# SSDs encriptados de Kingston

## Habilitar e inhabilitar BitLocker con eDrive para aprovechar el encriptado por hardware

**Introducción**

Este documento describe cómo habilitar y deshabilitar la función BitLocker eDrive de Microsoft para aprovechar el encriptado por hardware en su SSD de Kingston. Este procedimiento se aplica a los SSDs de Kingston que son compatibles con el conjunto de funciones TCG OPAL 2.0 e IEEE1667. Si no tiene un SSD de Kingston compatible con TCG OPAL 2.0 e IEEE1667, este proceso no funcionará. Si no está seguro, póngase en contacto con el soporte técnico de Kingston @ www.kingston.com/support

*Este documento se referirá a BitLocker con eDrive de Microsoft como "eDrive" por el resto del tutorial. Los procedimientos que se describen a continuación pueden cambiar según las versiones y las actualizaciones de Windows.*

**Requisitos del sistema**

-SSD de Kingston que utiliza el conjunto de funciones de seguridad TCG Opal 2.0 e IEEE1667
-Software Kingston SSD Manager https://www.kingston.com/ssdmanager
-Sistema de hardware y BIOS compatible con las características de seguridad TCG Opal 2.0 e IEEE1667

**Requisitos del SO / BIOS**

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

*Nota: Todas las unidades de estado sólido encriptadas deben estar conectadas a controladores que no sean RAID para funcionar correctamente en Windows 8, 10 y/o Server 2012*

Para usar una unidad de estado sólido encriptada en Windows 8, 10 o Windows Server 2012 como **unidades de datos**:

- La unidad debe estar en un estado no inicializado.
- La unidad debe estar en un estado inactivo de seguridad.

Para unidades de estado sólido encriptadas utilizadas como**unidad de arranque**:

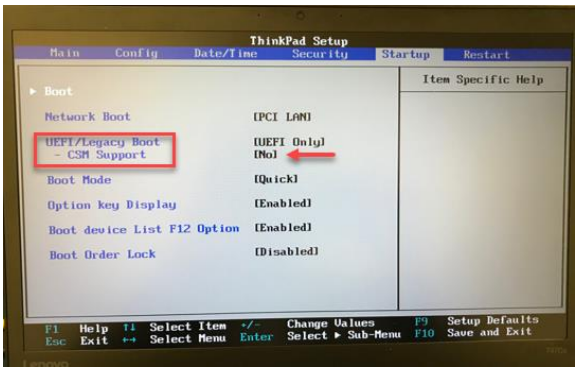
- La unidad debe estar en un estado no inicializado.
- La unidad debe estar en un estado inactivo de seguridad.
- La computadora debe estar basada en UEFI 2.3.1 y tener definido el EFI_STORAGE_SECURITY_COMMAND_PROTOCOL. (Este protocolo se utiliza para permitir que los programas que se ejecutan en el entorno de servicios de arranque EFI envíen comandos del protocolo de seguridad a la unidad).
- La computadora debe tener el Módulo de soporte de compatibilidad "Compatibility Support Module" (CSM) deshabilitado en UEFI.
- La computadora siempre debe arrancar de forma nativa desde UEFI.

Para obtener más información, consulte el artículo de Microsoft sobre este tema que se encuentra aquí:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

## Habilitar Microsoft eDrive en el arranque del SSD

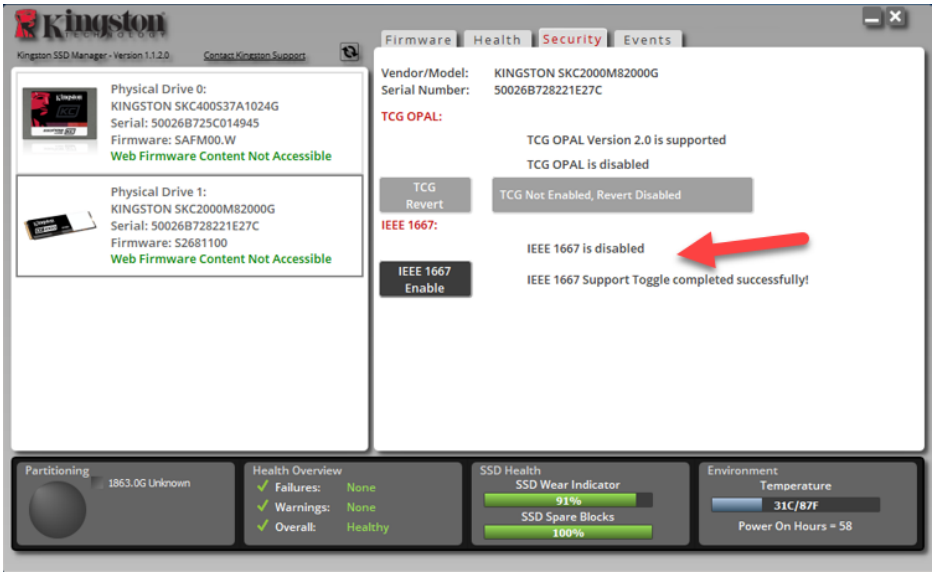
### Configuración del BIOS

1. Consulte la documentación del fabricante de su sistema para confirmar que el BIOS de su sistema está basado en UEFI 2.3.1 y tener definido el EFI_STORAGE_SECURITY_COMMAND_PROTOCOL.
2. Ingrese al BIOS y deshabilite el Módulo de soporte de compatibilidad (CSM)

