie souvent que le disque SSD ne permet PAS d'utiliser le chiffrement matériel, mais seulement le chiffrement logiciel.



6. Si la procédure vous le demande, redémarrez le système, puis lancez à nouveau **Manage BitLocker** pour confirmer le statut du chiffrement du disque SSD.



7. Vous pouvez aussi vérifier le statut du chiffrement du SSD chiffré en ouvrant **cmd.exe** où vous saisirez la ligne suivante : **manage-bde -status**

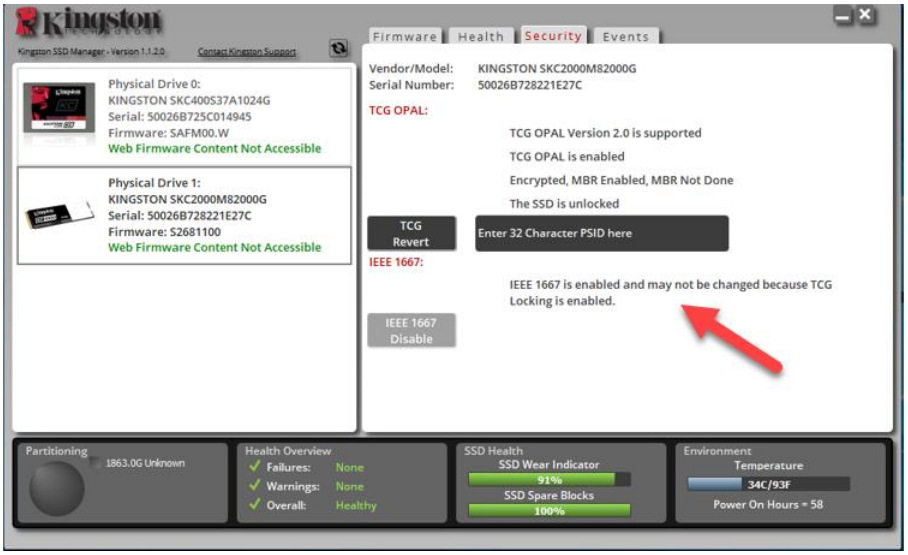


Activer Microsoft eDrive sous Windows 10 (version 1903+)

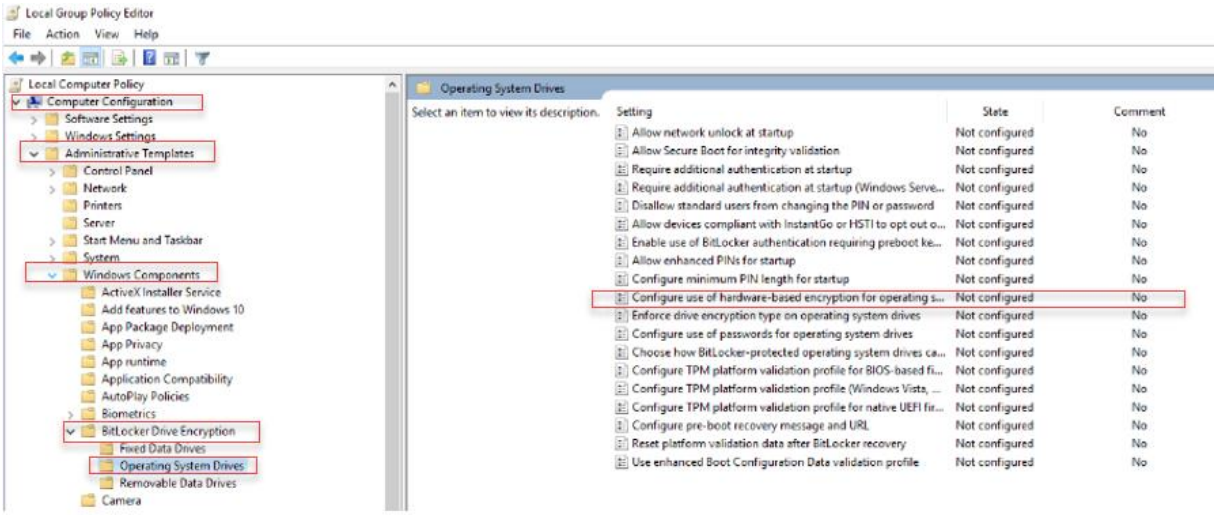
Microsoft a modifié le comportement par défaut de Windows 10 appliqué au chiffrement eDrive depuis la version 1903 de Windows 10. Pour activer eDrive avec cette version, et possiblement avec les versions ultérieures, vous devez exécuter ***gpedit*** *pour activer le chiffrement matériel.*

