



Kingston Encrypted SSDs **Enabling and Disabling BitLocker with eDrive to** **Utilise Hardware Encryption**

Introduction

This document describes how to enable and disable Microsoft's BitLocker eDrive feature to leverage hardware encryption on your Kingston SSD. This procedure applies to Kingston SSDs that support the TCG OPAL 2.0 and IEEE1667 feature set. If you do not have a Kingston SSD with TCG OPAL 2.0 and IEEE1667 support, this process will not work. If you are unsure, please contact Kingston Technical support at www.kingston.com/support

This document refers to Microsoft's BitLocker with eDrive as 'eDrive' for the remainder of the walkthrough. The procedures described below may change depending upon Windows version(s) and updates.

System Requirements

- Kingston SSD utilising TCG Opal 2.0 and IEEE1667 security feature set
- Kingston SSD Manager software <https://www.kingston.com/ssdmanager>
- System hardware and BIOS supporting TCG Opal 2.0 and IEEE1667 security features

OS / BIOS Requirements

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

Note: All encrypted solid-state drives must be attached to non-RAID controllers to function properly in Windows 8, 10 and/or Server 2012

To use an encrypted solid-state drive on Windows 8, 10 or Windows Server 2012 as **data drives**:

- The drive must be in an uninitialised state.
- The drive must be in a security inactive state.

For encrypted solid-state drives used as **start-up drives**:

- The drive must be in an uninitialised state.
- The drive must be in a security inactive state.
- The computer must be UEFI 2.3.1 based and have the EFI_STORAGE_SECURITY_COMMAND_PROTOCOL defined. (This protocol is used to allow programs running in the EFI boot services environment to send security protocol commands to the drive.)
- The computer must have the Compatibility Support Module (CSM) disabled in UEFI.
- The computer must always boot natively from UEFI.

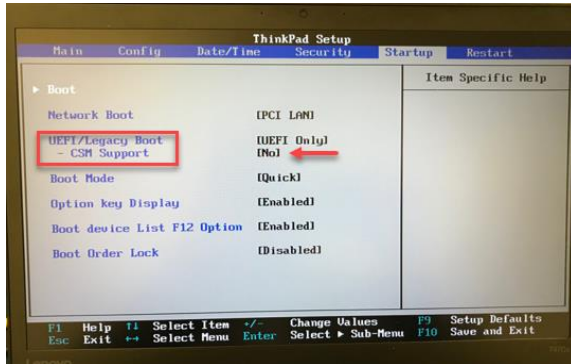
For additional information, please refer to Microsoft's article on this topic located here:

[https://docs.microsoft.com/en-gb/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627\(v=ws.11\)](https://docs.microsoft.com/en-gb/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11))

Enable Microsoft eDrive on Boot SSD

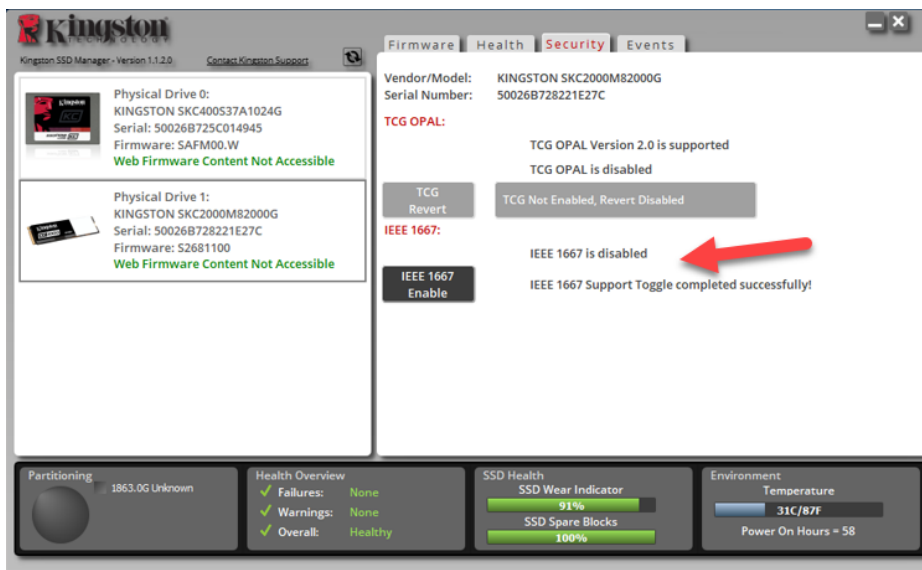
BIOS Configuration

1. Refer to your system manufacturer's documentation to confirm your system's BIOS is UEFI 2.3.1 based and has the EFI_STORAGE_SECURITY_COMMAND_PROTOCOL defined.
2. Enter BIOS and disable Compatibility Support Module (CSM)

