



## **Szyfrowane dyski SSD firmy Kingston**

**Włączanie i wyłączanie funkcji BitLocker eDrive w celu wykorzystania szyfrowania sprzętowego**

## Wprowadzenie

Ten dokument przedstawia sposób włączania i wyłączania funkcji Microsoft BitLocker eDrive w celu wykorzystania szyfrowania sprzętowego dysku SSD firmy Kingston. Ta procedura ma zastosowanie do dysków SSD firmy Kingston, które obsługują zestaw funkcji TCG OPAL 2.0 oraz IEEE1667. Jeśli posiadany dysk SSD firmy Kingston nie obsługuje funkcji TCG OPAL 2.0 i IEEE1667, ten proces nie będzie działać. Jeśli nie masz pewności co do obsługiwanych funkcji, skontaktuj się z działem pomocy technicznej firmy Kingston na stronie [www.kingston.com/support](http://www.kingston.com/support)

*Na potrzeby opisanego w tym dokumencie funkcja Microsoft BitLocker eDrive będzie nazywana funkcją „eDrive”. Przedstawione niżej procedury mogą ulegać pewnym zmianom w zależności od wersji systemu Windows i zainstalowanych pakietów serwisowych.*

## Wymagania systemowe

- Dysk SSD firmy Kingston wyposażony w zestaw funkcji zabezpieczeń TCG Opal 2.0 oraz IEEE1667
- Oprogramowanie Kingston SSD Manager <https://www.kingston.com/ssdmanager>
- Sprzęt i system BIOS z obsługą funkcji zabezpieczeń TCG Opal 2.0 oraz IEEE1667

## Wymagania dotyczące systemu operacyjnego i BIOS

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

*Uwaga: Szyfrowane dyski SSD nie mogą być podłączone do kontrolerów RAID – w przeciwnym razie nie będą działać prawidłowo w systemach Windows 8, 10 oraz Server 2012*

Aby użyć szyfrowanego dysku SSD w systemie Windows 8, 10 lub Windows Server 2012 jako **dysku danych**:

- Dysk musi być w stanie niezainicjowanym.
- Dysk musi być w stanie nieaktywnych zabezpieczeń.

Aby użyć szyfrowanego dysku SSD jako **dysku rozruchowego**:

- Dysk musi być w stanie niezainicjowanym.
- Dysk musi być w stanie nieaktywnych zabezpieczeń.
- Komputer musi obsługiwać standard UEFI 2.3.1 i mieć zdefiniowany protokół EFI\_STORAGE\_SECURITY\_COMMAND\_PROTOCOL. (Protokół ten umożliwia programom uruchamianym w środowisku usług rozruchowych EFI wysyłanie poleceń protokołu zabezpieczeń do dysku).
- W ustawieniach UEFI komputera musi być wyłączony moduł CSM (Compatibility Support Module).
- Komputer musi być zawsze uruchamiany w rodzimym środowisku UEFI.

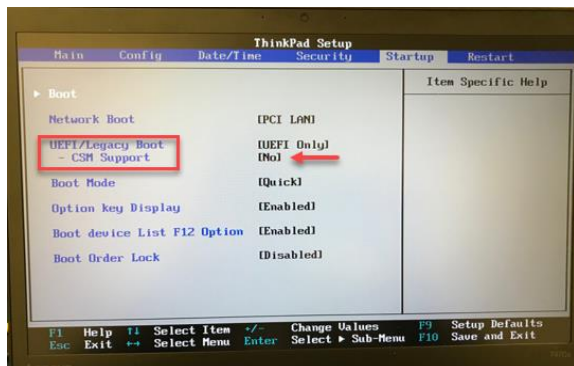
Dodatkowe informacje na ten temat zawiera następujący artykuł w witrynie firmy Microsoft:  
[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11))



## Włączanie funkcji Microsoft eDrive na rozruchowym dysku SSD

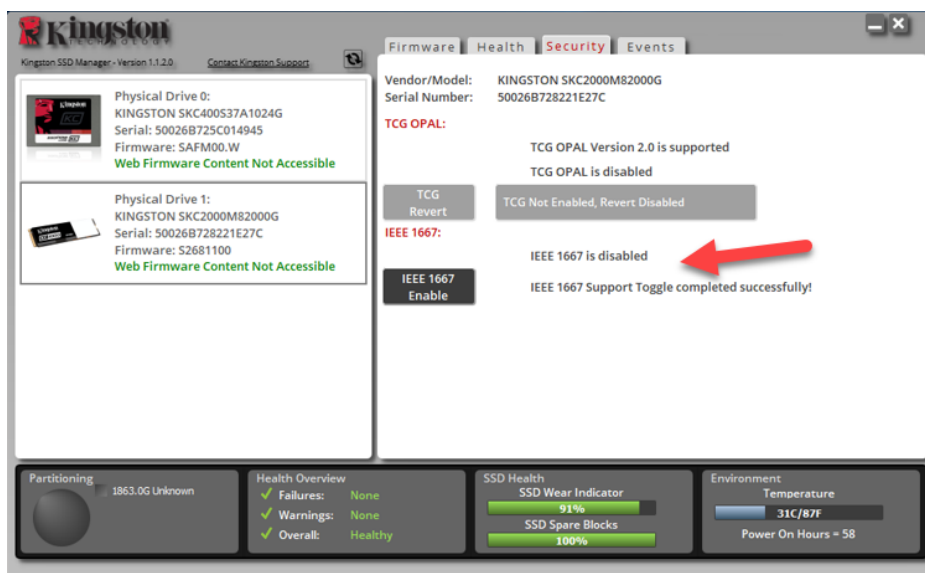
### Konfiguracja systemu BIOS

1. Sprawdź w dokumentacji otrzymanej od producenta komputera, czy system BIOS obsługuje standard UEFI 2.3.1 i czy ma zdefiniowany protokół EFI\_STORAGE\_SECURITY\_COMMAND\_PROTOCOL.
2. Przejdź do systemu BIOS i wyłącz moduł CSM (Compatibility Support Module)

