Kingston verschlüsselte SSDs

Aktivieren und Deaktivieren von BitLocker mit eDrive zur Nutzung der Hardwareverschlüsselung

Einführung

Dieses Dokument beschreibt, wie Sie die BitLocker eDrive-Funktion von Microsoft aktivieren und deaktivieren, um die Hardwareverschlüsselung auf Ihrer Kingston SSD zu nutzen. Dieses Verfahren gilt für Kingston SSDs, die den Funktionsumfang von TCG OPAL 2.0 und IEEE1667 unterstützen. Wenn Sie keine Kingston SSD mit TCG OPAL 2.0 und IEEE1667 Unterstützung haben, funktioniert dieser Prozess nicht. Wenn Sie sich nicht sicher sind, wenden Sie sich bitte an den technischen Support von Kingston unter www.kingston.com/support

Dieses Dokument bezieht sich im Folgenden auf Microsofts BitLocker mit eDrive als „eDrive". Die im Folgenden beschriebenen Verfahren können sich je nach Windows-Version(en) und Updates ändern.

Systemvoraussetzungen

- Kingston SSD mit TCG Opal 2.0 und IEEE1667 Sicherheitsfunktionsumfang
- Kingston SSD Manager Software https://www.kingston.com/ssdmanager
- System-Hardware und BIOS mit Unterstützung von TCG Opal 2.0 und IEEE1667 Sicherheitsfunktionen

OS-/BIOS-Anforderungen

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

Hinweis: Alle verschlüsselten SSD-Laufwerke müssen an Nicht-RAID-Controller angeschlossen sein, damit sie unter Windows 8, 10 und/oder Server 2012 ordnungsgemäß funktionieren

So verwenden Sie ein verschlüsseltes SSD-Laufwerk unter Windows 8, 10 oder Windows Server 2012 als **Datenlaufwerk**:

- Das Laufwerk muss sich in einem nicht initialisierten Zustand befinden.
- Das Laufwerk muss sich in einem sicherheitsinaktiven Zustand befinden.

Für verschlüsselte SSD-Laufwerke, die als **Startlaufwerke**verwendet werden:

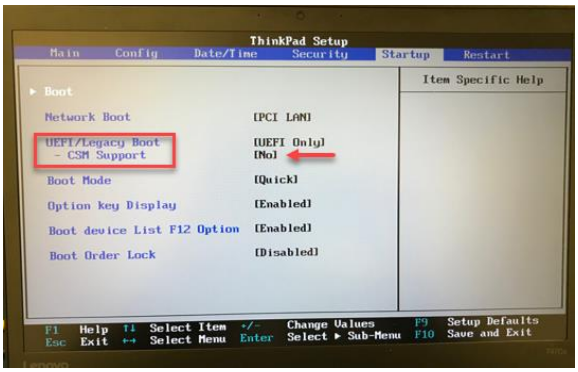
- Das Laufwerk muss sich in einem nicht initialisierten Zustand befinden.
- Das Laufwerk muss sich in einem sicherheitsinaktiven Zustand befinden.
- Der Computer muss auf UEFI 2.3.1 basieren und EFI_STORAGE_SECURITY_COMMAND_PROTOCOL muss definiert sein. (Dieses Protokoll wird verwendet, damit Programme, die in der EFI-Boot-Services-Umgebung ausgeführt werden, Sicherheitsprotokollbefehle an das Laufwerk senden können).
- Auf dem Computer muss das Compatibility Support Module (CSM) im UEFI deaktiviert sein.
- Der Computer muss immer nativ von UEFI booten.

Weitere Informationen finden Sie im Microsoft-Artikel zu diesem Thema hier:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Microsoft eDrive auf der Boot-SSD aktivieren

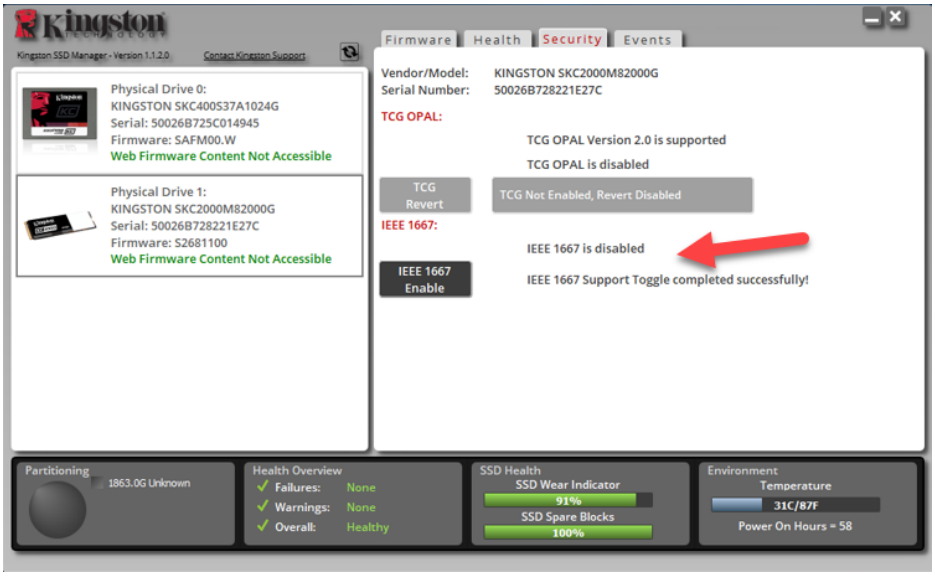
BIOS-Konfiguration

1. Vergewissern Sie sich in der Dokumentation Ihres Systemherstellers, dass das BIOS Ihres Systems auf UEFI 2.3.1 basiert und dass EFI_STORAGE_SECURITY_COMMAND_PROTOCOL definiert ist.
2. Rufen Sie das BIOS auf und deaktivieren Sie das Compatibility Support Module (CSM)

