SSD crittografati Kingston

Abilitazione e disabilitazione di BitLocker con eDrive per l'utlilizzo delle funzioni di crittografia hardware

Introduzione

Questo documento descrive in che modo abilitare e disabilitare la funzione eDrive di BitLocker di Microsoft, per sfruttare appieno le funzionalità di crittografia hardware del vostro SSD Kingston. Questa procedura è applicabile agli SSD Kingston che supportano la funzionalità TCG Opal 2.0 e il set di funzionalità IEEE1667. Qualora non si dovesse disporre di un SSD Kingston dotato di tecnologia TCG Opal 2.0 e supporto alle funzionalità IEEE1667, la procedura descritta in questo documento non sarà applicabile. In caso di dubbi, contattare il servizio di supporto tecnico di Kingston, al link seguente: www.kingston.com/support

Questo documento farà riferimento a Microsoft BitLocker con eDrive con la semplice definizione "eDrive" all'interno del presente documento. Le procedure descritte sotto possono cambiare in base alle versioni e agli aggiornamenti di Windows.

Requisiti di sistema

- SSD Kingston SSD che utilizzano il set di funzionalità di sicurezza TCG Opal 2.0 e IEEE1667
- Software Kingston SSD Manager https://www.kingston.com/ssdmanager
- Supporto per hardware di sistema e BIOS funzionalità di sicurezza TCG Opal 2.0 e IEEE1667

Requisiti SO / BIOS

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

Nota: Tutti i drive a stato solido crittografati devono essere collegati a controller non-RAID per poter funzionare correttamente con i sistemi operativi Windows 8, 10, e/o Server 2012

Per utilizzare i drive a stato solido crittografati su Windows 8, 10 o Windows Server 2012 come **drive per dati**:

- Il drive deve essere in modalità non inizializzata.
- Il drive deve essere impostato con stato di sicurezza inattivo.

Nel caso di drive a stato solido crittografati utilizzati come **unità di avvio**:

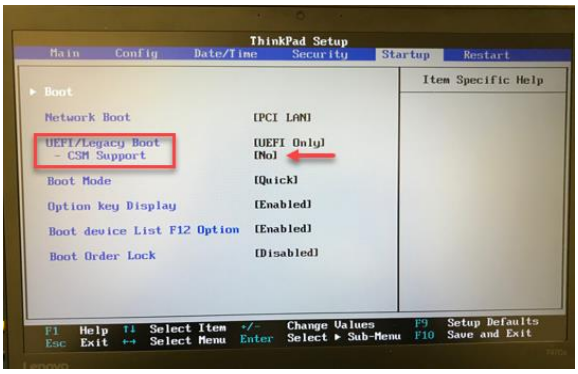
- Il drive deve essere in modalità non inizializzata.
- Il drive deve essere impostato con stato di sicurezza inattivo.
- Il computer deve essere basato su UEFI 2.3.1 e avere il protocollo UEFI_STORAGE_SECURITY_COMMAND_PROTOCOL configurato. (questo protocollo è utilizzato per consentire ai programmi di operare nell'ambiente dei servizi di avvio EFI, per inviare i comandi del protocollo di sicurezza al drive).
- Il computer deve avere l'opzione CSM (Compatibility Support Module) disabilitata nell'UEFI.
- L'avvio del computer deve sempre essere effettuato nativamente dall'UEFI.

Per ulteriori informazioni, fare riferimento all'articolo specifico di Microsoft sull'argomento, situato qui: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Abilitazione di Microsoft eDrive sull'SSD di avvio

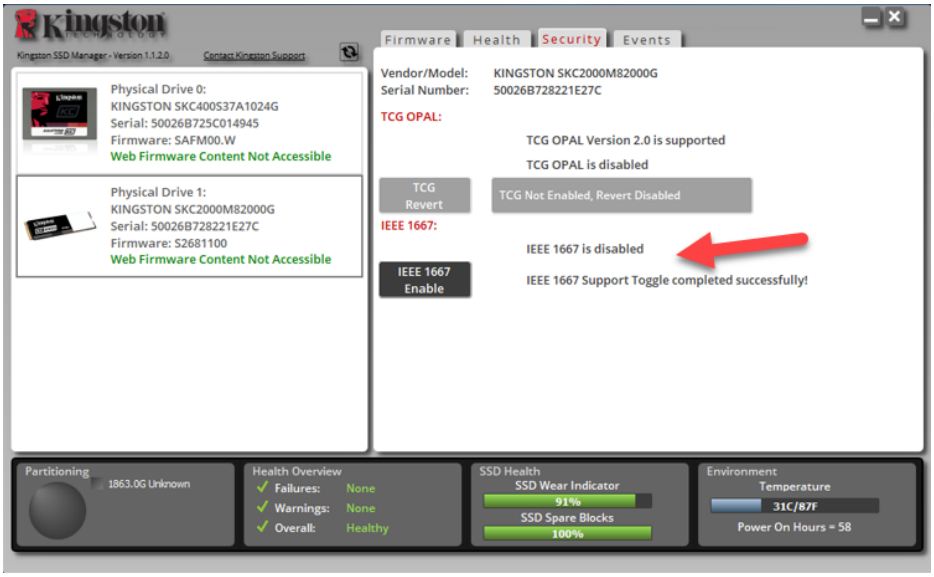
Configurazione BIOS

1. Consultare la documentazione del produttore, per confermare che il BIOS di sistema sia basato su UEFI 3.2.1 e che abbia il protocollo UEFI_STORAGE_SECURITY_COMMAND_PROTOCOL configurato.
2. Accedere al BIOS e disabilitare il CSM (Compatibility Support Module)

