SSD mã hóa Kingston

Bật và tắt BitLocker với eDrive để tận dụng mã hóa phần cứng

Giới thiệu

Tài liệu này mô tả cách bật và tắt tính năng BitLocker eDrive của Microsoft để tận dụng mã hóa phần cứng trên SSD Kingston của bạn. Quy trình này áp dụng với SSD Kingston hỗ trợ bộ tính năng TCG OPAL 2.0 và IEEE1667. Nếu bạn không có SSD Kingston hỗ trợ TCG OPAL 2.0 và IEEE1667, quá trình này sẽ không hoạt động. Nếu bạn không chắc chắn, vui lòng liên hệ Hỗ trợ kỹ thuật của Kingston tại www.kingston.com/vn/support

Tài liệu này sẽ sử dụng 'eDrive' để chỉ BitLocker với eDrive của Microsoft trong toàn bộ phần còn lại của hướng dẫn. Các quy trình được mô tả dưới đây có thể thay đổi tùy thuộc vào phiên bản Windows và các bản cập nhật.

Yêu cầu hệ thống

-SSD Kingston sử dụng bộ tính năng bảo mật TCG Opal 2.0 và IEEE1667
-Phần mềm Kingston SSD Manager https://www.kingston.com/ssdmanager
-Phần cứng hệ thống và BIOS hỗ trợ các tính năng bảo mật TCG Opal 2.0 và IEEE1667

Yêu cầu HĐH/BIOS

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

Lưu ý: Tất cả ổ cứng thể rắn mã hóa phải được gắn vào các bộ điều khiển phi RAID để hoạt động bình thường trên Windows 8, 10 và/hoặc Server 2012

Để sử dụng ổ cứng thể rắn trên Windows 8, 10 hoặc Windows Server 2012 làm **ổ dữ liệu**:

- Ổ phải trong trạng thái chưa khởi tạo.
- Ổ phải trong trạng thái không hoạt động bảo mật.

Đối với ổ cứng thể rắn mã hóa sử dụng làm **ổ khởi động**:

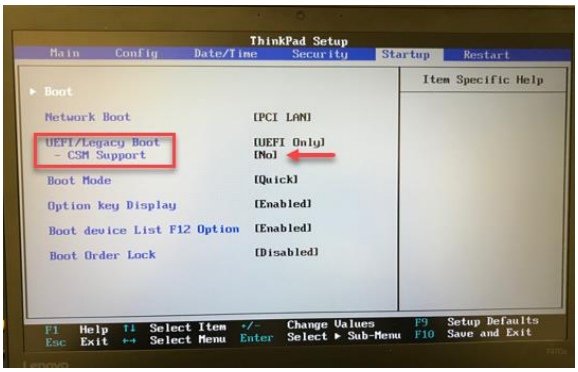
- Ổ phải trong trạng thái chưa khởi tạo.
- Ổ phải trong trạng thái không hoạt động bảo mật.
- Máy tính phải chạy trên UEFI 2.3.1 và có giao thức EFI_STORAGE_SECURITY_COMMAND_PROTOCOL được định nghĩa. (Giao thức này được dùng để cho phép các chương trình chạy trong môi trường dịch vụ khởi động EFI gửi các lệnh giao thức bảo mật đến ổ).
- Máy tính phải có Mô-đun Hỗ trợ Tương thích (CSM) được tắt đi trong UEFI.
- Máy tính phải luôn khởi động trực tiếp từ UEFI.

Để biết thêm thông tin, vui lòng tham khảo bài viết của Microsoft về chủ đề này tại đây:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Bật Microsoft eDrive trên SSD khởi động

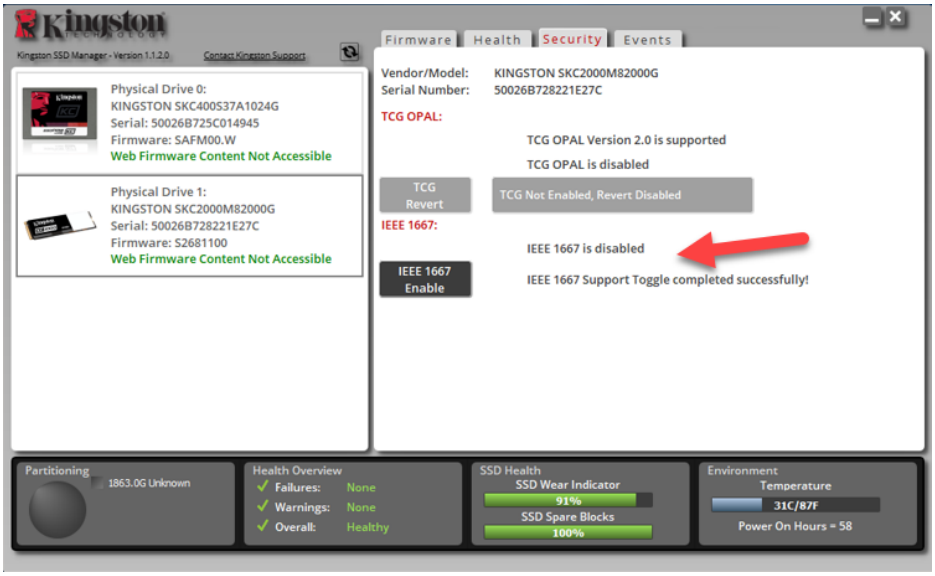
Cấu hình BIOS

1. Tham khảo tài liệu của nhà sản xuất hệ thống của bạn để xác nhận BIOS của hệ thống chạy trên UEFI 2.3.1 và có giao thức EFI_STORAGE_SECURITY_COMMAND_PROTOCOL được định nghĩa.
2. Vào BIOS và tắt Mô-đun Hỗ trợ Tương thích (CSM)