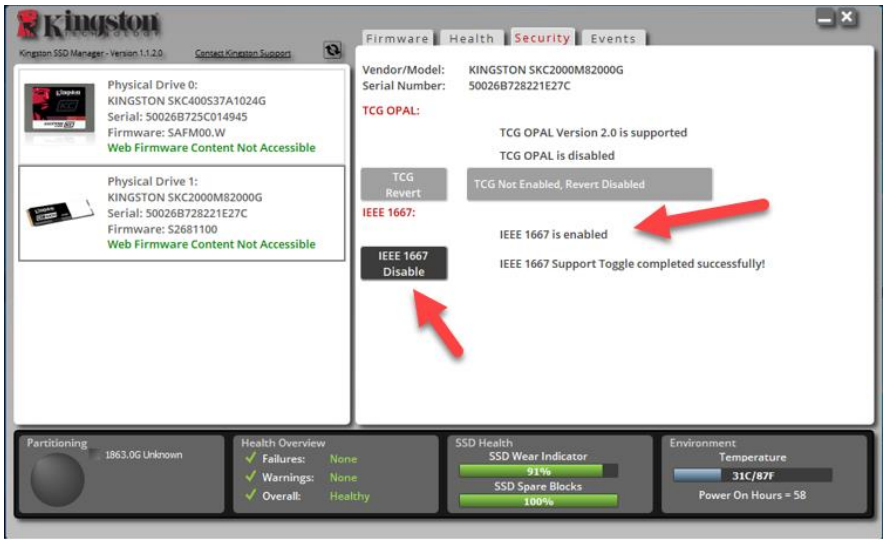


Vorbereitung des Laufwerks

1. Wenn Sie Kingston SSD Manager (KSM) noch nicht heruntergeladen haben, tun Sie dies bitte jetzt. https://www.kingston.com/ssdmanager
2. Löschen Sie die Ziel-SSD mit der KSM-Software oder einer anderen branchenüblichen Methode.
3. Richten Sie die Ziel-SSD als sekundäre Festplatte ein, um den IEEE1667-Status zu bestätigen. Das Laufwerk muss sich im Modus **Deaktiviert (Disabled)** befinden.



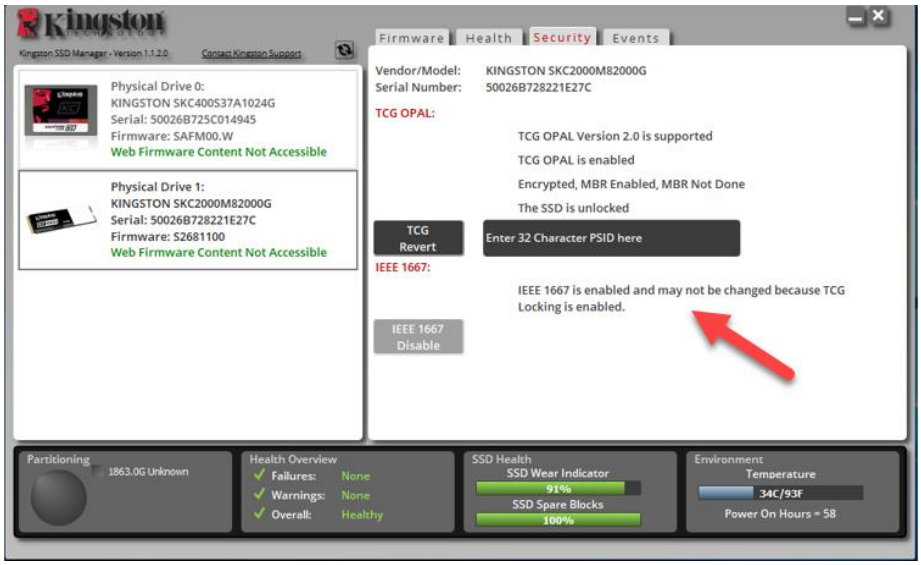
4. Wählen Sie die IEEE1667-Taste und **Aktivieren** Sie die Funktion. Bestätigen Sie, dass die Funktion erfolgreich umgeschaltet wurde.