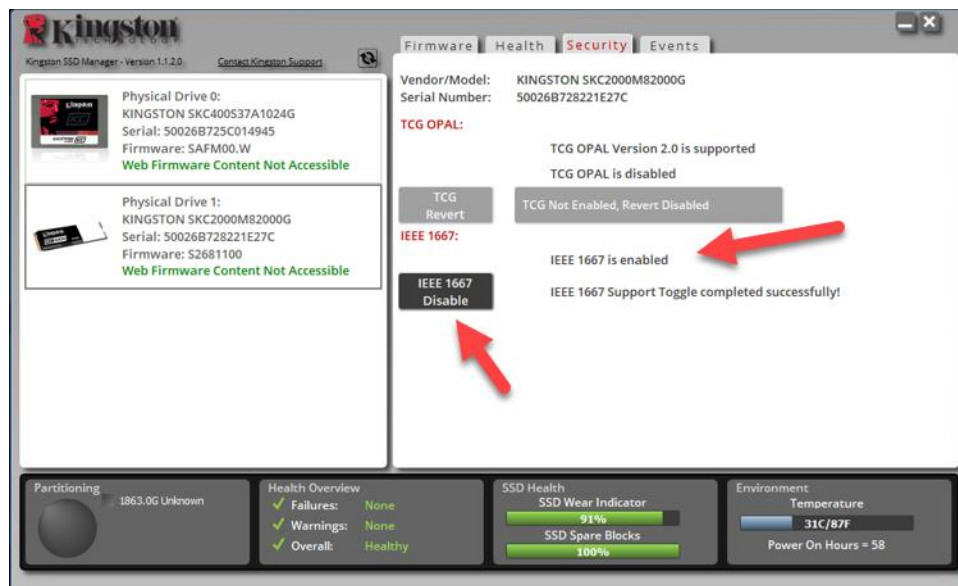


### Przygotowanie dysku

1. Jeśli nie masz jeszcze oprogramowania Kingston SSD Manager (KSM), pobierz je teraz.  
<https://www.kingston.com/ssdmanager>
2. Wykonaj bezpieczne wymazywanie docelowego dysku SSD za pomocą programu KSM lub inną standardową metodą.
3. Podłącz docelowy dysk SSD jako dysk dodatkowy, aby sprawdzić stan funkcji IEEE1667. Dysk powinien być w trybie **Disabled** (Wyłączony).



4. Zaznacz opcję IEEE1667 i kliknij pozycję **Enable** (Włącz). Sprawdź, czy funkcja została włączona.

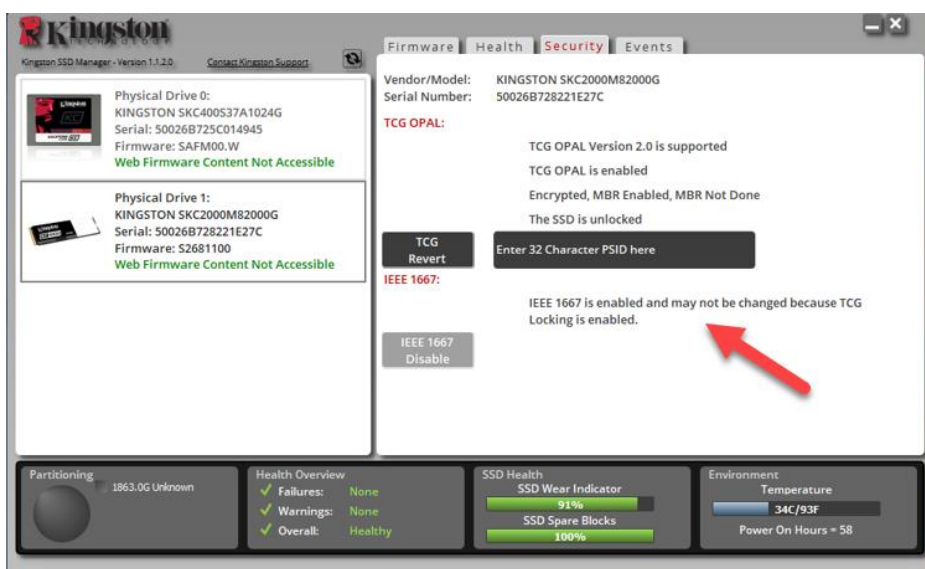


## Instalacja systemu operacyjnego

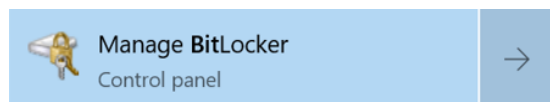
**Uwaga:** Nie należy klonować systemu operacyjnego na docelowy dysk SSD. Sklonowanie systemu operacyjnego na docelowy dysk SSD uniemożliwi włączenie szyfrowania sprzętowego za pomocą funkcji eDrive. Aby używać szyfrowania sprzętowego za pomocą funkcji eDrive, na docelowym dysku SSD należy zainstalować od początku nowy system operacyjny.

