Kingston Encrypted SSDs

Enabling and Disabling BitLocker with eDrive to Utilize 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 @ www.kingston.com/support

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

System Requirements

-Kingston SSD utilizing 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 uninitialized state.
- The drive must be in a security inactive state.

For Encrypted Solid-State Drives used as **startup drives**:

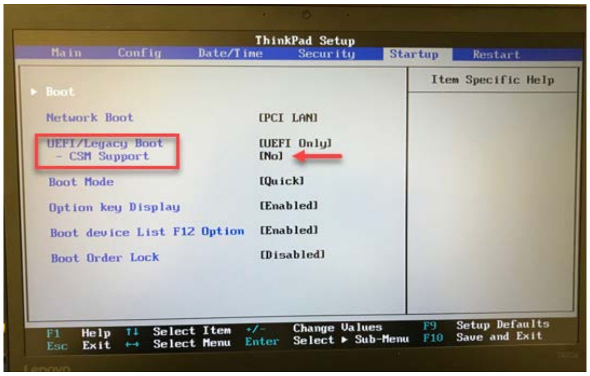
- The drive must be in an uninitialized state.
- The drive must be in a security inactive state.
- The computer must be UEFI 2.3.1 based and have the EFI_STORAGE_SECURITY_COMMAND_PROTOCOL defined. (This protocol is used to allow programs running in the EFI boot services environment to send security protocol 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-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Enable Microsoft eDrive on Boot SSD

BIOS Configuration

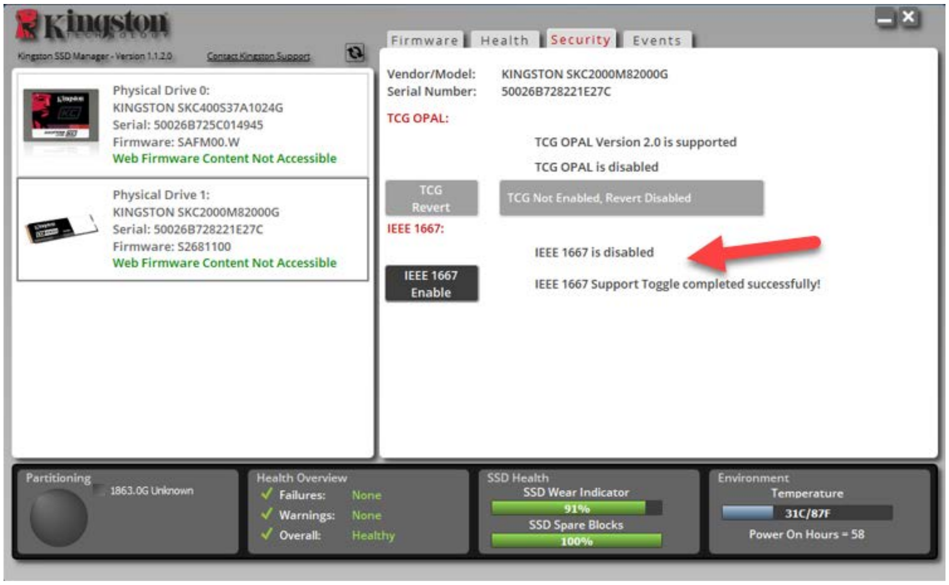
1. Refer to your system manufacturer's documentation to confirm your system's BIOS is UEFI 2.3.1 based and have the EFI_STORAGE_SECURITY_COMMAND_PROTOCOL defined.
2. Enter BIOS and disable Compatibility Support Module (CSM)



```
▸ Boot

Network Boot                    [PCI LAN]
UEFI/Legacy Boot                [UEFI Only]
 - CSM Support                  [No]
Boot Mode                       [Quick]
Option key Display              [Enabled]
Boot device List F12 Option     [Enabled]
Boot Order Lock                 [Disabled]
```

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 other industry-standard method.
3. Mount target SSD as a secondary disk to confirm IEEE1667 status. The drive should be in **Disabled** mode.



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:

TCG OPAL Version 2.0 is supported

TCG OPAL is disabled

TCG Not Enabled, Revert Disabled

IEEE 1667:

IEEE 1667 is disabled

IEEE 1667 Support Toggle completed successfully!