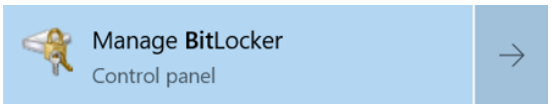
Installation des Betriebssystems (OS)

Hinweis: Klonen Sie ein Betriebssystem nicht auf Ihre Ziel-SSD*. Das Klonen eines Betriebssystems auf die Ziel-SSD verhindert, dass die Hardwareverschlüsselung mit eDrive aktiviert werden kann. Sie müssen eine neue Betriebssysteminstallation auf der Ziel-SSD bereitstellen, um die Vorteile der Hardwareverschlüsselung mit eDrive nutzen zu können.*

1. Installieren Sie das unterstützte Betriebssystem auf der Ziel-SSD.
2. Nach der Installation des Betriebssystems installieren Sie den Kingston SSD Manager (KSM). Führen Sie den KSM aus und bestätigen Sie, dass die folgende Meldung auf der Registerkarte Sicherheit in der Anwendung vorhanden ist:
   „EEE 1667 ist aktiviert und darf nicht geändert werden, weil TCG Locking aktiviert ist. (IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.)“

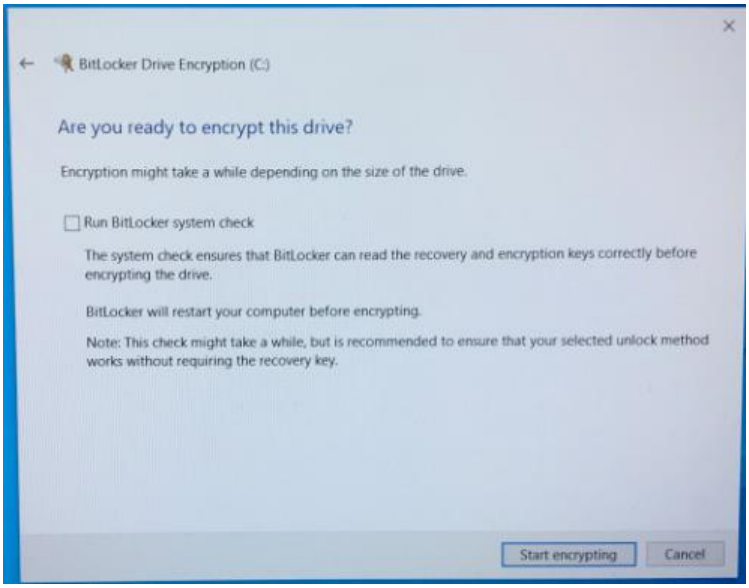


3. Verwenden Sie den Windows-Schlüssel, um nach **BitLocker verwalten (Manage BitLocker)** zu suchen und die Anwendung dann auszuführen.

