Kingston Şifrelenmiş SSD'ler

Donanım Şifrelemesini Kullanmak için eDrive ile BitLocker'in Etkinleştirilmesi ve Devre Dışı Bırakılması

Giriş

Bu belgede, Kingston SSD'nizdeki donanım şifrelemesini kullanmak amacıyla Microsoft'un BitLocker eDrive özelliğinin nasıl etkinleştirileceği ya da devre dışı bırakılacağı açıklanmaktadır. Bu işlem, TCG OPAL 2.0 ve IEEE1667 özellik setini destekleyen Kingston SSD'ler için geçerlidir. TCG OPAL 2.0 ve IEEE1667 desteğine sahip bir Kingston SSD'niz yoksa bu işlem işe yaramayacaktır. Emin değilseniz lütfen www.kingston.com/support adresinden Kingston Teknik Destek birimi ile iletişim kurun.

Bu belgenin ilerleyen bölümlerinde Microsoft'un eDrive'lı BitLocker özelliği ‘eDrive' olarak adlandırılacaktır. Aşağıda açıklanan prosedürler, Windows sürümlerine ve güncellemelerine göre farklılık gösterebilir.

Sistem Gereksinimleri

-TCG Opal 2.0 ve IEEE1667 güvenlik özelliği setini kullanan Kingston SSD
-Kingston SSD Manager yazılımı https://www.kingston.com/ssdmanager
-TCG Opal 2.0 ve IEEE1667 güvenlik özelliklerini destekleyen Sistem Donanımı ve BIOS

İşletim Sistemi / BIOS Gereksinimleri

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

Not: Tüm Şifrelenmiş Katı Hal Sürücülerinin (SSD), Windows 8, 10 ve/veya Server 2012'de düzgün çalışması için RAID olmayan denetleyicilere bağlanması gerekmektedir.

Windows 8, 10 ya da Windows Server 2012'de bir Şifrelenmiş Katı Hal Sürücüsünü **veri sürücüsü olarak kullanmak için**:

- Sürücünün başlatılmamış durumda olması gerekmektedir.
- Sürücünün güvenliği devre dışı durumda olması gerekmektedir.

Şifrelenmiş Katı Hal Sürücüleri (SSD) **sistem açılışı sürücüleri** olarak kullanmak için:

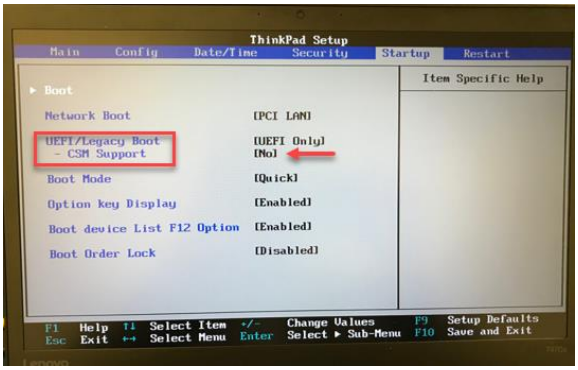
- Sürücünün başlatılmamış durumda olması gerekmektedir.
- Sürücünün güvenliği devre dışı durumda olması gerekmektedir.
- Bilgisayarın UEFI 2.3.1 tabanlı olması ve EFI_STORAGE_SECURITY_COMMAND_PROTOCOL tanımlanmış olmalıdır. (Bu protokol, EFI açılış hizmetleri ortamında çalışan programların, sürücüyle güvenlik protokolü komutları göndermesine izin vermek için kullanılır).
- Bilgisayarda, Uyumluluk Destek Modülünün (Compatibility Support Module - CSM) UEFI'da devre dışı bırakılmış olması gerekmektedir.
- Bilgisayarın her zaman ana olarak UEFI'dan açılıyor olması gerekmektedir.

Daha fazla bilgi için bu adreste bulunan konuyla ilgili Microsoft'un makalesine bakın:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Açılış SSD'de Microsoft eDrive'ın Etkinleştirilmesi