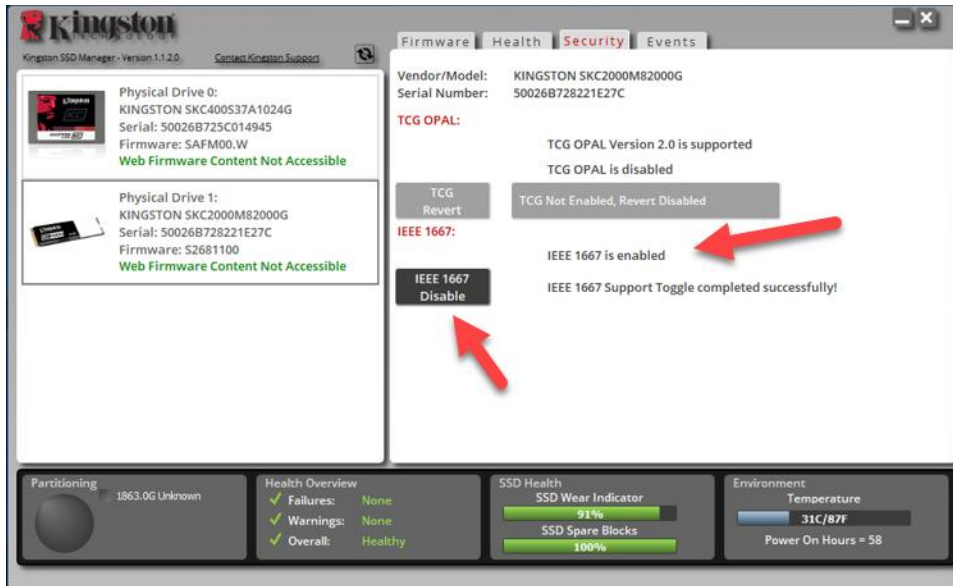


Drive Preparation

1. If you haven't already downloaded Kingston's SSD Manager (KSM), please do so now.
<https://www.kingston.com/ssdmanager>
2. Secure erase the target SSD using KSM software or another industry-standard method.
3. Mount target SSD as a secondary disk to confirm IEEE1667 status. The drive should be in **Disabled** mode.



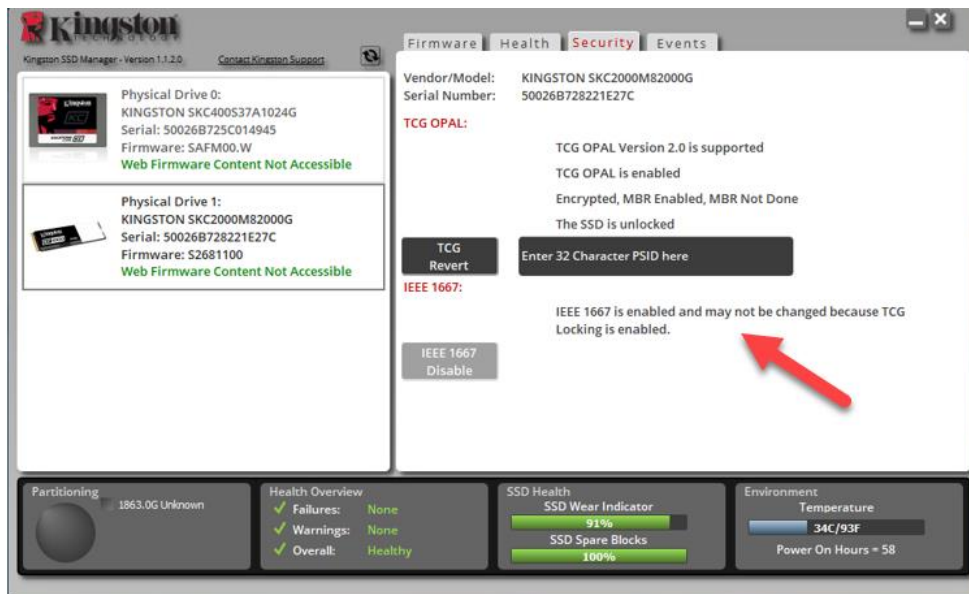
4. Select the IEEE1667 button and **Enable** the feature. Confirm that the feature is toggled successfully.



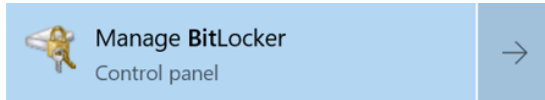
Operating System (OS) Installation

Note: Do not clone an operating system to your target SSD. Cloning an OS to the target SSD will prevent you from enabling hardware encryption using eDrive. You must deploy a fresh OS installation to the target SSD in order to take advantage of hardware encryption with eDrive.

1. Install a supported OS on the target SSD.
2. After the OS has installed, install Kingston SSD manager (KSM), run KSM and confirm that the following messaging is present on the Security tab within the application:
"IEEE 1667 is enabled and may not be changed because TCG Locking is enabled."