Remarque : Ne pas cloner le système d'exploitation sur votre SSD cible*. Le clonage d'un SE sur le disque cible vous empêchera d'activer le chiffrement matériel en utilisant eDrive. Vous devez installer le SE comme une première installation sur le disque cible pour utiliser le chiffrement matériel avec eDrive.*

1. Installez le SE requis sur le SSD cible.
2. Après l'installation du SE, installez le logiciel Kingston SSD manager (KSM) et lancez-le. Confirmez que le message suivant est affiché dans l'onglet Sécurité de l'application :
   "IEEE 1667 est activé et ne peut pas être modifié parce que TCG Locking est activé."

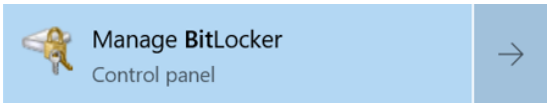


3. Lancez gpedit.msc pour modifier le paramètre du chiffrement.
    a. Allez jusqu'à **Modèles administratifs > Composants Windows > Chiffrement de disque BitLocker > Disques de système d'exploitation**
    b. Ensuite, sélectionnez **Configurer l'utilisation du chiffrement matériel pour les systèmes d'exploitation.**
    c. **Activez** la fonction, puis **Appliquer** le paramètre.



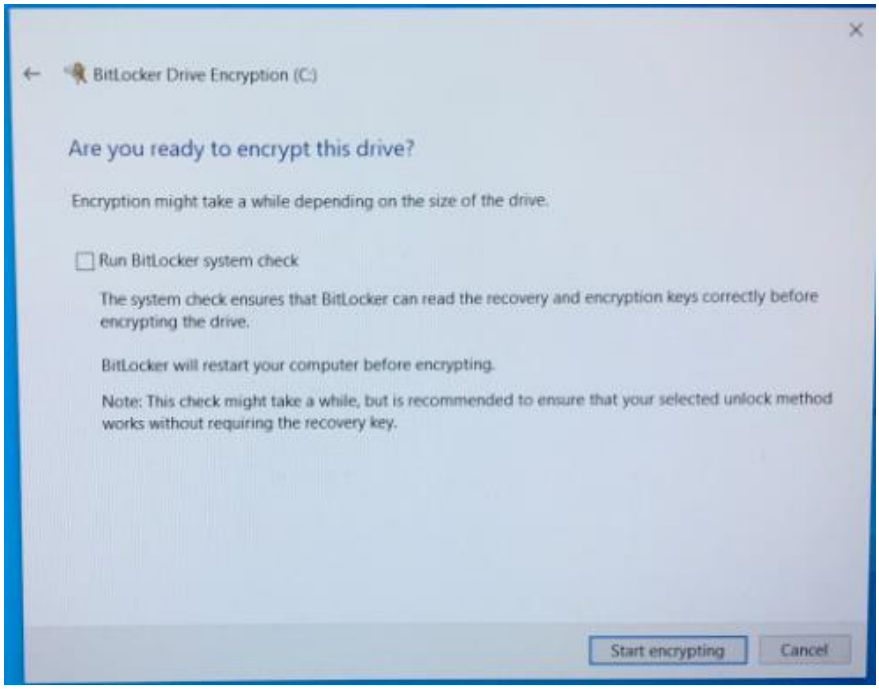
Remarque : Pour activer eDrive sur des disques de données, autres que le disque du système d'exploitation, vous pouvez appliquer les mêmes paramètres en sélectionnant : **Modèles administratifs > Composants Windows > Chiffrement de disque BitLocker > Disques de données fixes > Configurer l'utilisation du chiffrement matériel pour les disques de données fixes (Activer puis Appliquer).**