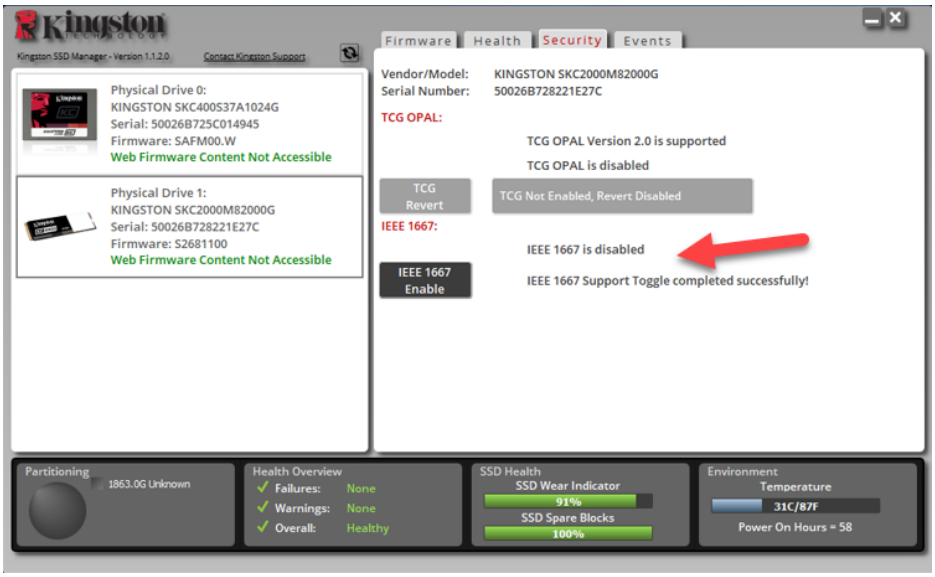
BIOS Yapılandırması

1. Sisteminizin üreticisinin belgelerine bakarak sisteminizin BIOS'unun UEFI 2.3.1 tabanlı ve EFI_STORAGE_SECURITY_COMMAND_PROTOCOL tanımlanmış olduğunu kontrol edin.
2. BIOS'a girin ve Uyumluluk Destek Modülünü (Compatibility Support Module - CSM) devre dışı bırakın.

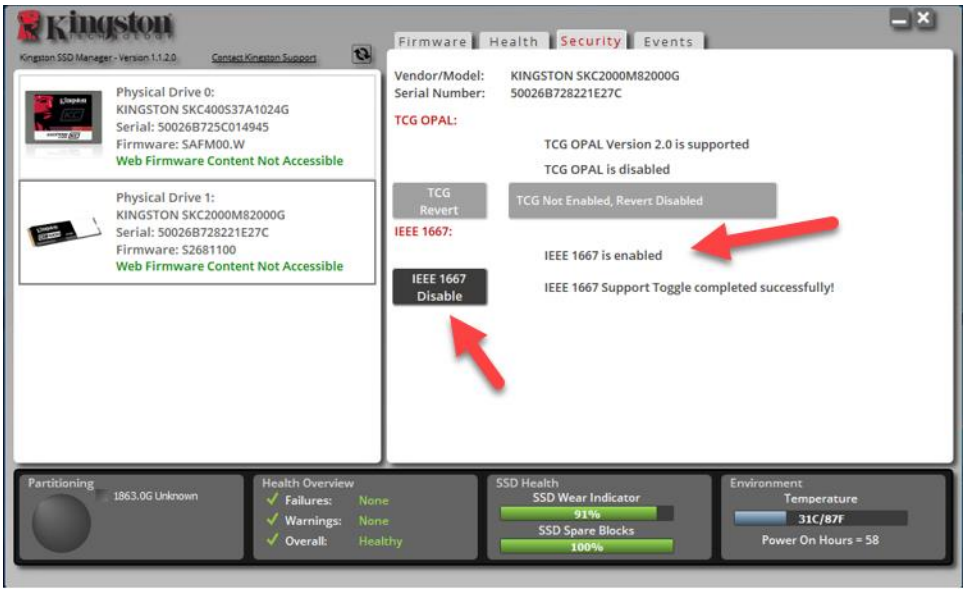


Sürücünün Hazırlanması

1. Kingston SSD Manager'ı (KSM) zaten indirmediyseniz lütfen şimdi indirin. https://www.kingston.com/ssdmanager
2. KSM yazılımını ya da diğer bir endüstri standardı yöntemini kullanarak hedef SSD'yi Güvenli Silin.
3. Hedef SSD'yi, IEEE1667 durumunu onaylamak için ikincil bir disk olarak tanımlayın. Sürücünün **Disabled** (Devre Dışı) modda olması gerekmektedir.



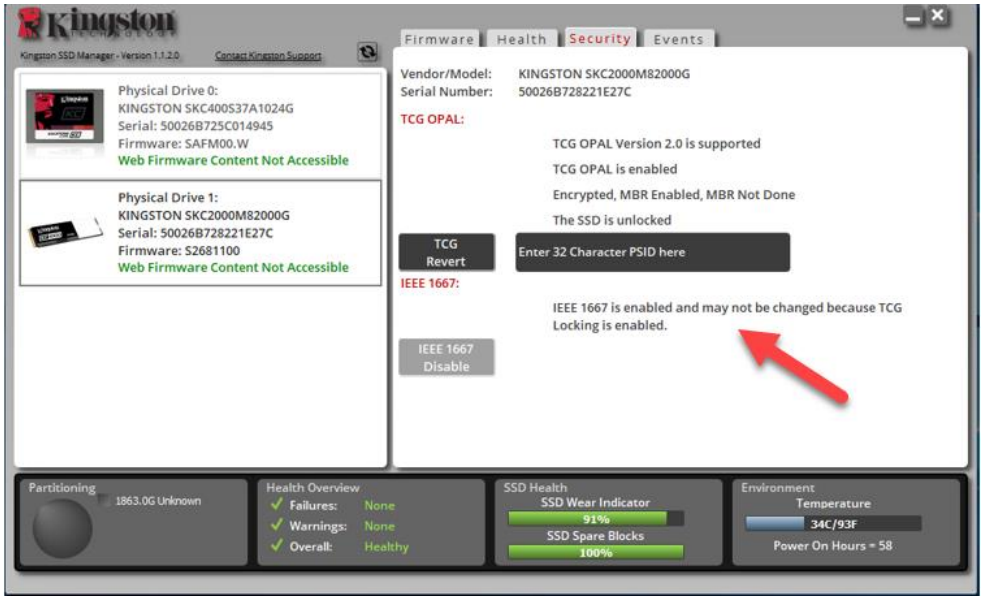
4. IEEE1667 düğmesini seçin ve özelliği **Enable** (Etkinleştir) durumuna getirin. Özelliğin başarıyla değiştiğini onaylayın.



