SSD เข้ารหัสจาก Kingston

การเปิดและปิดใช้งาน BitLocker กับ eDrive เพื่อใช้ฟังก์ชันเข้ารหัสฮาร์ดแวร์

เกริ่นนำ

เอกสารชุดนี้ระบุวิธีการเปิดใช้และปิดใช้งานฟีเจอร์ Microsoft BitLocker eDrive เพื่อเข้ารหัสฮาร์ดแวร์สำหรับ SSD จาก Kingston ของคุณ ซึ่งใช้สำหรับ SSD จาก Kingston ที่รองรับมาตรฐานการทำงาน TCG OPAL 2.0 และ IEEE 1667 หากคุณไม่มี Kingston SSD ที่รองรับมาตรฐาน TCG OPAL 2.0 และ IEEE1667 ขั้นตอนนี้จะไม่มีความจำเป็น สำหรับคุณ หากคุณไม่แน่ใจ กรุณาติดต่อฝ่ายบริการด้านเทคนิคของ Kingston ได้ที่ www.kingston.com/support

เอกสารชุดนี้อ้างอิงเกี่ยวกับระบบ BitLocker จาก Microsoft และ eDrive โดยจะอ้างอิงเป็น eDrive' ในส่วนที่เหลือของข้อมูลชุดนี้ กระบวนการที่ระบุต่อไปนี้อาจมีการเปลี่ยนแปลงขึ้นอยู่กับเวอร์ชั่นของ Windows และการอัพเดตที่มี

ความต้องการของระบบ

- Kingston SSD ที่รองรับระบบความปลอดภัย TCG Opal 2.0 และ IEEE1667
- ซอฟต์แวร์ Kingston SSD Manager https://www.kingston.com/ssdmanager
- ฮาร์ดแวร์ระบบและ BIOS ที่รองรับ TCG Opal 2.0 และระบบความปลอดภัย IEEE1667

ความต้องการของ OS / BIOS

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

หมายเหตุ: ไดร์ฟ Solid State แบบเข้ารหัสทั้งหมดจะต้องต่อเข้ากับชุดควบคุม Non-RAID เพื่อให้ทำงานได้ถูกต้องใน Windows 8, 10 และ/หรือ Server 2012

ใช้งานไดร์ฟ Solid State แบบเข้ารหัสใน Windows 8, 10 หรือ Windows Server 2012 เป็น**ไดร์ฟข้อมูล**:

- ไดร์ฟจะต้องอยู่ในสถานะที่ยังไม่มีการเริ่มใช้งาน
- ไดร์ฟจะต้องอยู่ในสถานะไม่ได้เปิดใช้งานระบบความปลอดภัย

สำหรับไดร์ฟ Solid State แบบเข้ารหัสที่ใช้เป็น**ไดร์ฟสำหรับเริ่มการทำงาน**:

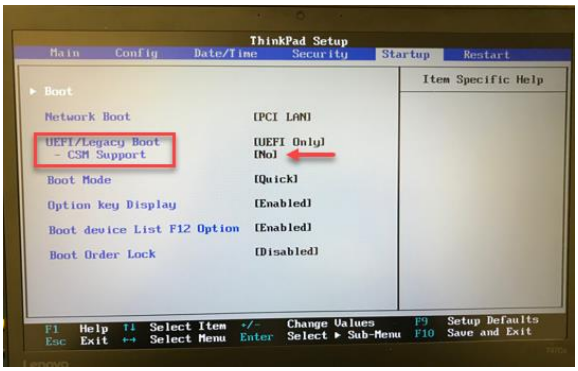
- ไดร์ฟจะต้องอยู่ในสถานะที่ยังไม่มีการเริ่มใช้งาน
- ไดร์ฟจะต้องอยู่ในสถานะไม่ได้เปิดใช้งานระบบความปลอดภัย
- คอมพิวเตอร์จะต้องรองรับอินเทอร์เฟซ UEFI 2.3.1 และกำหนดค่า EFI_STORAGE_SECURITY_COMMAND_PROTOCOL ไว้ (โปรโตคอลนี้ใช้เพื่อให้โปรแกรมที่ทำงานในส่วนบริการบูต EFI สามารถส่งคำสั่งโปรโตคอลด้านความปลอดภัยไปยังไดร์ฟได้)
- คอมพิวเตอร์จะต้องปิดใช้งาน Compatibility Support Module (CSM) จากใน UEFI
- คอมพิวเตอร์จะต้องบูตจากใน UEFI

ดูรายละเอียดเพิ่มเติมได้จากบทความของ Microsoft เกี่ยวกับหัวข้อนี้ซึ่งมีระบุไว้ที่นี่:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