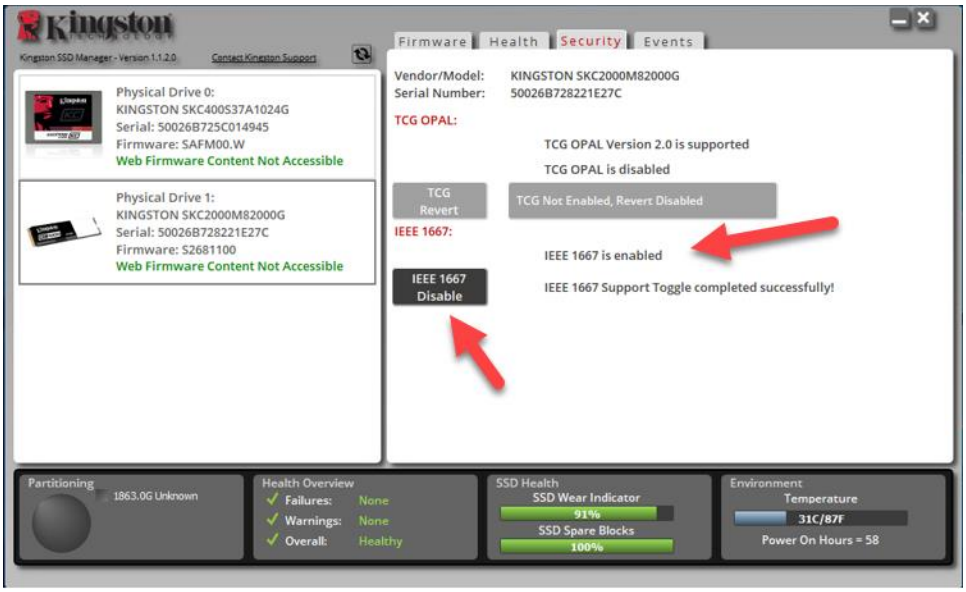



### Preparación de la unidad

1. Si aún no ha descargado el Kingston SSD Manager (KSM), hágalo ahora. https://www.kingston.com/ssdmanager
2. Borre de forma segura el SSD de destino utilizando el software KSM u otro método estándar de la industria.
3. Monte el SSD de destino como un disco secundario para confirmar el estado IEEE1667. La unidad debe estar en modo **deshabilitado** .



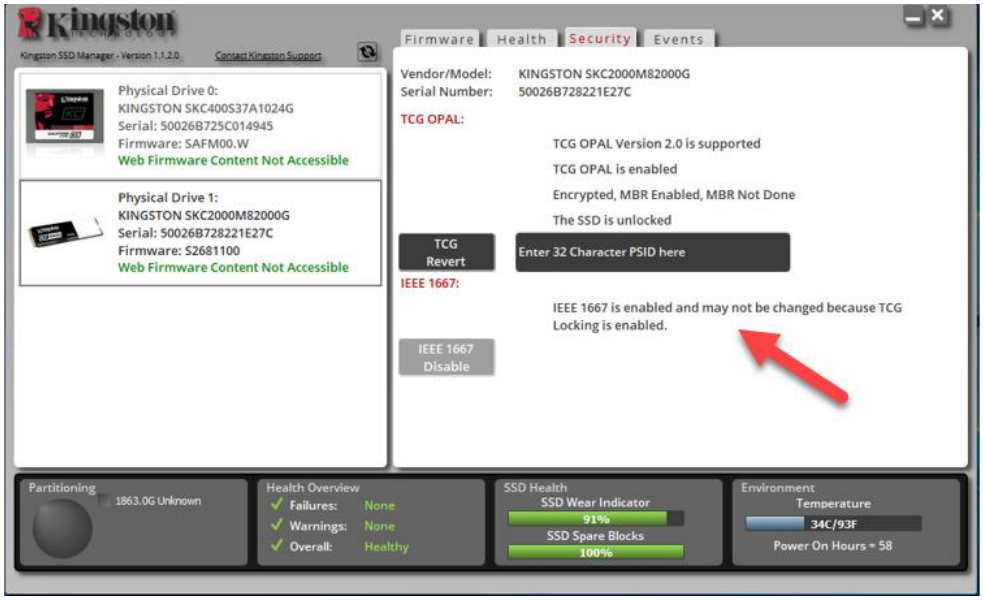
4. Seleccione el botón IEEE1667 y **habilite la** función. Confirme que la función se haya activado correctamente.