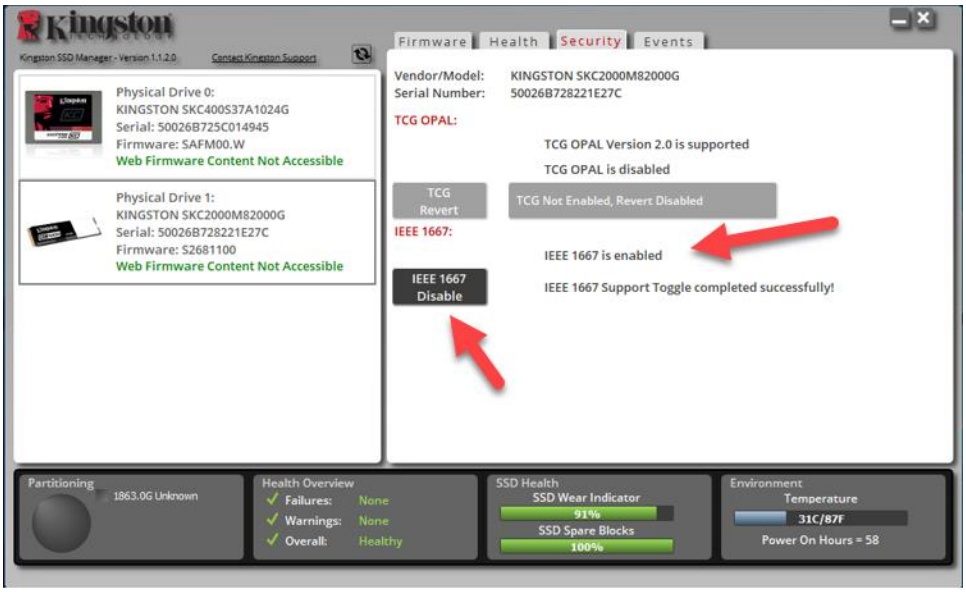


Chuẩn bị ổ

1. Nếu bạn chưa tải về SSD Manager của Kingston (KSM), vui lòng tải về ngay. https://www.kingston.com/ssdmanager
2. Xóa bảo mật SSD đích sử dụng phần mềm KSM hoặc phương thức tiêu chuẩn ngành khác.
3. Gắn SSD đích làm ổ phụ để xác nhận trạng thái IEEE1667. Ổ này cần ở trong chế độ **Disabled**.



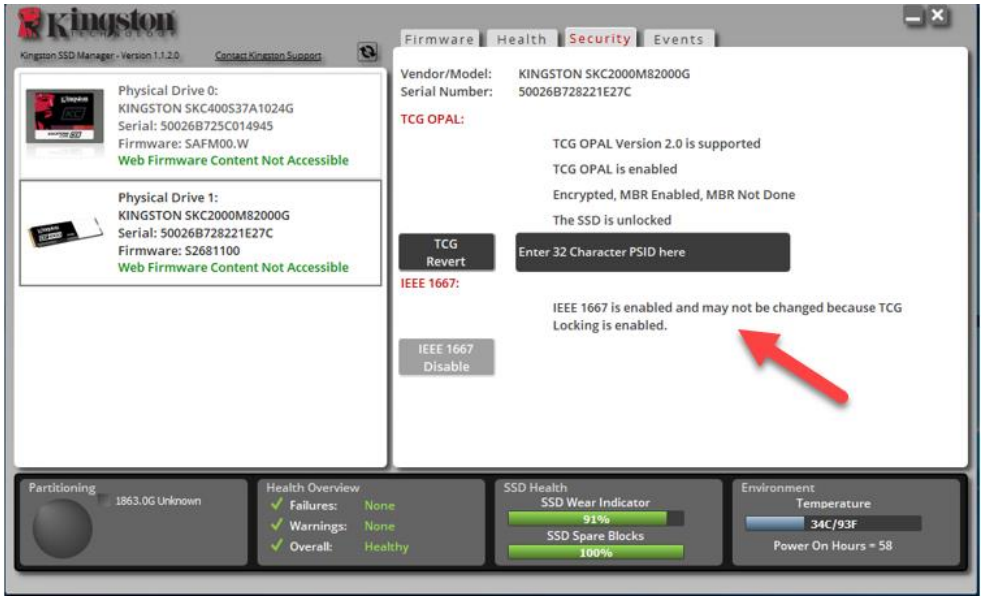
4. Chọn nút IEEE1667 và **Enable** tính năng. Xác nhận tính năng được bật thành công.