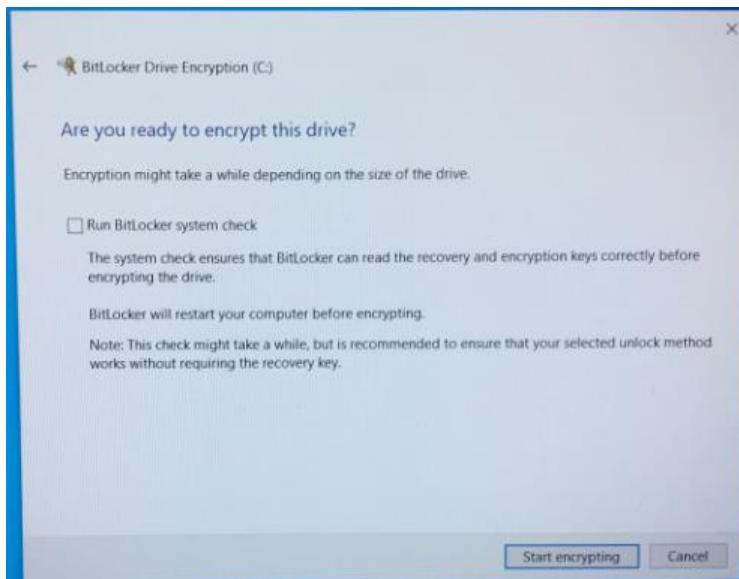
- Use the Windows Key to search for **Manage BitLocker** and then run the application.



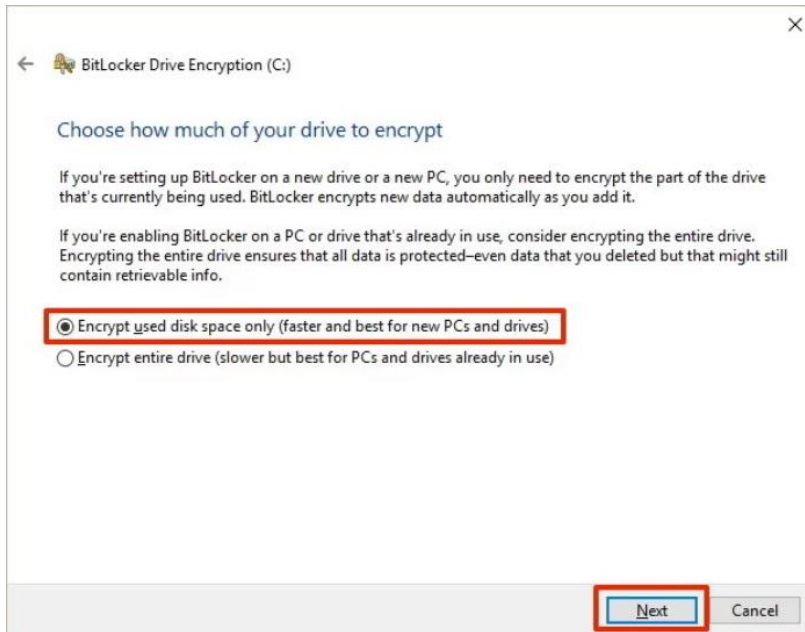
- Select **Turn on BitLocker** from within the Explorer window.



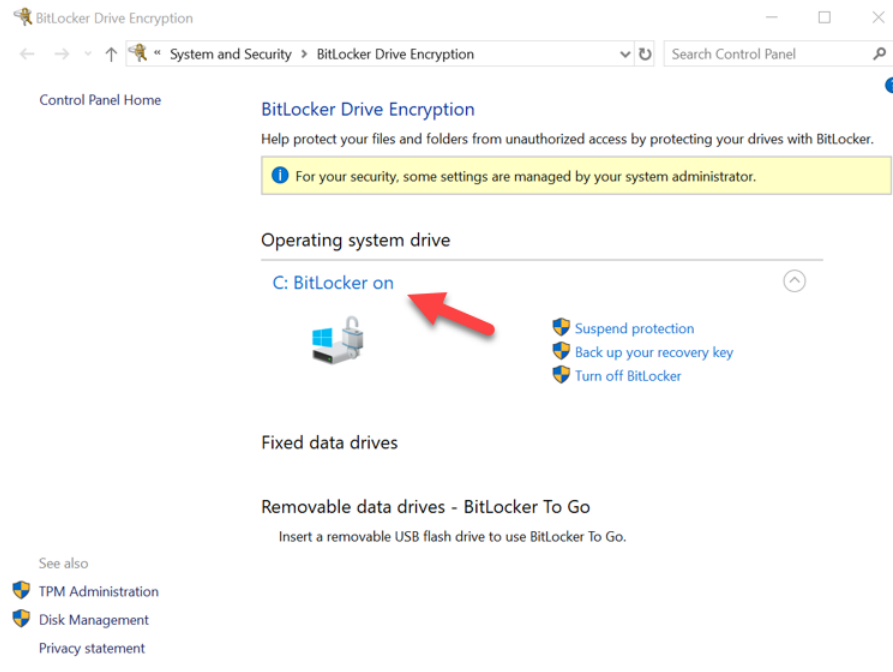
- Continue through the prompts to configure the target SSD. When prompted, select **Start encrypting**. By default, **Run BitLocker system check** is selected. We advise that you proceed with this setting enabled. However, if it is not selected, you will be able to confirm if hardware encryption is enabled without requiring a system reboot.