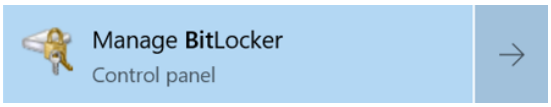

**Instalación del sistema operativo (SO)**

***Nota: No clone un sistema operativo a su SSD****de destino. Clonar un SO en el SSD de destino evitará que pueda habilitar el encriptado por hardware con eDrive. Debe implementar una nueva instalación del SO en el SSD de destino para aprovechar el encriptado por hardware con eDrive.*

1. Instale el SO compatible en el SSD de destino.
2. Después de instalar el SO, instale el Kingston SSD Manager (KSM), ejecute el KSM y confirme que el siguiente mensaje aparece en la pestaña Seguridad dentro de la aplicación:
   *"IEEE 1667 está habilitado y no se puede cambiar porque el bloqueo TCG está habilitado".*

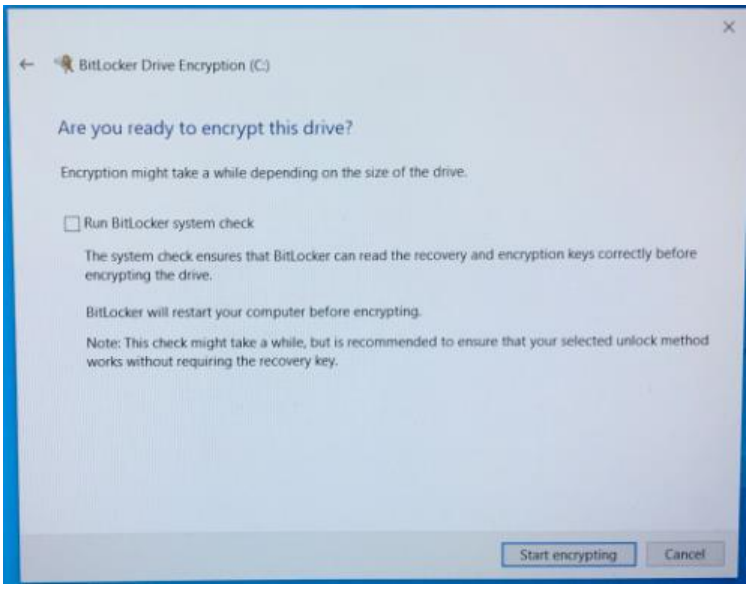


3. Use la tecla de Windows para buscar **Administrar BitLocker** y luego ejecute la aplicación.

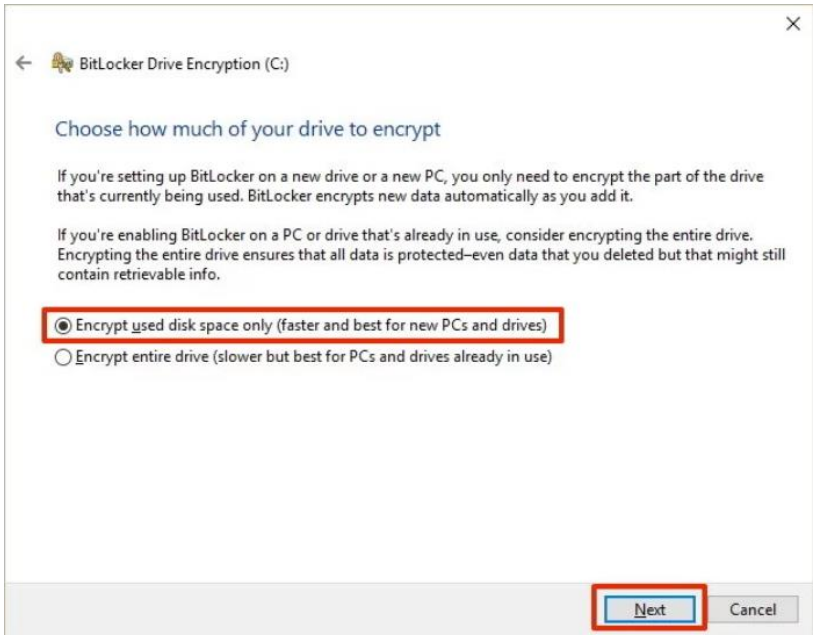



4. Seleccione **Activar BitLocker** desde la ventana del Explorador.