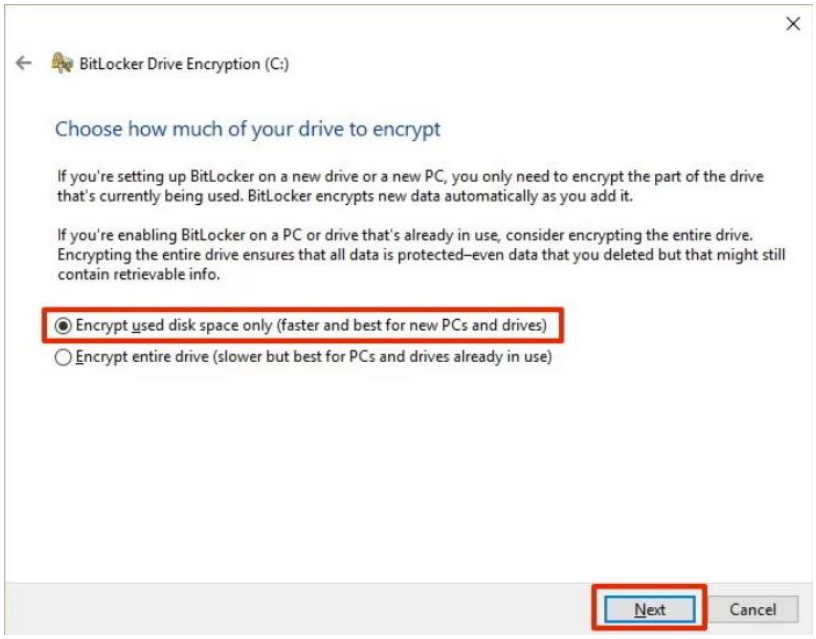


4. Wählen Sie **BitLocker aktivieren (Turn on BitLocker)** im Explorer-Fenster.

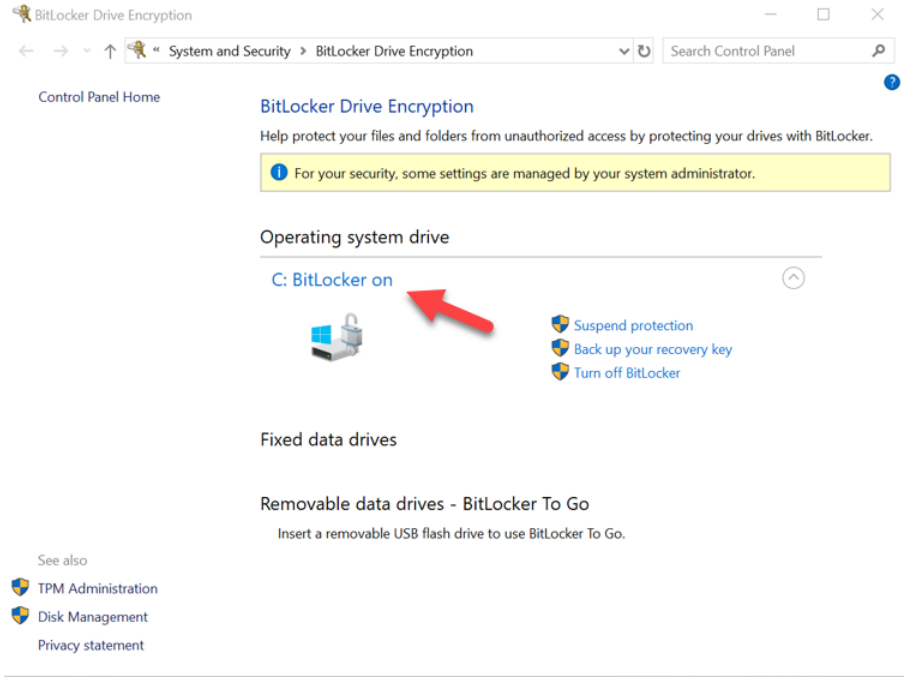
5. Arbeiten Sie alle Eingabeaufforderungen zur Konfiguration der Ziel-SSD ab. Wenn Sie dazu aufgefordert werden, wählen Sie **Verschlüsselung starten (Start encrypting).** Standardmäßig ist **BitLocker Systemtest ausführen (Run BitLocker system check)** aktiviert. Es ist ratsam, mit dieser aktivierten Einstellung fortzufahren. Wenn Sie das Kontrollkästchen deaktivieren, können Sie jedoch bestätigen, ob die Hardwareverschlüsselung aktiviert ist, ohne dass ein Neustart des Systems erforderlich ist.



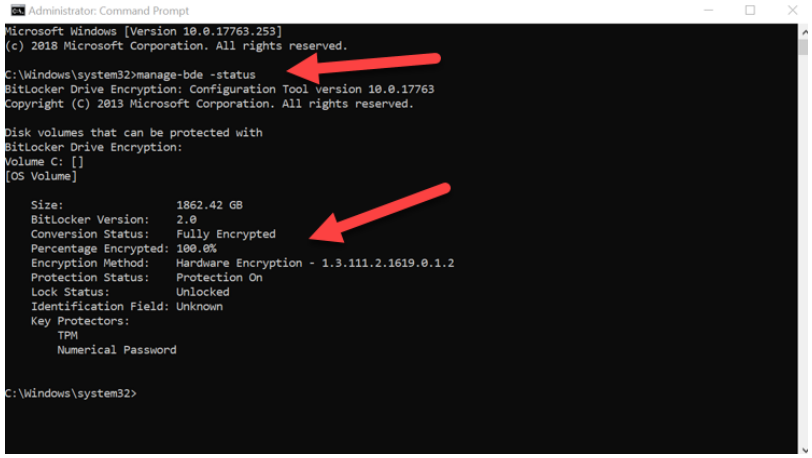
Hinweis: Wenn Sie in einem Fenster aufgefordert werden, „Auswählen, wie viel des Laufwerks verschlüsselt werden soll (Choose how much of your drive to encrypt)“, bedeutet dies oft, dass auf der Ziel-SSD KEINE Hardwareverschlüsselung aktiviert wird, sondern stattdessen eine Softwareverschlüsselung verwendet wird.



6. Starten Sie bei Bedarf das System neu und starten Sie dann **BitLocker verwalten (Manage BitLocker)** neu, um den Verschlüsselungsstatus der Ziel-SSD zu bestätigen.



7. Sie können den Verschlüsselungsstatus der Ziel-SSD auch überprüfen, indem Sie cmd.exe öffnen und Folgendes eingeben: **manage-bde -status**

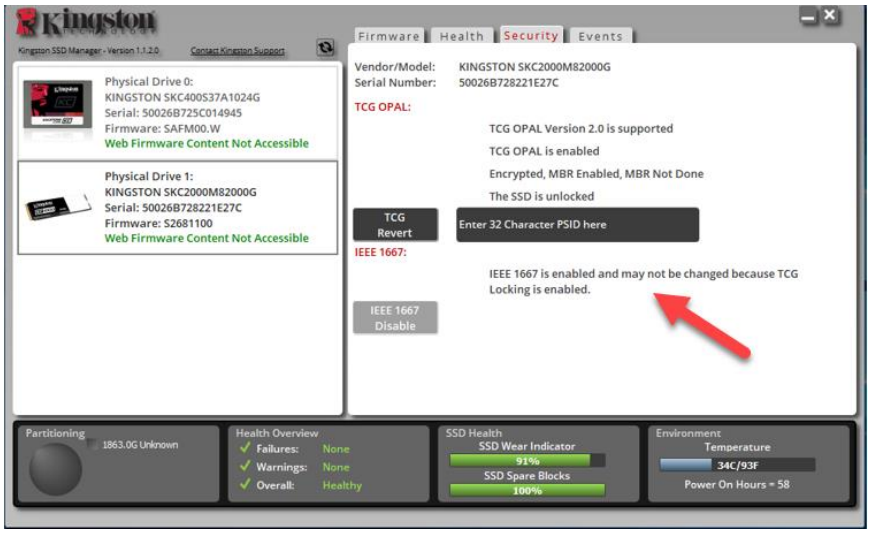


Microsoft eDrive unter Windows 10 aktivieren (Version 1903+)