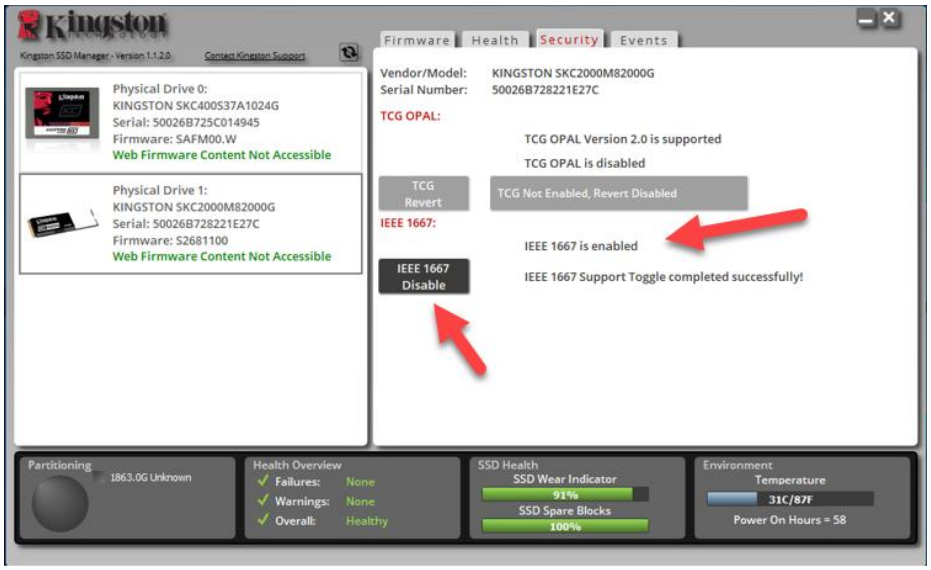


Preparazione del drive

1. Se non avete ancora scaricato Kingston SSD Manager (KSM), sarà necessario scaricarlo. https://www.kingston.com/ssdmanager
2. Effettuare la cancellazione sicura dell'SSD di destinazione mediante il software KSM, oppure mediante altri metodi standard.
3. Installare un SSD di destinazione come disco secondario per confermare lo stato della certificazione IEEE1667. Il drive deve essere impostato in modalità **Disabilitata**.



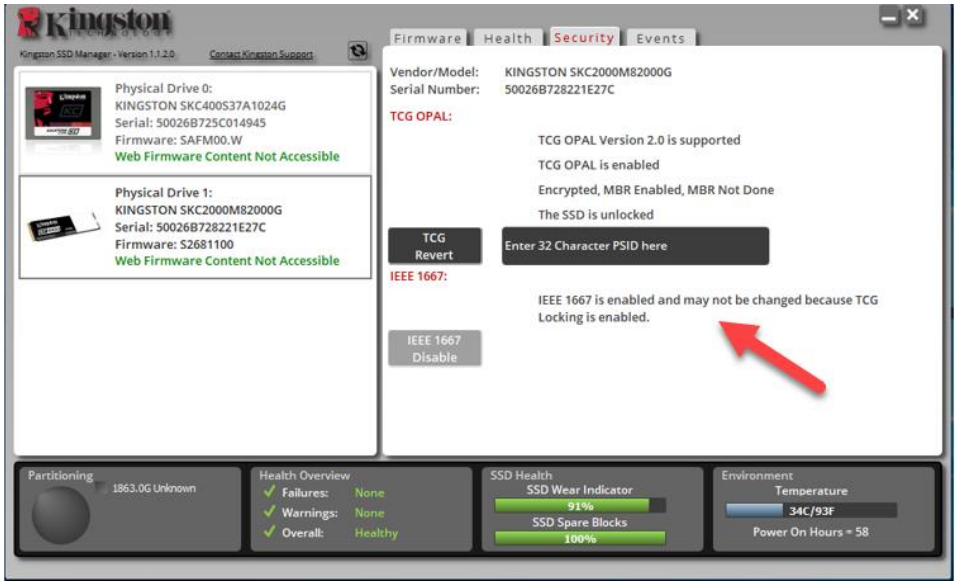
4. Selezionare il pulsante IEEE1667 e quindi impostare la modalità **Abilitato**. Assicurarsi che la funzione sia stata attivata correttamente.