1. Zainstaluj obsługiwany system operacyjny na docelowym dysku SSD.
2. Po zainstalowaniu systemu operacyjnego zainstaluj oprogramowanie Kingston SSD Manager (KSM), uruchom program KSM i sprawdź, czy na karcie Security (Zabezpieczenia) tego programu jest wyświetlony następujący komunikat:

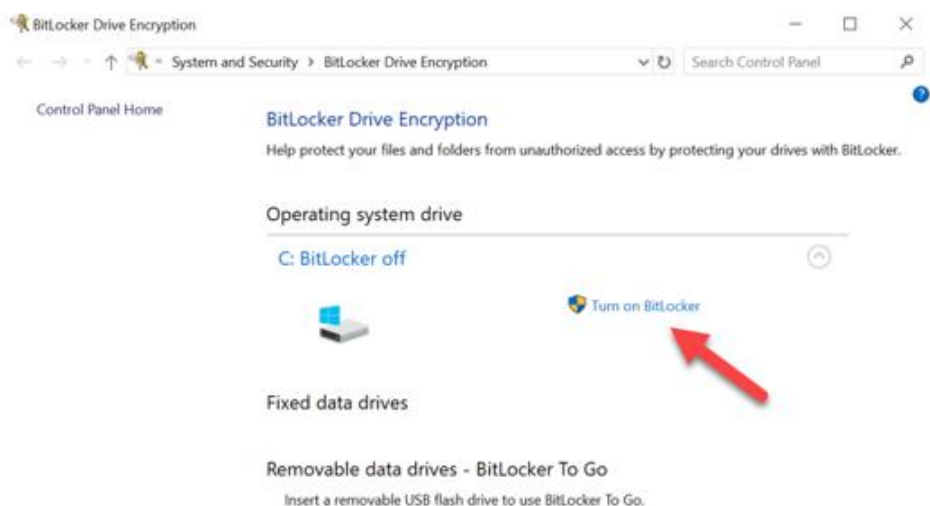
„IEEE 1667 is enabled and may not be changed because TCG Locking is enabled” (Funkcja IEEE 1667 jest włączona i nie może zostać zmieniona, ponieważ włączono blokadę TCG).



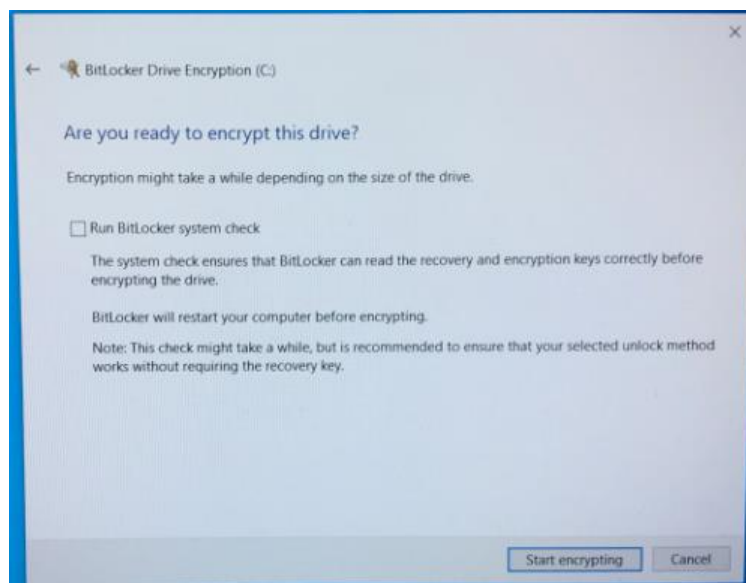
3. Naciśnij klawisz Windows i wyszukaj na komputerze aplikację **Manage BitLocker**, a następnie uruchom ją.



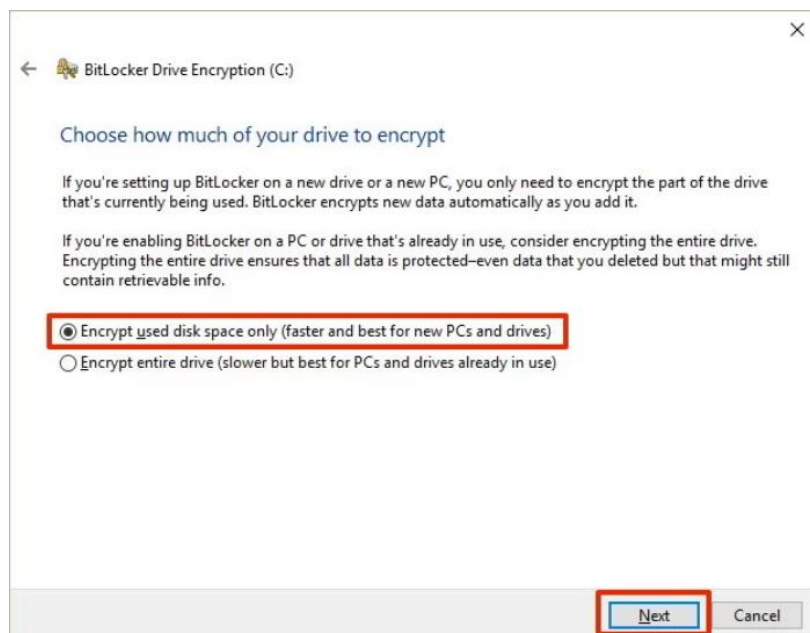
4. W oknie Eksploratora Windows wybierz pozycję **Turn on BitLocker** (Włącz funkcję BitLocker).