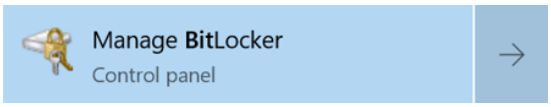
İşletim Sistemi (OS) Kurulumu

Not: Hedef SSD'ye bir işletim sistemini kopyalamayın*. Bir İşletim Sisteminin hedef SSD'ye klonlanması, eDrive kullanarak Donanım Şifrelemesini etkinleştirmenizi önleyecektir. eDrive ile Donanım Şifrelemesinden yararlanmak için hedef SSD'ye yeni bir İşletim Sistemi kurulumu yapmanız gerekecektir.*

1. Hedef SSD'ye desteklenen bir işletim sistemi kurun.
2. İşletim sistemi kurulduktan sonra Kingston SSD Manager'ı (KSM) kurun, KSM'yi çalıştırın, ve uygulamanın Security (Güvenlik) sekmesinde aşağıdaki mesajların var olduğunu onaylayın:
   "IEEE 1667 is enabled an may not be changed because TCG Locking is enabled."

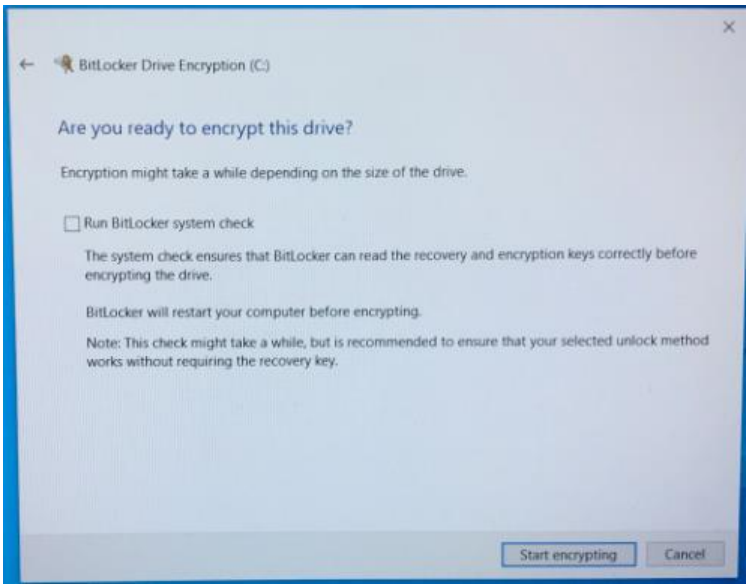


3. Windows Tuşunu kullanarak **Manage BitLocker** (BitLocker'ı Yönet) araması yapın ve uygulamayı çalıştırın.

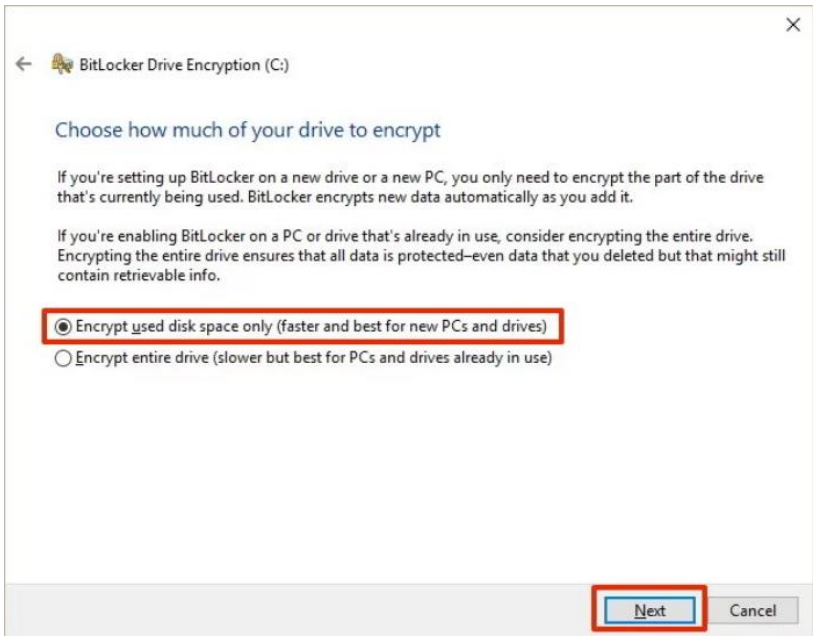


4. Explorer penceresinde **Turn on BitLocker**'ı (BitLocker'ı Aç) seçin.

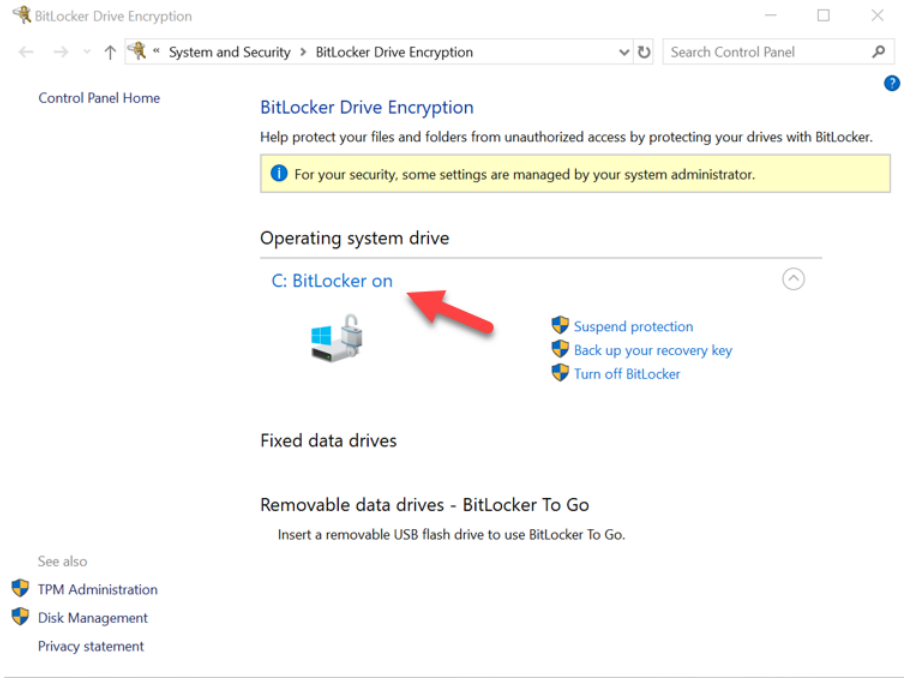