เปิดใช้งาน Microsoft eDrive ผ่าน SSD บู๊ต

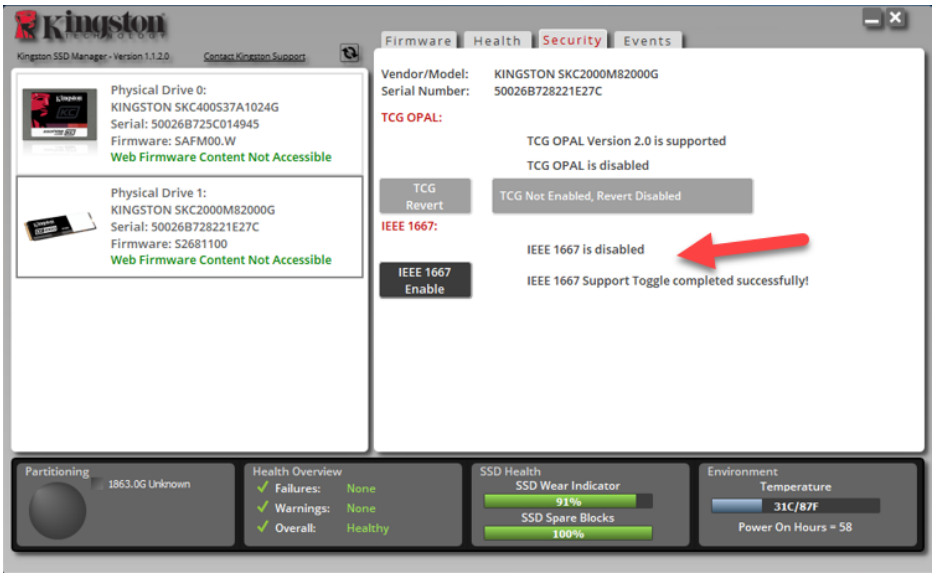
การกำหนดค่า BIOS

1. ตรวจสอบเอกสารกำกับจากผู้ผลิตเครื่องเพื่อยืนยันค่า BIOS ของเครื่องคุณว่ารองรับ UEFI 2.3.1 และกำหนดโปรโตคอล EFI_STORAGE_SECURITY_COMMAND_PROTOCOL ไว้
2. เข้าไปใน BIOS และปิด Compatibility Support Module (CSM)

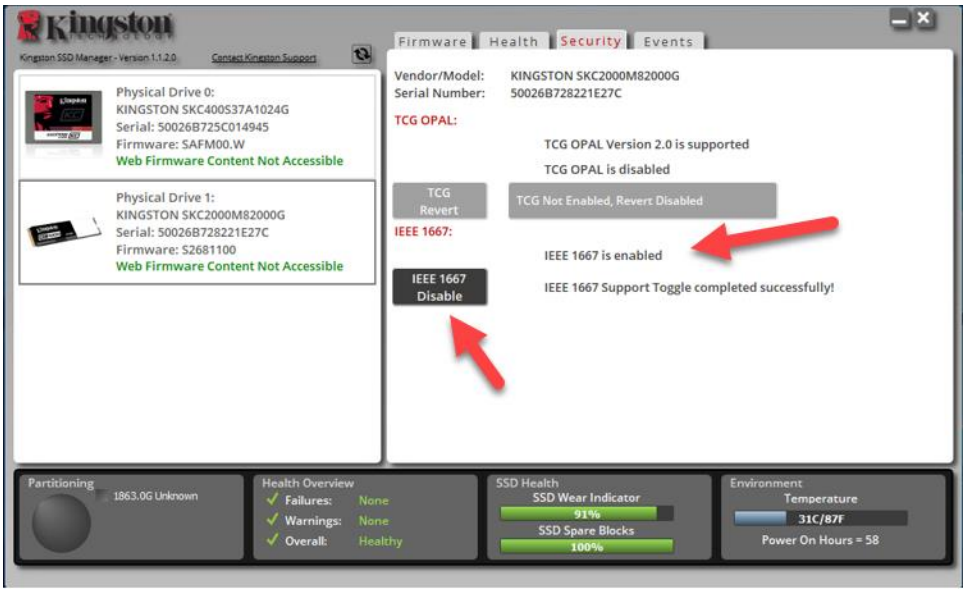


การเตรียมไดร์ฟ

1. หากคุณยังไม่ได้ดาวน์โหลด Kingston SSD Manager (KSM) กรุณาดาวน์โหลดในตอนนี้ https://www.kingston.com/ssdmanager
2. ลบข้อมูลใน SSD เป้าหมายแบบปลอดภัยโดยใช้ซอฟต์แวร์ KSM หรือวิธีการอื่น ๆ ที่ได้มาตรฐานอุตสาหกรรม
3. เชื่อมต่อ SSD เป้าหมายเป็นดิสก์สำรองเพื่อยืนยันสถานะ IEEE1667 ไดร์ฟควรอยู่ในโหมด **ปิดใช้งาน**



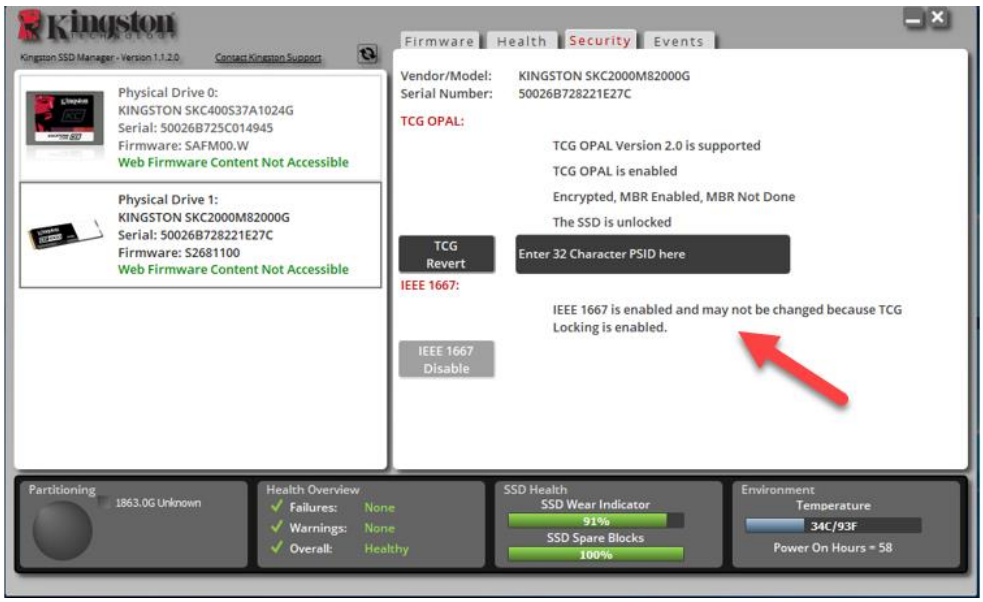
4. เลือกปุ่ม IEEE1667 และ**เปิดใช้งาน**คุณสมบัติดังกล่าว ยืนยันว่าเปิดปิดคุณสมบัติการทำงานได้ถูกต้อง