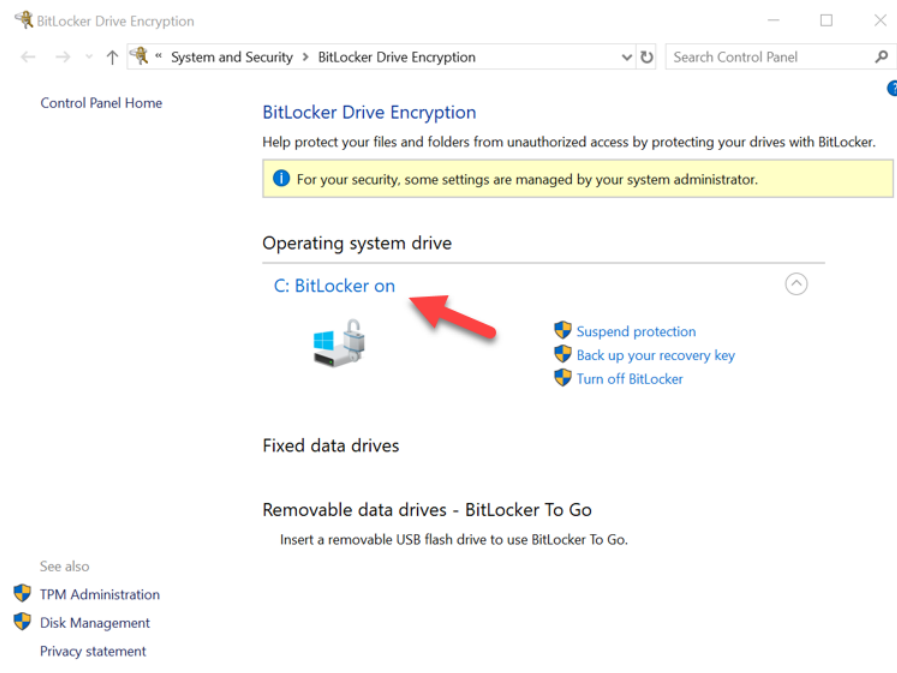
5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby skonfigurować docelowy dysk SSD. Po wyświetleniu monitu wybierz pozycję **Start encrypting** (Rozpocznij szyfrowanie). Domyślnie opcja **Run BitLocker system check** (Uruchom test systemu BitLocker) jest zaznaczona. Zalecamy pozostawienie tej opcji włączonej. Jeśli jednak ta opcja zostanie wyłączona, będzie można potwierdzić, czy szyfrowanie sprzętowe jest włączone, bez ponownego uruchamiania systemu.



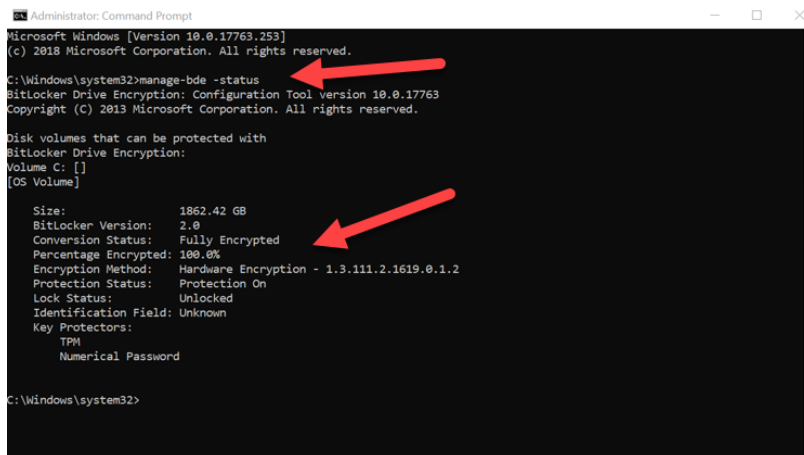
**Uwaga:** Wyświetlenie monitu „Choose how much of your drive do encrypt” (Wybierz część dysku do zaszyfrowania) zwykle oznacza, że na docelowym dysku SSD NIE ZOSTANIE włączone szyfrowanie sprzętowe, a będzie używane szyfrowanie programowe.



6. W razie potrzeby uruchom ponownie system, a następnie ponownie uruchom aplikację **Manage BitLocker**, aby sprawdzić stan szyfrowania docelowego dysku SSD.



7. Stan szyfrowania docelowego dysku SSD można również sprawdzić, uruchamiając program **cmd.exe** i wpisując następujące polecenie: **manage-bde -status**



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (c) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: [ ]
[OS Volume]

Size: 1862.42 GB
BitLocker Version: 2.0
Conversion Status: Fully Encrypted
Percentage Encrypted: 100.0%
Encryption Method: Hardware Encryption - 1.3.111.2.1619.0.1.2
Protection Status: Protection On
Lock Status: Unlocked
Identification Field: Unknown
Key Protectors:
    TPM
    Numerical Password