5. Hedef SSD'yi yapılandırmak için istemlerde belirtilenleri gerçekleştirin. Sorulduğunda **Start encrypting'i (Şifrelemeye başla) seçin.** Varsayılan olarak **Run BitLocker system check** (BitLocker sistem kontrolünü çalıştır) seçilidir. Bu ayar etkin halde işleme devam etmeniz önerilir. Ancak işaretli değilse, donanım şifrelemesinin sistemi tekrar başlatmasına gerek olmadan etkinleştirilmesini onaylayabilirsiniz.



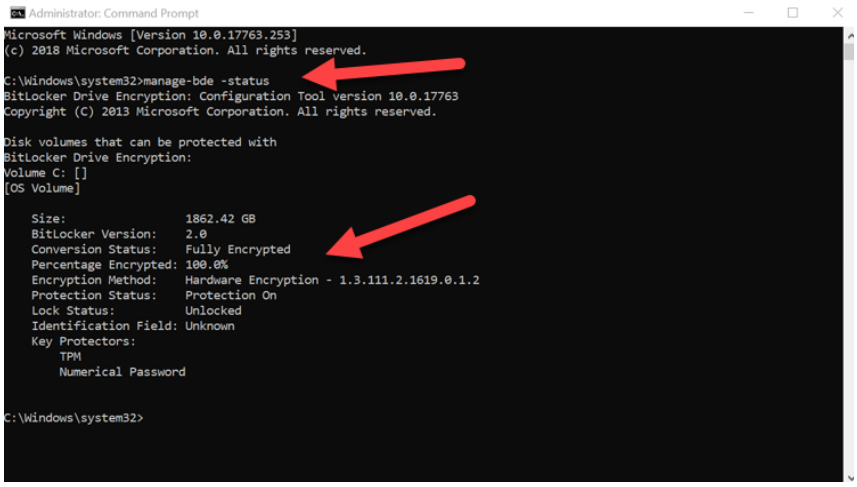
Not: Eğer "Choose how much of your drive to encrypt" (Sürücünüzün ne kadarını şifrelemek istediğiniz seçin) mesajının yer aldığı bir ekran açılırsa bu durum hedef SSD'nin donanım şifrelemesini ETKİNLEŞTİRMEYECEĞİNİ, bunun yerine yazılım şifrelemesini kullanacağını belirtir.



6. Gerektiğinde sistemi yeniden başlatın ve hedef SSD'nin şifreleme durumunu onaylamak için **Manage BitLocker**'ı (BitLocker'ı Yönet) yeniden başlatın.



7. Aynı zamanda hedef SSD'nin şifreleme durumunu kontrol etmek için **cmd.exe**'yi açıp **manage-bde -status** yazabilirsiniz