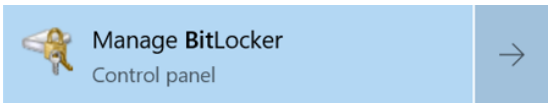
การติดตั้งระบบปฏิบัติการ (OS)

หมายเหตุ: อย่าโคลนระบบปฏิบัติการไปที่ SSD เป้าหมายของคุณ *การโคลน OS ไปยัง SSD เป้าหมายจะทำให้คุณ ไม่สามารถเปิดใช้งานการเข้ารหัสเชิงฮาร์ดแวร์ผ่าน eDrive ได้ คุณจะต้องใช้ส่วนการติดตั้ง OS ใหม่ทั้งหมดกับ SSD เป้าหมายเพื่อใช้ประโยชน์จากระบบเข้ารหัสเชิงฮาร์ดแวร์ผ่าน eDrive*

1. ติดตั้ง OS ที่รองรับกับ SSD เป้าหมาย
2. หลังจากติดตั้ง OS แล้ว ให้ติดตั้ง Kingston SSD Manager (KSM) ให้เรียกใช้ KSM แล้วตรวจสอบว่ามีข้อความต่อไปนี้อยู่ที่แท็บ Security ภายในแอปพลิเคชันดังกล่าว:
   "เปิดใช้งาน IEEE 1667 แล้วแต่เปลี่ยนแปลงไม่ได้เนื่องจากเปิดใช้งาน TCG Locking อยู่"