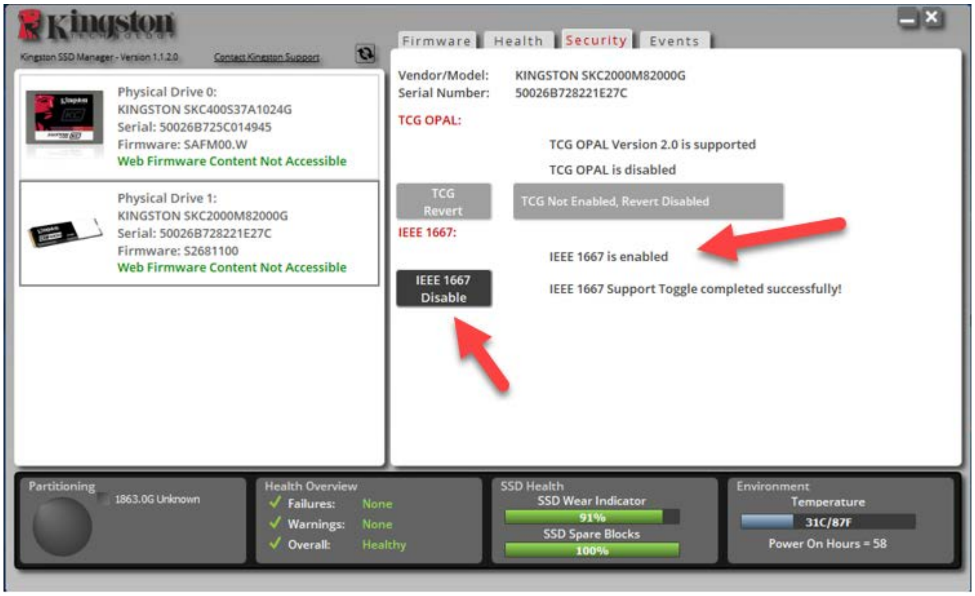
1863.0G Unknown

✓ Failures: None
✓ Warnings: None
✓ Overall: Healthy

SSD Wear Indicator 91%
SSD Spare Blocks 100%

Temperature 31C/87F
Power On Hours = 58

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



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:
TCG OPAL Version 2.0 is supported
TCG OPAL is disabled
TCG Not Enabled, Revert Disabled

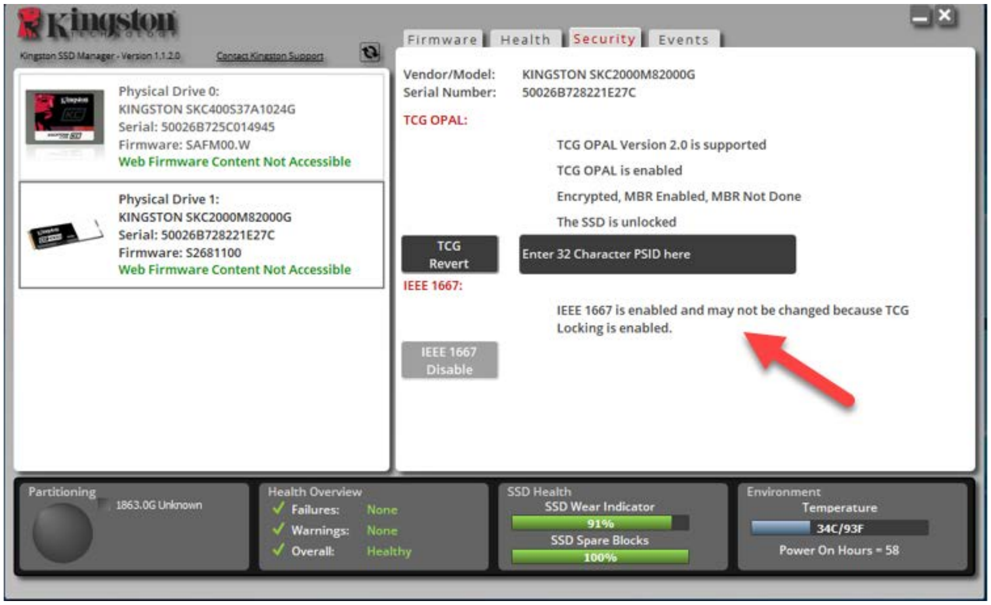
IEEE 1667:
IEEE 1667 is enabled
IEEE 1667 Support Toggle completed successfully!

1863.0G Unknown
Failures: None
Warnings: None
Overall: Healthy
SSD Wear Indicator 91%
SSD Spare Blocks 100%
Temperature 31C/87F
Power On Hours = 58

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 supported OS on target SSD.
2. After the OS is 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 an may not be changed because TCG Locking is enabled."



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

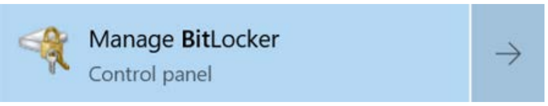
Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:
TCG OPAL Version 2.0 is supported
TCG OPAL is enabled
Encrypted, MBR Enabled, MBR Not Done
The SSD is unlocked
Enter 32 Character PSID here

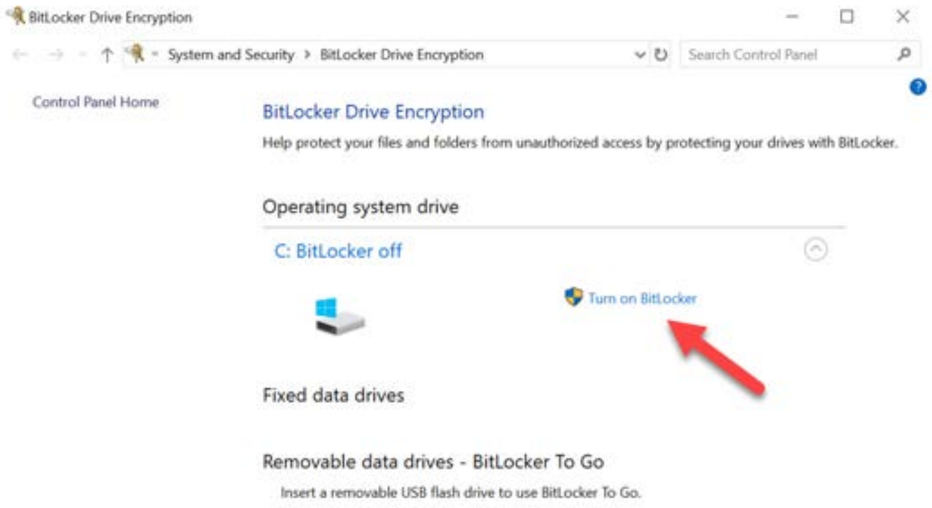
IEEE 1667:
IEEE 1667 is enabled and may not be changed because TCG Locking is enabled.