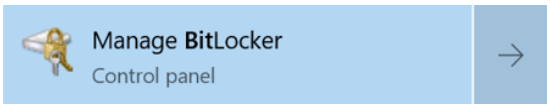
Installazione del sistema operativo (SO)

Nota: Evitare di clonare un sistema operativo sull'SSD target*. La clonazione di un sistema operativo su un SSD target non consente di abilitare la crittografia hardware mediante eDrive. Al fine di poter utilizzare la crittografia hardware con eDrive sarà necessario implementare una nuova installazione del sistema operativo sull'SSD di destinazione.*

1. Installare il sistema operativo supportato sull'SSD di destinazione.
2. Dopo che il sistema operativo è stato installato, installare Kingston SSD Manager (KSM), eseguire KSM e assicurarsi che sia presente il seguente messaggio sulla scheda "Sicurezza" dell'applicazione: *"IEEE 1667 is enabled an may not be changed because TCG Locking is enabled." (IEEE 1667 è abilitato e non può essere modificato in quanto il blocco TCG è abilitato).*

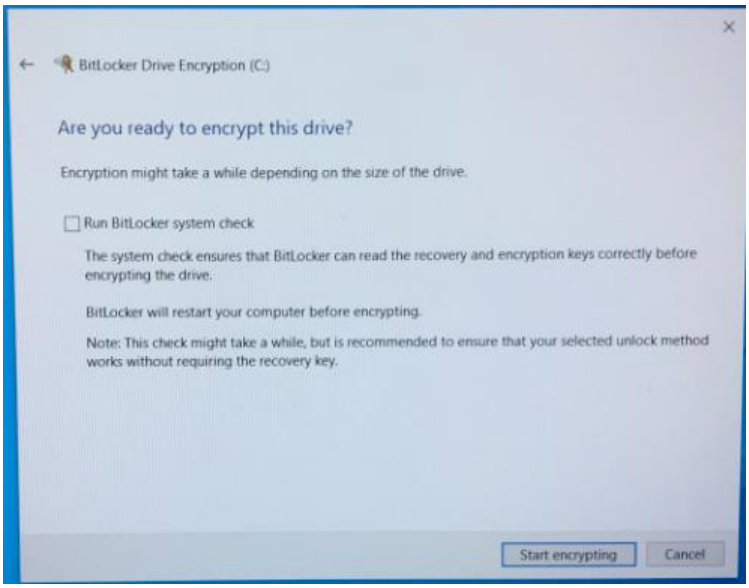


3. Utilizzare il tasto Windows per cercare l'opzione **Gestione BitLocker**; quindi, eseguire l'applicazione.

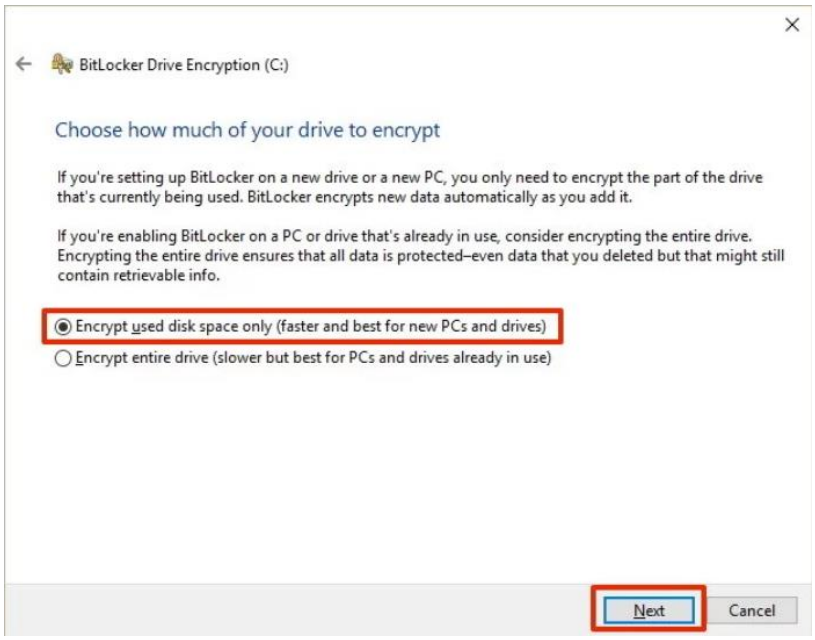


4. Selezionare l'opzione **Attiva BitLocker**, dalla schermata di Esplora risorse.

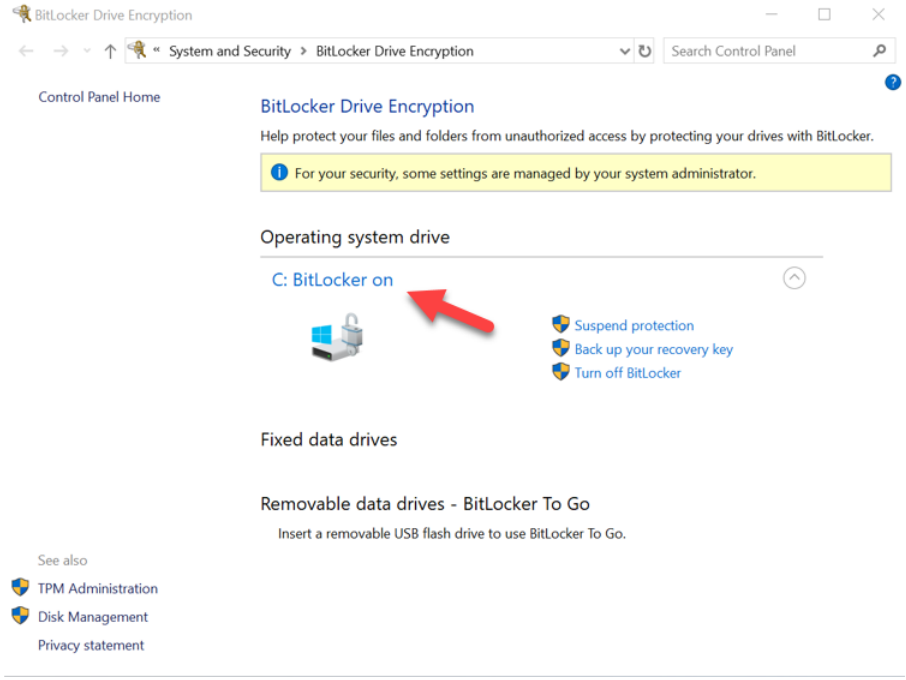
