

# SSD cifradas de Kingston

Activación y desactivación de BitLocker con eDrive para utilizar el cifrado de hardware



#### Introducción

El presente documento describe cómo activar y desactivar la función BitLocker con eDrive de Microsoft para aprovechar el cifrado de hardware de su SSD de Kingston. Este procedimiento es aplicable a las SSD de Kingston compatibles con las normas TCG OPAL 2.0 e IEEE1667. Si no tiene una SSD de Kingston compatible con TCG OPAL 2.0 e IEEE1667, este procedimiento no surtirá ningún efecto. Si no está seguro, sírvase ponerse en contacto con el Servicio de Asistencia técnica de Kingston en <u>www.kingston.com/support</u>

En el resto de este procedimiento, denominaremos 'eDrive' a BitLocker con eDrive de Microsoft. El procedimiento descrito puede variar en función de las versiones y actualizaciones de Windows.

# Requisitos del sistema

- SSD de Kingston compatible con las normas de seguridad TCG Opal 2.0 e IEEE1667
- Software SSD Manager de Kingston https://www.kingston.com/ssdmanager
- Hardware del sistema y BIOS compatibles con las normas de seguridad TCG Opal 2.0 e IEEE1667

# Requisitos de sistema operativo/BIOS

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

Nota: Todas las unidades de estado sólido cifradas deben conectarse a controladores no RAID para funcionar correctamente en Windows 8, 10 o Server 2012

Para utilizar la unidad de estado sólido cifrada en Windows 8, 10 o Windows Server 2012 como **unidades de datos**:

- La unidad no debe haberse inicializado.
- La unidad debe estar en estado de seguridad inactiva.

Para unidades de estado sólido cifradas utilizadas como unidades de arranque:

- La unidad no debe haberse inicializado.
- La unidad debe estar en estado de seguridad inactiva.
- El ordenador debe estar basado en UEFI 2.3.1 y tener definido el protocolo 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 de protocolos de seguridad a la unidad).
- El ordenador debe tener desactivado el Módulo de soporte de compatibilidad (CSM) en UEFI.
- El ordenador siempre debe arrancar nativamente desde UEFI.

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



# Activación de Microsoft eDrive en la SSD de arranque

#### **Configuración de BIOS**

- 1. Consulte la documentación del fabricante de su sistema para confirmar que el BIOS de su sistema esté basado en UEFI 2.3.1 y tenga definido el protocolo EFI\_STORAGE\_SECURITY\_COMMAND\_PROTOCOL.
- 2. Entre al BIOS y desactive el Módulo de soporte de compatibilidad (CSM)



#### Preparativos de la unidad

- 1. Si todavía no ha descargado el SSD Manager (KSM) de Kingston, hágalo ahora. <u>https://www.kingston.com/ssdmanager</u>
- 2. Efectúe un borrado de seguridad de la SSD de destino utilizando el software KSM u otro método estándar del sector.
- 3. Instale la SSD de destino como disco secundario para confirmar el estado de IEEE1667. La unidad debe estar en modo **Desactivado**.



4. Seleccione el botón IEEE1667 para Activar la función. Confirme que ha alternado correctamente la función.

Kingston S50 Manager- Version 1.1.2.9 Contest Kingston Support	Firmware Health Security Events
Physical Drive 0:   KINGSTON SKC400S37A1024G   Serial: 500268725C014945   Firmware: SAFM00.W   Web Firmware Content Not Accessible   Physical Drive 1:   KINGSTON SKC2000M82000G   Serial: 500268728221E27C   Firmware: S2681100   Web Firmware Content Not Accessible	Vendor/Model: KINGSTON SKC2000M82000G Serial Number: 500268728221E27C TCG OPAL: TCG OPAL Version 2.0 is supported TCG OPAL is disabled TCG Revert. IEEE 1667: IEEE 1667 is enabled IEEE 1667 IEEE 1667 Support Toggle completed successfully!
Partitioning 1863.0G Unknown ✓ Failures: Non ✓ Warnings: Non ✓ Overall: Heat	e SSD Health SSD Wear Indicator e 91% SSD Spare Blocks thy 100% Power On Hours = 58

#### Instalación del sistema operativo

**Nota: No clone un sistema operativo en la SSD de destino**. Clonar un sistema operativo en la SSD de destino le impedirá activar el cifrado de hardware mediante eDrive. Debe realizar una instalación nueva de sistema operativo en la SSD de destino para poder cifrar el hardware con eDrive.

- 1. Instale el sistema operativo compatible en la SSD de destino.
- Una vez instalado el sistema operativo, instale el SSD Manager de Kingston (KSM), ejecútelo y confirme que, en la pestaña Seguridad de la aplicación, aparezca este mensaje: *"IEEE 1667 está activado y no puede modificarse porque TCG Locking está activado".*



3. Utilice la clave de Windows para buscar Administrar BitLocker y, a continuación, ejecute la aplicación.



4. Seleccione Activar BitLocker desde dentro de la ventana Explorador.



5. Continúe configurando la SSD de destino siguiendo las instrucciones. Cuando aparezca el mensaje a tal efecto, seleccione Iniciar cifrado. De manera predeterminada, aparecerá seleccionado Ejecutar comprobación del sistema BitLocker. Se recomienda continuar con esta opción activada. No obstante, si no estuviese activada, podrá confirmar si el cifrado de hardware está activado sin necesidad de reiniciar el sistema.



Nota: Si aparece un mensaje pidiendo "Elegir qué cantidad de la unidad desea cifrar", normalmente se refiere a que la SSD de destino NO activará el cifrado de hardware, sino que utilizará el cifrado de software.



6. Si fuese necesario, reinicie el sistema y vuelva a ejecutar **Administrar BitLocker** para confirmar el estado de cifrado de la SSD de destino.