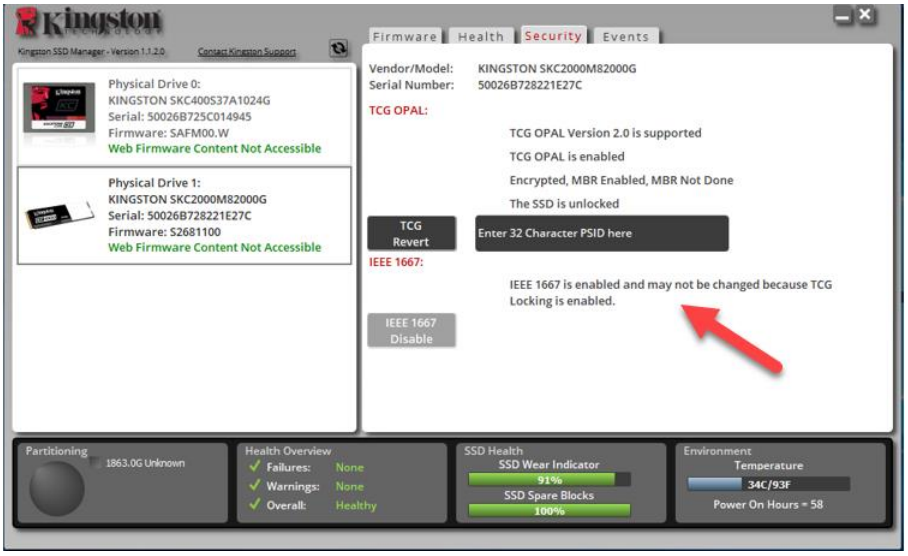


Windows 10'da (sürüm 1903+) Microsoft eDrive'ı etkinleştirme

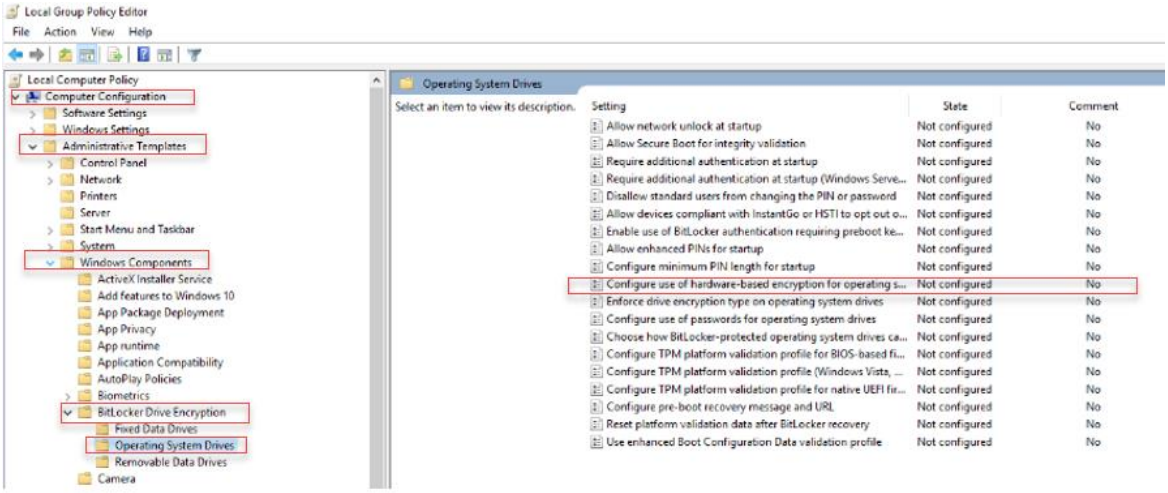
*Microsoft, Windows 10 sürüm 1903'ü çıkarttığında eDrive şifreleme açısından Windows 10'un varsayılan davranışını değiştirdi. Bu sürümde ve muhtemelen ilerideki sürümlerde eDrive'ı etkinleştirmek için **gpedit**'i çalıştırarak donanım Şifrelemesini etkinleştirmeniz gerekecektir.*

***Not: Hedef SSD'ye bir işletim sistemini kopyalamayın**. Bir İşletim Sisteminin hedef SSD'ye klonlanması, eDrive kullanarak Donanım Şifrelemesini etkinleştirmenizi önleyecektir. eDrive ile Donanım Şifrelemesinden yararlanmak için hedef SSD'ye yeni bir İşletim Sistemi kurulumu yapmanız gerekecektir.*

1. Hedef SSD'ye desteklenen bir işletim sistemi kurun.
2. İşletim sistemi kurulduktan sonra Kingston SSD Manager'ı (KSM) kurun, KSM'yi çalıştırın, ve uygulamanın Security (Güvenlik) sekmesinde aşağıdaki mesajların var olduğunu onaylayın:
   "IEEE 1667 is enabled an may not be changed because TCG Locking is enabled."

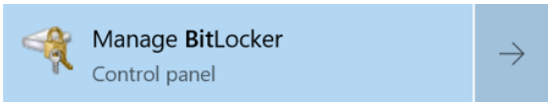


3. Şifreleme ayarlarını değiştirmek için gpedit.msc'yi çalıştırın.
    a. **Administrative Templates> Windows Components> BitLocker Drive Encryption> Operating System Drives** (Yönetici Şablonlar> Windows Bileşenleri> BitLocker Sürücü Şifrelemesi > İşletim Sistemi Sürücüleri) kısmına ilerleyin
    b. Daha sonra **Configure use of hardware-based encryption for operating systems**'i (İşletim sistemleri için donanım tabanlı şifrelemenin kullanımını yapılandır) seçin
    c. **Özelliği etkinleştirin** ve ayarı **Uygulayın**