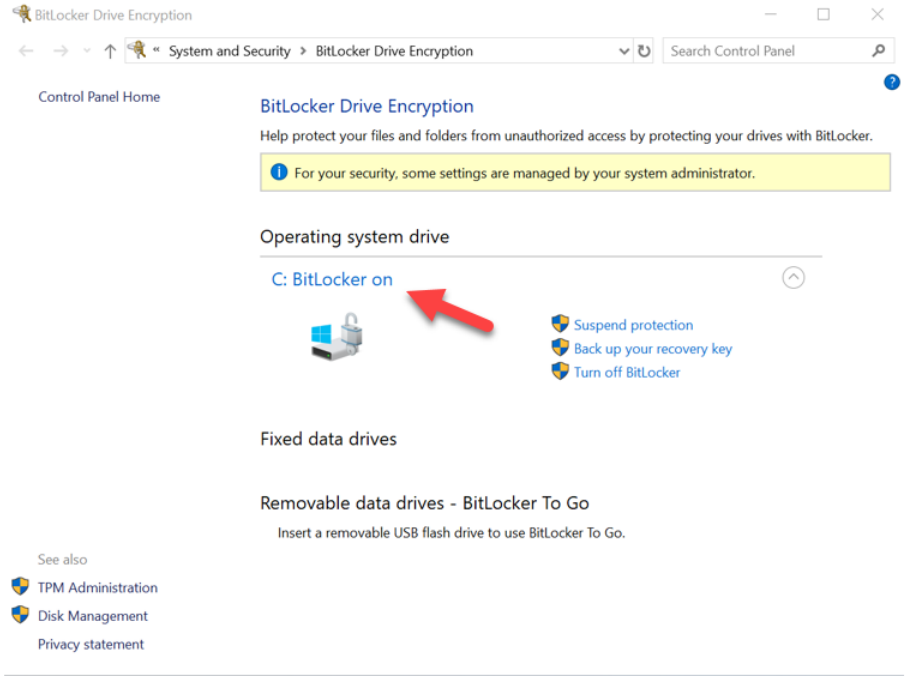

5. Continúe con las indicaciones para configurar el SSD de destino. Cuando se le solicite, seleccione **Iniciar encriptación.** Por defecto, **Ejecutar comprobación del sistema BitLocker** está seleccionado. Es aconsejable continuar con esta configuración. Sin embargo, cuando no esté marcada, podrá confirmar si el encriptado por hardware está habilitado sin necesidad de reiniciar el sistema.



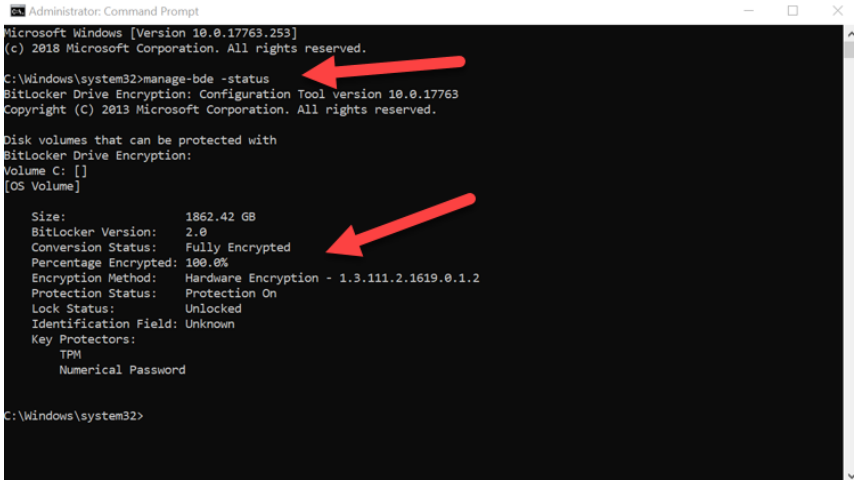
**Nota: Si le parece una pantalla que dice "Elija cuánto encriptar su unidad", esto a menudo implica que el SSD de destino NO habilitará el encriptado por hardware, sino que utilizará el encriptado por software.**




6. Si es necesario, reinicie el sistema y luego vuelva a ejecutar **Administrar BitLocker** para confirmar el estado del encriptado del SSD de destino.



7. También puede verificar el estado del encriptado del SSD de destino abriendo **cmd.exe** y escribiendo: **manage-bde -status**