1863.0G Unknown
Failures: None
Warnings: None
Overall: Healthy
SSD Wear Indicator 91%
SSD Spare Blocks 100%
Temperature 34C/93F
Power On Hours = 58

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



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


BitLocker Drive Encryption
System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

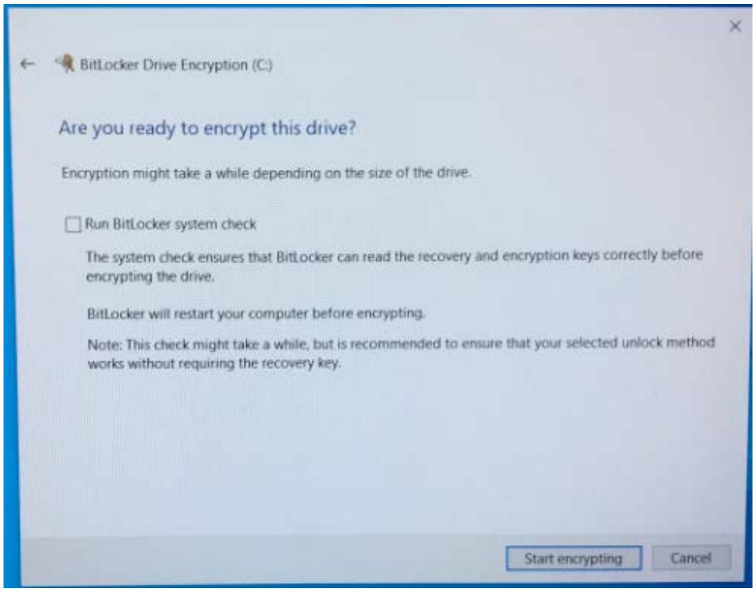
Turn on BitLocker

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

5. Continue through the prompts to configure the target SSD. When prompted, select **Start encrypting.** By default, **Run BitLocker system check** is selected. It is advisable to proceed with this setting enabled. However, when unchecked, you will be able to confirm if hardware encryption is enabled without requiring a system reboot.



Are you ready to encrypt this drive?

Encryption might take a while depending on the size of the drive.

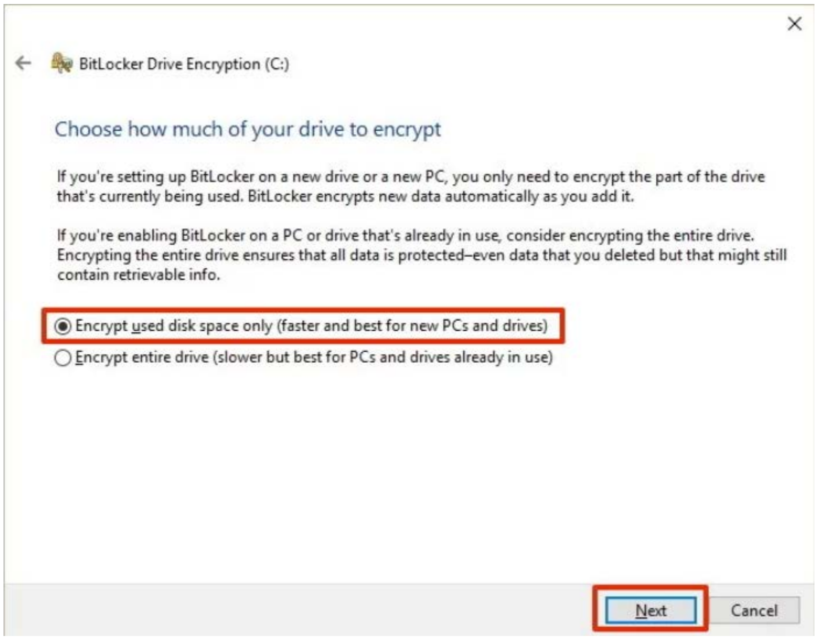
□ Run BitLocker system check

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.

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



BitLocker Drive Encryption (C:)

Choose how much of your drive to encrypt

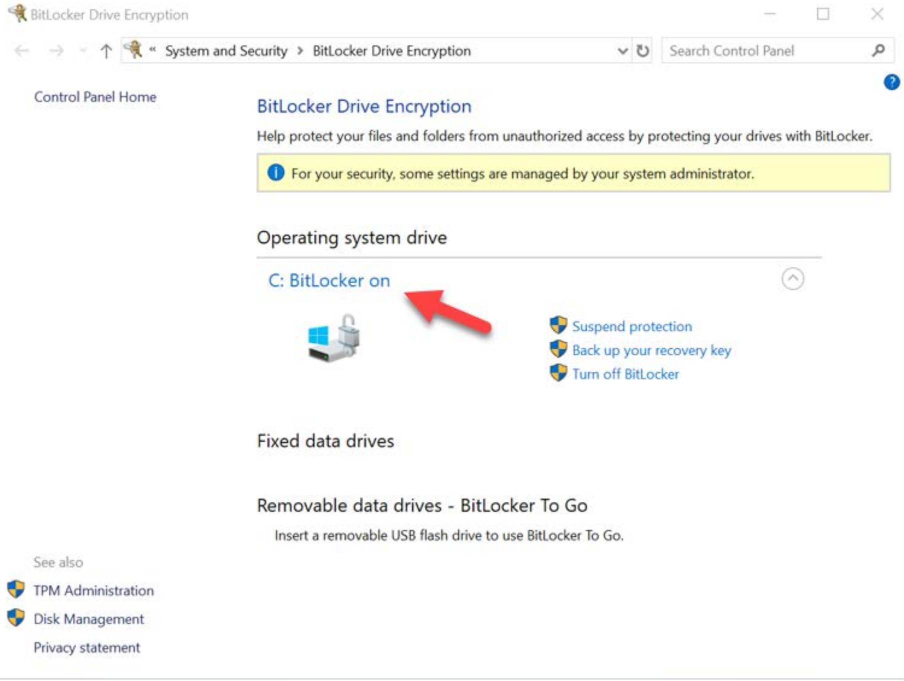
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