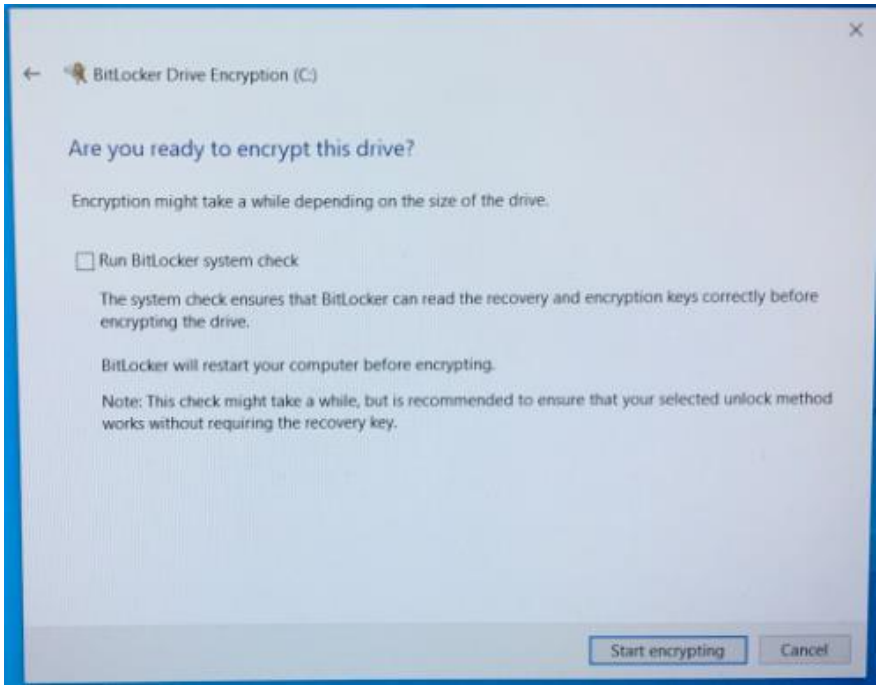
Not: İşletim Sistemi sürücüsü dışından sürücülerde eDrive'ı etkinleştirmek için bunu seçin: **Administrative Templates> Windows Components> BitLocker Drive Encryption> Fixed Data Drives> Configure use of hardware-based encryption for fixed data drives (Yönetici Şablonlar> Windows Bileşenleri> BitLocker Sürücü Şifrelemesi > Sabit Veri Sürücüleri > Sabit veri sürücüleri için donanım tabanlı şifrelemenin kullanımını yapılandırın) (Etkinleştirin ve Uygulayın)**

4. Windows Tuşunu kullanarak **Manage BitLocker** (BitLocker'ı Yönet) araması yapın ve uygulamayı çalıştırın.

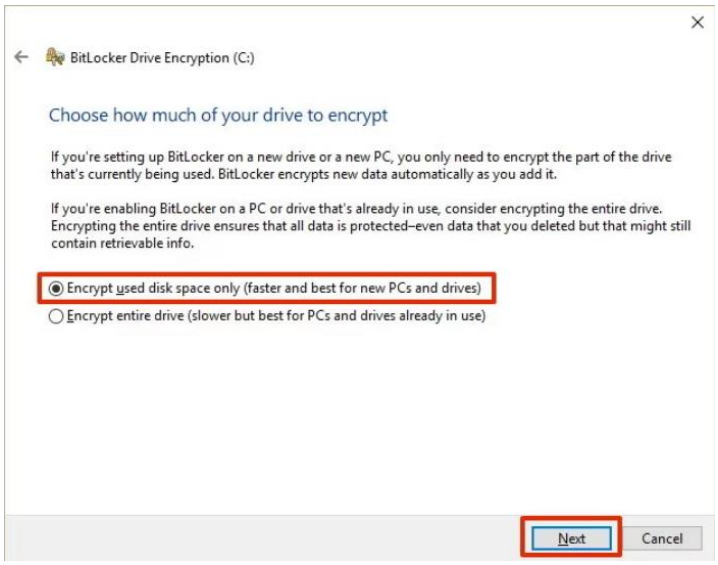


5. Explorer penceresinde **Turn on BitLocker**'ı (BitLocker'ı Aç) seçin.

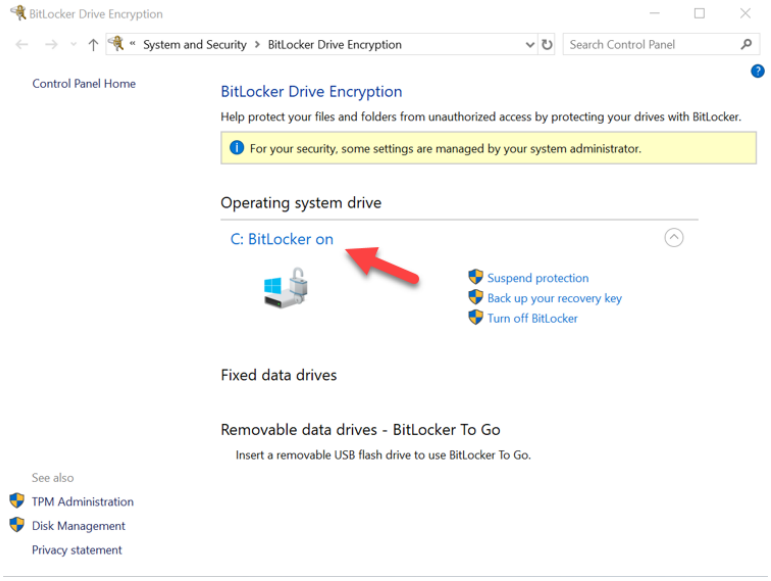
6. Hedef SSD'yi yapılandırmak için istemlerde belirtilenleri gerçekleştirin. Sorulduğunda **Start encrypting'i (Şifrelemeye başla) seçin.** Varsayılan olarak **Run BitLocker system check** (BitLocker sistem kontrolünü çalıştır) seçilidir. Bu ayar etkin halde işleme devam etmeniz önerilir. Ancak işaretli değilse, donanım şifrelemesinin sistemi tekrar başlatmasına gerek olmadan etkinleştirilmesini onaylayabilirsiniz.