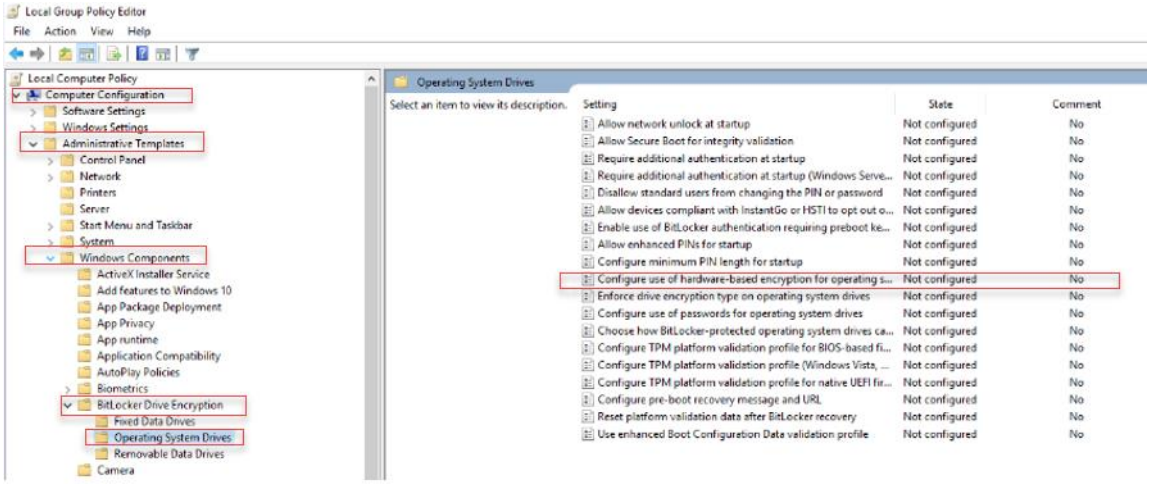
*Microsoft hat mit der Veröffentlichung von Windows 10 Version 1903 das Standardverhalten von Windows 10 in Bezug auf die eDrive-Verschlüsselung geändert. Zur Aktivierung von eDrive in dieser und möglicherweise auch in späteren Versionen müssen Sie **gpedit** ausführen, um die Hardwareverschlüsselung zu aktivieren.*

***Hinweis: Klonen Sie ein Betriebssystem nicht auf Ihre Ziel-SSD**. Das Klonen eines Betriebssystems auf die Ziel-SSD verhindert, dass die Hardwareverschlüsselung mit eDrive aktiviert werden kann. Sie müssen eine neue Betriebssysteminstallation auf der Ziel-SSD bereitstellen, um die Vorteile der Hardwareverschlüsselung mit eDrive nutzen zu können.*

1. Installieren Sie das unterstützte Betriebssystem auf der Ziel-SSD.
2. Nach der Installation des Betriebssystems installieren Sie den Kingston SSD Manager (KSM). Führen Sie den KSM aus und bestätigen Sie, dass die folgende Meldung auf der Registerkarte Sicherheit in der Anwendung vorhanden ist:
   „EEE 1667 ist aktiviert und darf nicht geändert werden, weil TCG Locking aktiviert ist. (IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.)“

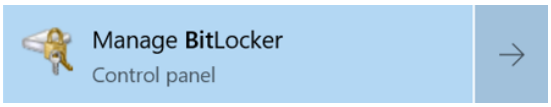


3. Führen Sie gpedit.msc aus, um die Verschlüsselungseinstellung zu ändern.
    a. Navigieren Sie zu **Verwaltungsvorlagen > Windows-Komponenten > BitLocker Laufwerksverschlüsselung > Betriebssystemlaufwerke**
    b. Wählen Sie dann die Option **Verwendung von hardwarebasierter Verschlüsselung für Betriebssysteme konfigurieren (Configure use of hardware-based encryption for operating systems)**
    c. **Aktivieren** Sie die Funktion und **Übernehmen** Sie dann die Einstellung.



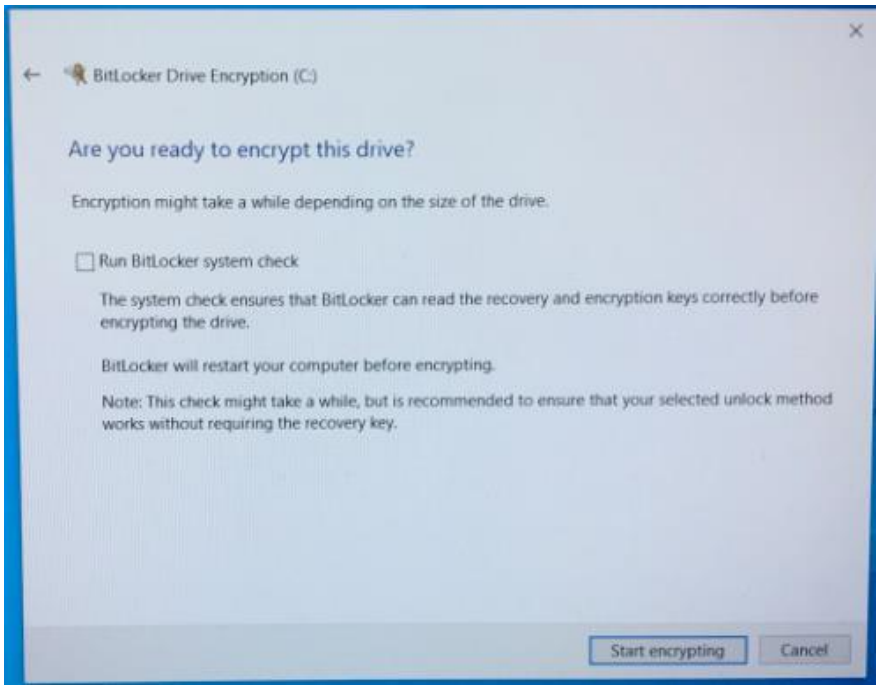
Hinweis: Zum Aktivieren von eDrive auf anderen Laufwerken als dem Betriebssystem-Laufwerk können Sie die gleichen Einstellungen durch die Auswahl von Folgendem übernehmen: **Verwaltungsvorlagen > Windows-Komponenten > BitLocker Laufwerksverschlüsselung > Feste Datenlaufwerke> Verwendung von hardwarebasierter Verschlüsselung für feste Datenlaufwerke konfigurieren (Configure use of hardware-based encryption for fixed data drives) („Aktivieren“ und dann „Übernehmen“)**