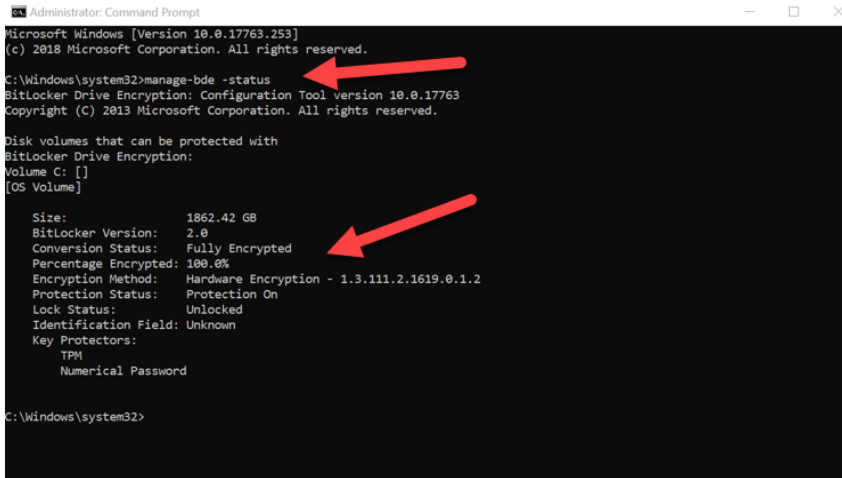
Note: If you are prompted with a screen that asks you to “Choose how much of your drive to encrypt”, this often implies that the target SSD will NOT enable hardware encryption, but instead utilise software encryption.



6. If required, reboot the system and then relaunch **Manage BitLocker** to confirm the target SSD’s encryption status.



7. You can also check the target SSD's encryption status by opening **cmd.exe** and typing: **manage-bde -status**

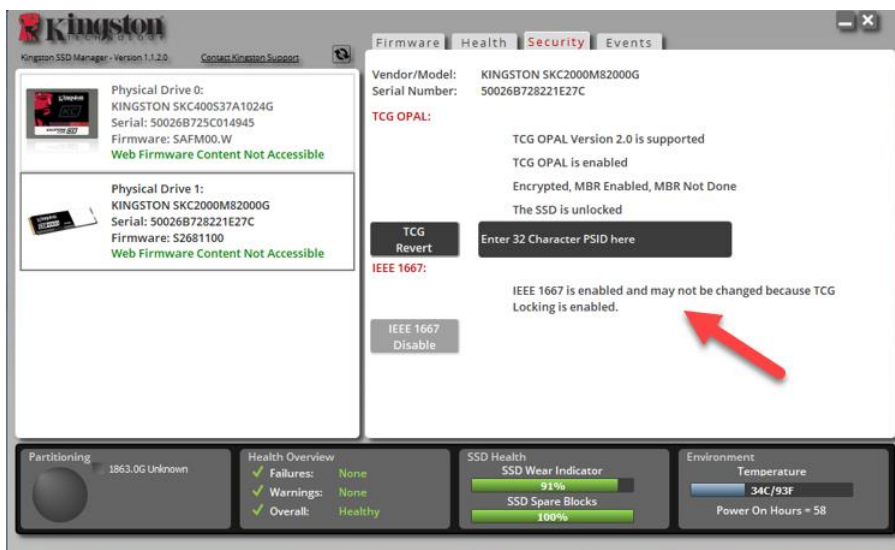


Enable Microsoft eDrive with Windows 10 (version 1903+)

Microsoft changed the default behaviour of Windows 10 with regards to eDrive encryption it released Windows 10 version 1903. To enable eDrive in this build, and possibly later builds, you will need to run **gpedit** in order to enable hardware encryption.