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)

○ Encrypt entire drive (slower but best for PCs and drives already in use)

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



BitLocker Drive Encryption
System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

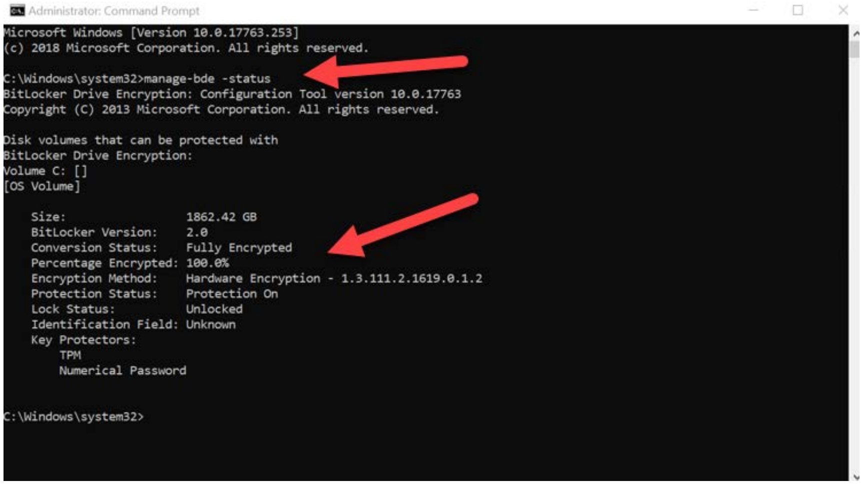
C: BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

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

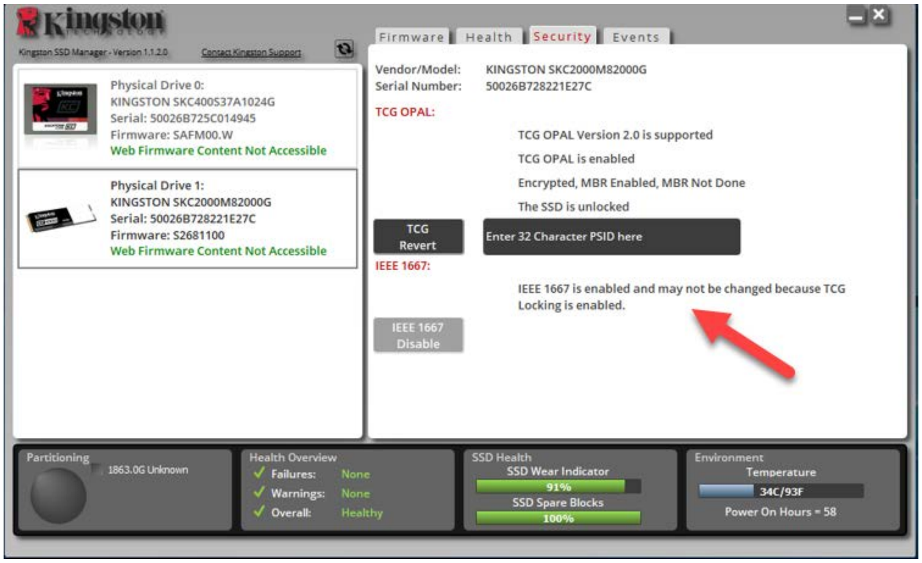


```
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: []
[OS Volume]

    Size:                 1862.42 GB
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    Hardware Encryption - 1.3.111.2.1619.0.1.2
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        TPM
        Numerical Password


C:\Windows\system32>
```

Enable Microsoft eDrive with Windows 10 (version 1903+)
*Microsoft changed the default behavior of Windows 10 with regards to eDrive encryption when they 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 supported OS on target SSD.
2. After the OS is 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 an may not be changed because TCG Locking is enabled.”



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:
TCG OPAL Version 2.0 is supported
TCG OPAL is enabled
Encrypted, MBR Enabled, MBR Not Done
The SSD is unlocked

Enter 32 Character PSID here

IEEE 1667:
IEEE 1667 is enabled and may not be changed because TCG Locking is enabled.