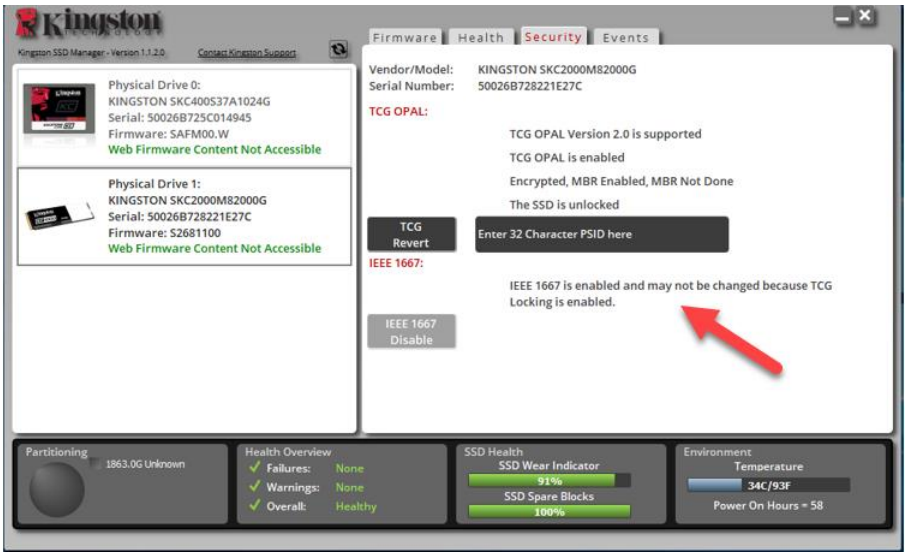



**Habilite Microsoft eDrive con Windows 10 (versión 1903+)**

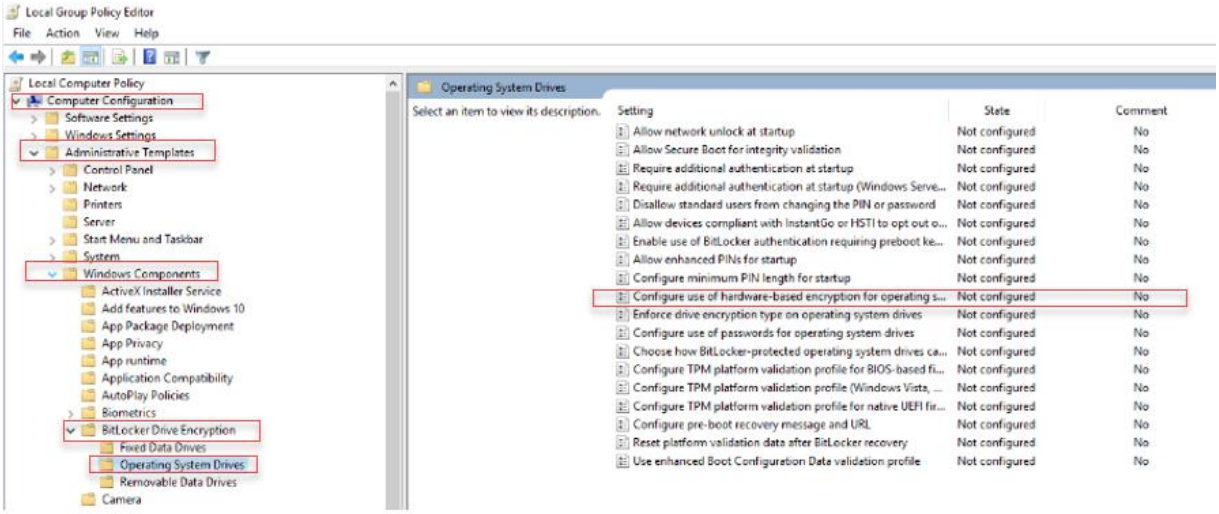
*Microsoft cambió el comportamiento predeterminado de Windows 10 con respecto al encriptado por eDrive cuando lanzaron Windows 10 versión 1903. Para habilitar eDrive en este sistema, y posiblemente en sistemas posteriores, deberá ejecutar* ***gpedit*** *para habilitar el encriptado por hardware.*

***Nota: No clone un sistema operativo a su SSD****de destino. Clonar un SO en el SSD de destino evitará que pueda habilitar el encriptado por hardware con eDrive. Debe implementar una nueva instalación del SO en el SSD de destino para aprovechar el encriptado por hardware con eDrive.*

1. Instale el SO compatible en el SSD de destino.
2. Después de instalar el SO, instale el Kingston SSD Manager (KSM), ejecute el KSM y confirme que el siguiente mensaje aparece en la pestaña Seguridad dentro de la aplicación:
   *"IEEE 1667 está habilitado y no se puede cambiar porque el bloqueo TCG está habilitado".*

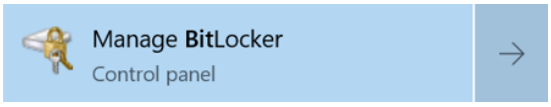


3. Ejecute gpedit.msc para modificar la configuración del encriptado.
    a. Vaya a **Plantillas administrativas> Componentes de Windows> Encriptado de unidad BitLocker> Unidades del sistema operativo**
    b. Luego, seleccione **Configurar el uso de encriptación basada en hardware para unidades de sistema operativo**
    c. **Habilite** la función y luego **Aplique** la configuración.