C:\Windows\system32>
```

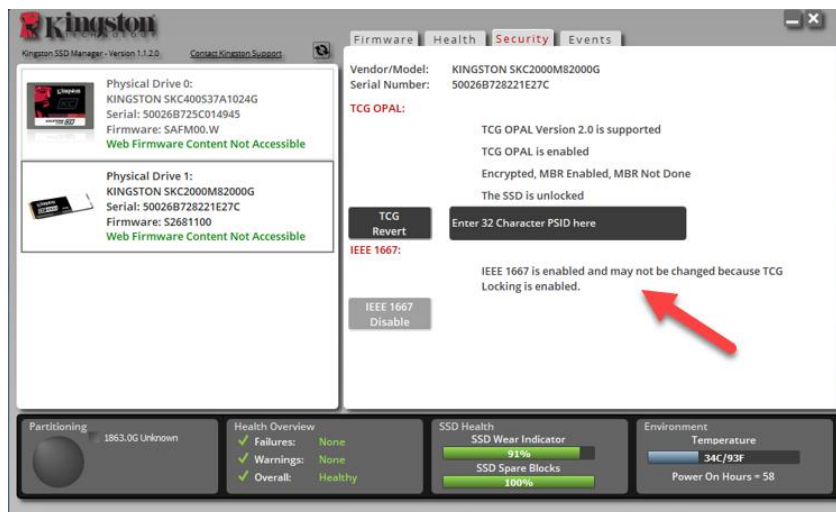
### Włączanie funkcji Microsoft eDrive w systemie Windows 10 (wersja 1903+)

W wersji 1903 systemu operacyjnego Windows 10 firma Microsoft zmieniła zachowanie systemu operacyjnego względem funkcji szyfrowania eDrive. Aby móc używać funkcji eDrive w tej wersji systemu Windows (i prawdopodobnie także w nowszych wersjach), należy uruchomić program **gpedit** w celu włączenia szyfrowania sprzętowego.

**Uwaga: Nie należy klonować systemu operacyjnego na docelowy dysk SSD.** Sklonowanie systemu operacyjnego na docelowy dysk SSD uniemożliwi włączenie szyfrowania sprzętowego za pomocą funkcji eDrive. Aby używać szyfrowania sprzętowego za pomocą funkcji eDrive, na docelowym dysku SSD należy zainstalować od początku nowy system operacyjny.

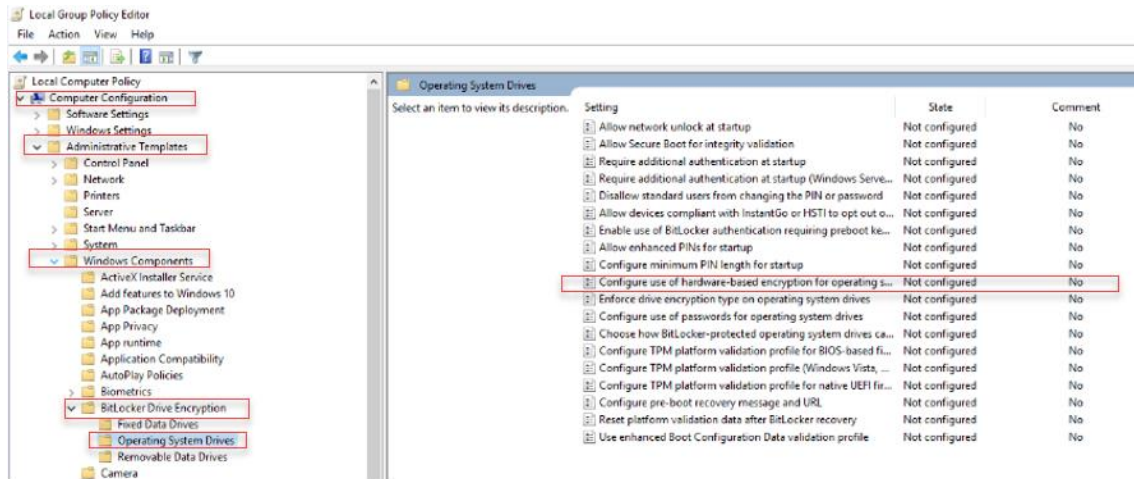
1. Zainstaluj obsługiwany system operacyjny na docelowym dysku SSD.
2. Po zainstalowaniu systemu operacyjnego zainstaluj oprogramowanie Kingston SSD Manager (KSM), uruchom program KSM i sprawdź, czy na karcie Security (Zabezpieczenia) tego programu jest wyświetlony następujący komunikat:

„IEEE 1667 is enabled and may not be changed because TCG Locking is enabled” (Funkcja IEEE 1667 jest włączona i nie może zostać zmieniona, ponieważ włączono blokadę TCG).



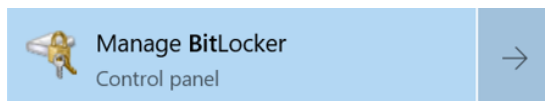