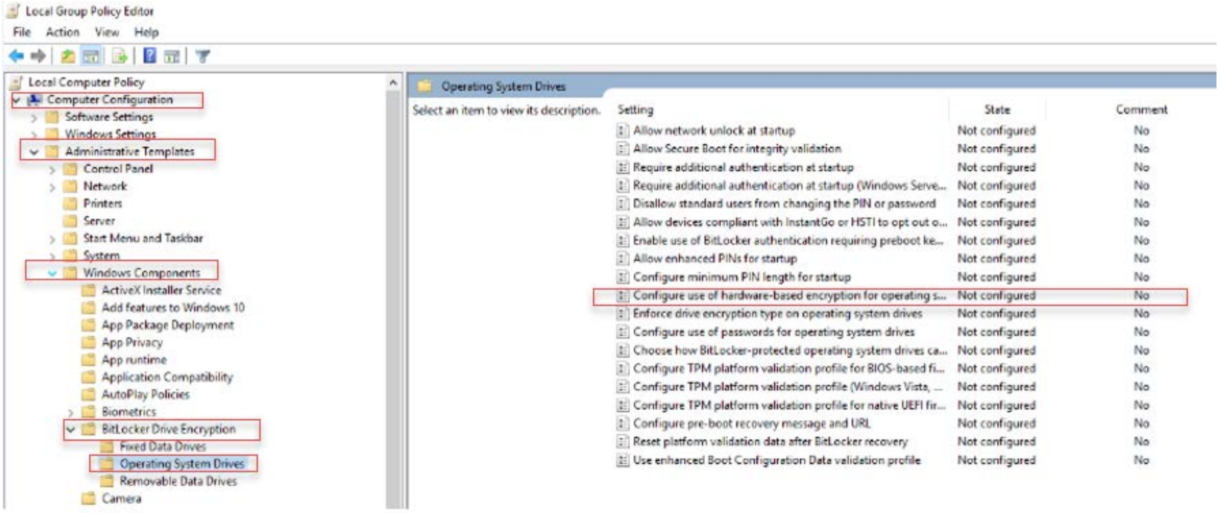
Partitioning
1863.0G Unknown

Health Overview
✓ Failures: None
✓ Warnings: None
✓ Overall: Healthy

SSD Health
SSD Wear Indicator 91%
SSD Spare Blocks 100%

Environment
Temperature 34C/93F
Power On Hours = 58

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.

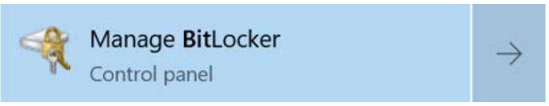


Select an item to view its description.

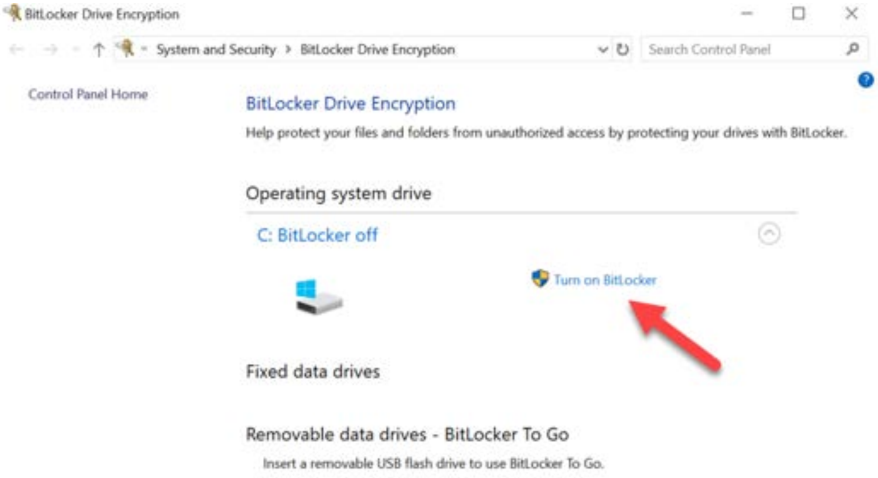
Setting	State	Comment
Allow network unlock at startup	Not configured	No
Allow Secure Boot for integrity validation	Not configured	No
Require additional authentication at startup	Not configured	No
Require additional authentication at startup (Windows Serve...	Not configured	No
Disallow standard users from changing the PIN or password	Not configured	No
Allow devices compliant with InstantGo or HSTI to opt out o...	Not configured	No
Enable use of BitLocker authentication requiring preboot ke...	Not configured	No
Allow enhanced PINs for startup	Not configured	No
Configure minimum PIN length for startup	Not configured	No
Configure use of hardware-based encryption for operating s...	Not configured	No
Enforce drive encryption type on operating system drives	Not configured	No
Configure use of passwords for operating system drives	Not configured	No
Choose how BitLocker-protected operating system drives ca...	Not configured	No
Configure TPM platform validation profile for BIOS-based fi...	Not configured	No
Configure TPM platform validation profile (Windows Vista, ...	Not configured	No
Configure TPM platform validation profile for native UEFI fir...	Not configured	No
Configure pre-boot recovery message and URL	Not configured	No
Reset platform validation data after BitLocker recovery	Not configured	No
Use enhanced Boot Configuration Data validation profile	Not configured	No

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.



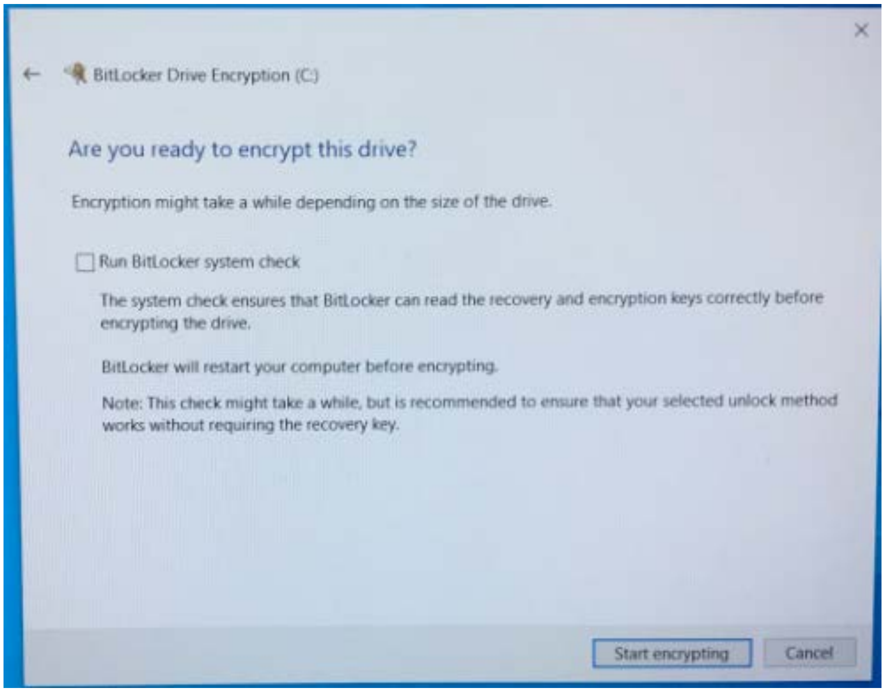
5. Select **Turn on BitLocker** from within the Explorer window.