5. Proseguire seguendo le istruzioni della procedura guidata, fino alla completa configurazione dell'SSD di destinazione. Quando richiesto, selezionare l'opzione **"Inizia crittografazione".** L'impostazione selezionata di default è **Esegui controllo sistema Bitlocker**. Si consiglia di proseguire la procedura con questa opzione abilitata. Tuttavia, quando tale opzione non è selezionata, sarà possibile confermare se si dispone di crittografia hardware senza alcuna necessità di effettuare un riavvio.



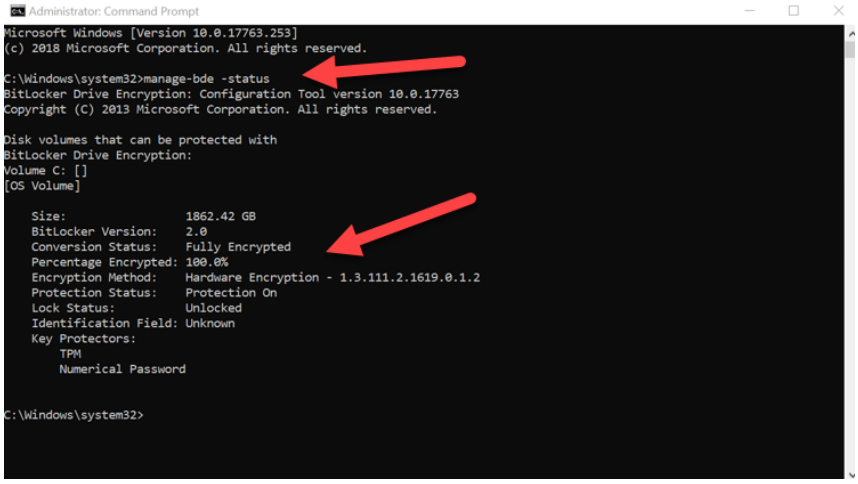
Nota: Se viene visualizzata una schermata che richiede all'utente di "Selezionare la dimensione del drive da crittografare", ciò spesso indica che l'SSD di destinazione NON è in grado di abilitare la funzione di crittografia hardware, ma soltanto quella software.



6. Se necessario, riavviare il sistema e quindi riavviare l'applicazione **Gestione BitLocker**, per verificare lo stato della crittografia sull'SSD di destinazione.



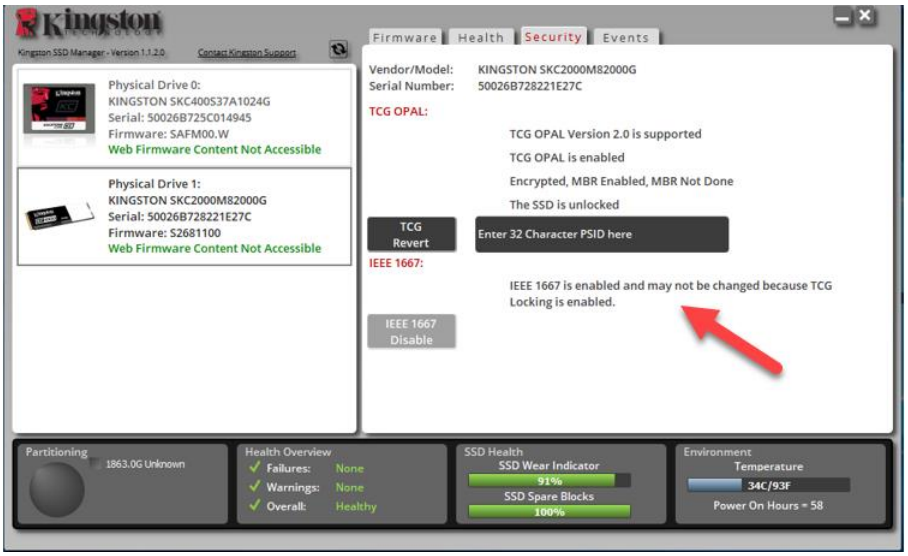
7. È anche possibile verificare la crittografia sull'SSD di destinazione aprendo il comando **cmd.exe** e digitando il comando: **manage-bde -status**