4. Verwenden Sie den Windows-Schlüssel, um nach **BitLocker verwalten (Manage BitLocker)** zu suchen und die Anwendung dann auszuführen.

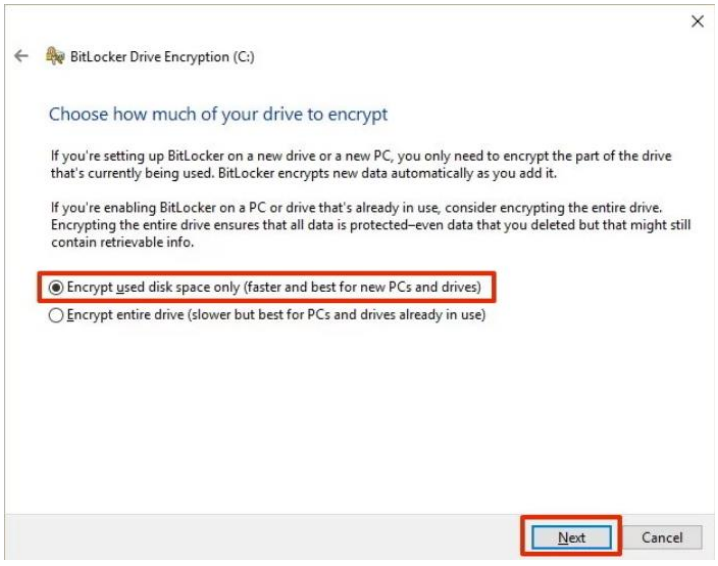


5. Wählen Sie **BitLocker aktivieren (Turn on BitLocker)** im Explorer-Fenster.

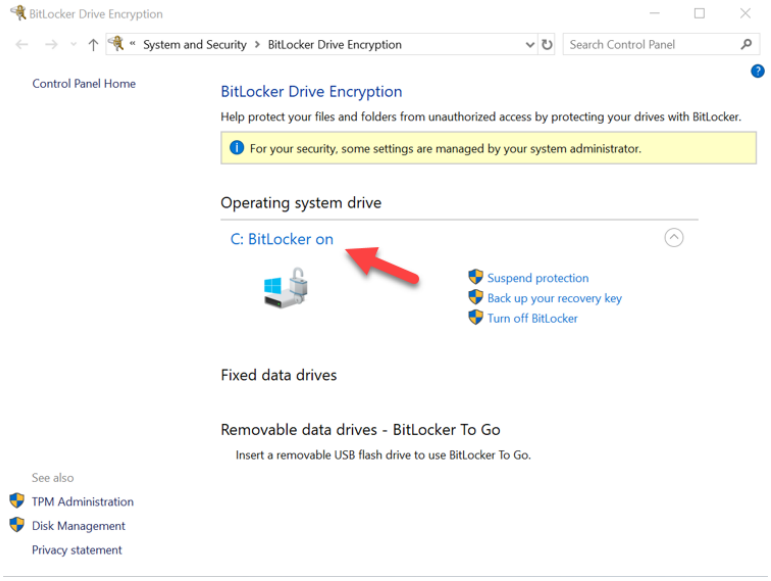
6. Arbeiten Sie alle Eingabeaufforderungen zur Konfiguration der Ziel-SSD ab. Wenn Sie dazu aufgefordert werden, wählen Sie **Verschlüsselung starten (Start encrypting).** Standardmäßig ist **BitLocker Systemtest ausführen (Run BitLocker system check)** aktiviert. Es ist ratsam, mit dieser aktivierten Einstellung fortzufahren. Wenn Sie das Kontrollkästchen deaktivieren, können Sie jedoch bestätigen, ob die Hardwareverschlüsselung aktiviert ist, ohne dass ein Neustart des Systems erforderlich ist.