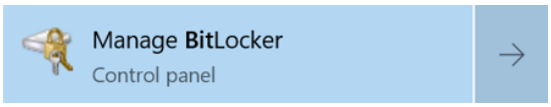
Cài đặt hệ điều hành (HĐH)

***Lưu ý: Không nhân bản hệ điều hành sang SSD đích của bạn**. Nhân bản HĐH sang SSD đích sẽ ngăn bạn bật Mã hóa Phần cứng sử dụng eDrive. Bạn phải tiến hành cài đặt HĐH mới hoàn toàn lên SSD đích để tận dụng Mã hóa Phần cứng với eDrive.*

1. Cài đặt HĐH được hỗ trợ trên SSD đích.
2. Sau khi cài đặt HĐH, hãy cài đặt Kingston SSD manager (KSM), chạy KSM, và xác nhận rằng thông điệp sau xuất hiện trên thẻ Security bên trong ứng dụng:
   "IEEE 1667 is enabled an may not be changed because TCG Locking is enabled."

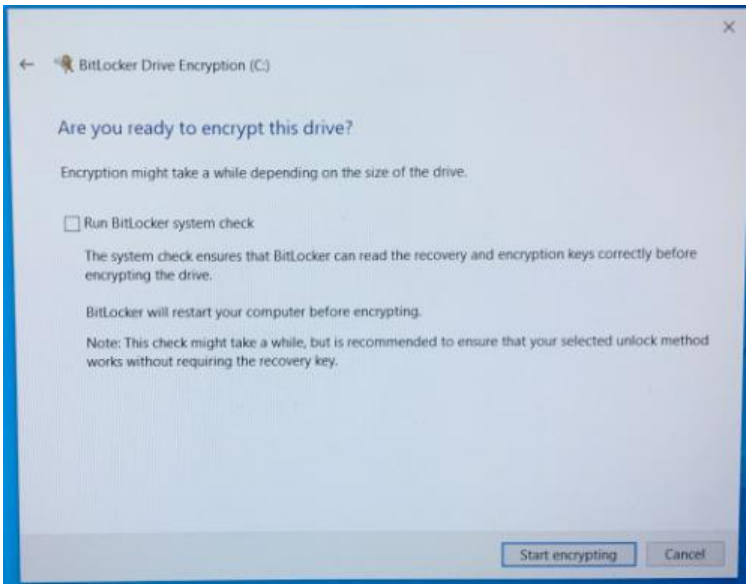


3. Sử dụng phím Windows để tìm kiếm **Manage BitLocker** và sau đó chạy ứng dụng.

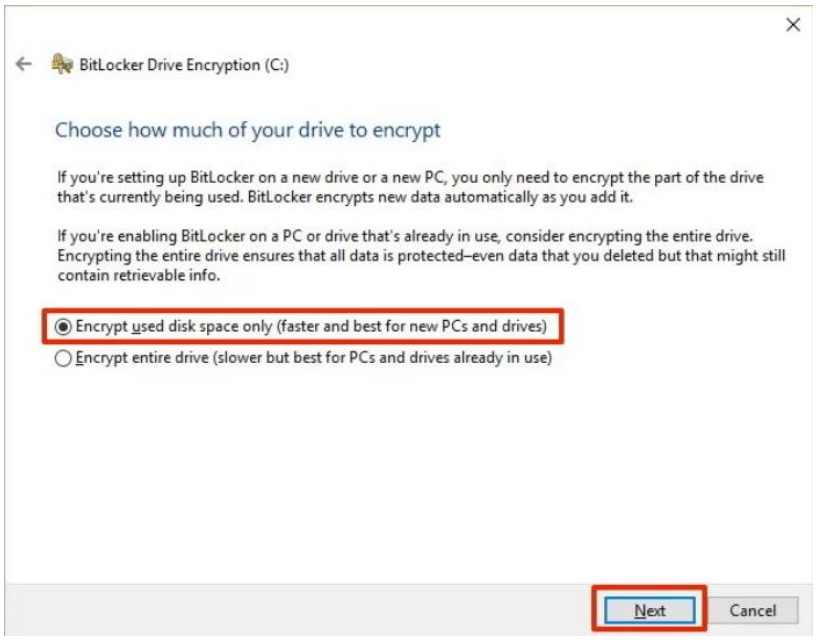


4. Chọn **Turn on BitLocker** từ bên trong cửa sổ Explorer.

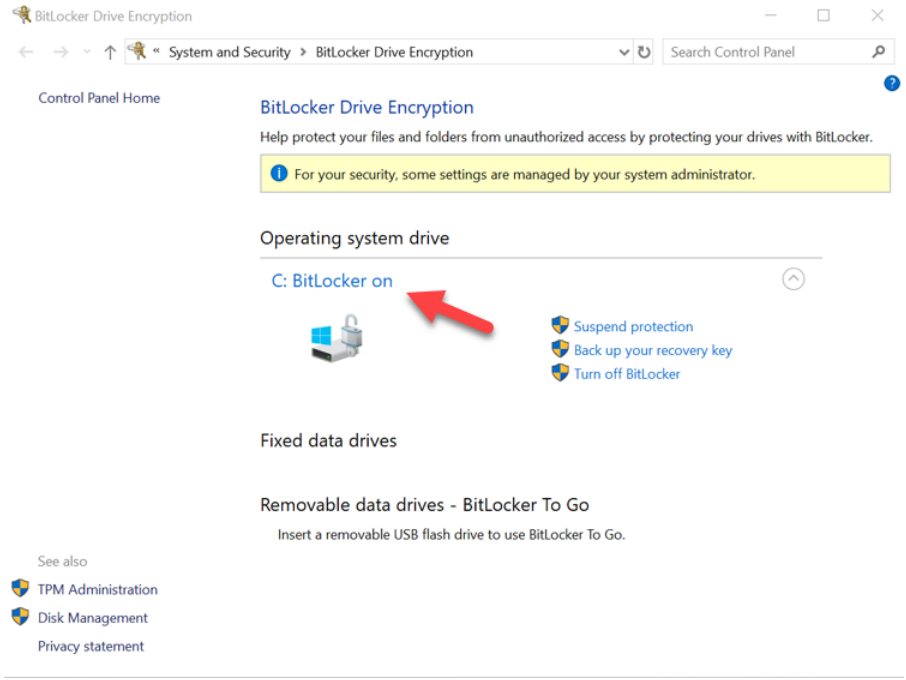