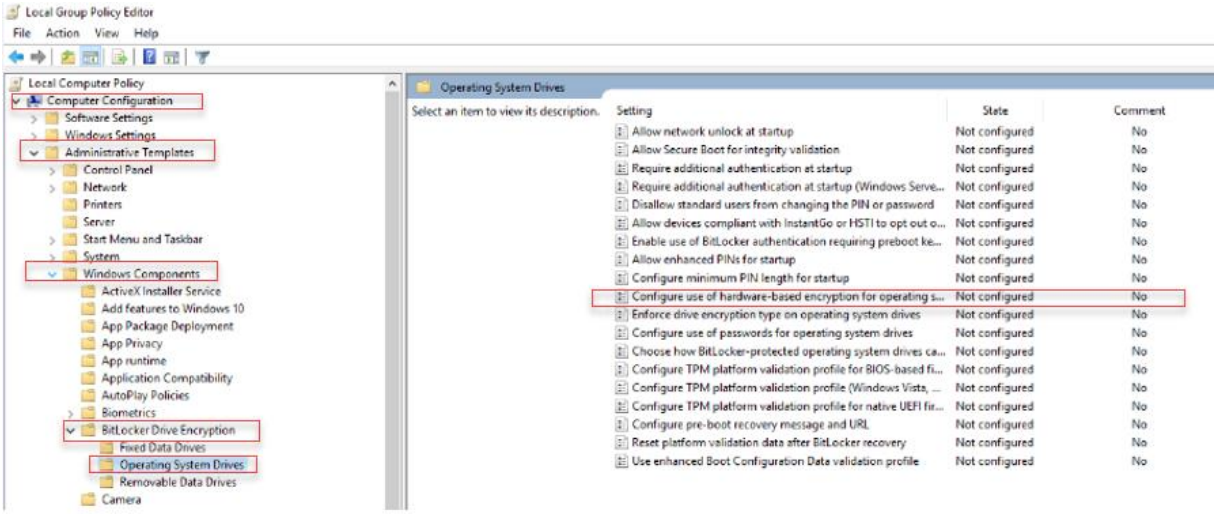
Gestione di Microsoft eDrive con Windows 10 (versione 1903 o superiore)
Con il rilascio di Windows 10 versione 1903, Microsoft ha modificato il comportamento di Windows 10 in relazione alla crittografia con eDrive. Al fine di abilitare eDrive in questa versione e, probabilmente, sulle versioni successive, è necessario eseguire ***gpedit*** *al fine di abilitare la crittografia hardware.*

Nota: Evitare di clonare un sistema operativo sull'SSD target*. La clonazione di un sistema operativo su un SSD target non consente di abilitare la crittografia hardware mediante eDrive. Al fine di poter utilizzare la crittografia hardware con eDrive sarà necessario implementare una nuova installazione del sistema operativo sull'SSD di destinazione.*

1. Installare il sistema operativo supportato sull'SSD di destinazione.
2. Dopo che il sistema operativo è stato installato, installare Kingston SSD Manager (KSM), eseguire KSM e assicurarsi che sia presente il seguente messaggio sulla scheda "Sicurezza" dell'applicazione:
   "IEEE 1667 is enabled an may not be changed because TCG Locking is enabled." (IEEE 1667 è abilitato e non può essere modificato in quanto il blocco TCG è abilitato).

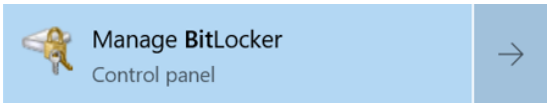


3. Eseguire il comando "gpedit.msc" per modificare le impostazioni di crittografia.
    a. Accedere alla sezione **Administrative Templates> Windows Components> BitLocker Drive Encryption> Operating System Drives**
    b. Quindi, selezionare **Configurazione dell'uso della crittografia basata sull'hardware per i sistemi operativi**
    c. **Abilitare** la funzionalità e quindi selezionare **Applica** per impostare la funzione.