4. Utilisez la clé Windows pour chercher **Manage BitLocker** puis lancez cette application.

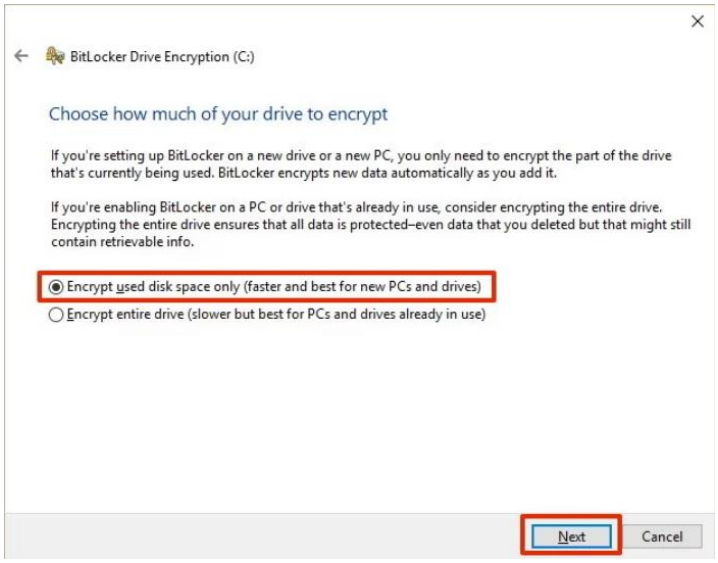


5. Sélectionnez **Activer BitLocker** dans la fenêtre de l'Explorateur.

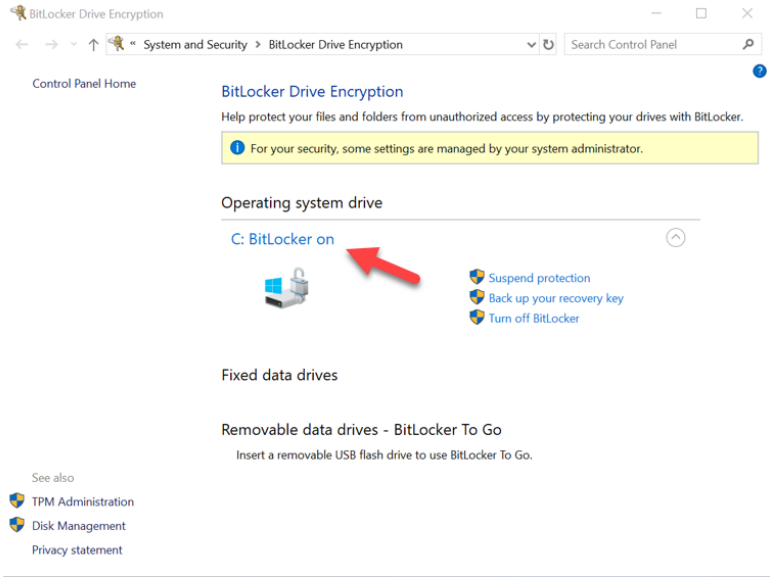
6. Continuez en suivant les instructions pour configurer le SSD cible. Lorsque le système vous le demande, sélectionnez la commande **Démarrer le chiffrement.** Par défaut, l'option **Lancer BitLocker Système** est activée. Nous recommandons de vérifier que ce paramètre est coché avant de continuer. Si ce paramètre n'est pas coché, vous pourrez vérifier si le chiffrement matériel est activé sans avoir à redémarrer le système.



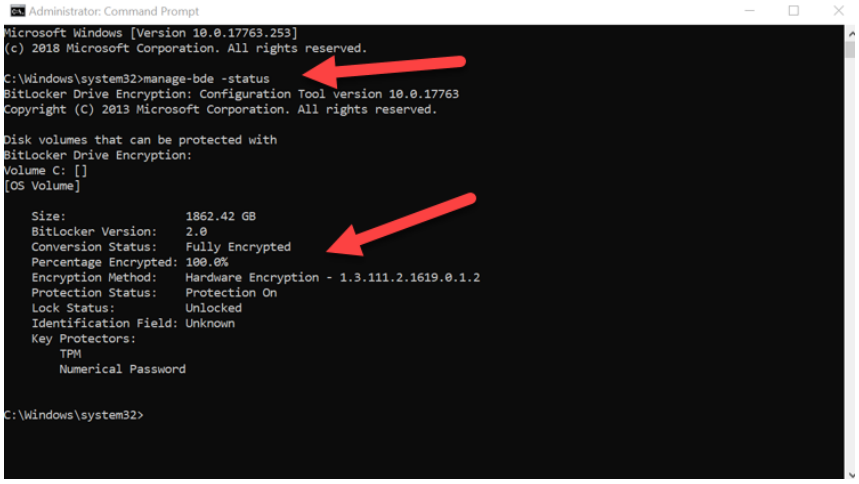
Remarque : Si un message vous demande de "Choisir le volume partiel du disque à chiffrer", cela signifie souvent que le disque SSD ne permet PAS d'utiliser le chiffrement matériel, mais seulement le chiffrement logiciel.