5. Tiếp tục làm theo các lời nhắc để cấu hình SSD đích. Khi được yêu cầu, hãy chọn **Start encrypting.**
Theo mặc định, **Run BitLocker system check** được chọn. Bạn nên tiến hành với tùy chọn này bật. Tuy nhiên, khi bỏ chọn, bạn sẽ có thể xác nhận xem mã hóa phần cứng có bật hay không mà không yêu cầu khởi động lại hệ thống.



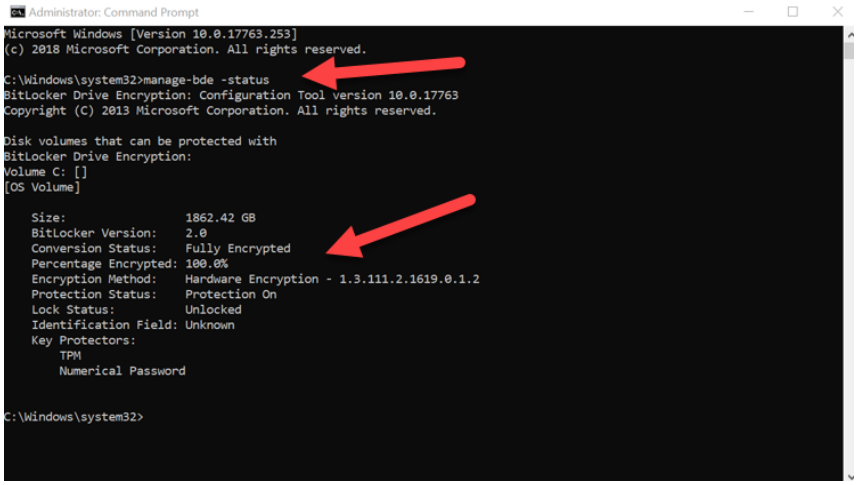
Lưu ý: Nếu bạn gặp một màn hình yêu cầu bạn "Choose how much of your drive to encrypt", điều này thường cho biết rằng SSD đích sẽ KHÔNG bật mã hóa phần ứng mà thay vào đó sẽ sử dụng mã hóa phần mềm.



6. Nếu được yêu cầu, hãy khởi động lại hệ thống và sau đó mở lại **Manage BitLocker** để xác nhận trạng thái mã hóa của SSD đích.



7. Bạn cũng có thể kiểm tra trạng thái mã hóa của SSD đích bằng cách mở **cmd.exe** và gõ: **manage-bde -status**

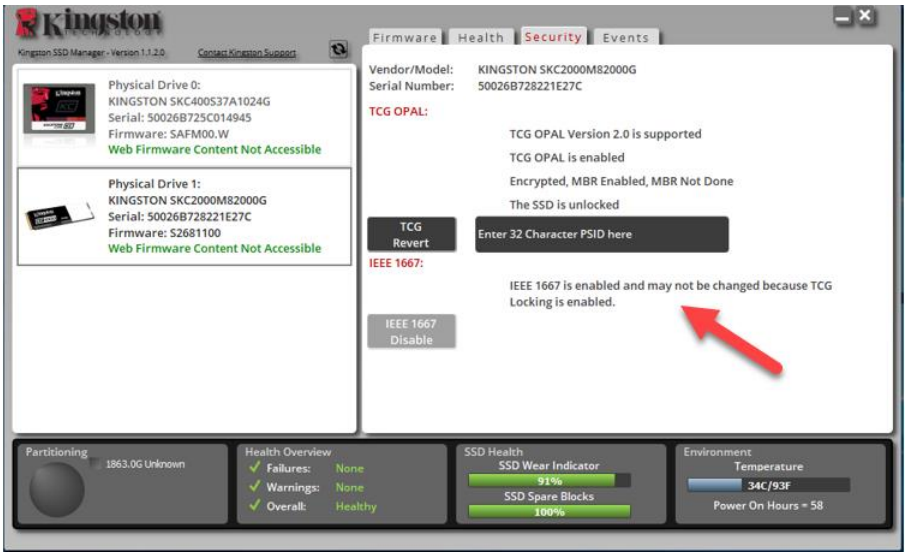


Bật Microsoft eDrive với Windows 10 (phiên bản 1903+)