BitLocker Drive Encryption
System and Security
BitLocker Drive Encryption
Search Control Panel
Control Panel Home
BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

Insert a removable USB flash drive to use BitLocker To Go.

6. Continue through the prompts to configure the target SSD. When prompted, select **Start encrypting.** By default, **Run BitLocker system check** is selected. It is advisable to proceed with this setting enabled. However, when unchecked, you will be able to confirm hardware encryption is enabled without requiring a system reboot.



BitLocker Drive Encryption (C:)

Are you ready to encrypt this drive?

Encryption might take a while depending on the size of the drive.

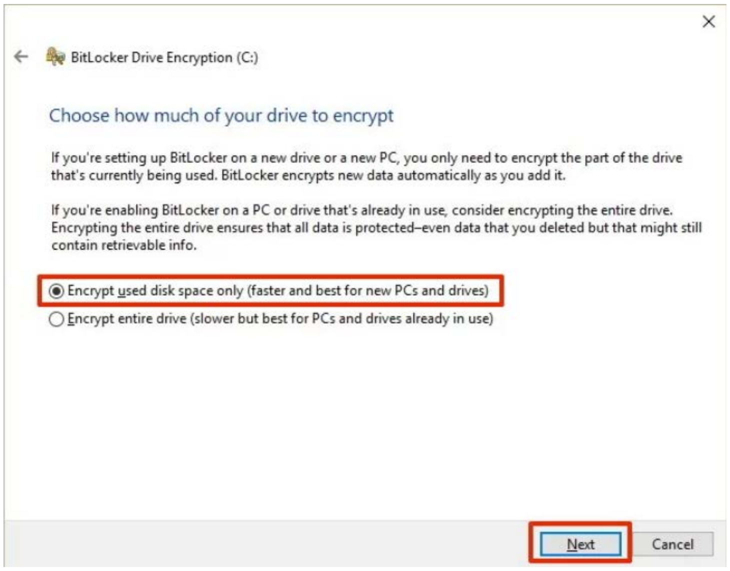
□ Run BitLocker system check

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.

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



BitLocker Drive Encryption (C:)

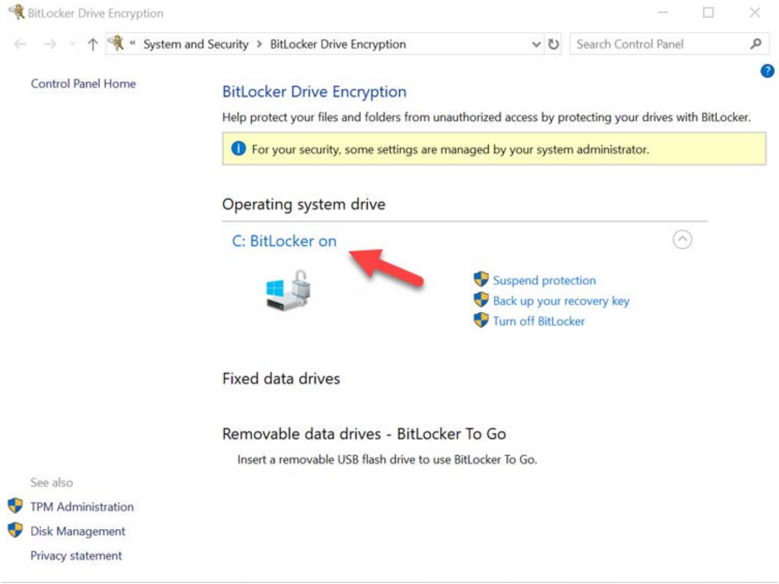
Choose how much of your drive to encrypt

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)
○ Encrypt entire drive (slower but best for PCs and drives already in use)

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


BitLocker Drive Encryption
System and Security > BitLocker Drive Encryption
Search Control Panel
Control Panel Home

BitLocker Drive Encryption

Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.

For your security, some settings are managed by your system administrator.

Operating system drive

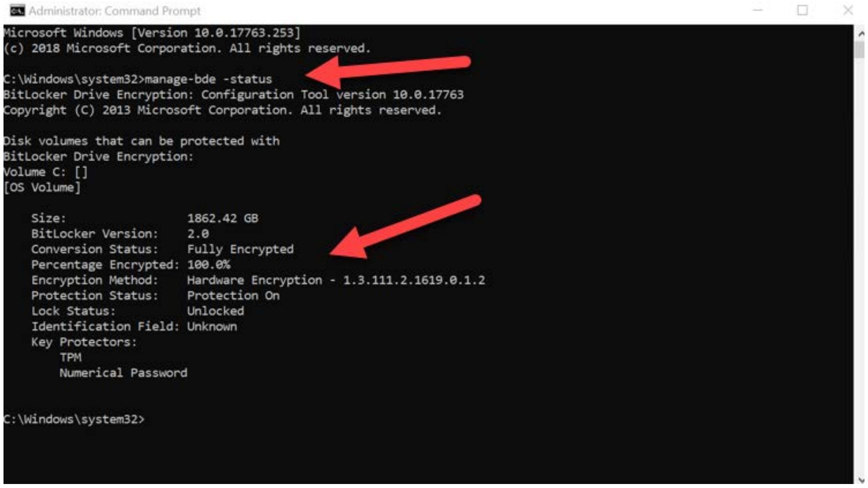
C: BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

Insert a removable USB flash drive to use BitLocker To Go.