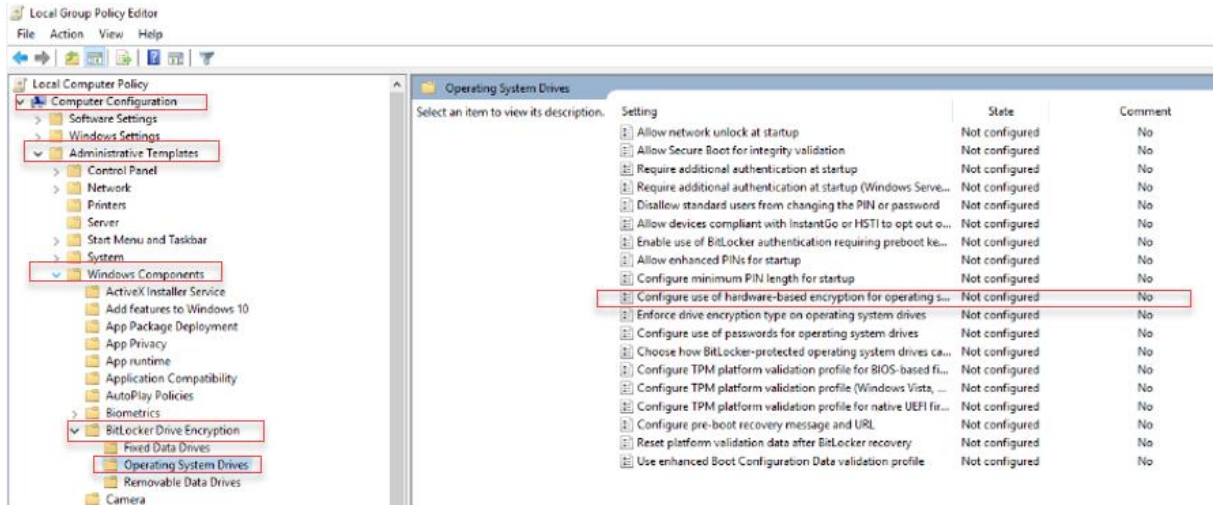
Note: Do not clone an operating system to your target SSD. Cloning an OS to the target SSD will prevent you from enabling hardware encryption using eDrive. You must deploy a fresh OS installation to the target SSD in order to take advantage of hardware encryption with eDrive.

1. Install a supported OS on the target SSD.
2. After the OS has installed, install Kingston SSD manager (KSM), run KSM and confirm that the following messaging is present on the Security tab within the application:
“IEEE 1667 is enabled and may not be changed because TCG Locking is enabled.”



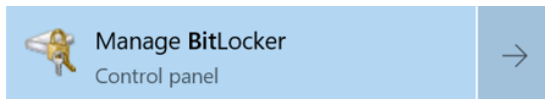
3. Run gpedit.msc to modify the encryption setting.

- a. Navigate to **Administrative Templates> Windows Components> BitLocker Drive Encryption> Operating System Drives**
- b. Then, select **Configure use of hardware-based encryption for operating systems**
- c. **Enable** the feature and then **Apply** the setting.

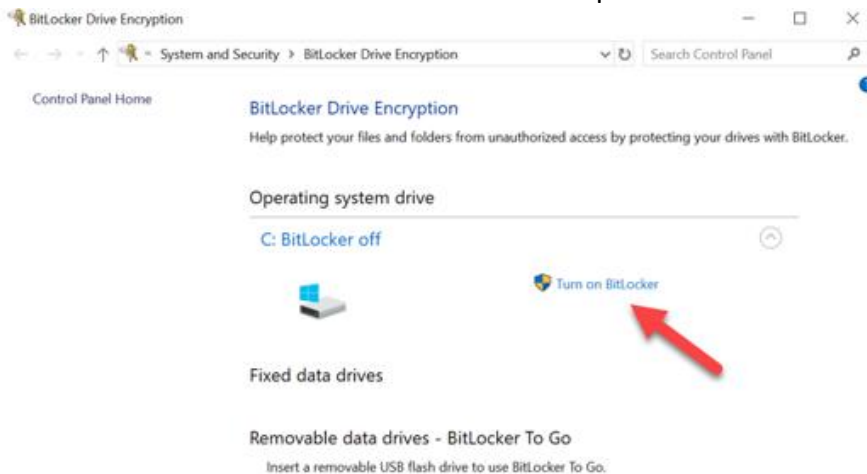


Note: To enable eDrive on drives other than the operating system drive, you can apply the same settings by selecting: **Administrative Templates> Windows Components> BitLocker Drive Encryption> Fixed Data Drives> Configure use of hardware-based encryption for fixed data drives (Enable and then Apply)**