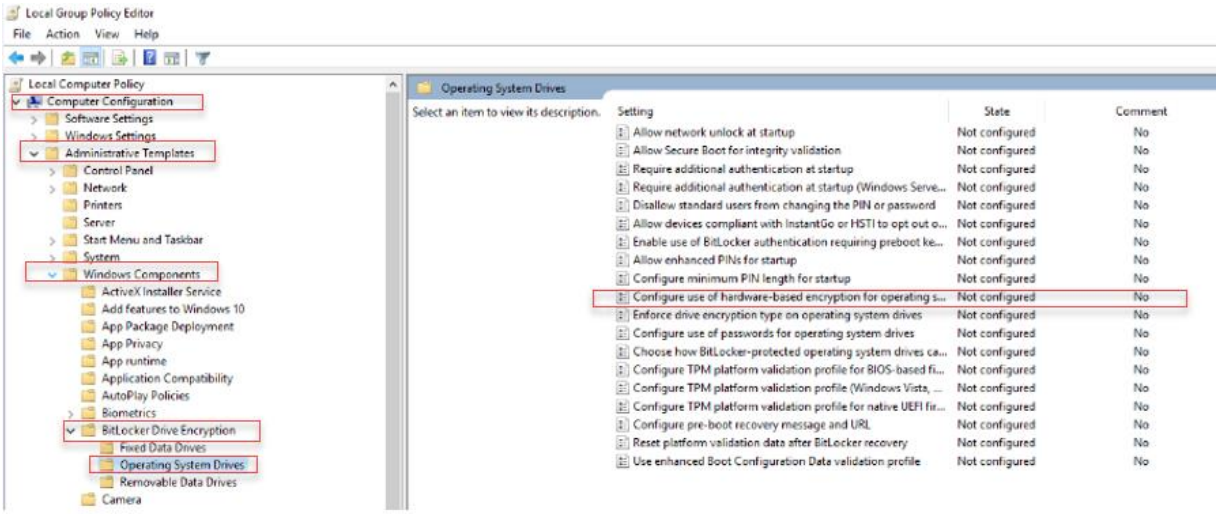
*Microsoft đã thay đổi hành vi mặc định của Windows 10 đối với mã hóa eDrive khi phát hành Windows 10 phiên bản 1903. Để bật eDrive trong bản dựng này và có thể ở các bản sau này, bạn sẽ cần chạy **gpedit** để bật mã hóa phần cứng.*

***Lưu ý: Không nhân bản hệ điều hành sang SSD đích của bạn**. Nhân bản HĐH sang SSD đích sẽ ngăn bạn bật Mã hóa Phần cứng sử dụng eDrive. Bạn phải tiến hành cài đặt HĐH mới hoàn toàn lên SSD đích để tận dụng Mã hóa Phần cứng với eDrive.*

1. Cài đặt HĐH được hỗ trợ trên SSD đích.
2. Sau khi cài đặt HĐH, hãy cài đặt Kingston SSD manager (KSM), chạy KSM, và xác nhận rằng thông điệp sau xuất hiện trên thẻ Security bên trong ứng dụng:
   "IEEE 1667 is enabled an may not be changed because TCG Locking is enabled."

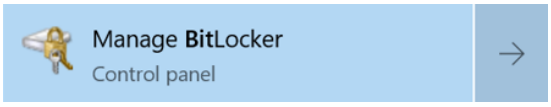


3. Chạy gpedit.msc để sửa đổi cài đặt mã hóa.
    a. Di chuyển đến **Administrative Templates> Windows Components> BitLocker Drive Encryption> Operating System Drives**
    b. Sau đó chọn **Configure use of hardware-based encryption for operating systems**
    c. **Bật** tính năng và sau đó **Áp dụng** cài đặt.



