Kingston の暗号化 SSD

eDrive で BitLocker を有効/無効にしてハードウェア暗号化を利用

製品説明

本書はお手元のキングストン製 SSD でハードウェア暗号化を活用する場合に、Microsoft 社の BitLocker eDrive 機能を有効/無効化する方法について説明します。 この手順は、TCG OPAL 2.0 および IEEE1667 の機能に対応するキングストン製 SSD が対象となります。 お手元のキングストン製 SSD が TCG OPAL 2.0 および IEEE1667 に未対応の場合、このプロセスは機能しません。 ご不明な点があれば、キングストンの技術サポート (@www.kingston.com/support) にお問い合わせください。

本書は以降、Microsoft eDrive 内蔵の BitLocker を 'eDrive と呼びます。 以下に説明する各手順は、Windows のバージョンや更新プログラムによって異なる場合があります。

システム要件

-TCG Opal 2.0 および IEEE1667 セキュリティ機能セットを利用するキングストン製 SSD
-Kingston SSD Manager ソフトウェア https://www.kingston.com/ssdmanager
-TCG Opal 2.0 および IEEE1667 セキュリティ機能をサポートするシステムハードウェアおよび BIOS

OS/BIOS の要件

-Windows 8 および 8.1 (Pro/Enterprise)
-Windows 10 (Pro、Enterprise、Education)
-Windows Server 2012

注 : Windows 8、10、および/または Server 2012 で正常に機能させるには、暗号化されたすべてのソリッドステートドライブ (SSD) を非 RAID コントローラーに接続しなければなりません。

Windows 8、10、または Windows Server 2012 で暗号化ソリッドステートドライブを**データドライブ**として使用する場合 :

- ドライブは非初期化状態でなければなりません。
- セキュリティは無効にされていなければなりません。

暗号化 SSD が**起動ドライブ**として使われている場合 :

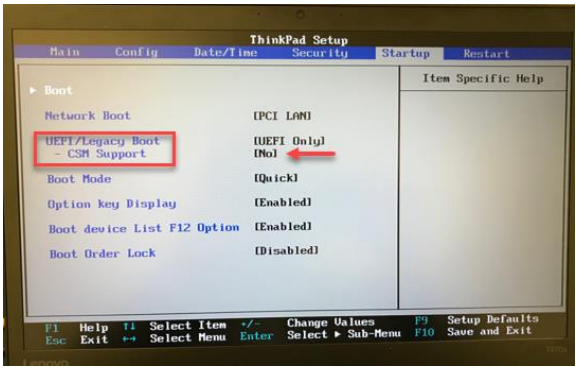
- ドライブは非初期化状態でなければなりません。
- セキュリティは無効にされていなければなりません。
- コンピュータは UEFI 2.3.1 ベースで、EFI_STORAGE_SECURITY_COMMAND_PROTOCOL が定義済みでなければなりません。(このプロトコルは、EFI ブートサービス環境で実行されている各プログラムが、セキュリティプロトコルコマンドをドライブに送信可能にするために使用されます。)
- コンピュータは、UEFI で無効にした互換性サポートモジュール (CSM) を備えなければなりません。
- コンピュータは常に UEFI からネイティブで起動しなければなりません。

詳細については、以下の Microsoft 社の記事をご覧ください :
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