3. Uruchom program gpedit.msc, aby zmienić ustawienie szyfrowania.

- Przejdź do ekranu **Administrative Templates (Szablony administracyjne) > Windows Components (Składniki systemu Windows) > BitLocker Drive Encryption (Szyfrowanie dysków funkcją BitLocker) > Operating System Drives (Dyski z systemem operacyjnym)**
- Następnie wybierz polecenie **Configure use of hardware-based encryption for operating systems** (Konfiguruj użycie szyfrowania sprzętowego w systemach operacyjnych).
- Włącz** tę funkcję, a następnie kliknij przycisk **Apply** (Zastosuj).

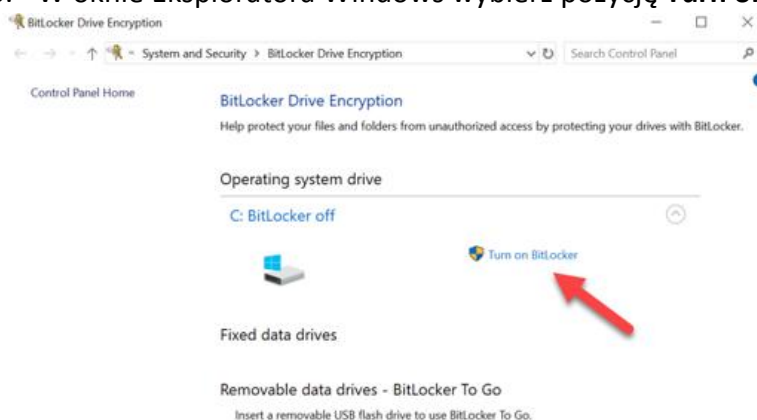


Uwaga: Aby włączyć funkcję eDrive dla dysków innych niż dysk z systemem operacyjnym, można zastosować te same ustawienia, wybierając kolejno: **Administrative Templates (Szablony administracyjne) > Windows Components (Składniki systemu Windows) > BitLocker Drive Encryption (Szyfrowanie dysków funkcją BitLocker) > Fixed Data Drives (Stałe dyski danych) > Configure use of hardware-based encryption for fixed data drives (Konfiguruj użycie szyfrowania sprzętowego dla stałych dysków danych)**. Następnie należy zaznaczyć pozycję **Enable (Włącz)** i kliknąć przycisk **Apply (Zastosuj)**

4. Naciśnij klawisz Windows i wyszukaj na komputerze aplikację **Manage BitLocker**, a następnie uruchom ją.

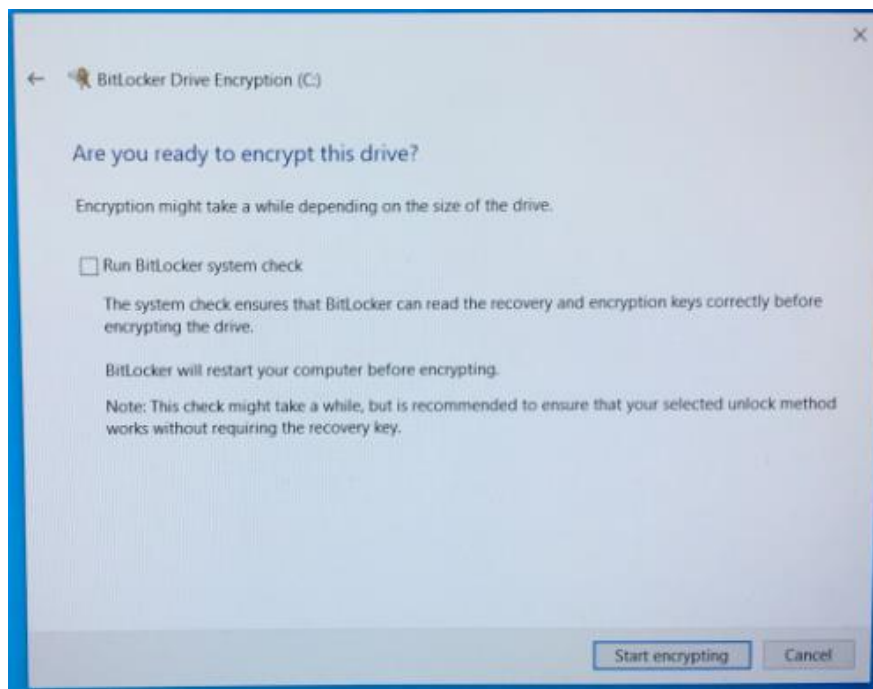