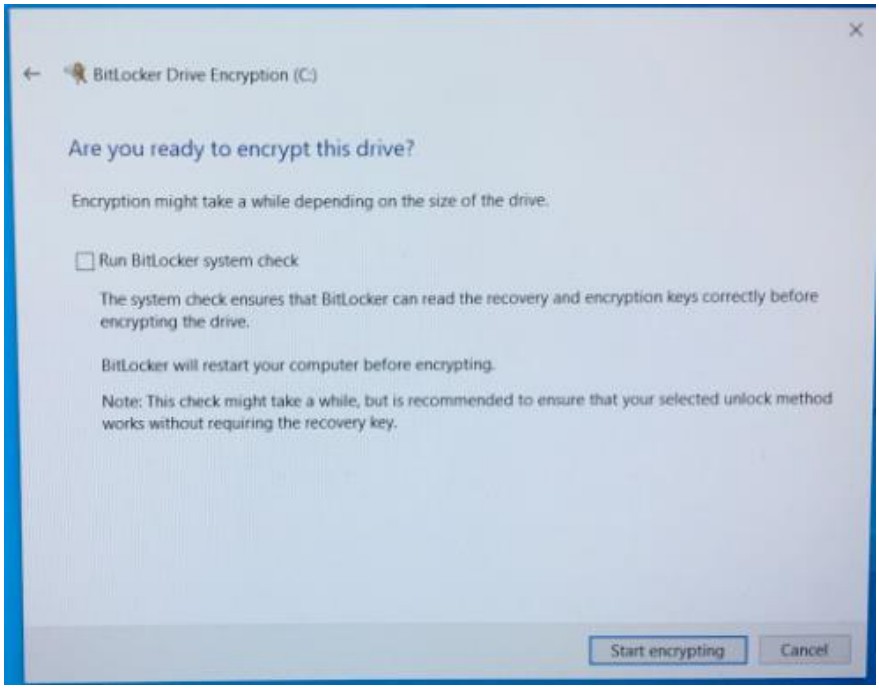
Lưu ý: Để bật eDrive trên các ổ khác ngoài ổ chứa hệ điều hành, bạn có thể áp dụng các cài đặt tương tự bằng cách: **Administrative Templates> Windows Components> BitLocker Drive Encryption> Fixed Data Drives> Configure use of hardware-based encryption for fixed data drives (Bật và sau đó Áp dụng)**

4. Sử dụng phím Windows để tìm kiếm **Manage BitLocker** và sau đó chạy ứng dụng.

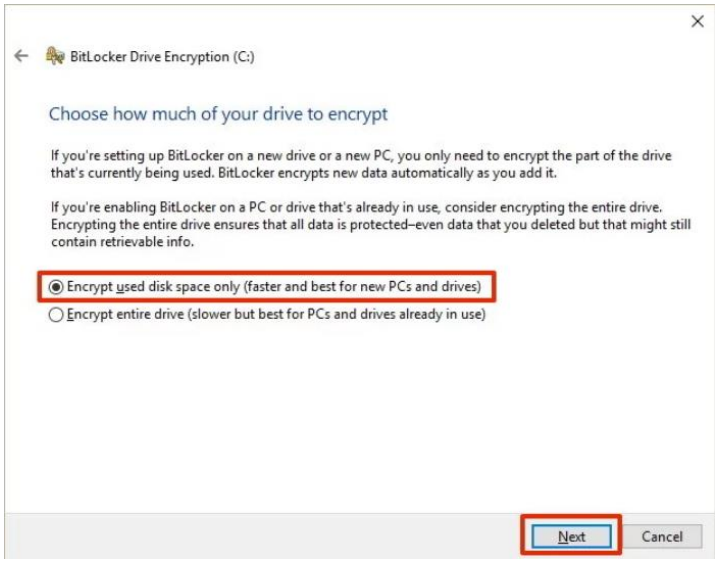


5. Chọn **Turn on BitLocker** từ cửa sổ Explorer.

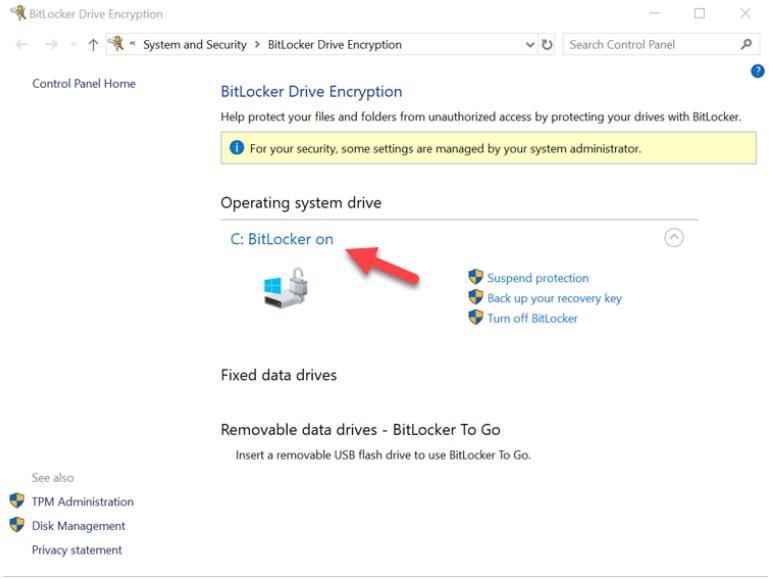
6. Tiếp tục làm theo các lời nhắc để cấu hình SSD đích. Khi được yêu cầu, hãy chọn **Start encrypting.** Theo mặc định, **Run BitLocker system check** được chọn. Bạn nên tiến hành với tùy chọn này bật. Tuy nhiên, khi bỏ chọn, bạn sẽ có thể xác nhận xem mã hóa phần cứng có bật hay không mà không yêu cầu khởi động lại hệ thống.