ブート SSD で Microsoft eDrive を有効にする場合

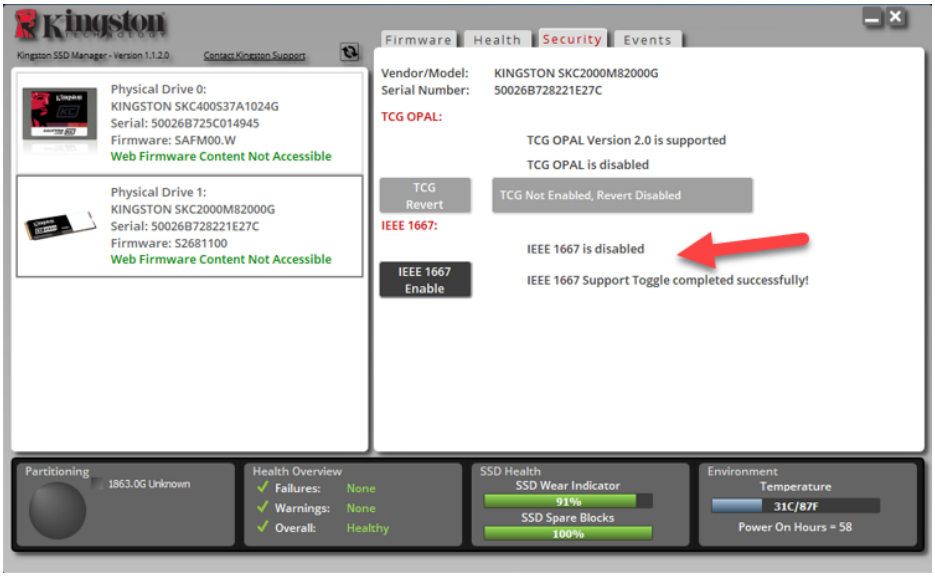
BIOS 設定

1. ユーザーシステムの BIOS が UEFI 2.3.1 ベースで、定義済みの EFI_STORAGE_SECURITY_COMMAND_PROTOCOL を持つことを確認する場合は、システムメーカーのドキュメントをご覧ください。
2. BIOS 設定に入り、Compatibility Support Module (CSM) を無効にしてください。

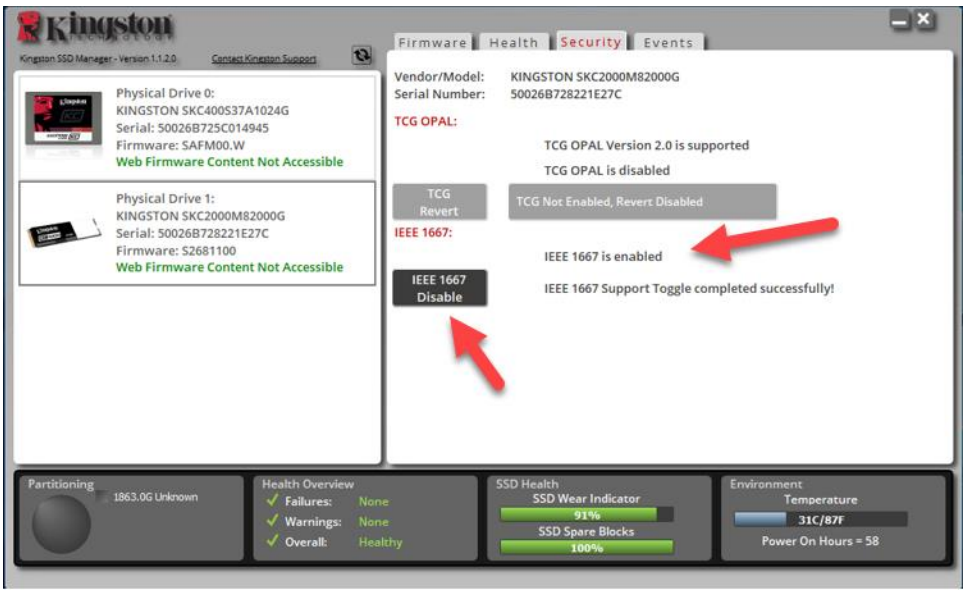


ドライブの準備

1. Kingston SSD Manager (KSM) をまだダウンロードしていない場合は、直ちにダウンロードしてください。https://www.kingston.com/ssdmanager
2. KSM ソフトウェアまたは他の業界標準の方法を用いて、ターゲット SSD を消去します。
3. ターゲット SSD をセカンダリーディスクとしてマウントし、IEEE 1667 のステータスを確認します。ドライブは、**無効**モードでなければなりません。



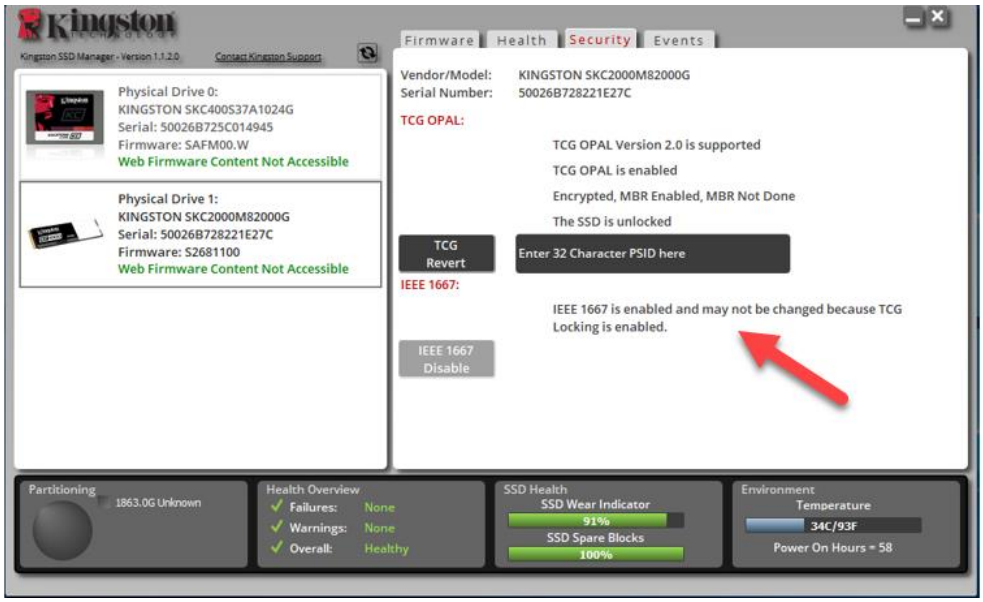
4. IEEE1667 ボタンを選択し、機能を**有効**にします。機能が正常に切り替えられるか確認します。