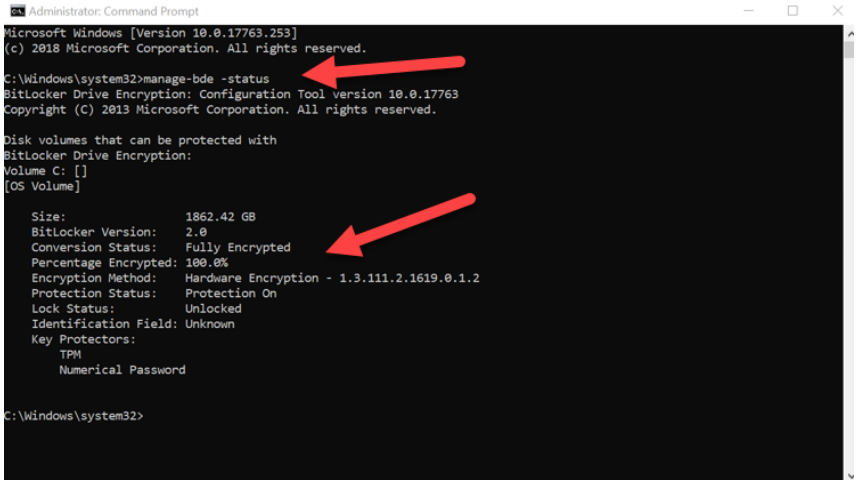
Hinweis: Wenn Sie in einem Fenster aufgefordert werden, „Auswählen, wie viel des Laufwerks verschlüsselt werden soll (Choose how much of your drive to encrypt)“, bedeutet dies oft, dass auf der Ziel-SSD KEINE Hardwareverschlüsselung aktiviert wird, sondern stattdessen eine Softwareverschlüsselung verwendet wird.



7. Starten Sie bei Bedarf das System neu und starten Sie dann **BitLocker verwalten (Manage BitLocker)** neu, um den Verschlüsselungsstatus der Ziel-SSD zu bestätigen.



8. Sie können den Verschlüsselungsstatus der Ziel-SSD auch überprüfen, indem Sie cmd.exe **öffnen und Folgendes eingeben: manage-bde -status**



Microsoft eDrive Support deaktivieren

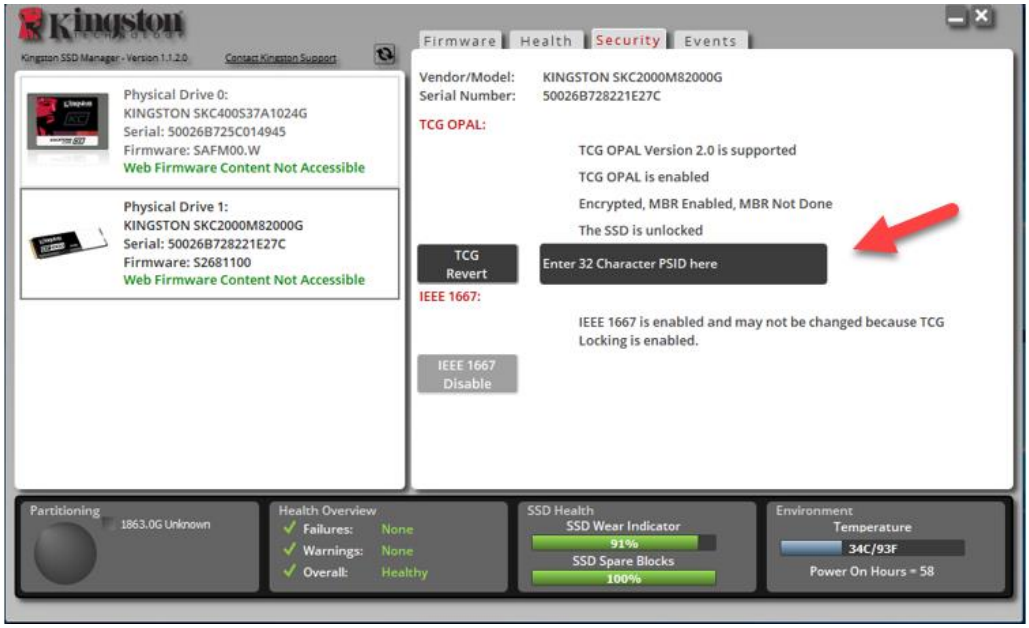
Zum Löschen der Daten Ihrer Ziel-SSDs und zum Entfernen der BitLocker eDrive-Unterstützung vom Laufwerk, führen Sie bitte die folgenden Schritte aus.

Hinweis: Dieser Vorgang setzt Ihre Ziel-SSD zurück und ALLE AUF DEM LAUFWERK VORHANDENEN DATEN GEHEN UNWIEDERBRINGLICH VERLOREN.