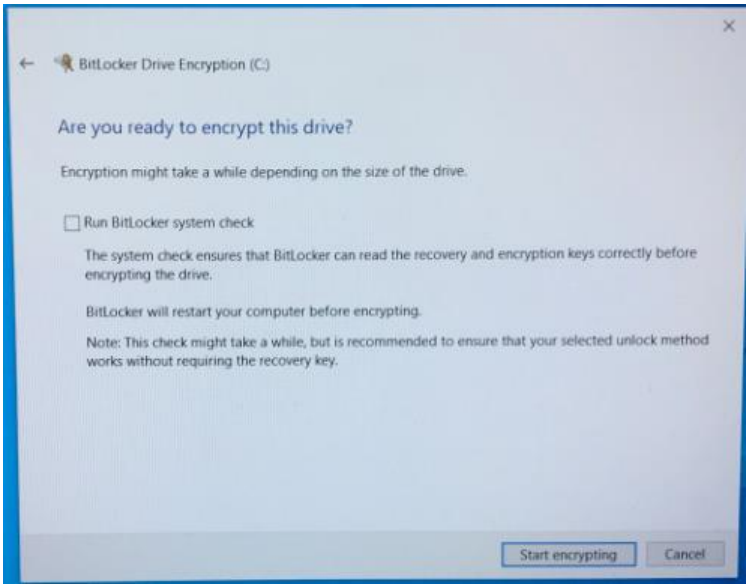


3. ใช้ปุ่ม Windows เพื่อค้นหา **จัดการ BitLocker** จากนั้นเรียกใช้แอปพลิเคชัน

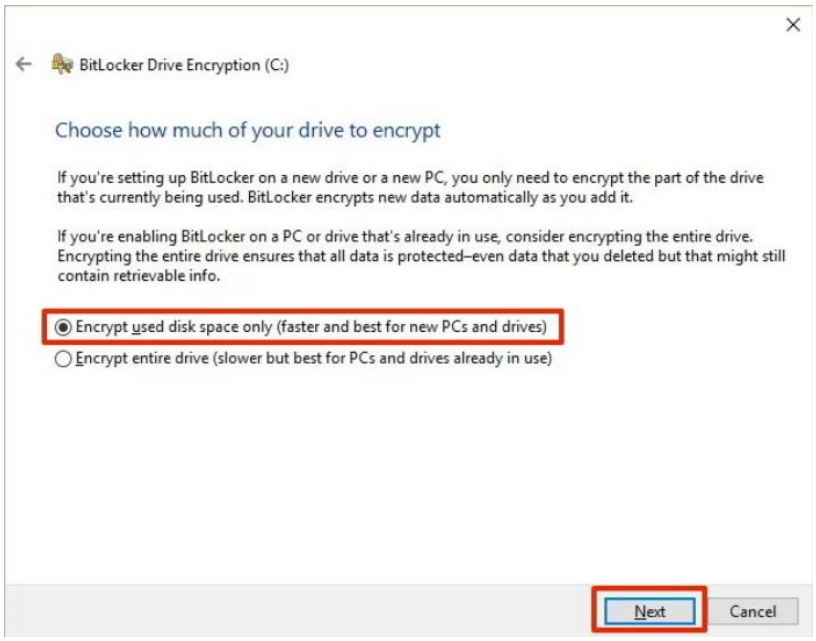


4. เลือก **เปิด BitLocker** จากในหน้าต่าง Explorer

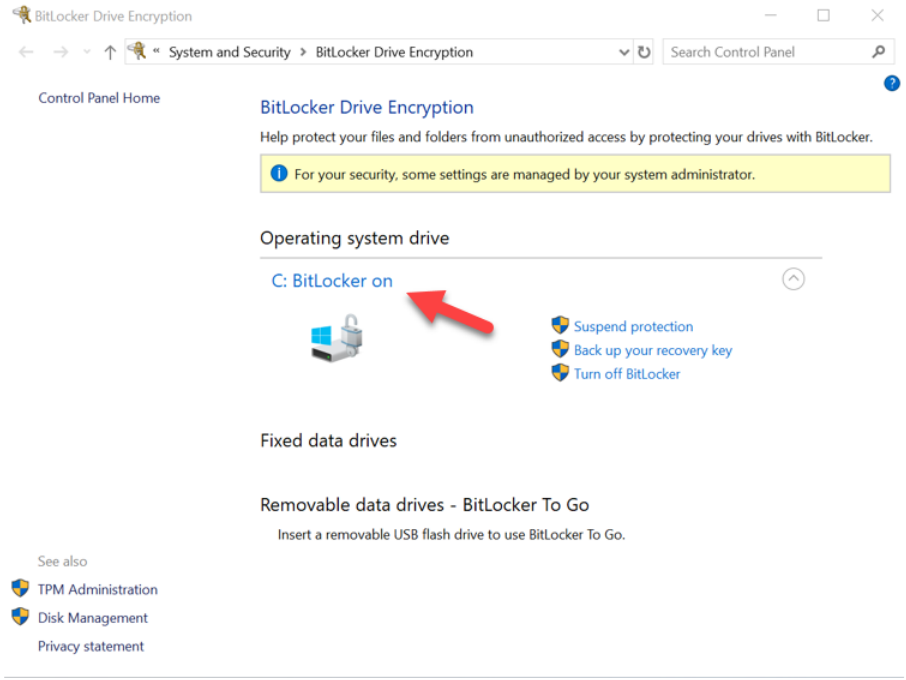
5. ทำตามที่ระบบแจ้งเพื่อกำหนดค่า SSD เป้าหมาย เมื่อได้รับแจ้ง ให้เลือก **เริ่มเข้ารหัส** ตามค่าเริ่มต้น **เรียกใช้การตรวจสอบระบบ BitLocker** จะถูกเลือกไว้ แนะนำให้เปิดใช้งานค่านี้ไว้ ทั้งนี้หากไม่ได้เลือกรายการนี้ คุณจะสามารถตรวจสอบได้ว่ามีการเข้ารหัสเชิงฮาร์ดแวร์หรือไม่โดยไม่ต้องรีบูตเครื่อง



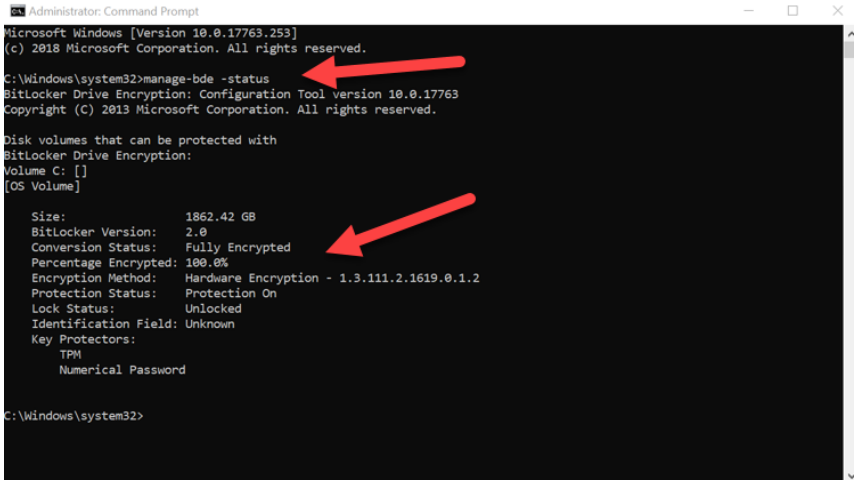
หมายเหตุ: หากคุณได้รับแจ้งจากหน้าจอเพื่อแจ้งให้คุณ "เลือกปริมาณที่ต้องการเข้ารหัสในไดรฟ์" แสดงว่า SSD เป้าหมายจะไม่เปิดใช้งานการเข้ารหัสเชิงฮาร์ดแวร์ แต่จะใช้การเข้ารหัสเชิงซอฟต์แวร์แทน



6. ในกรณีที่จำเป็น ให้รีบูตเครื่องและเรียกใช้ **จัดการ BitLocker** อีกครั้งเพื่อยืนยันสถานะการเข้ารหัส SSD เป้าหมาย



7. นอกจากนี้คุณยังสามารถตรวจสอบสถานะการเข้ารหัสของ SSD เป้าหมายโดยการเปิดไฟล์ **cmd.exe** และพิมพ์: **manage-bde -status**

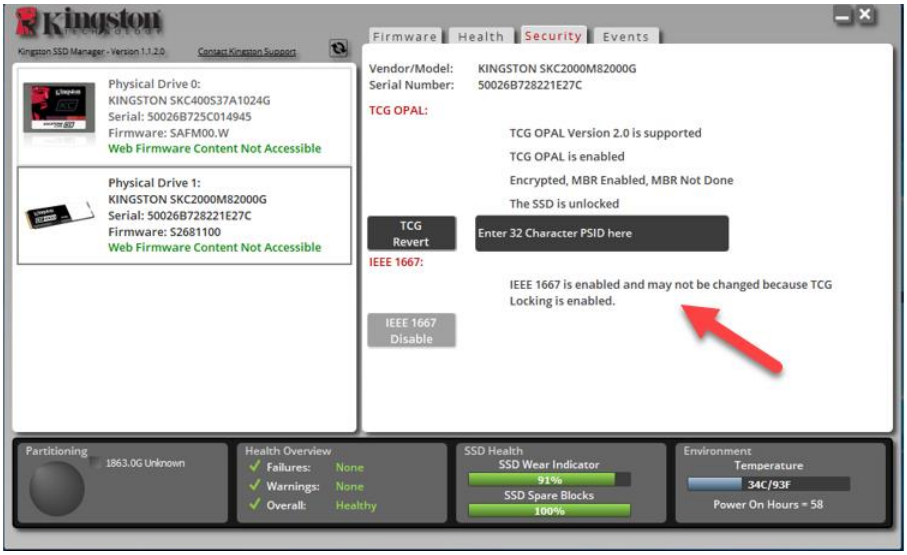


เปิดใช้งาน Microsoft eDrive ผ่าน Windows 10 (เวอร์ชั่น 1903+)