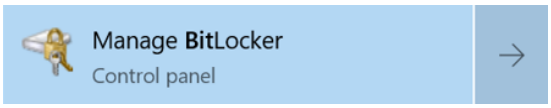
OS (オペレーティングシステム) のインストール

注：ターゲット SSD に、OS のクローンを作成しないでください。 *ターゲット SSD に OS をクローンすると、eDrive を使用したハードウェア暗号化を有効にできなくなります。 eDrive でハードウェア暗号化を利用するには、ターゲット SSD に新しい OS インストールを展開しなければなりません。*

1. サポートされている OS を、ターゲット SSD にインストールします。
2. OS のインストール後、Kingston SSD Manager（KSM）をインストールして実行し、アプリケーションの [セキュリティ] タブに次のメッセージが表示されることを確認します。
   「IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.」
   （IEEE 1667 が有効になっており、TCG ロックが有効になっているため、変更できません。）

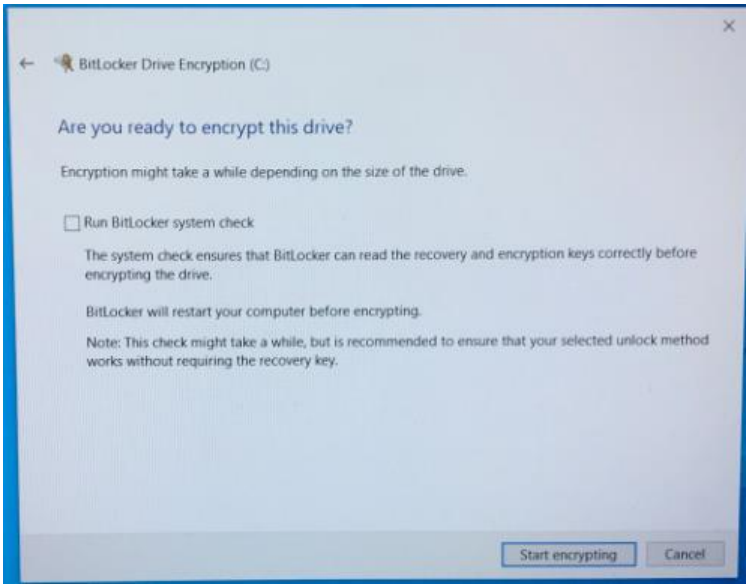


3. Windows キーを使用して 「**Manage BitLocker**」（BitLocker の管理） を検索し、アプリケーションを実行します。

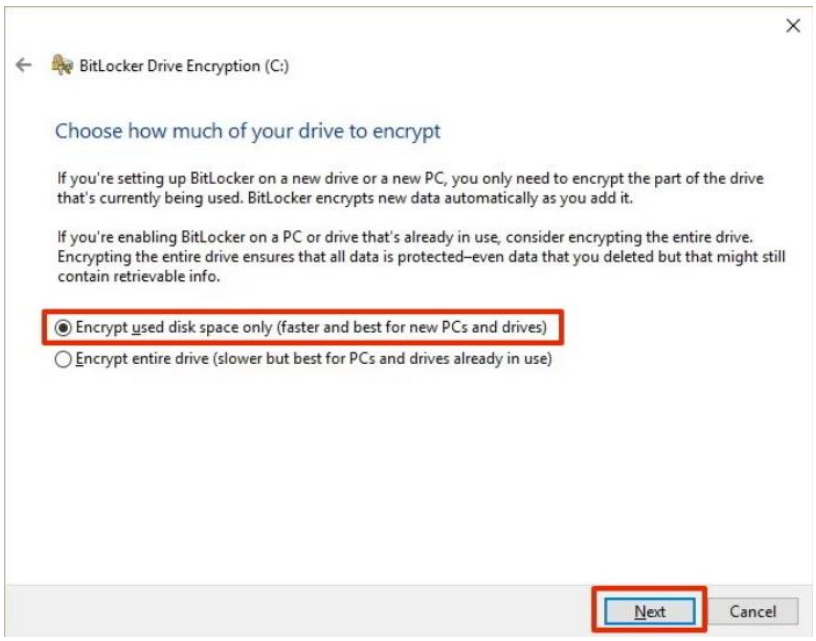