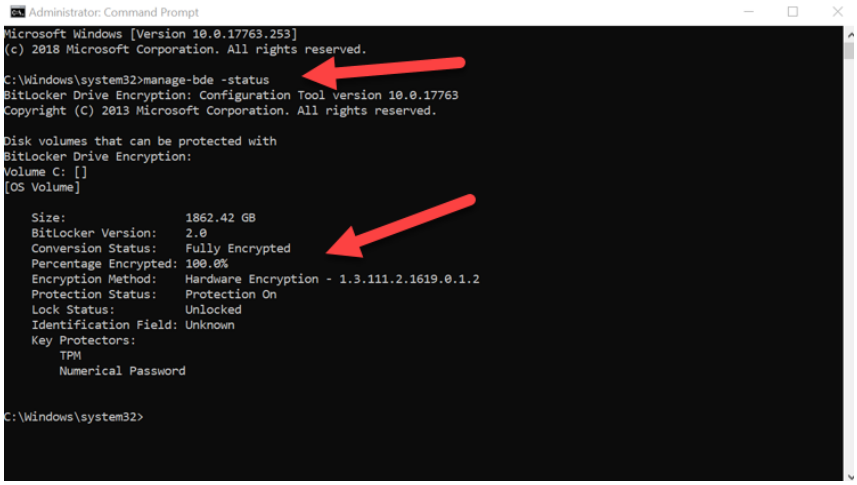
Not: Eğer "Choose how much of your drive to encrypt" (Sürücünüzün ne kadarını şifrelemek istediğiniz seçin) mesajının yer aldığı bir ekran açılırsa bu durum hedef SSD'nin donanım şifrelemesini ETKİNLEŞTİRMEYECEĞİNİ, bunun yerine yazılım şifrelemesini kullanacağını belirtir.



7. Gerektiğinde sistemi yeniden başlatın ve hedef SSD'nin şifreleme durumunu onaylamak için **Manage BitLocker**'ı (BitLocker'ı Yönet) yeniden başlatın.



8. Aynı zamanda hedef SSD'nin şifreleme durumunu kontrol etmek için **cmd.exe**'yi açıp **manage-bde -status** yazabilirsiniz



Microsoft eDrive Desteğini Devre Dışı Bırakma

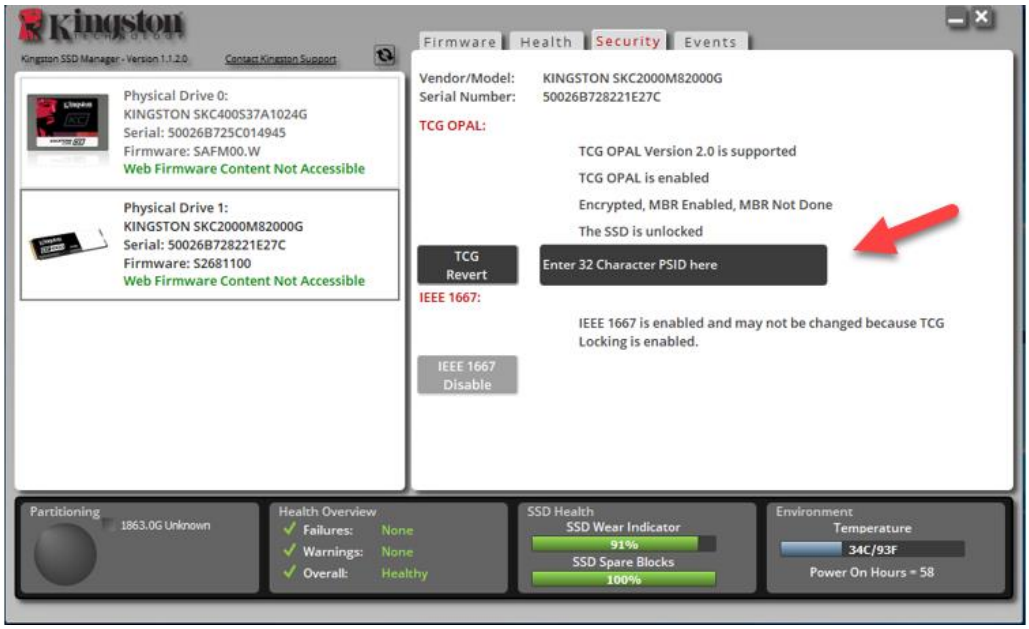
Hedef SSD'lerinizdeki verileri silmek ve sürücüden BitLocker eDrive desteğini kaldırmak için lütfen aşağıdaki adımları uygulayın.

Not: Bu işlem Hedef SSD'nizi sıfırlar ve SÜRÜCÜDE YER ALAN TÜM VERİLER KAYBOLUR.