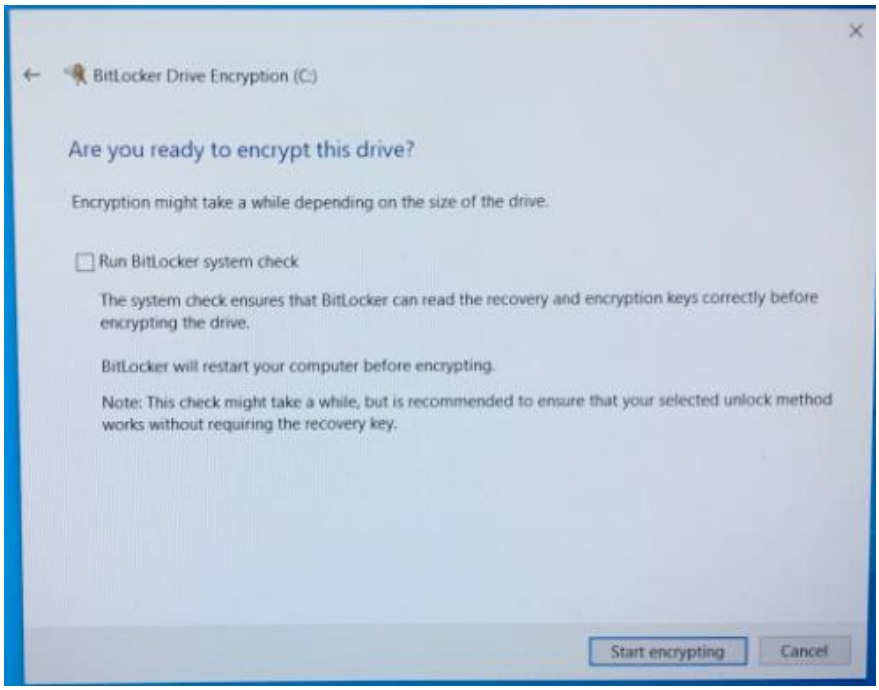
Nota: Per abilitare eDrive sui drive differenti da quello su cui risiede il sistema operativo, è possibile applicare le medesime impostazioni selezionando: **Administrative Templates> Windows Components> BitLocker Drive Encryption> Fixed Data Drives> Configure use of hardware-based encryption for fixed data drives (selezionare "Abilita" e quindi "Applica")**

4. Utilizzare il tasto Windows per cercare l'opzione **Gestione BitLocker**; quindi, eseguire l'applicazione.

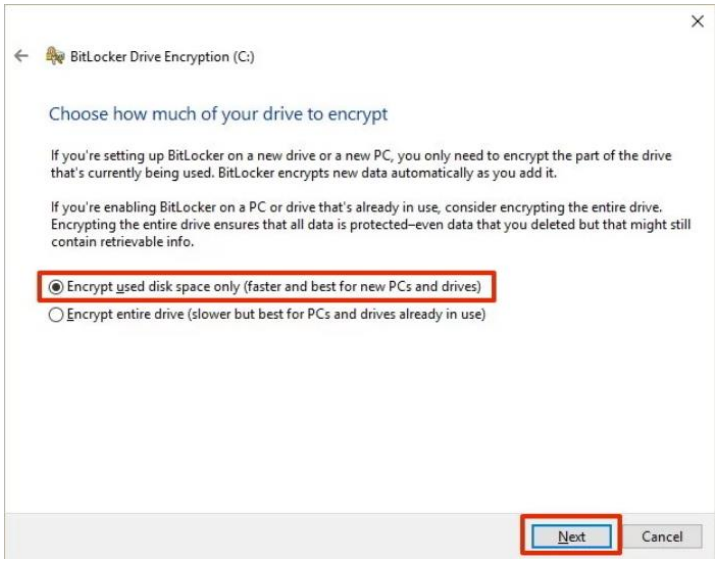


5. Selezionare l'opzione **Attiva BitLocker**, dalla schermata di Esplora risorse.

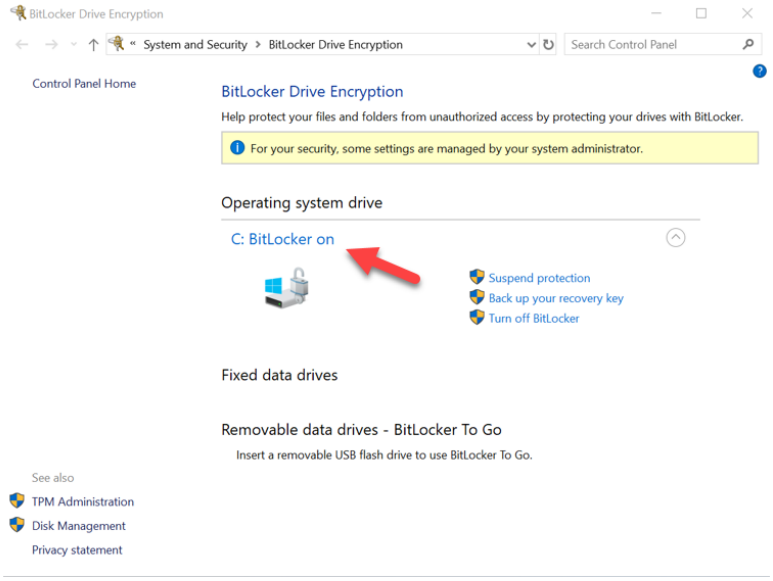
6. Proseguire seguendo le istruzioni della procedura guidata, fino alla completa configurazione dell'SSD di destinazione. Quando richiesto, selezionare l'opzione **"Inizia crittografazione".** L'impostazione selezionata di default è **Esegui controllo sistema Bitlocker**. Si consiglia di proseguire la procedura con questa opzione abilitata. Tuttavia, quando tale opzione non è selezionata, sarà possibile confermare se si dispone di crittografia hardware senza alcuna necessità di effettuare un riavvio.