7. Si la procédure vous le demande, redémarrez le système, puis lancez à nouveau **Manage BitLocker** pour confirmer le statut du chiffrement du disque SSD.



8. Vous pouvez aussi vérifier le statut du chiffrement du SSD chiffré en ouvrant **cmd.exe** où vous saisirez la ligne suivant : **manage-bde -status**



Désactiver le support Microsoft eDrive

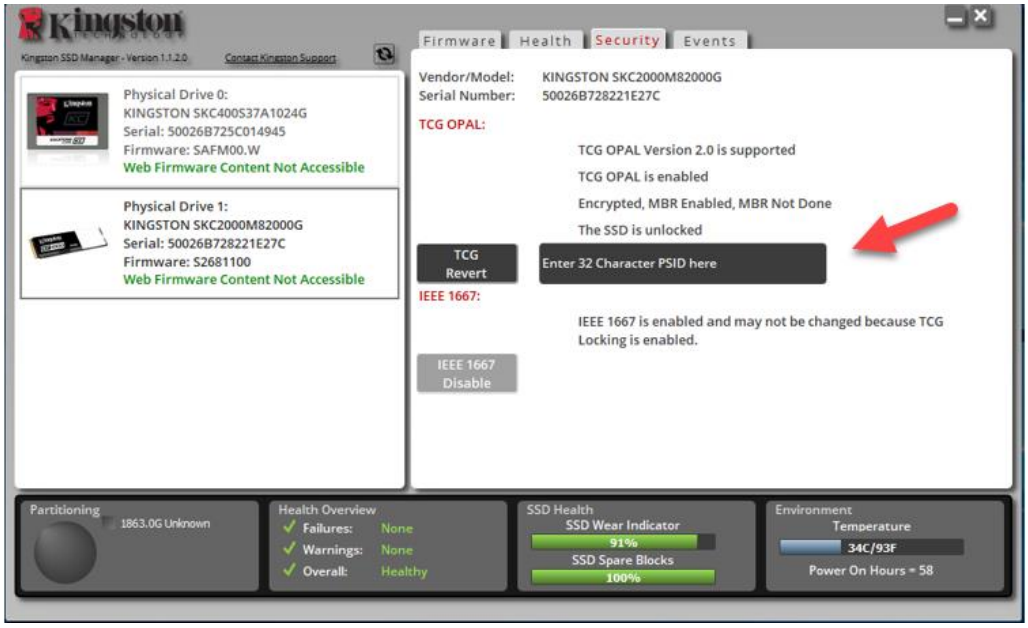
Pour effacer le contenu de vos disques SSD, et désactiver le support BitLocker eDrive sur chaque disque, veuillez suivre les instructions ci-dessous.

Remarque : Ce processus réinitialisera votre disque SSD et LA TOTALITÉ DES DONNÉES PRÉSENTES SUR CE DISQUE SERONT DÉFINITIVEMENT PERDUES.

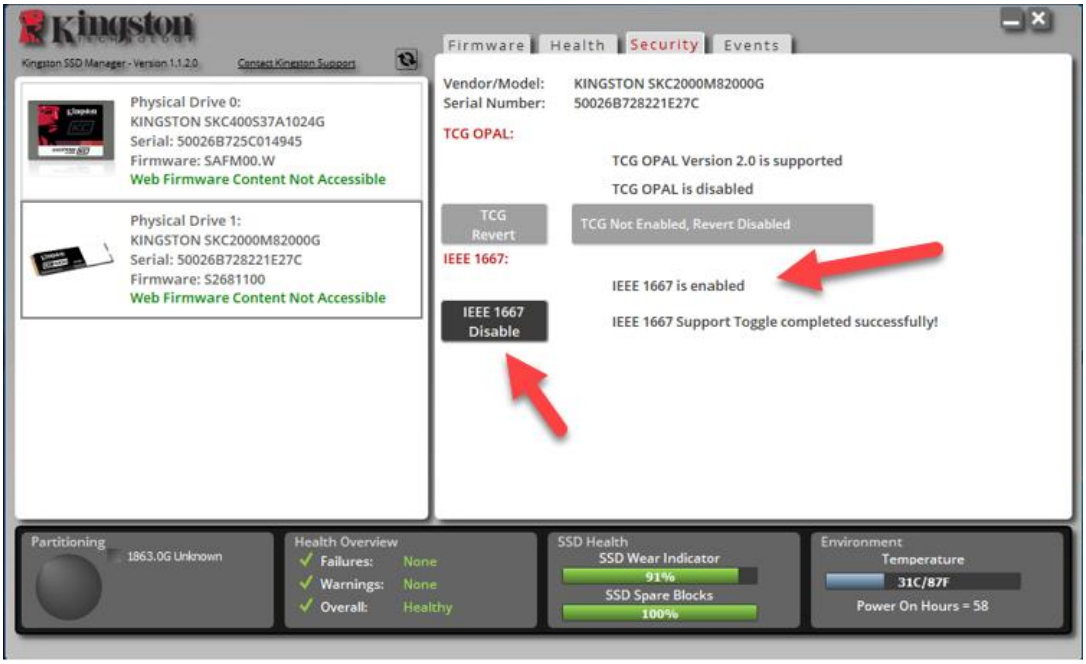
1. Prenez note de la valeur PSID du disque SSD cible. Cette valeur est inscrite sur l'étiquette.