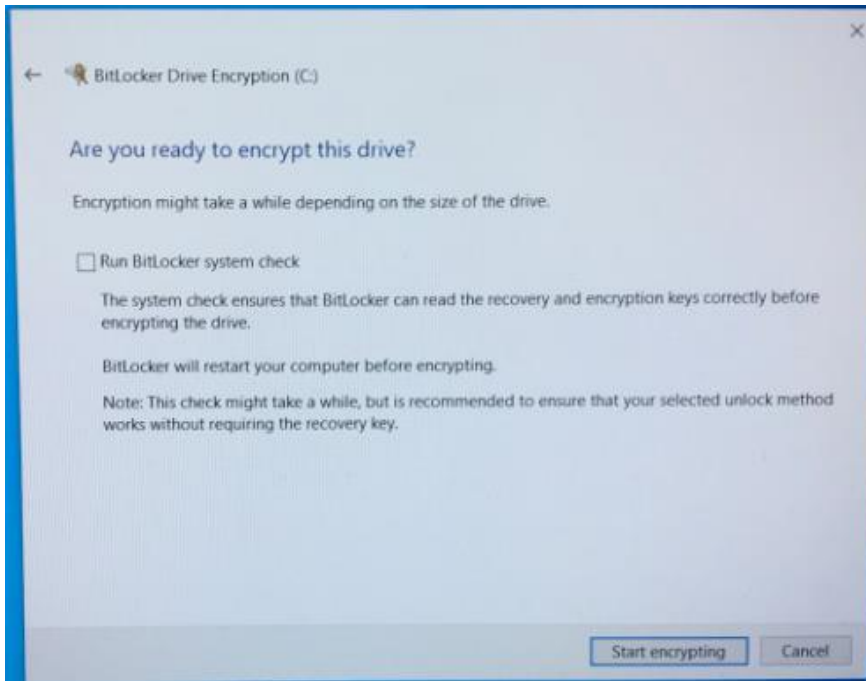
4. Use the Windows Key to search for **Manage BitLocker** and then run the application.



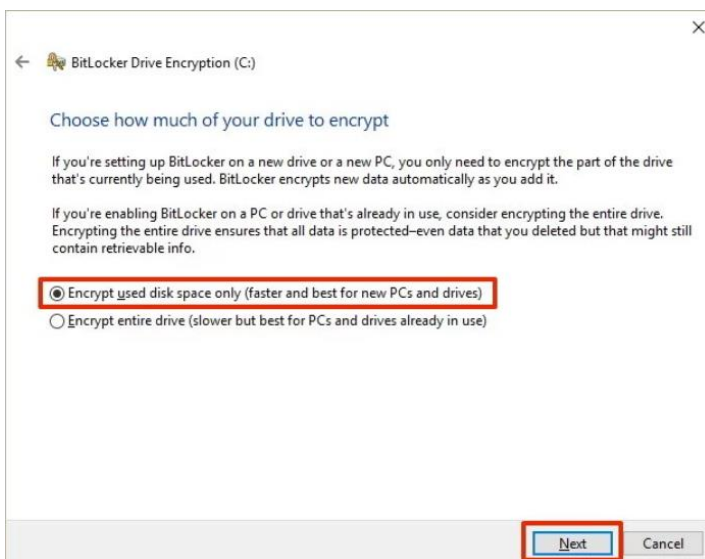
5. Select **Turn on BitLocker** from within the Explorer window.



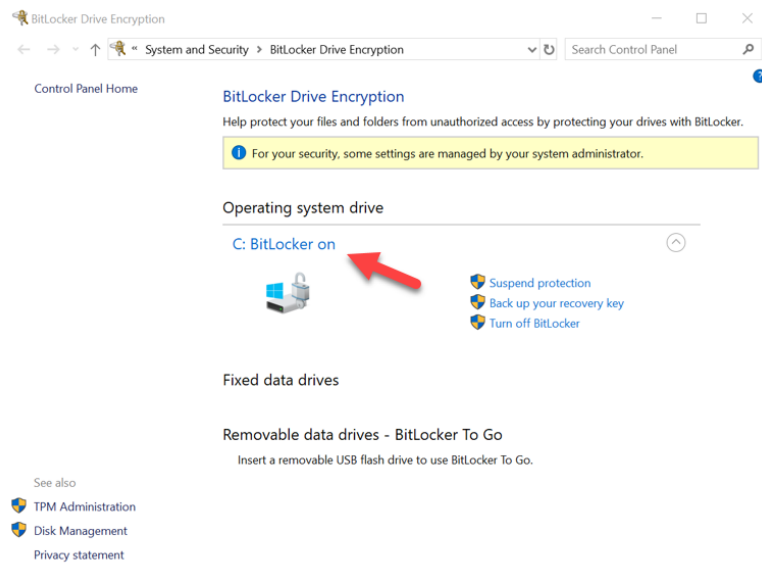
6. Continue through the prompts to configure the target SSD. When prompted, select **Start encrypting**. By default, **Run BitLocker system check** is selected. We advise that you proceed with this setting enabled. However, if it is not selected, you will be able to confirm if hardware encryption is enabled without requiring a system reboot.