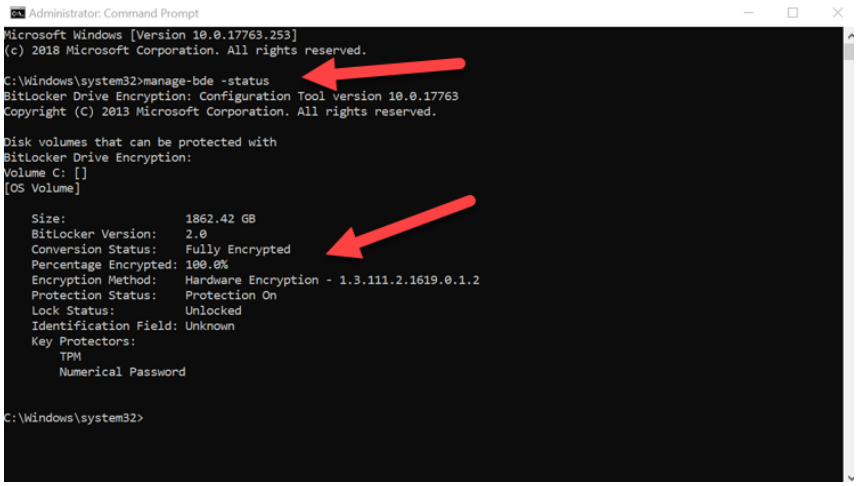
Lưu ý: Nếu bạn gặp một màn hình yêu cầu bạn "Choose how much of your drive to encrypt", điều này thường cho biết rằng SSD đích sẽ KHÔNG bật mã hóa phần ứng mà thay vào đó sẽ sử dụng mã hóa phần mềm.



7. Nếu được yêu cầu, hãy khởi động lại hệ thống và sau đó mở lại **Manage BitLocker** để xác nhận trạng thái mã hóa của SSD đích.



8. Bạn cũng có thể kiểm tra trạng thái mã hóa của SSD đích bằng cách mở **cmd.exe** và gõ: **manage-bde -status**



Tắt hỗ trợ Microsoft eDrive

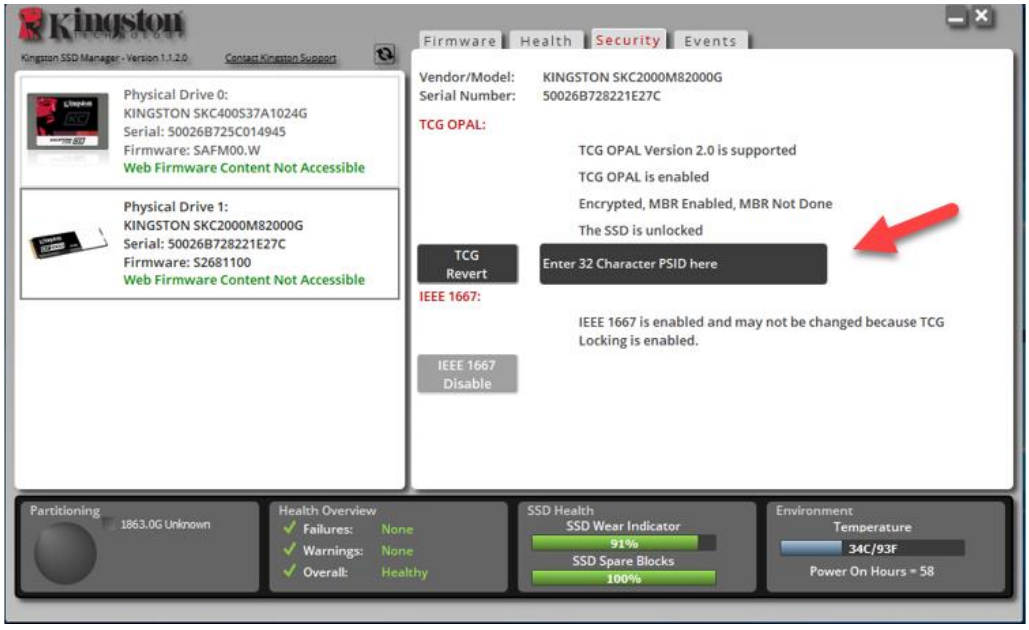
Để xóa SSD đích của bạn và xóa hỗ trợ BitLocker eDrive khỏi ổ, vui lòng thực hiện các bước sau.

Lưu ý: Quá trình này sẽ đặt lại SSD đích của bạn và TẤT CẢ DỮ LIỆU CÓ TRÊN Ổ SẼ BỊ XÓA.