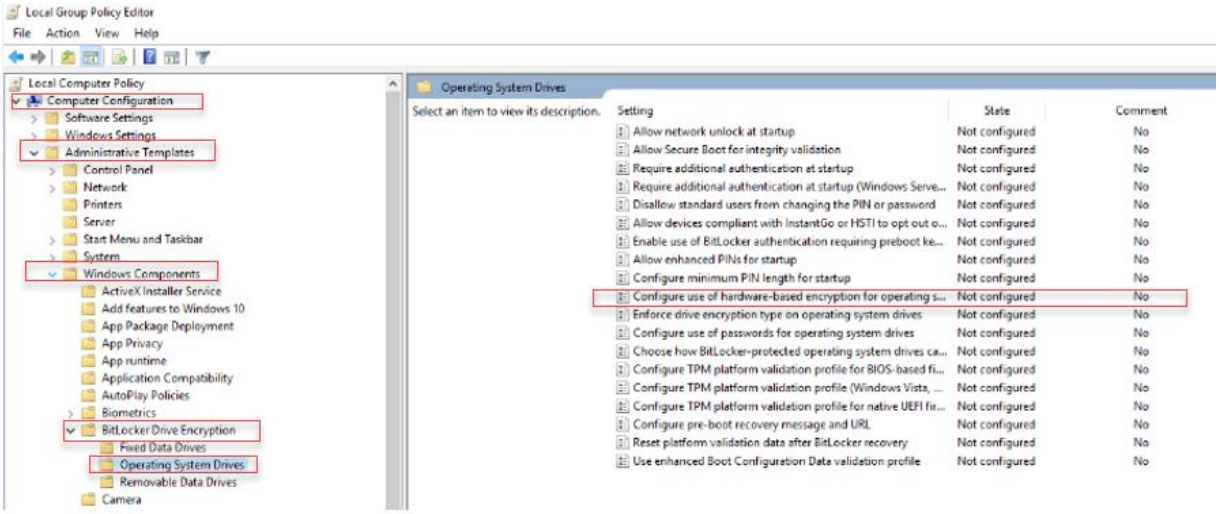
Microsoft มีการปรับเปลี่ยนค่าการทำงานเริ่มต้นสำหรับ Windows 10 ในการเข้ารหัส eDrive เมื่อตอนที่มีการเผยแพร่ Windows 10 เวอร์ชั่น 1903 เปิดใช้งาน eDrive ในบิลด์นี้และรุ่นถัด ๆ มาโดยคุณจะต้องเรียกใช้ ***gpedit*** *เพื่อเปิดใช้งานการเข้ารหัสเชิงฮาร์ดแวร์*

หมายเหตุ: อย่าโคลนระบบปฏิบัติการไปที่ SSD เป้าหมายของคุณ *การโคลน OS ไปยัง SSD เป้าหมายจะทำให้คุณไม่สามารถเปิดใช้งานการเข้ารหัสเชิงฮาร์ดแวร์ผ่าน eDrive ได้ คุณจะต้องใช้ส่วนการติดตั้ง OS ใหม่ทั้งหมดกับ SSD เป้าหมายเพื่อใช้ประโยชน์จากระบบเข้ารหัสเชิงฮาร์ดแวร์ผ่าน eDrive*

1. ติดตั้ง OS ที่รองรับกับ SSD เป้าหมาย
2. หลังจากติดตั้ง OS แล้ว ให้ติดตั้ง Kingston SSD Manager (KSM) เรียกใช้ KSM
   จากนั้นตรวจสอบว่ามีข้อความต่อไปนี้อยู่ที่แท็บการรักษาความปลอดภัยภายในแอปพลิเคชันดังกล่าว:
   "เปิดใช้งาน IEEE 1667 แล้วแต่เปลี่ยนแปลงไม่ได้เนื่องจากเปิดใช้งาน TCG Locking อยู่"

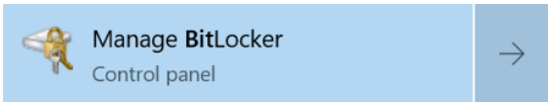


3. เรียกใช้ gpedit.msc เพื่อแก้ไขค่าการเข้ารหัส
   a. ไปที่ **เทมเพลตดูแลจัดการ> องค์ประกอบ Windows> การเข้ารหัสไดรฟ์ BitLocker> ไดรฟ์ระบบปฏิบัติการ**
   b. จากนั้นเลือก **กำหนดค่าการใช้ฟังก์ชันการเข้ารหัสฮาร์ดแวร์สำหรับระบบปฏิบัติการ**
   c. **เปิดใช้งาน**คุณสมบัติการทำงานนี้ จากนั้น**ปรับใช้**ค่าดังกล่าว