5. W oknie Eksploratora Windows wybierz pozycję **Turn on BitLocker** (Włącz funkcję BitLocker).

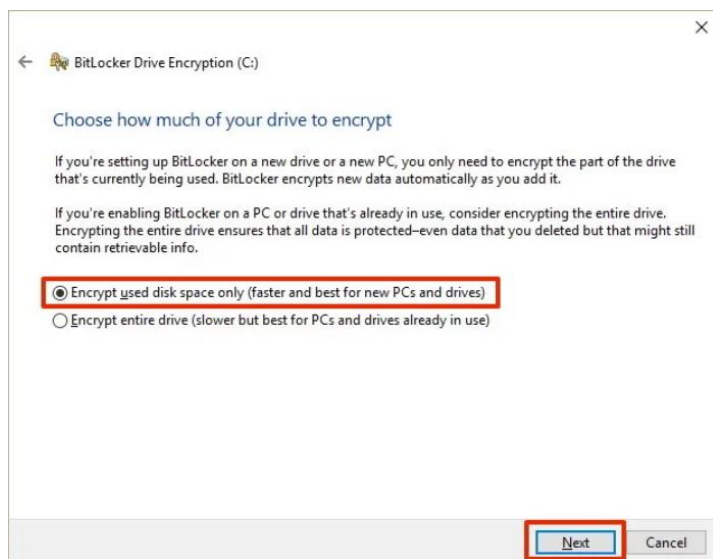




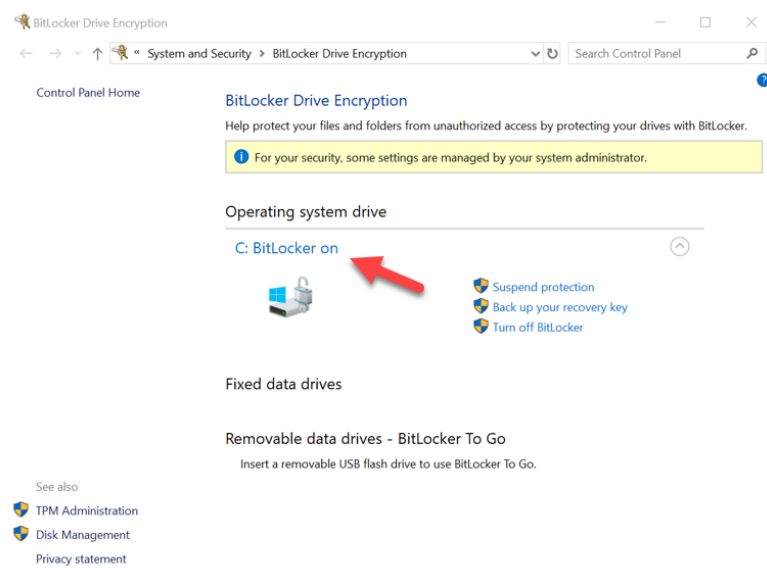
6. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby skonfigurować docelowy dysk SSD. Po wyświetleniu monitu wybierz pozycję **Start encrypting** (Rozpocznij szyfrowanie). Domyślnie opcja **Run BitLocker system check** (Uruchom test systemu BitLocker) jest zaznaczona. Zalecamy pozostawienie tej opcji włączonej. Jeśli jednak ta opcja zostanie wyłączona, będzie można potwierdzić, czy szyfrowanie sprzętowe jest włączone, bez ponownego uruchamiania systemu.



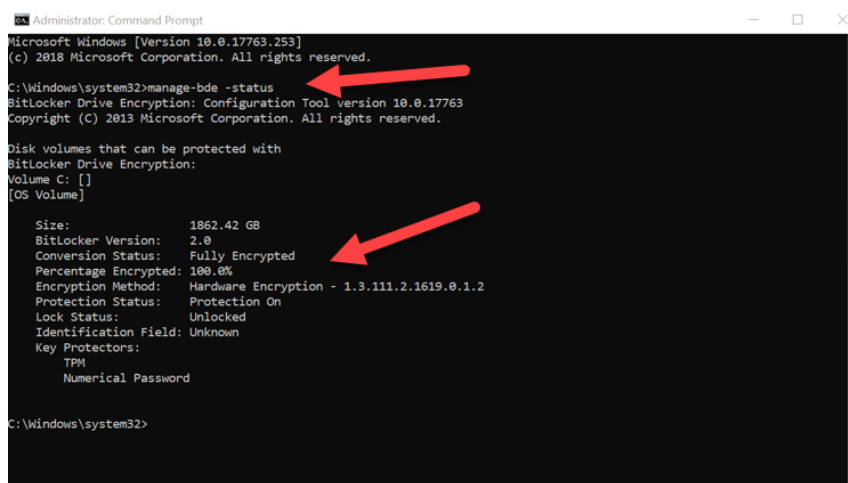
**Uwaga:** Wyświetlenie monitu „Choose how much of your drive to encrypt” (Wybierz część dysku do zaszyfrowania) zwykle oznacza, że na docelowym dysku SSD NIE ZOSTANIE włączone szyfrowanie sprzętowe, a będzie używane szyfrowanie programowe.



7. W razie potrzeby uruchom ponownie system, a następnie ponownie uruchom aplikację **Manage BitLocker**, aby sprawdzić stan szyfrowania docelowego dysku SSD.



8. Stan szyfrowania docelowego dysku SSD można również sprawdzić, uruchamiając program **cmd.exe** i wpisując następujące polecenie: **manage-bde -status**



## Wyłączanie funkcji Microsoft eDrive

Aby wymazać dane z docelowego dysku SSD i wyłączyć obsługę funkcji BitLocker eDrive dla tego dysku, należy wykonać następującą procedurę.