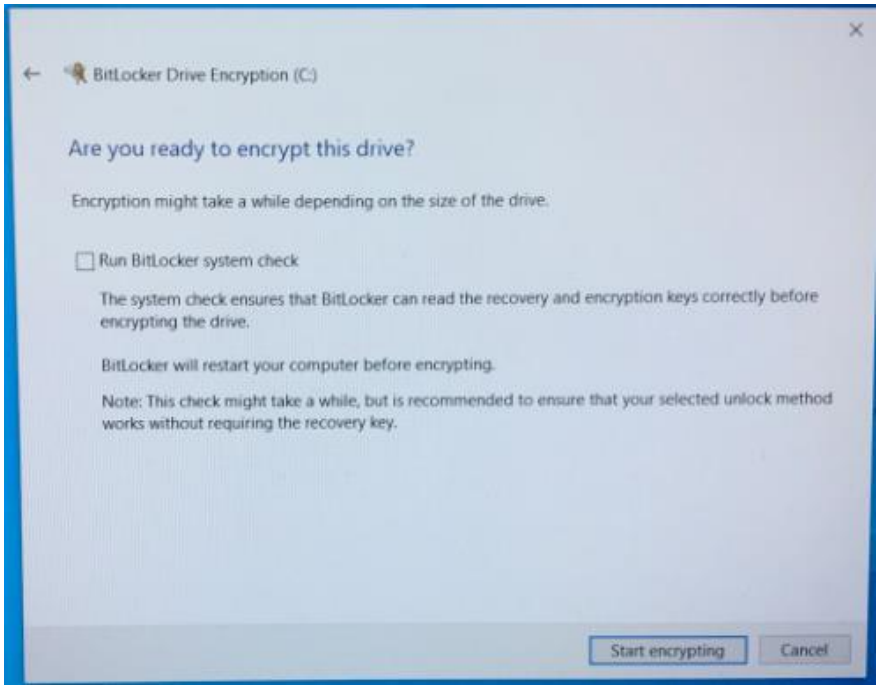

Nota: Para habilitar eDrive en unidades que no sean la unidad del sistema operativo, puede aplicar la misma configuración seleccionando: **Plantillas administrativas> Componentes de Windows> Encriptado de unidad BitLocker> Unidades de datos fijas> Configure el uso de encriptación basada en hardware para unidades de datos fijas (Habilite y luego Aplique)**

4. Use la tecla de Windows para buscar **Administrar BitLocker** y luego ejecute la aplicación.

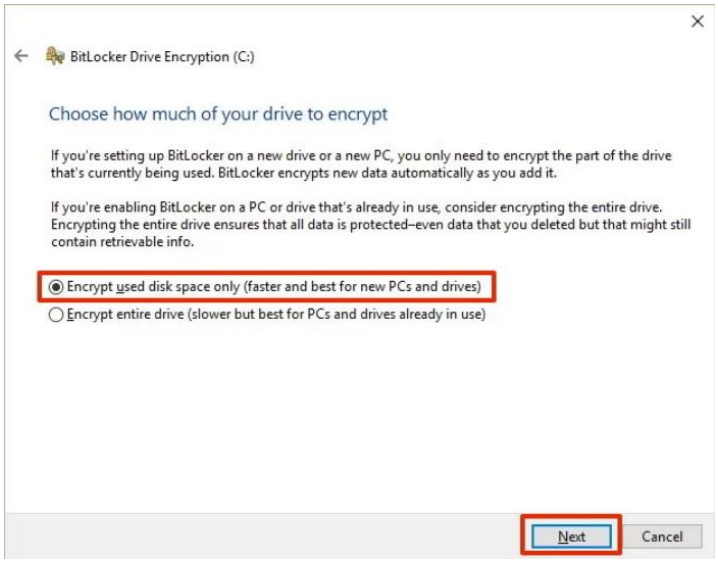



5. Seleccione **Activar BitLocker** desde la ventana del Explorador.

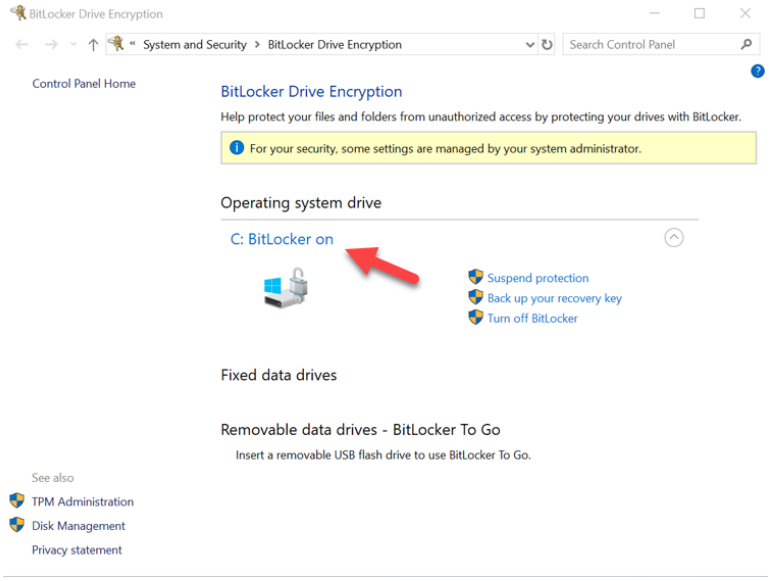
6. Continúe con las indicaciones para configurar el SSD de destino. Cuando se le solicite, seleccione **Iniciar encriptación.** Por defecto, **Ejecutar comprobación del sistema BitLocker** está seleccionado. Es aconsejable continuar con esta configuración. Sin embargo, cuando no esté marcada, podrá confirmar si el encriptado por hardware está habilitado sin necesidad de reiniciar el sistema.