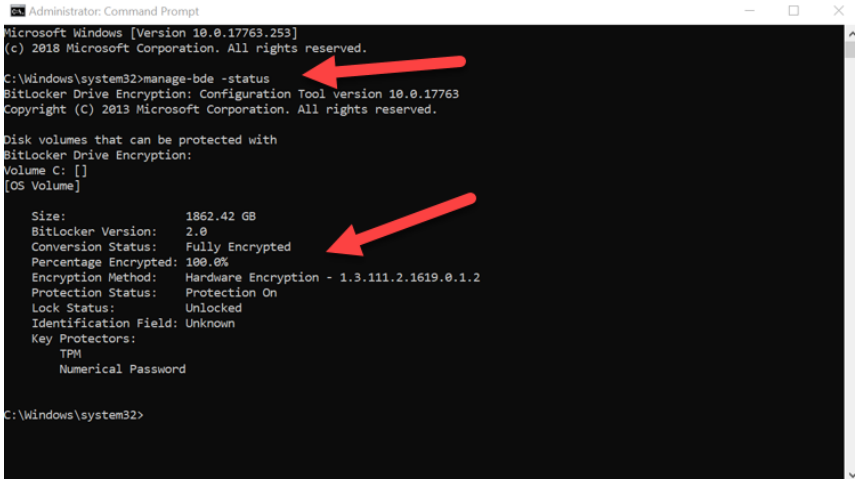
Nota: Se viene visualizzata una schermata che richiede all'utente di "Selezionare la dimensione del drive da crittografare", ciò spesso indica che l'SSD di destinazione NON è in grado di abilitare la funzione di crittografia hardware, ma soltanto quella software.



7. Se necessario, riavviare il sistema e quindi riavviare l'applicazione **Gestione BitLocker**, per verificare lo stato della crittografia sull'SSD di destinazione.



8. È anche possibile verificare la crittografia sull'SSD di destinazione aprendo il comando **cmd.exe** e digitando il comando: **manage-bde -status**



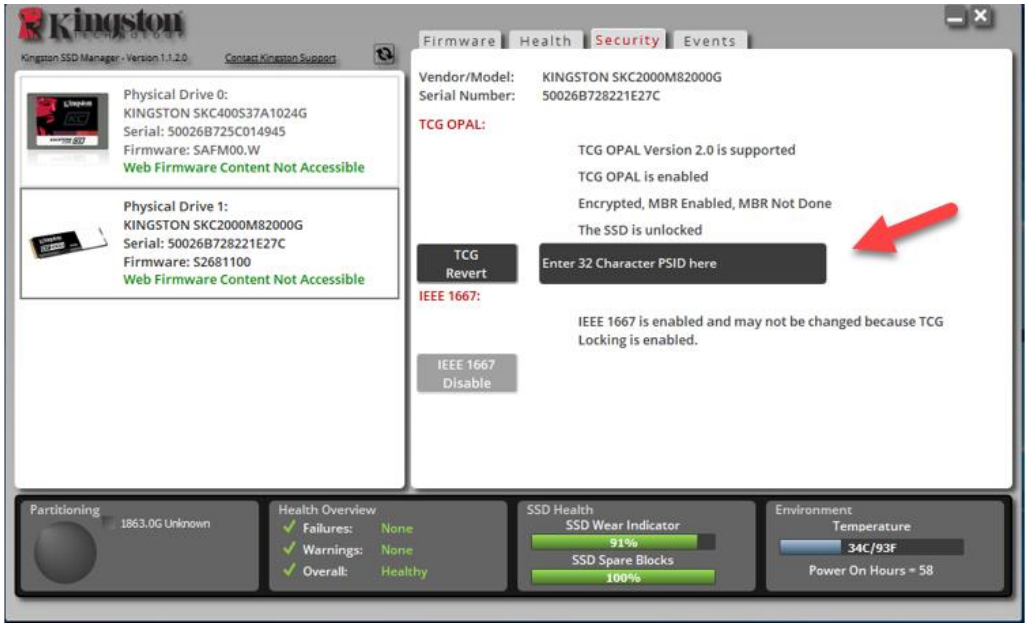
Disabilitazione del supporto per Microsoft eDrive
Seguire la procedura sotto per cancellare i dati dall'SSD di destinazione e rimuovere il supporto per BitLocker eDrive dal drive.

Nota: Questa procedura consente il reset dell'SSD di destinazione. TUTTI I DATI CONTENUTI NEL DRIVE SARANNO ELIMINATI.