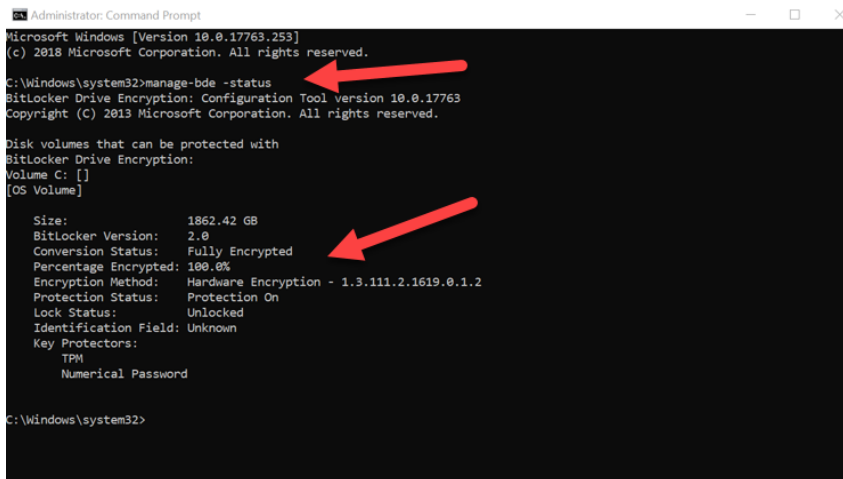
Note: If you are prompted with a screen that asks you to “Choose how much of your drive to encrypt”, this often implies that the target SSD will NOT enable hardware encryption, but instead utilise software encryption.



- If required, reboot the system and then relaunch **Manage BitLocker** to confirm the target SSD's encryption status.



- You can also check the target SSD's encryption status by opening **cmd.exe** and typing: **manage-bde -status**



Disable Microsoft eDrive Support

To erase your target SSD's data and remove BitLocker eDrive support from the drive, please proceed with the following steps.

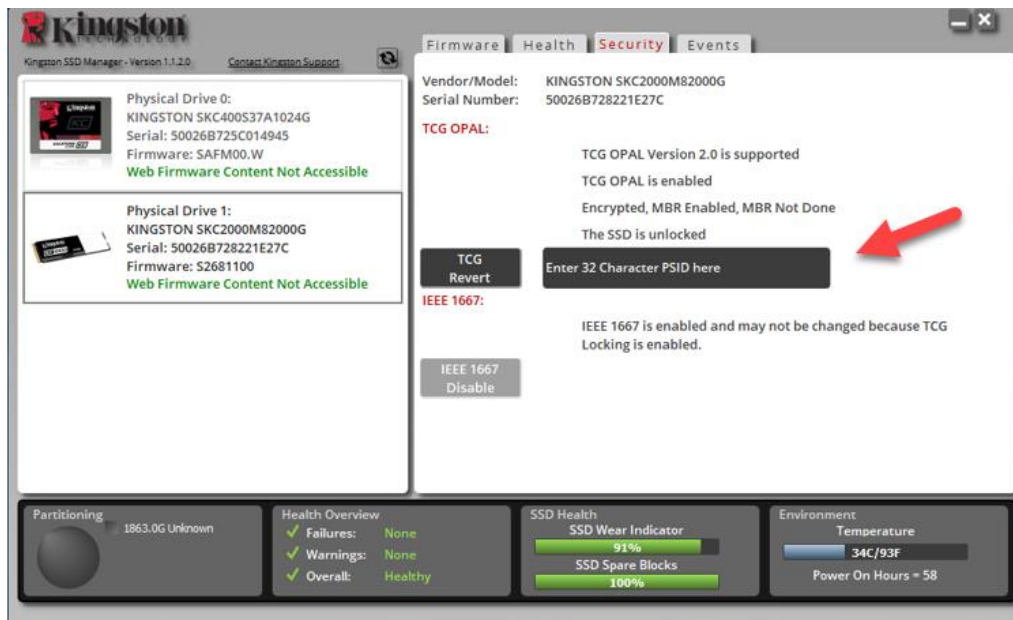
Note: This process will reset your target SSD and ALL DATA PRESENT ON THE DRIVE WILL BE LOST.