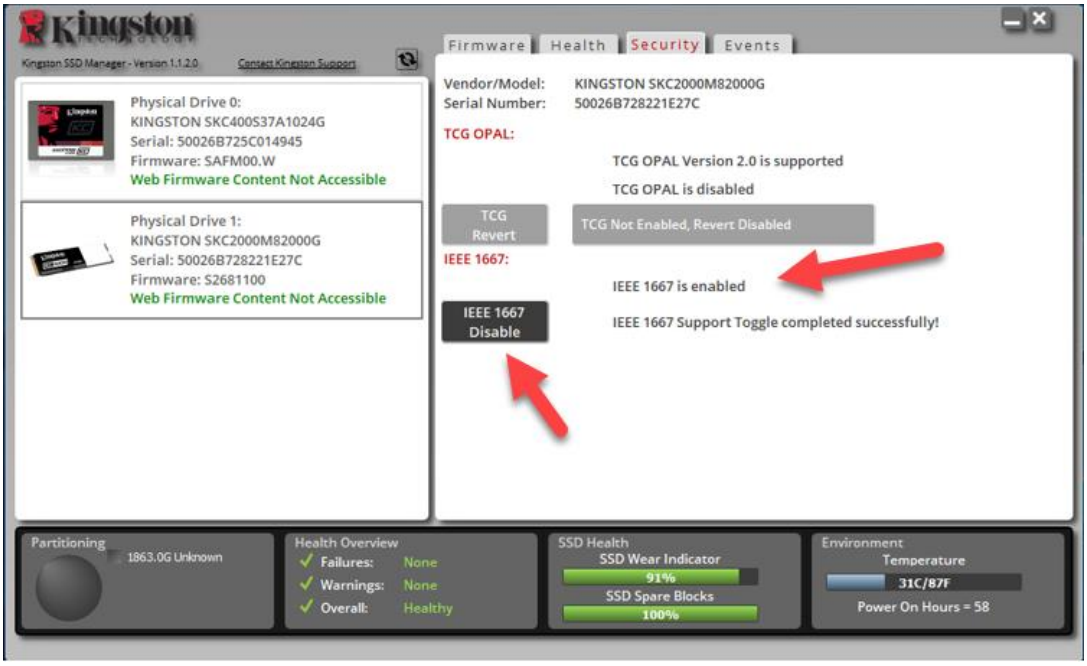
1. Notieren Sie sich den PSID-Wert der Ziel-SSD. Dieser wird auf das Etikett gedruckt.

Bsp.: KC2000 PSID-Wert

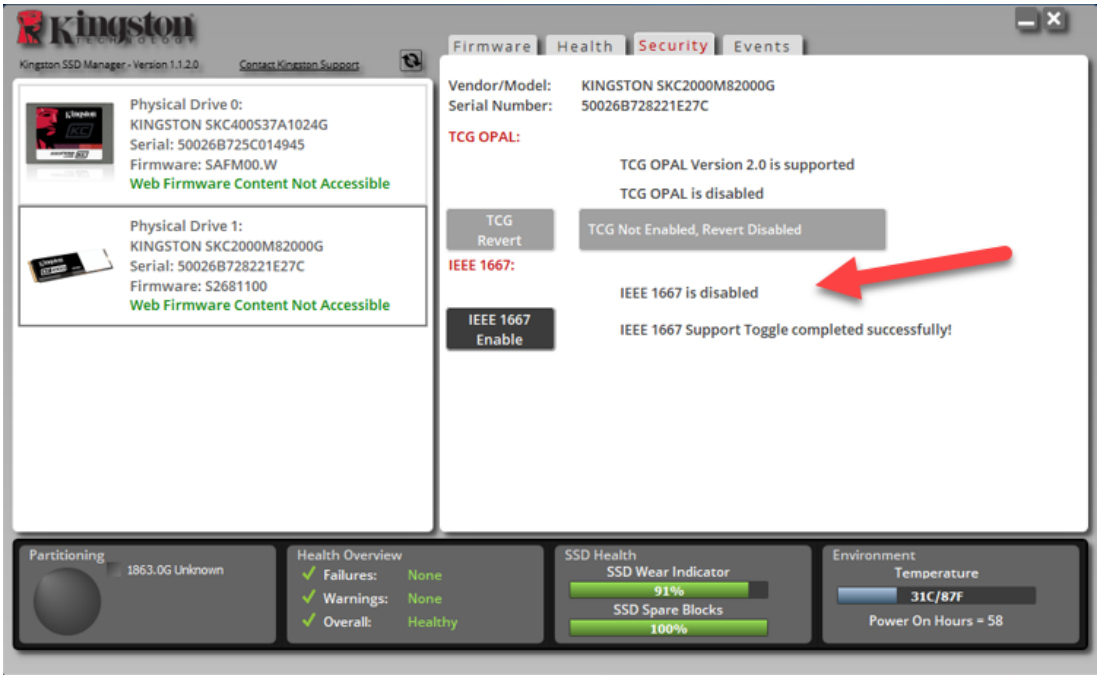
2. Richten Sie die Ziel-SSD als Sekundärlaufwerk ein und führen Sie Kingston SSD Manager (KSM) aus.
3. Wählen Sie die Registerkarte Sicherheit **und führen Sie TCG Zurücksetzen (Revert)** durch, indem Sie den 32-stelligen PSID-Wert aus Schritt 1 eingeben und dann **TCG Zurücksetzen (Revert)** auswählen. Nach Abschluss des Vorgangs wird die Meldung **TCG Zurücksetzen erfolgreich abgeschlossen (TCG Revert completed successfully)** angezeigt. Wenn die Meldung nicht angezeigt wird, geben Sie bitte den PSID-Wert erneut ein und versuchen Sie erneut, das Zurücksetzen durchzuführen.



4. Sobald das Laufwerk erfolgreich zurückgesetzt wurde, haben Sie die Möglichkeit, den IEEE1667-Support zu deaktivieren. Bitte wählen Sie **IEEE1667 deaktivieren (disable)** und warten Sie auf die Meldung „Umschaltung IEEE1667-Support erfolgreich abgeschlossen (IEEE1667 Support Toggle completed successfully)“.



5. Vergewissern Sie sich, dass der IEEE1667-Support deaktiviert ist.



6. Ihre Ziel-SSD ist bereit für die Wiederverwendung.