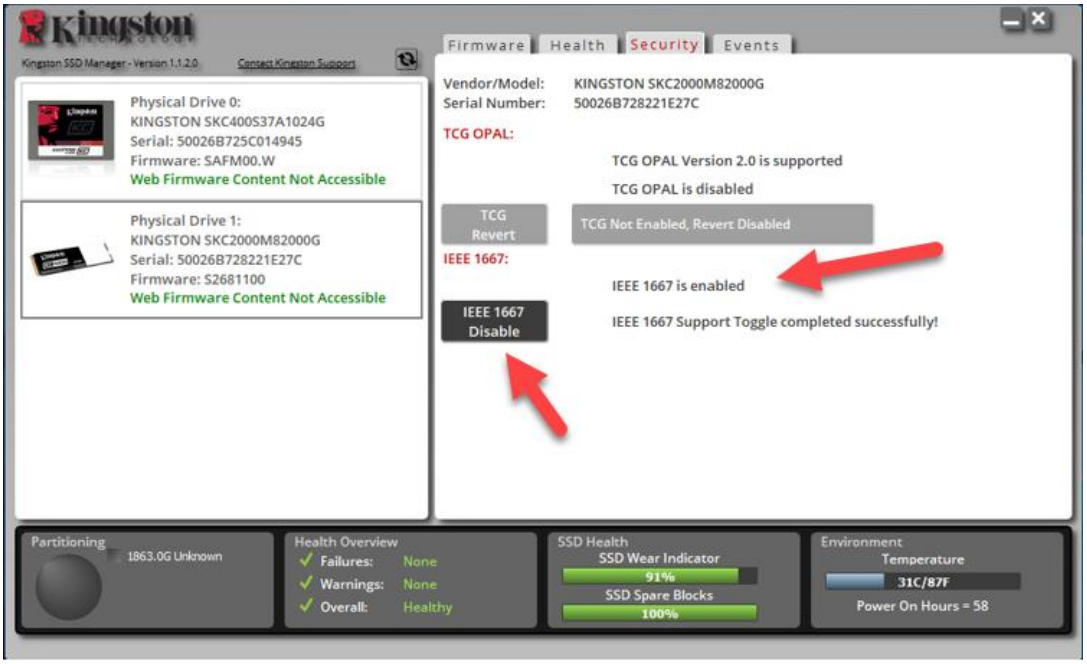
1. Annotare il valore PSID dell'SSD di destinazione. Tale valore è stampato sull'etichetta.

Es.: Valore PSID del modello KC2000

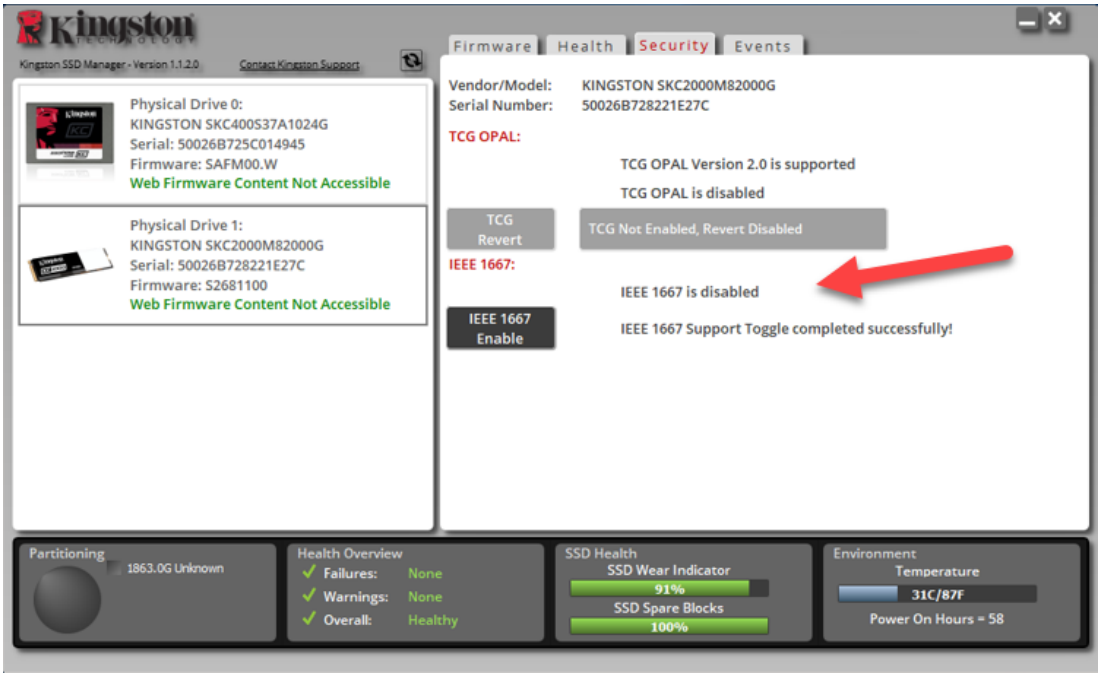
2. Montare l'SSD di destinazione come drive secondario e quindi eseguire Kingston SSD Manager (KSM).
3. Selezionare la scheda **Sicurezza** ed eseguire una procedura di **TCG Revert** inserendo il valore PSID composto da 32 cifre, precedentemente annotato durante la fase uno; quindi selezionare **"TCG Revert".** Una volta completata l'operazione, sarà visualizzato il messaggio **TCG Revert completed successfully** (TCG Revert completato con successo). Se il messaggio non viene visualizzato, re-inserire il valore PSID e provare a eseguire nuovamente la procedura di revert.



4. Una volta che il drive è stato recuperato con successo, sarà possibile disabilitare il supporto IEEE1667. Selezionare l'opzione **Disabilita IEEE1667**; quindi, attendere la visualizzazione del messaggio "IEEE1667 Support Toggle completed successfully" (Modifica supporto IEEE1667 completata con successo).



5. Assicurarsi che il supporto IEEE1667 sia disabilitato.



6. L'SSD di destinazione è ora pronto per il riutilizzo.