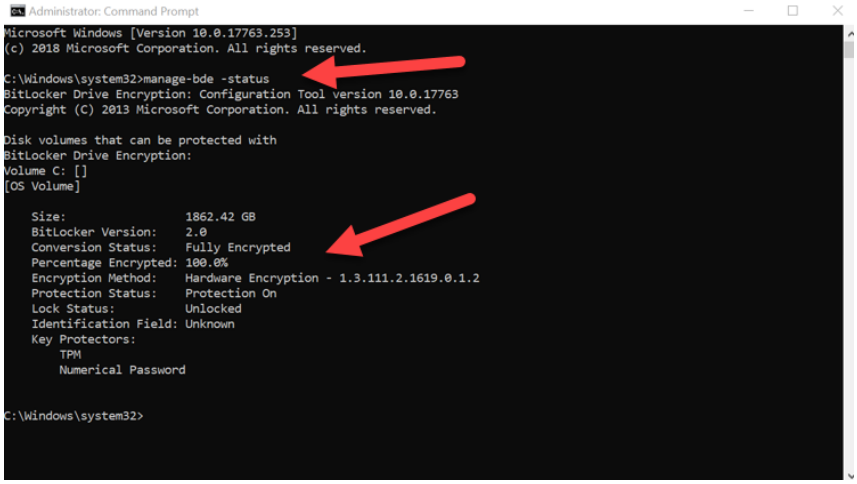

**Nota: Si le parece una pantalla que dice "Elija cuánto encriptar su unidad", esto a menudo implica que el SSD de destino NO habilitará el encriptado por hardware, sino que utilizará el encriptado por software.**



7. Si es necesario, reinicie el sistema y luego vuelva a ejecutar **Administrar BitLocker** para confirmar el estado del encriptado del SSD de destino.




8. También puede verificar el estado del encriptado del SSD de destino abriendo **cmd.exe** y escribiendo: **manage-bde -status**



**Deshabilitar el soporte de Microsoft eDrive**

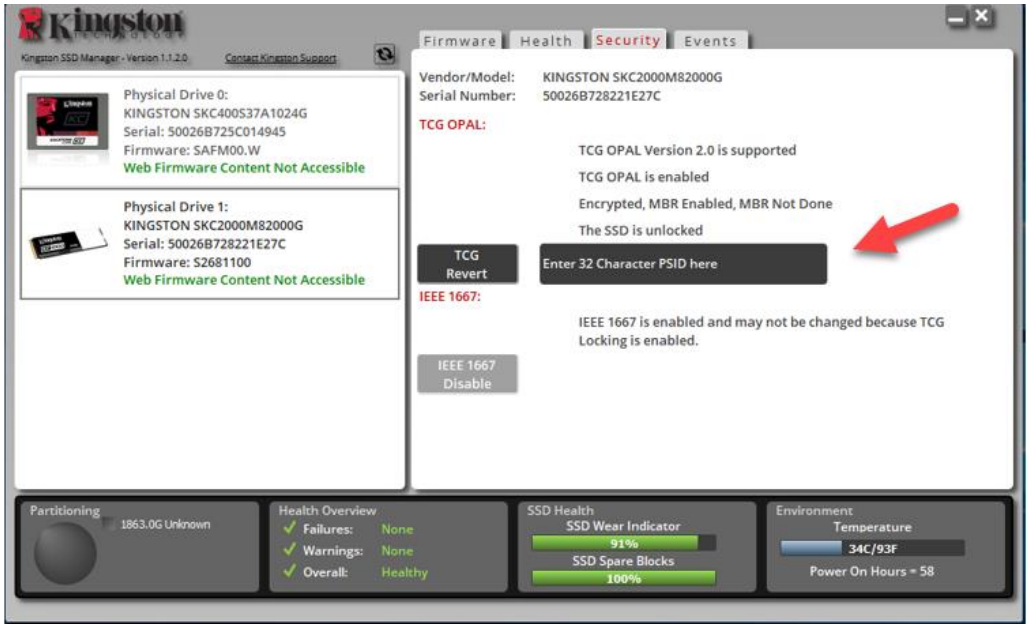
Para borrar los datos del SSD de destino y eliminar el soporte de eDrive BitLocker de la unidad, continúe con los siguientes pasos.