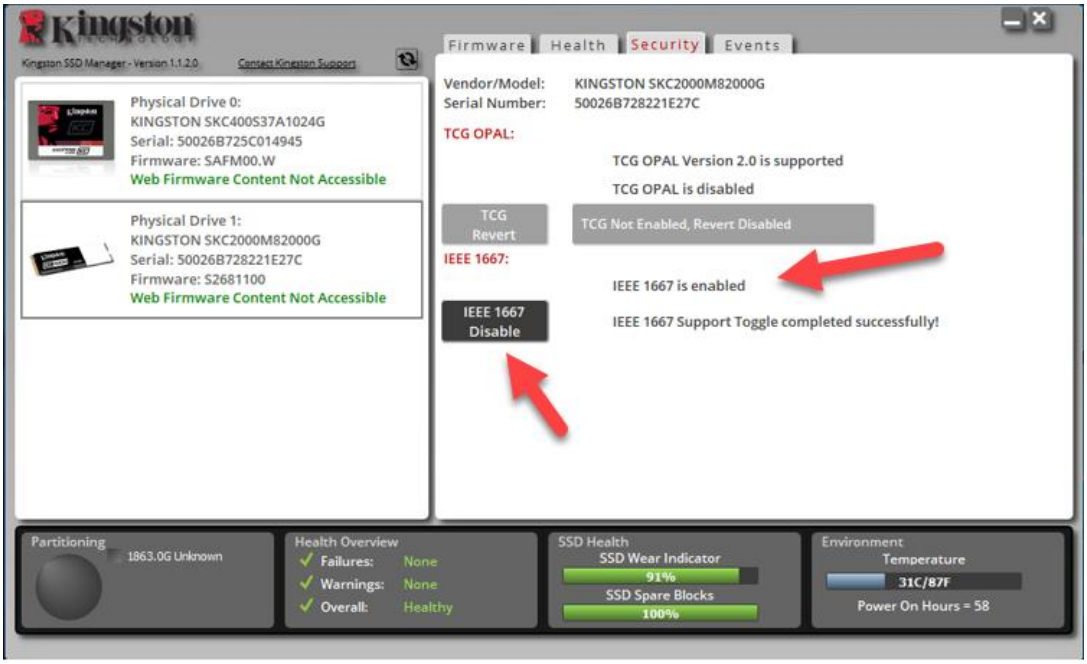
1. Hedef SSD'nin PSID değerini bir yere yazın. Bu bilgi, etiket üzerinde basılıdır.

Ör: KC2000 PSID Değeri

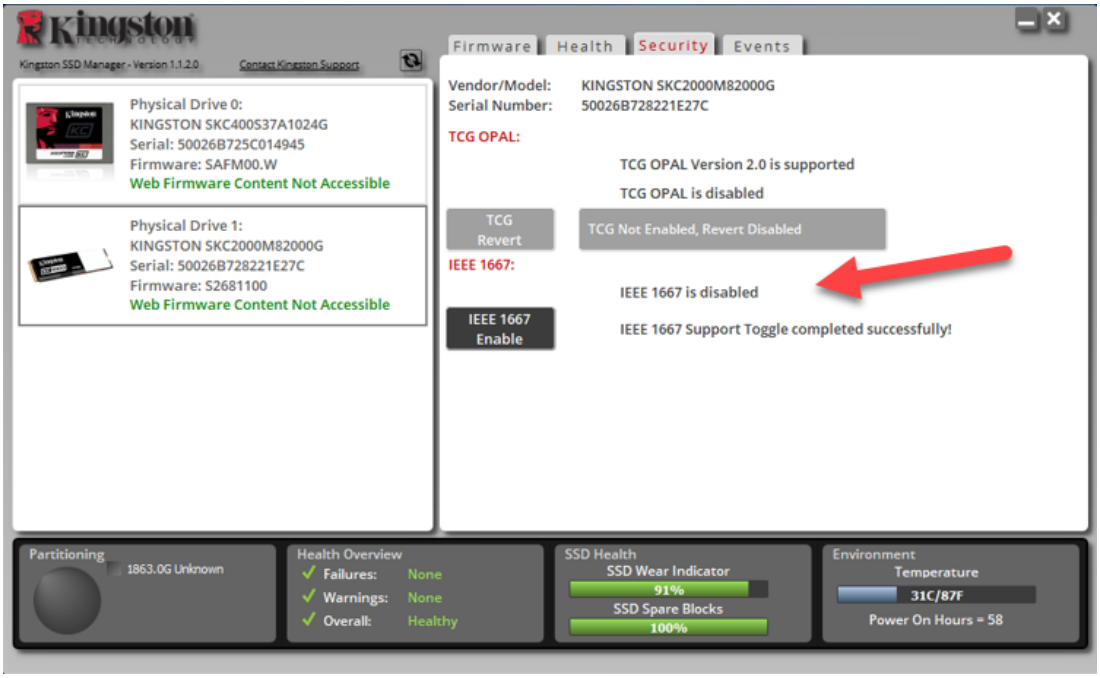
2. Hedef SSD'yi ikincil sürücü olarak tanımlayın ve Kingston SSD Manager'ı (KSM) çalıştırın.
3. **Güvenlik** sekmesini seçin ve birinci adımdaki 32-basamaklı PSID değerini girerek ve ardından **TCG Revert seçerek TCG Revert** gerçekleştirin. Tamamlandığında **TCG Revert completed successfully** (TCG Revert başarıyla tamamlandı) mesajı görürsünüz. Mesaj yoksa, lütfen PSID değerini tekrar girin ve geri çevirmeyi tekrar deneyin.



4. Sürücü başarıyla geri çevrildiğinde IEEE1667 desteğini devre dışı bırakma seçeneğine sahip olacaksınız. Lütfen **IEEE1667 Disable**'yi (IEEE1667 Devre Dışı) seçin ve "IEEE1667 Support Toggle completed successfully" (IEEE1667 Desteği Değiştirmesi başarıyla tamamlandı) mesajı bekleyin.



5. IEEE1667 desteğinin devre dışı kaldığını onaylayın.



6. Hedef SSD'niz yeniden kullanıma hazırdır.