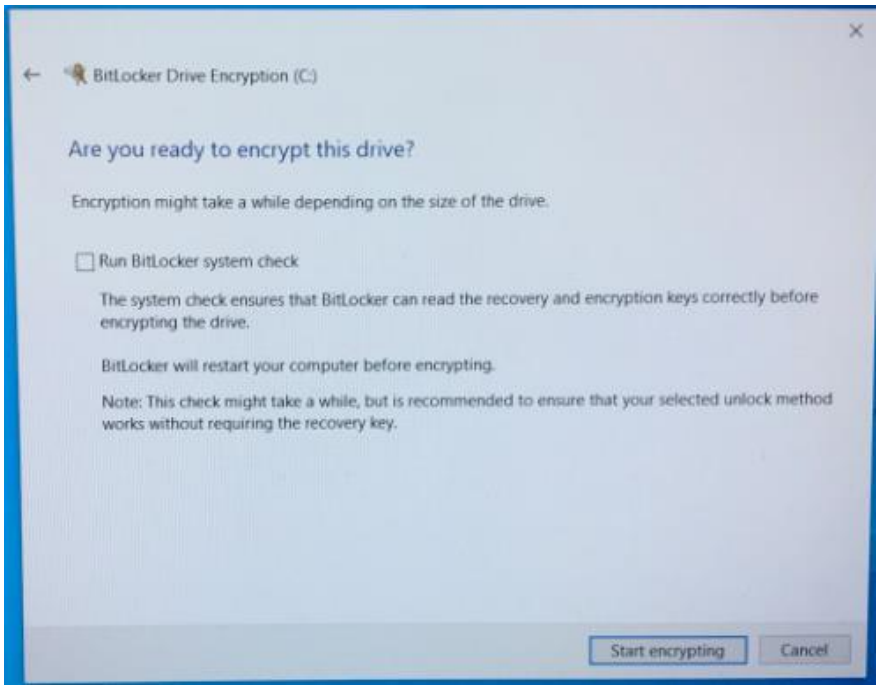
หมายเหตุ: เปิดใช้งาน eDrive ในไดร์ฟที่ไม่ใช่ไดร์ฟระบบปฏิบัติการ
โดยคุณสามารถปรับใช้ค่าเดียวกันนี้โดยเลือก: **เทมเพลตดูแลจัดการ> องค์ประกอบ Windows> การเข้ารหัสไดรฟ์ BitLocker> ไดรฟ์ข้อมูลแบบตายตัว> กำหนดค่าการใช้ฟังก์ชันการเข้ารหัสฮาร์ดแวร์สำหรับไดรฟ์ข้อมูลแบบตายตัว (เปิดใช้งานแล้วนำไปใช้)**

4. ใช้ปุ่ม Windows เพื่อค้นหา **จัดการ BitLocker** จากนั้นเรียกใช้แอปพลิเคชัน

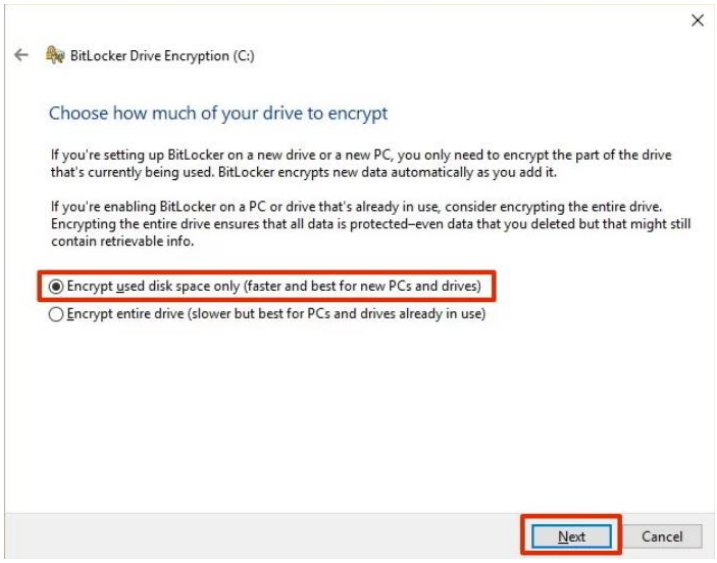


5. เลือก **เปิด BitLocker** จากหน้าต่าง Explorer

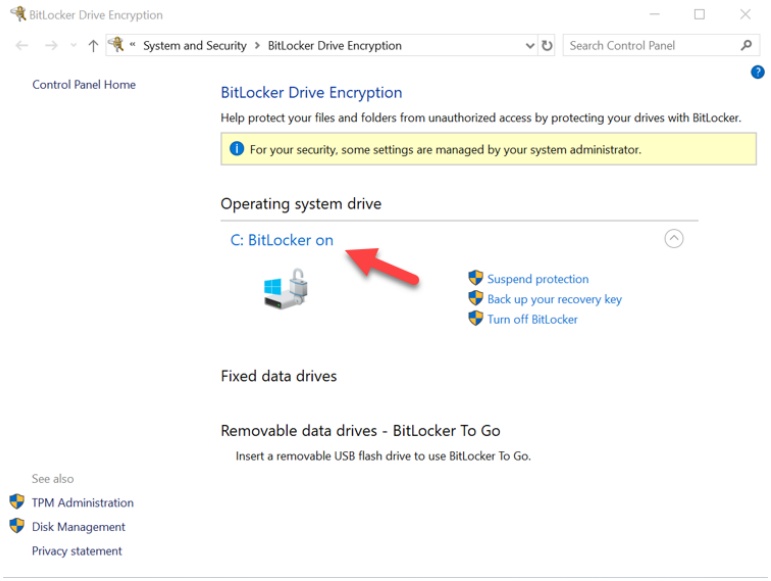
6. ทำตามที่ระบบแจ้งเพื่อกำหนดค่า SSD เป้าหมาย เมื่อได้รับแจ้ง ให้เลือก **เริ่มเข้ารหัส** ตามค่าเริ่มต้น **เรียกใช้การตรวจสอบระบบ BitLocker** จะถูกเลือกไว้ แนะนำให้เปิดใช้งานค่านี้ไว้ ทั้งนี้หากไม่ได้เลือกรายการนี้ คุณจะสามารถตรวจสอบได้ว่ามีการเข้ารหัสเชิงฮาร์ดแวร์หรือไม่โดยไม่ต้องรีบูตเครื่อง