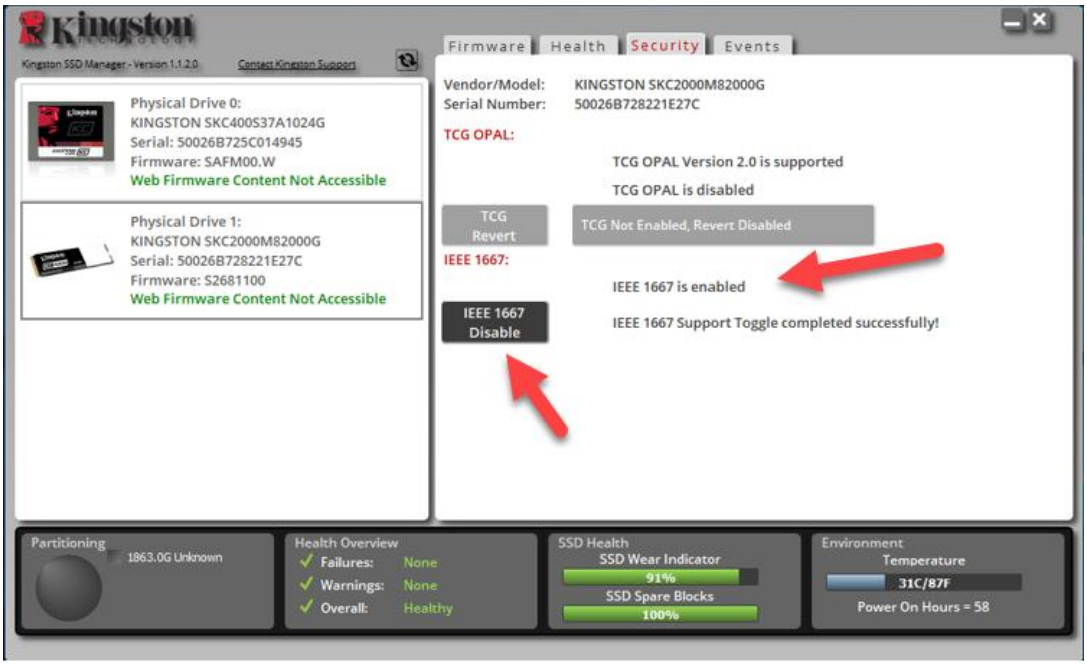
1. Ghi lại giá trị PSID của SSD đích. Giá trị này được in trên nhãn.

Ví dụ: Giá trị PSID KC2000

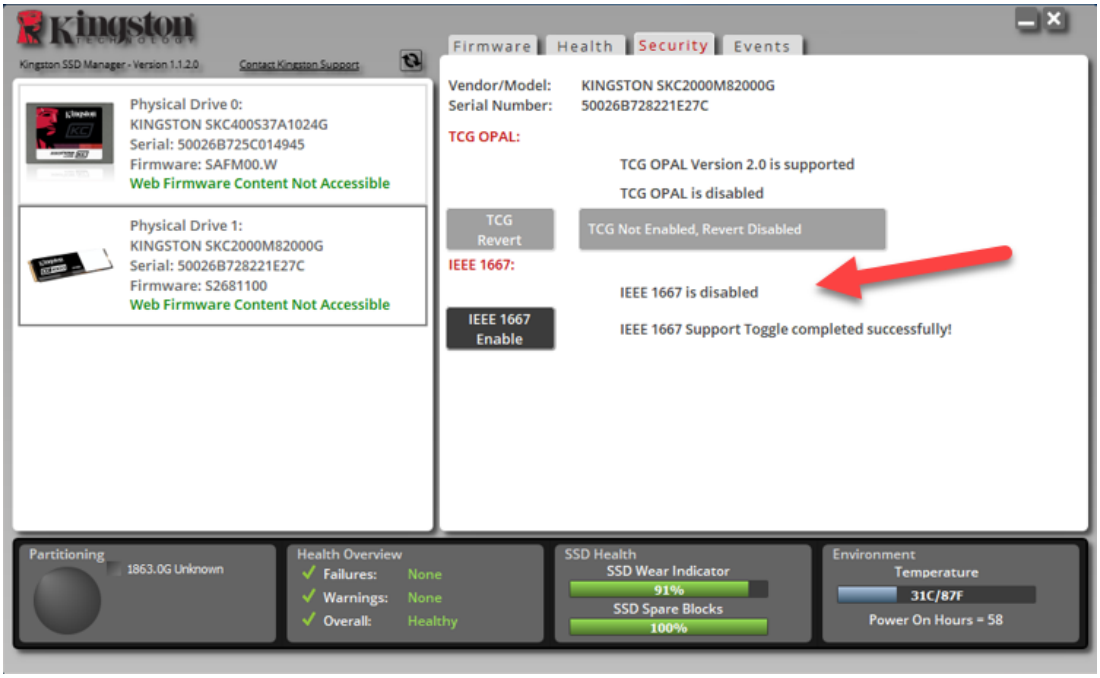
2. Gắn SSD đích làm ổ phụ và chạy Kingston SSD Manager (KSM).
3. Chọn thẻ **Security** và thực hiện **TCG Revert** bằng cách nhập vào giá trị PSID gồm 32 chữ số từ bước một, sau đó chọn **TCG Revert.** Sau khi hoàn thành, bạn sẽ thấy thông báo **TCG Revert completed successfully**. Nếu thông báo không xuất hiện, vui lòng nhập lại giá trị PSID của bạn và thử hoàn nguyên lại.



4. Một khi ổ đã được hoàn nguyên, bạn sẽ có tùy chọn để tắt hỗ trợ IEEE1667. Vui lòng chọn **IEEE1667 Disable** và chờ thông báo “IEEE1667 Support Toggle completed successfully”.



5. Xác nhận rằng hỗ trợ IEEE1667 đã được tắt.



6. SSD đích của bạn đã sẵn sàng để tái sử dụng.