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



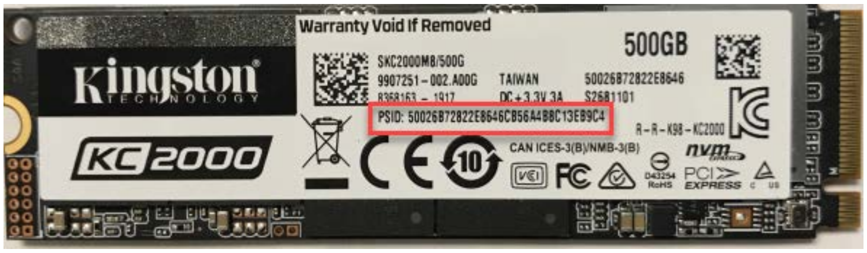
```
Microsoft Windows [Version 10.0.17763.253]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>manage-bde -status
BitLocker Drive Encryption: Configuration Tool version 10.0.17763
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

Disk volumes that can be protected with
BitLocker Drive Encryption:
Volume C: []
[OS Volume]

    Size:                 1862.42 GB
    BitLocker Version:    2.0
    Conversion Status:    Fully Encrypted
    Percentage Encrypted: 100.0%
    Encryption Method:    Hardware Encryption - 1.3.111.2.1619.0.1.2
    Protection Status:    Protection On
    Lock Status:          Unlocked
    Identification Field: Unknown
    Key Protectors:
        TPM
        Numerical Password


C:\Windows\system32>
```

Disable Microsoft eDrive Support

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

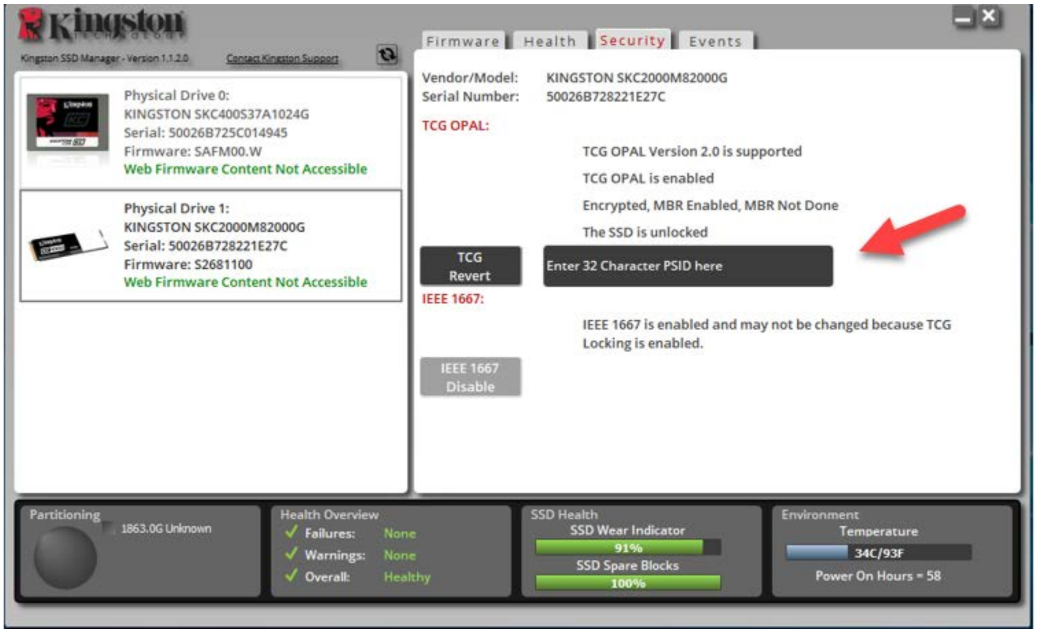
Note: This process will reset your Target SSD and ALL DATA PRESENT ON THE DRIVE WILL BE LOST.

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



Ex: KC2000 PSID Value

2. Mount target SSD as 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 **TCG Revert completed successfully** messaging. If the message is not present, please re-enter your PSID value and retry the revert.



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:

TCG OPAL Version 2.0 is supported
TCG OPAL is enabled
Encrypted, MBR Enabled, MBR Not Done
The SSD is unlocked

Enter 32 Character PSID here

IEEE 1667:

IEEE 1667 is enabled and may not be changed because TCG Locking is enabled.