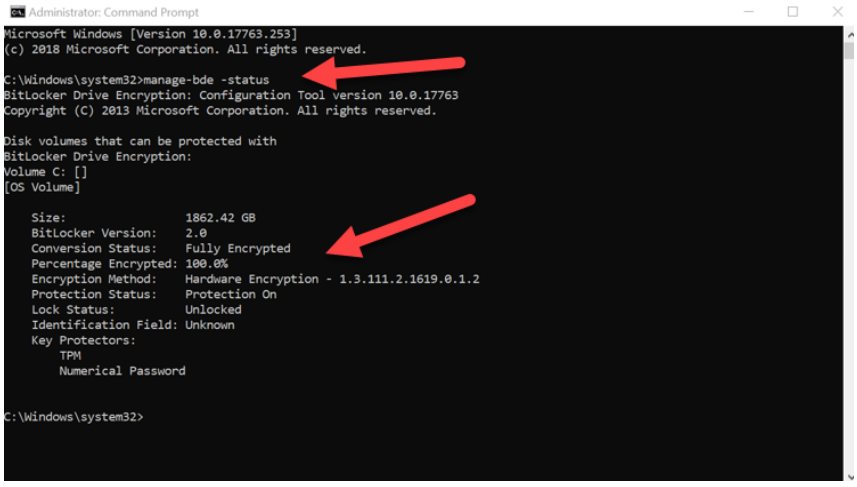
หมายเหตุ: หากคุณได้รับแจ้งจากหน้าจอเพื่อแจ้งให้คุณ "เลือกปริมาณที่ต้องการเข้ารหัสในไดรฟ์" แสดงว่า SSD เป้าหมายจะไม่เปิดใช้งานการเข้ารหัสเชิงฮาร์ดแวร์ แต่จะใช้การเข้ารหัสเชิงซอฟต์แวร์แทน



7. ในกรณีที่จำเป็น ให้รีบูตเครื่องและเรียกใช้ **จัดการ BitLocker** ใหม่เพื่อยืนยันสถานะการเข้ารหัสของ SSD เป้าหมาย



8. นอกจากนี้คุณยังสามารถตรวจสอบสถานะการเข้ารหัสของ SSD เป้าหมายโดยการเปิดไฟล์ **cmd.exe** และพิมพ์: **manage-bde -status**



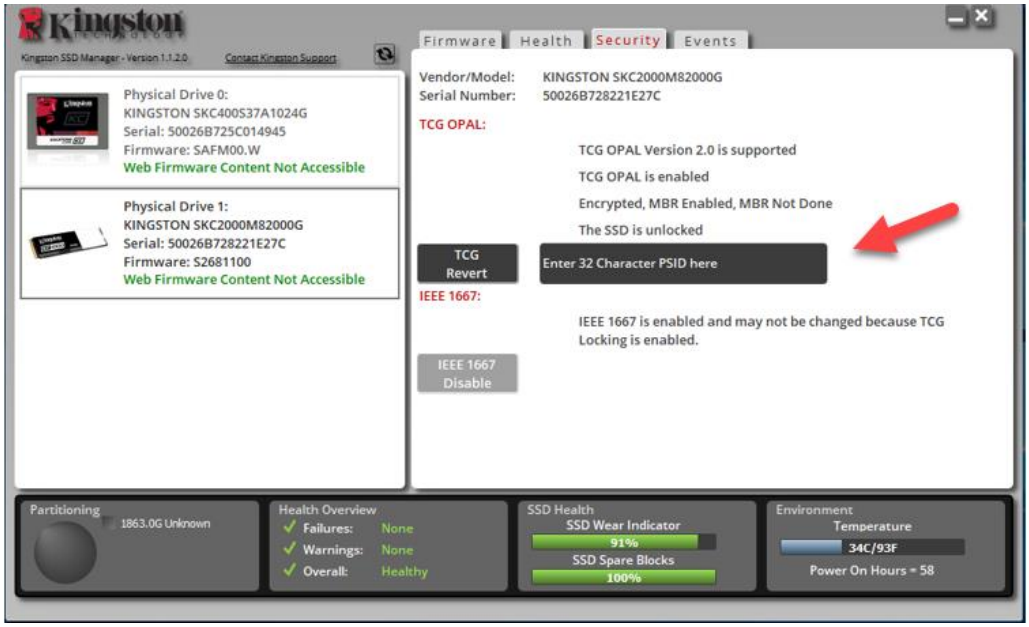
ปิดใช้งานส่วนรองรับ Microsoft eDrive
ลบข้อมูล SSD เป้าหมายของคุณและส่วนรองรับ BitLocker eDrive จากไดร์ฟโดยทำตามขั้นตอนต่อไปนี้

หมายเหตุ: กระบวนการนี้จะเป็นการรีเซ็ต SSD เป้าหมายของคุณและข้อมูลทั้งหมดในไดร์ฟจะหายไป