1. Write down target SSD's PSID value. This will be printed on the label.

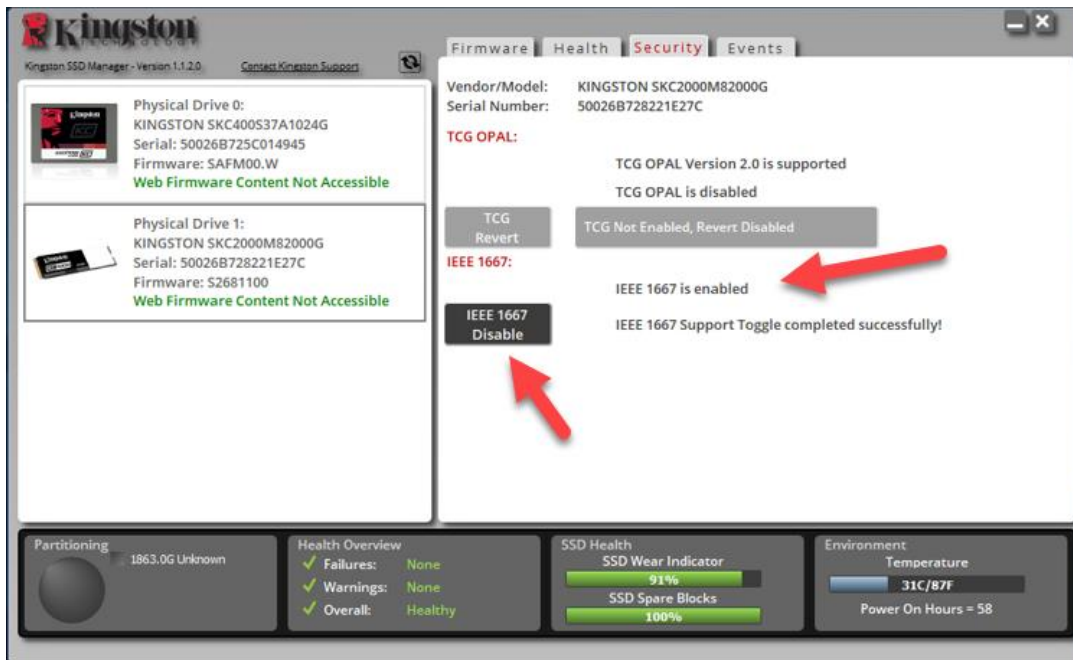


Example: KC2000 PSID Value

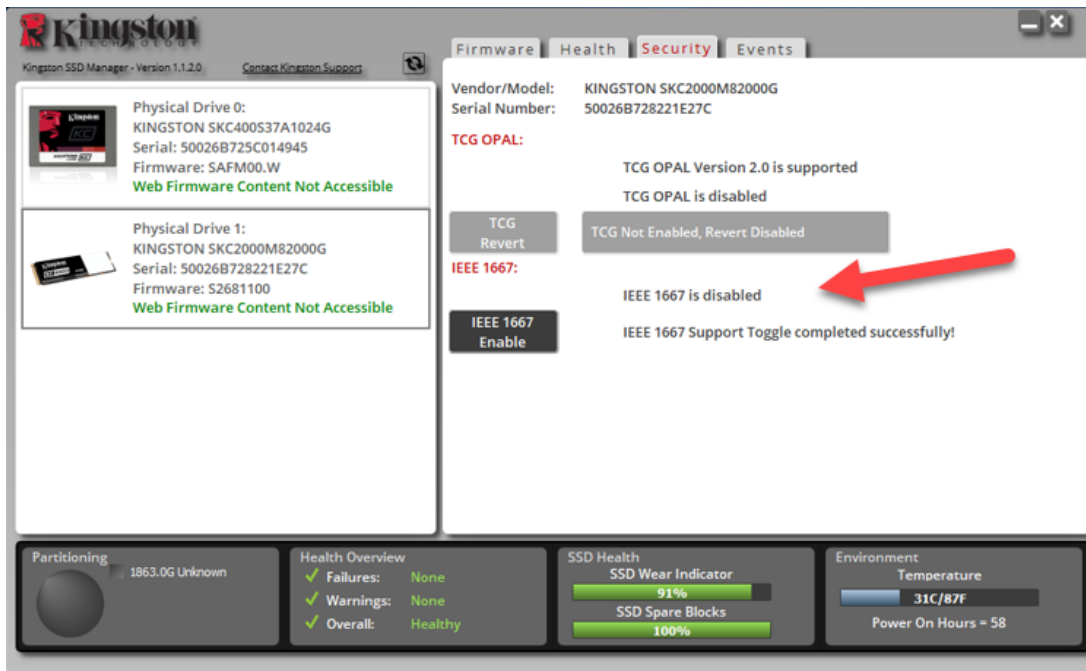
2. Mount the target SSD as a secondary drive and run Kingston SSD Manager (KSM).
3. Select the **Security** tab and perform a **TCG Revert** by entering in the 32-digit PSID value from step one, then selecting **TCG Revert**. Once complete, you will see the message **TCG Revert completed successfully**. If the message is not present, please re-enter your PSID value and retry the revert.



- Once the drive has been successfully reverted, you will have the option to disable IEEE1667 support. Select **IEEE1667 Disable** and wait for the “IEEE1667 Support Toggle completed successfully” message.



- Confirm that IEEE1667 support is disabled.



- Your target SSD is ready for reuse.



©2019 Kingston Technology Europe Ltd and Kingston Digital Europe Ltd, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, England. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469. All rights reserved. All trademarks and registered trademarks are the property of their respective owners.