Control Panel Home	BitLocker Drive Encryption			
	Help protect your files and folders from unauthorized access by protecting your drives with BitLock			
	• For your security, some settings are managed by your system administrator.			
	Operating system drive			
	C: BitLocker on	$\bigcirc$		
	Suspend protection			
	Back up your recovery key			
	💎 Turn off BitLocker			
	Fixed data drives			
	Removable data drives - BitLocker To Go			
	Insert a removable USB flash drive to use BitLocker To Go.			
See also				
TPM Administration				
Disk Management				



7. También podrá comprobar el estado de cifrado de la SSD de destino abriendo **cmd.exe** y escribiendo: **manage-bde -status** 



# Activación de Microsoft eDrive con Windows 10 (versión 1903+)

Microsoft modificó el comportamiento predeterminado de Windows 10 con respecto al cifrado de eDrive cuando lanzó la versión 1903 de Windows 10. Para activar eDrive en esta versión, y posiblemente en las posteriores, tendrá que ejecutar **gpedit** para posibilitar el cifrado de hardware.

**Nota: No clone un sistema operativo en la SSD de destino**. Clonar un sistema operativo en la SSD de destino le impedirá activar el cifrado de hardware mediante eDrive. Debe realizar una instalación nueva de sistema operativo en la SSD de destino para poder cifrar el hardware con eDrive.

- 1. Instale el sistema operativo compatible en la SSD de destino.
- Una vez instalado el sistema operativo, instale el SSD Manager de Kingston (KSM), ejecútelo y confirme que, en la pestaña Seguridad de la aplicación, aparezca este mensaje:

"IEEE 1667 está activado y no puede modificarse porque TCG Locking está activado".



- 3. Ejecute gpedit.msc para modificar la configuración del cifrado.
  - a. Vaya a Plantillas administrativas> Componentes de Windows> Cifrado de unidad BitLocker> Unidades del sistema operativo
  - b. A continuación, seleccione Configurar uso de cifrado basado en hardware para sistemas operativos
  - c. Seleccione **Activar** la función y, a continuación, **Aplicar** el ajuste.



Nota: Para activar eDrive en unidades que no sean la unidad del sistema operativo podrá aplicar los mismos ajustes seleccionando. Plantillas administrativas> Componentes de Windows> Cifrado de unidad BitLocker> Unidades de datos fijas> Configurar uso de cifrado basado en hardware para unidades de datos fijas (Activar y Aplicar)

X

ø

0

Utilice la clave de Windows para buscar **Administrar BitLocker** y, a continuación, ejecute la aplicación. 4.





6. Continúe configurando la SSD de destino siguiendo las instrucciones. Cuando aparezca el mensaje a tal efecto, seleccione Iniciar cifrado. De manera predeterminada, aparecerá seleccionado Ejecutar comprobación del sistema BitLocker. Se recomienda continuar con esta opción activada. No obstante, si no estuviese activada, podrá confirmar si el cifrado de hardware está activado sin necesidad de reiniciar el sistema.

t	R BitLocker Drive Encryption (C)	×
	Are you ready to encrypt this drive?	
	Encryption might take a while depending on the size of the drive.	
	Run BitLocker system check	
	The system check ensures that BitLocker can read the recovery and encryption keys correctly before encrypting the drive.	
	BitLocker will restart your computer before encrypting.	
	Note: This check might take a while, but is recommended to ensure that your selected unlock method works without requiring the recovery key.	
	Start encrypting Cancel	

Nota: Si aparece un mensaje pidiendo "Elegir qué cantidad de la unidad desea cifrar", normalmente se refiere a que la SSD de destino NO activará el cifrado de hardware, sino que utilizará el cifrado de software.

	×
÷	RitLocker Drive Encryption (C:)
	Choose how much of your drive to encrypt
	If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
	If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected-even data that you deleted but that might still contain retrievable info.
	Encrypt used disk space only (faster and best for new PCs and drives)
	O Encrypt entire drive (slower but best for PCs and drives already in use)
	<u>N</u> ext Cancel



7. Si fuese necesario, reinicie el sistema y vuelva a ejecutar **Administrar BitLocker** para confirmar el estado de cifrado de la SSD de destino.



8. También podrá comprobar el estado de cifrado de la SSD de destino abriendo **cmd.exe** y escribiendo: **manage-bde -status** 





#### Desactivación del soporte de Microsoft eDrive

Para borrar los datos de la SSD de destino y quitar el soporte de BitLocker eDrive de la unidad, efectúe el siguiente procedimiento.

# Nota: Este procedimiento restaurará la SSD de destino y SE PERDERÁN TODOS LOS DATOS EXISTENTES EN LA UNIDAD.

1. Escriba el valor PSID de la SSD de destino. Esto aparecerá impreso en la etiqueta.



Ejemplo: Valor PSID KC2000

- 2. Instale la SSD de destino como unidad secundaria y ejecute el SSD Manager de Kingston (KSM).
- Seleccione la pestaña Seguridad y ejecute una Reversión de TCG especificando el valor PSID de 32 dígitos del paso 1 y, a continuación, seleccione Revertir TCG. Cuando haya terminado, aparecerá el mensaje Reversión de TCG concluida correctamente. Si el mensaje no aparece, vuelva a introducir el valor de PSID y vuelta e intentar la reversión.





 Una vez realizada correctamente la reversión, tendrá la opción de desactivar la compatibilidad con IEEE1667. Seleccione Desactivar IEEE1667 y espere a que aparezca el mensaje "Reversión de compatibilidad con IEEE1667 concluida correctamente".



5. Confirme que se haya desactivado la compatibilidad con IEEE1667.



6. La SSD de destino ya está lista para ser reutilizada.



11