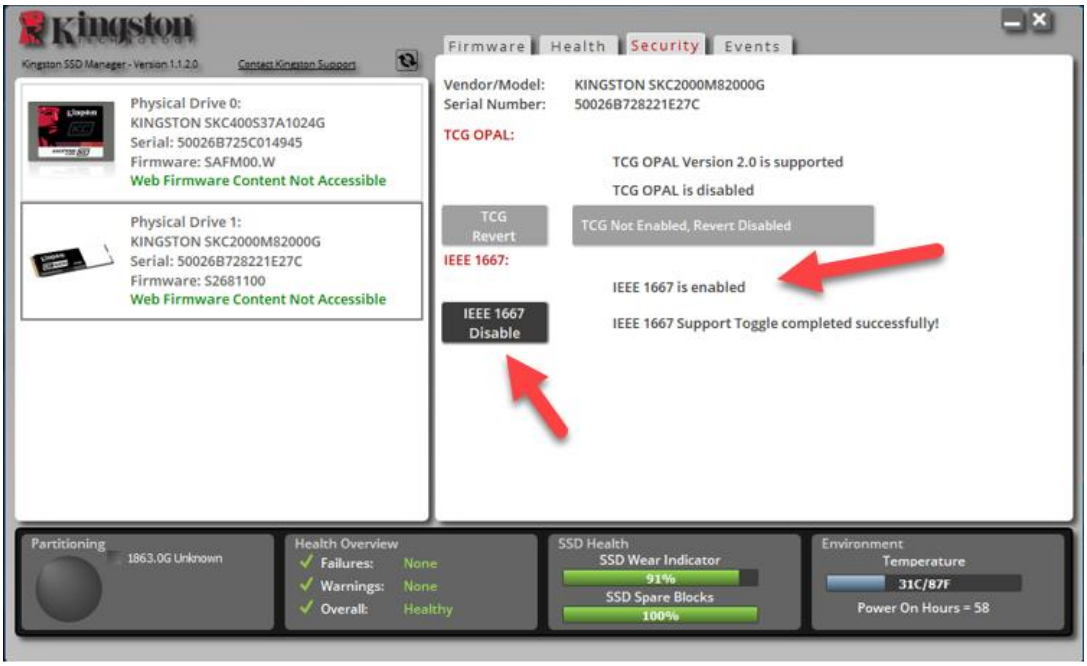
1. จดค่า PSID ของ SSD เป้าหมายไว้ ข้อมูลจะถูกจัดพิมพ์ที่ฉลาก

เช่น KC2000 PSID Value

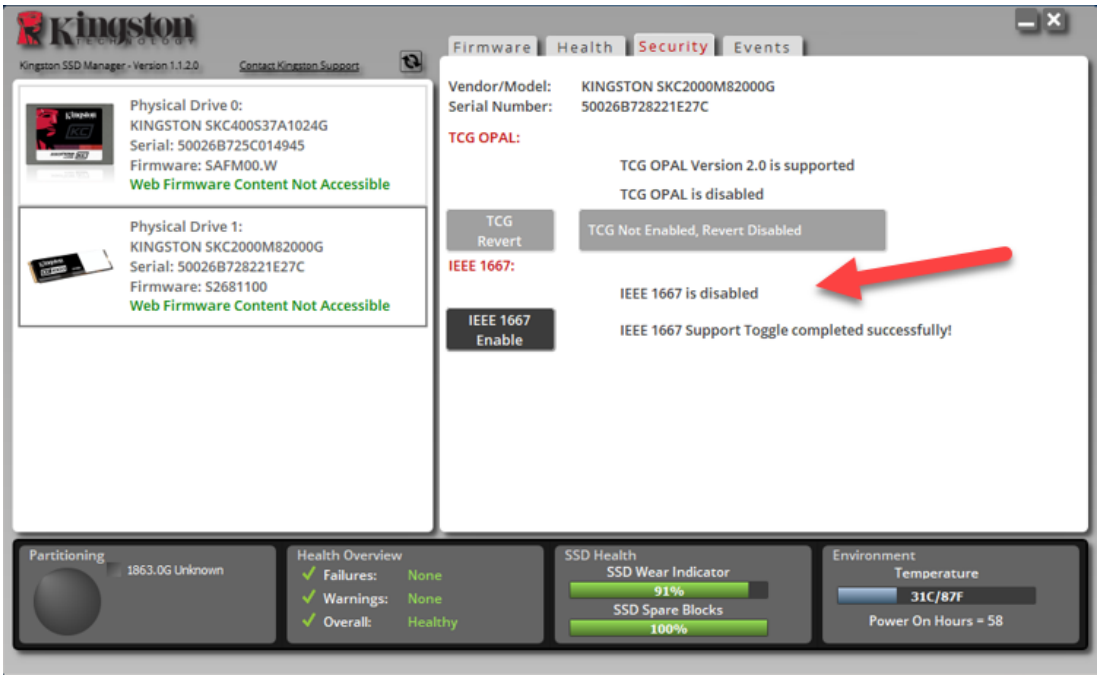
2. เชื่อมต่อ SSD เป้าหมายเป็นไดร์ฟสำรอง และเรียกใช้ Kingston SSD Manager (KSM)
3. เลือกแท็บ **การรักษาความปลอดภัย** แล้วเรียกใช้ **การคืนค่า TCG** โดยกรอกค่า PSID 32 ตัว จากขั้นตอนที่หนึ่ง จากนั้นเลือก **การคืนค่า TCG** หลังจากเสร็จสิ้น คุณจะพบข้อความ **การคืนค่า TCG เสร็จสมบูรณ์** หากข้อความไม่ปรากฏขึ้น ให้กรอกค่า PSID อีกครั้งและเรียกใช้การคืนค่าอีกครั้ง



4. หลังจากการคืนค่าไดร์ฟเสร็จสิ้น คุณสามารถเลือกปิดส่วนรองรับ IEEE1667 ได้ กรุณาเลือก **IEEE1667 ปิดใช้งาน** และรอให้ข้อความ "การเปิดปิดส่วนรองรับ IEEE1667 เสร็จสมบูรณ์" ปรากฏขึ้น



5. ยืนยันว่ามีการปิดใช้งานส่วนรองรับ IEEE1667 ไว้



6. SSD เป้าหมายของคุณพร้อมสำหรับการใช้งานใหม่แล้ว