Ex. : Valeur PSID KC2000

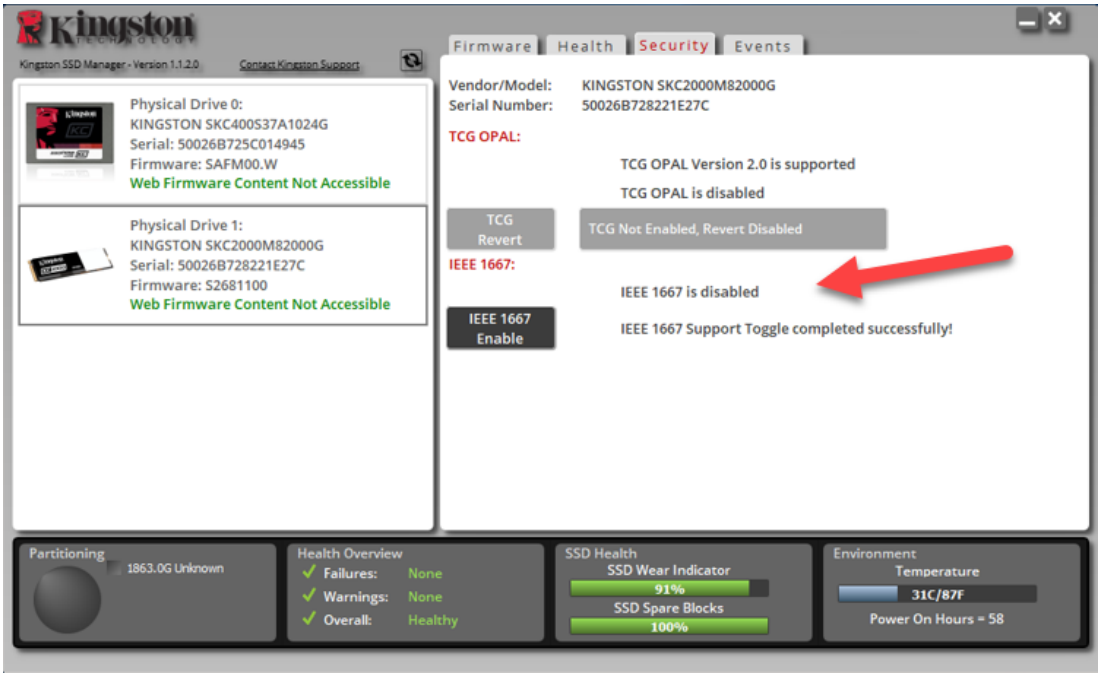
2. Montez le disque SSD cible comme disque secondaire, puis lancez le logiciel Kingston SSD Manager (KSM).
3. Sélectionnez l'onglet **Sécurité**, exécutez la fonction **TCG Revert** en saisissant la valeur PSID à 32 chiffres obtenues à l'étape 1. Sélectionnez **TCG Revert.** Lorsque l'opération est terminée, le message de réussite de **TCG Revert est** affiché. Si ce message n'apparaît pas, saisissez à nouveau la valeur PSID et lancez à nouveau la fonction TCG Revert.



4. Lorsque le disque est correctement rétabli, vous avez la possibilité de désactiver le support IEEE1667. Veuillez sélectionner **Désactiver IEEE1667** et attendez que le message “Changement du support IEEE1667 correctement effectué” soit affiché.



5. Confirmez que le support IEEE1667 est désactivé.



6. Votre disque SSD cible est prêt à être utilisé.