***Nota: Este proceso restablecerá su SSD de destino y TODOS LOS DATOS PRESENTES EN LA UNIDAD SE PERDERÁN.***

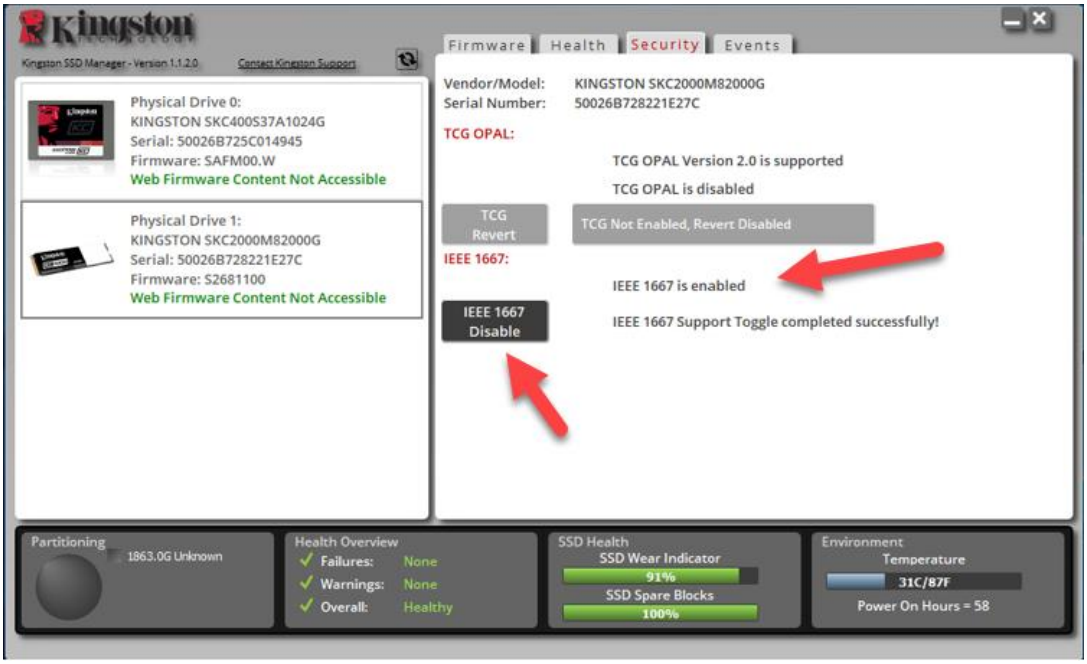
1. Anote el valor PSID del SSD de destino. Lo encontrará impreso en la etiqueta.


Ej.: Valor PSID KC2000

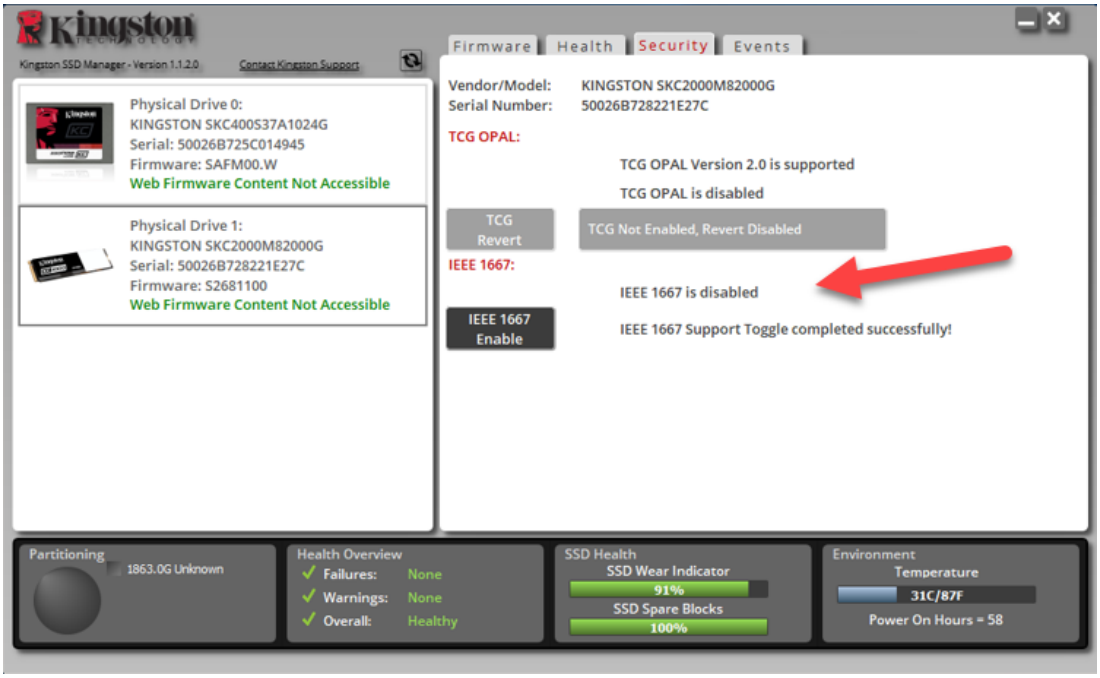
2. Monte el SSD de destino como unidad secundaria y ejecute Kingston SSD Manager (KSM).
3. Seleccione la pestaña **Seguridad** y realice una **reversión de TCG** ingresando el valor de PSID de 32 dígitos del paso uno, luego seleccionando **Revertir TCG.** Una vez terminado, verá el mensaje **Reversión de TCG finalizada con éxito** Si el mensaje no está presente, vuelva a ingresar su valor de PSID y vuelva a intentar la reversión.



4. Una vez que la unidad se haya revertido correctamente, tendrá la opción de deshabilitar el soporte IEEE1667. Seleccione **Deshabilitar IEEE1667** y espere el mensaje “El cambio de soporte IEEE1667 finalizó correctamente”.




5. Confirme que el soporte IEEE1667 está deshabilitado.




6. Su SSD de destino está listo para su reutilización.