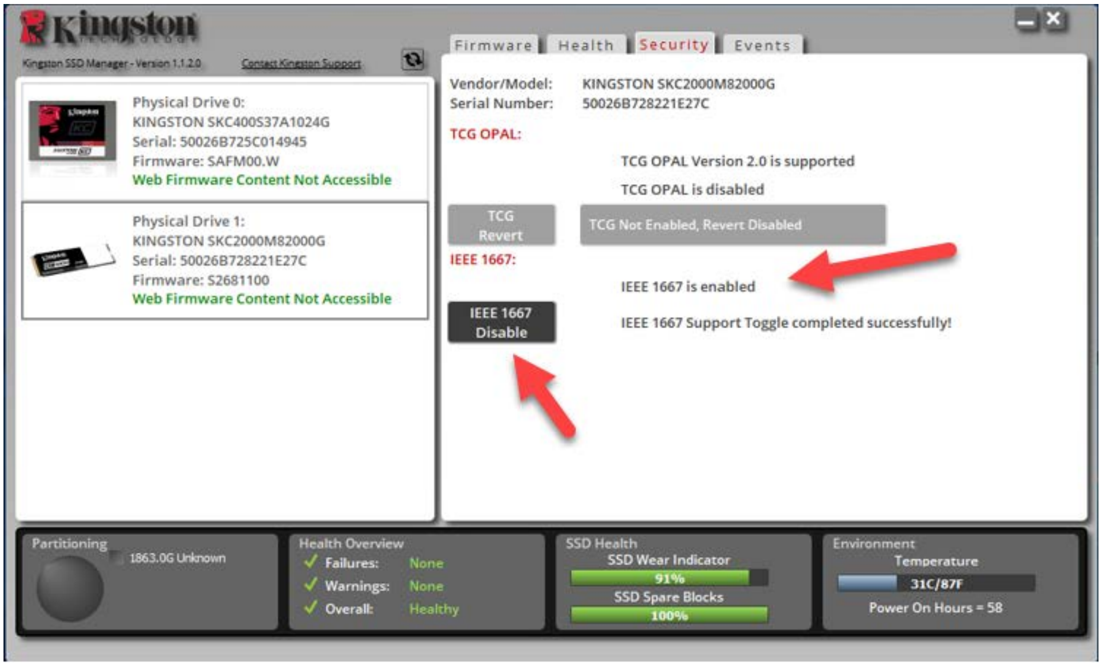
1863.0G Unknown

✓ Failures: None
✓ Warnings: None
✓ Overall: Healthy

SSD Wear Indicator 91%
SSD Spare Blocks 100%

Temperature 34C/93F
Power On Hours = 58

4. Once the drive is successfully reverted, you will have the option to disable IEEE1667 support. Please select **IEEE1667 Disable** and wait for the “IEEE1667 Support Toggle completed successfully” message.



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:

TCG OPAL Version 2.0 is supported

TCG OPAL is disabled

TCG Not Enabled, Revert Disabled

IEEE 1667:

IEEE 1667 is enabled

IEEE 1667 Support Toggle completed successfully!

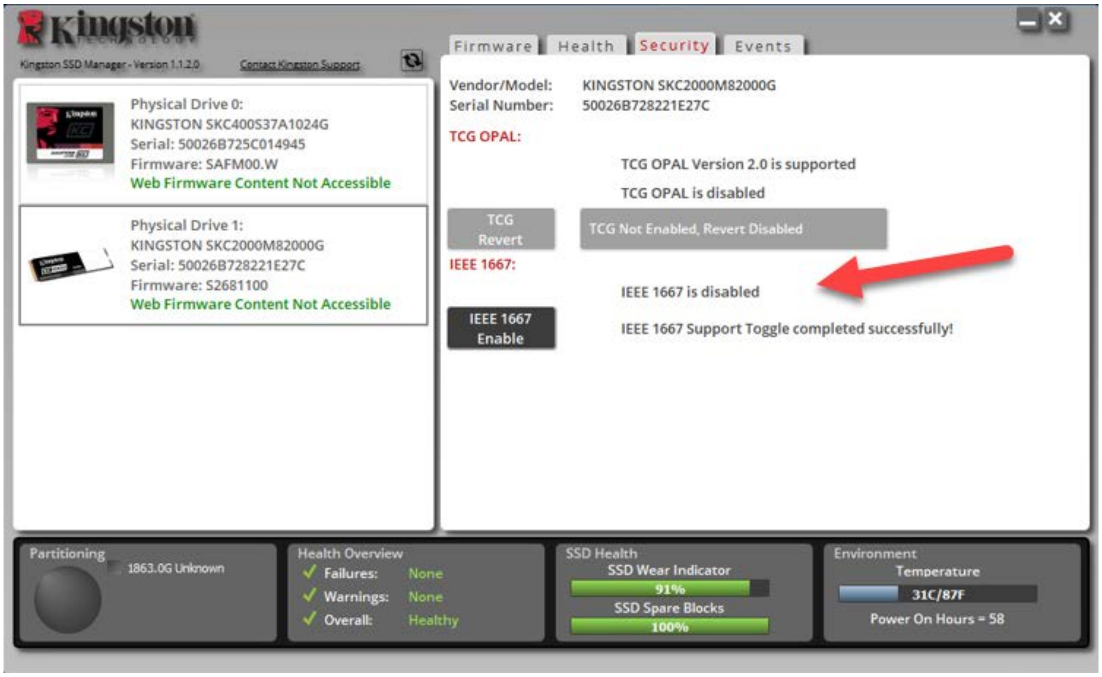
1863.0G Unknown

Failures: None
Warnings: None
Overall: Healthy

SSD Wear Indicator 91%
SSD Spare Blocks 100%

Temperature 31C/87F
Power On Hours = 58

5. Confirm that IEEE1667 support is disabled.



Physical Drive 0:
KINGSTON SKC400S37A1024G
Serial: 50026B725C014945
Firmware: SAFM00.W
Web Firmware Content Not Accessible

Physical Drive 1:
KINGSTON SKC2000M82000G
Serial: 50026B728221E27C
Firmware: S2681100
Web Firmware Content Not Accessible

Vendor/Model: KINGSTON SKC2000M82000G
Serial Number: 50026B728221E27C

TCG OPAL:

TCG OPAL Version 2.0 is supported

TCG OPAL is disabled

TCG Not Enabled, Revert Disabled

IEEE 1667:

IEEE 1667 is disabled

IEEE 1667 Support Toggle completed successfully!

1863.0G Unknown

Failures: None
Warnings: None
Overall: Healthy

SSD Wear Indicator 91%
SSD Spare Blocks 100%

Temperature 31C/87F
Power On Hours = 58

6. Your target SSD is ready for reuse.