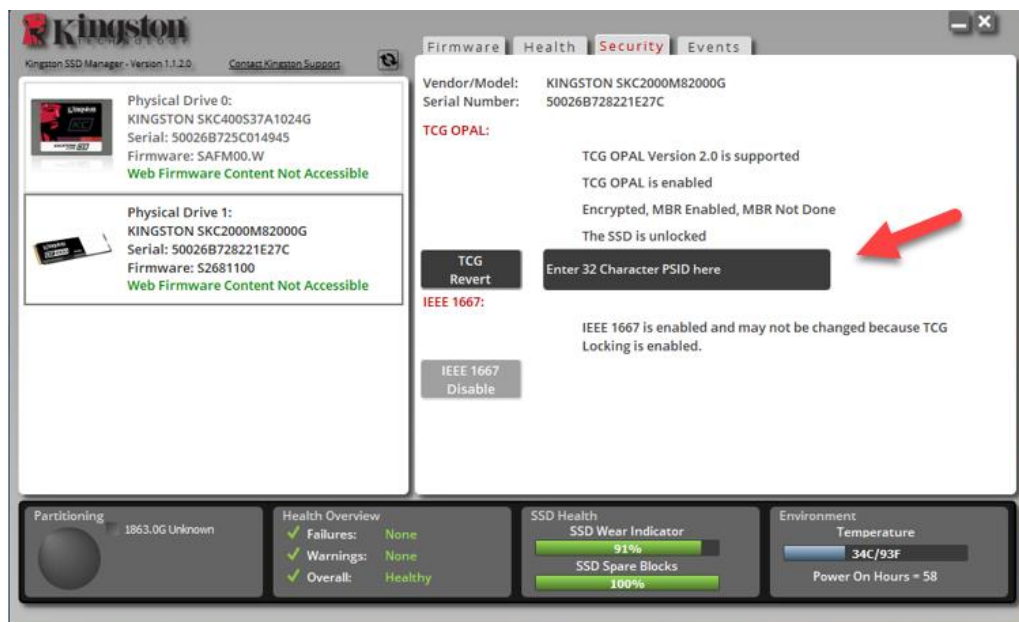
**Uwaga: Ta procedura spowoduje zresetowanie docelowego dysku SSD. WSZYSTKIE DANE ZAPISANE NA DYSKU ZOSTANĄ UTRACONE.**

1. Zapisz wartość PSID docelowego dysku SSD. Wartość ta jest wydrukowana na etykiecie dysku.

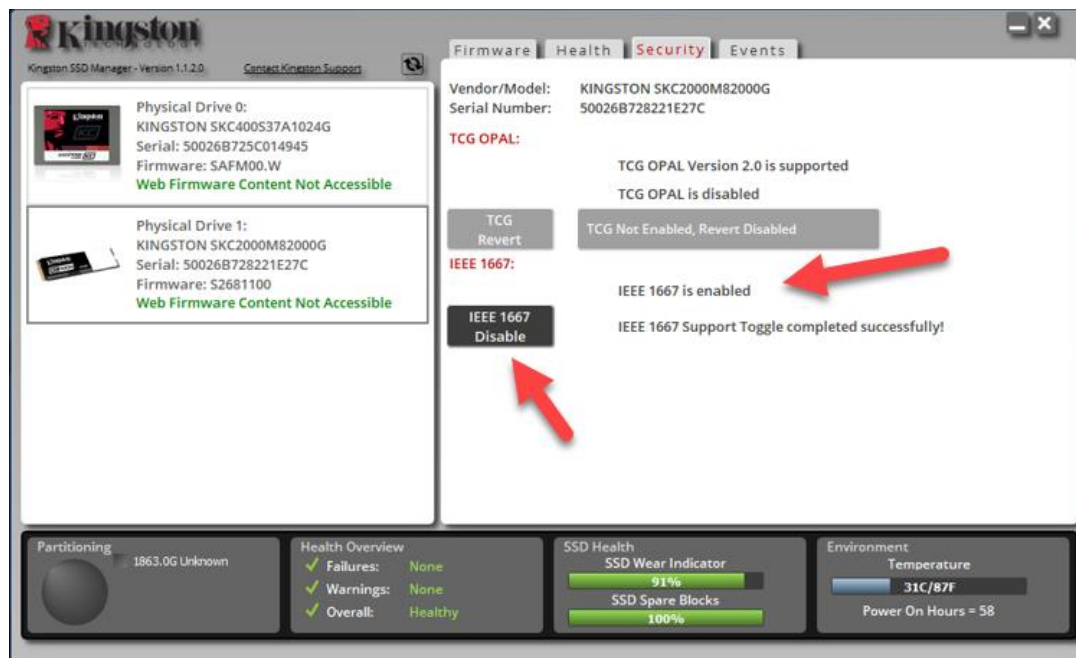


Przykład: wartość PSID KC2000

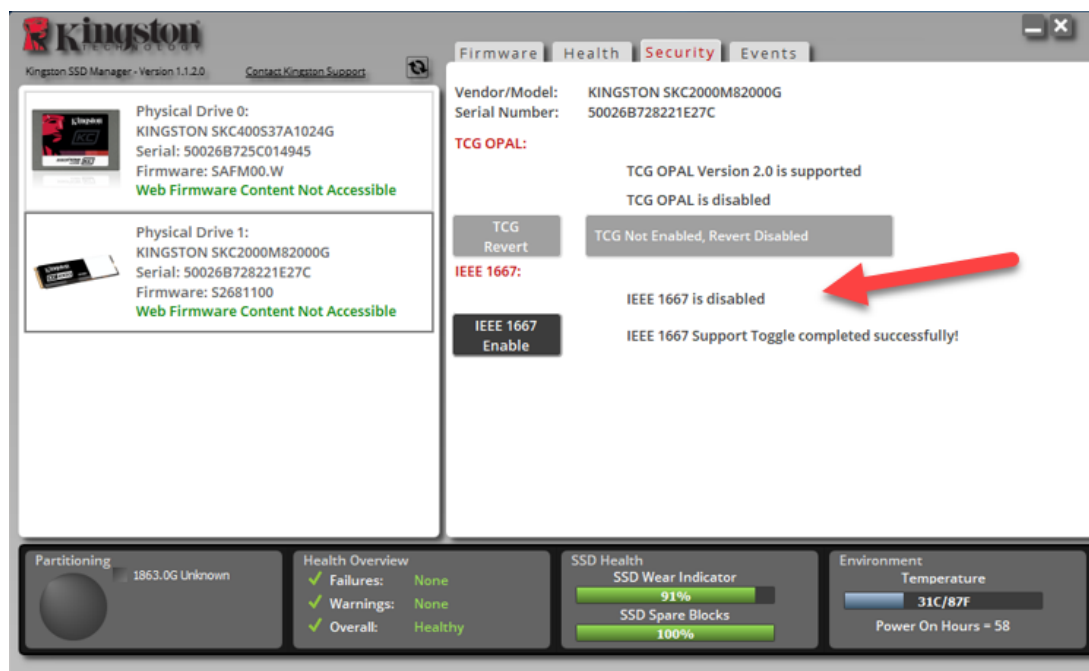
2. Podłącz docelowy dysk SSD jako dysk dodatkowy, a następnie uruchom program Kingston SSD Manager (KSM).
3. Wybierz kartę **Security** (Zabezpieczenia) i wykonaj operację **TCG Revert** (Wycofywanie TCG). W tym celu wpisz 32-cyfrową wartość PSID, a następnie wybierz opcję **TCG Revert**. Po zakończeniu procesu zostanie wyświetlony komunikat **TCG Revert completed successfully** (Wycofywanie TCG zostało ukończone pomyślnie). Jeśli ten komunikat nie zostanie wyświetlony, wpisz jeszcze raz wartość PSID i ponownie wykonaj procedurę.



4. Po pomyślnym wyłączeniu szyfrowania dysku będzie możliwe wyłączenie obsługi funkcji IEEE1667. Zaznacz opcję **IEEE1667 Disable** (Wyłącz funkcję IEEE1667) i zaczekaj, aż zostanie wyświetlony komunikat „IEEE1667 Support Toggle completed successfully” (Obsługa funkcji IEEE1667 została pomyślnie przełączona).



5. Sprawdź, czy obsługa funkcji IEEE1667 została wyłączona.



6. Docelowy dysk SSD jest gotowy do ponownego wykorzystania.