4. エクスプローラのウィンドウ内で、「**Turn on BitLocker**」（BitLocker を有効にする）を選択します。

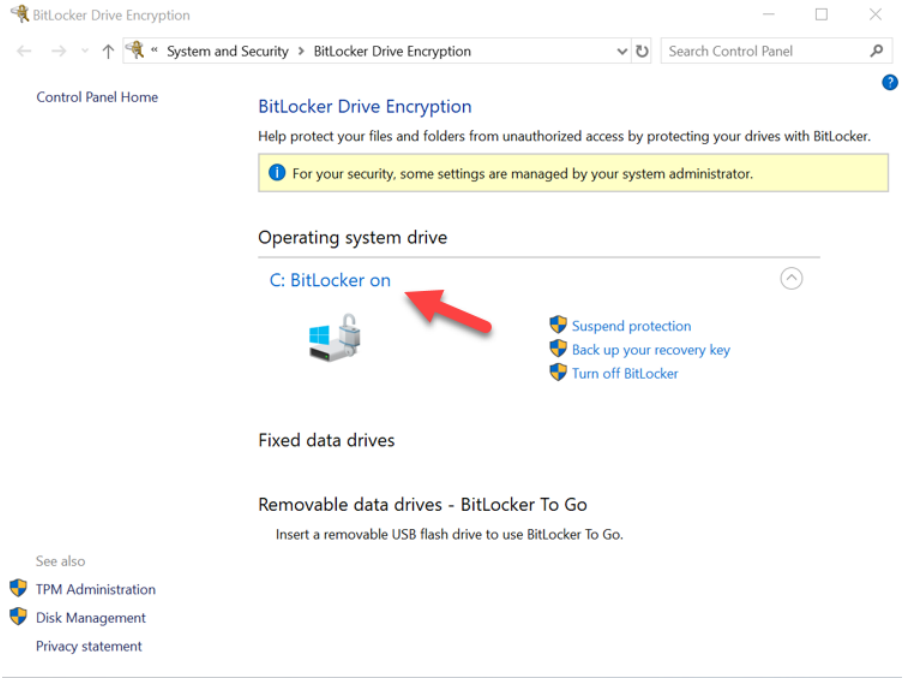
5. プロンプトメッセージに従って続行し、ターゲット SSD を構成します。プロンプトが示されたら、「**Start encrypting」 (暗号化を開始する) を選択します。** デフォルトで、「Run BitLocker system check」（**BitLocker のシステムチェックを実行する**）が選択されています。 この設定を有効にして続行することが推奨されます。 無効にした場合は、ハードウェア暗号化の際にシステムの再起動が必要かどうかを確認できます。



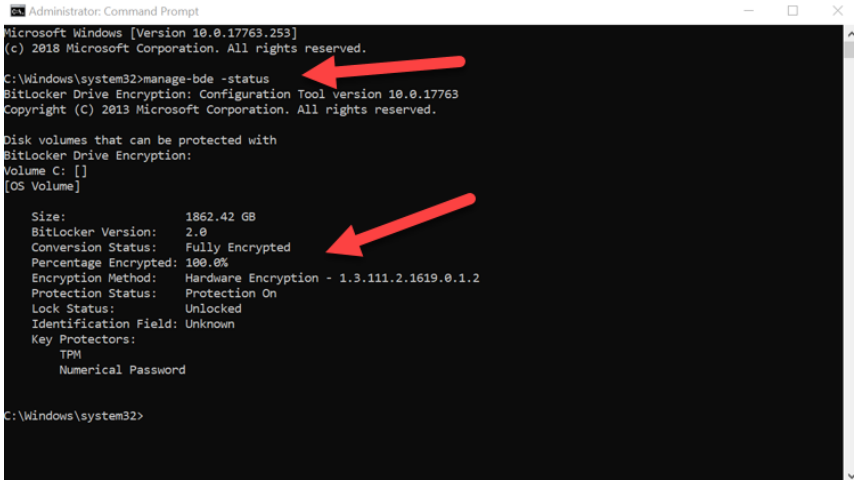
注：「Choose how much of your drive to encrypt」（暗号化するドライブの数を選択してください）という画面が表示されたら、多くの場合、ターゲット SSD がハードウェアの暗号化を有効にせず、代わりにソフトウェア暗号化を使うことを意味します。



6. 必要な場合は、システムを再ブートし、**Manage BitLocker** を再起動して、ターゲット SSD の暗号化の状態を確認してください。



7. また、**cmd.exe** を開いて **manage-bde -status** を入力すれば、ターゲット SSD の暗号化の状態をチェックできます。

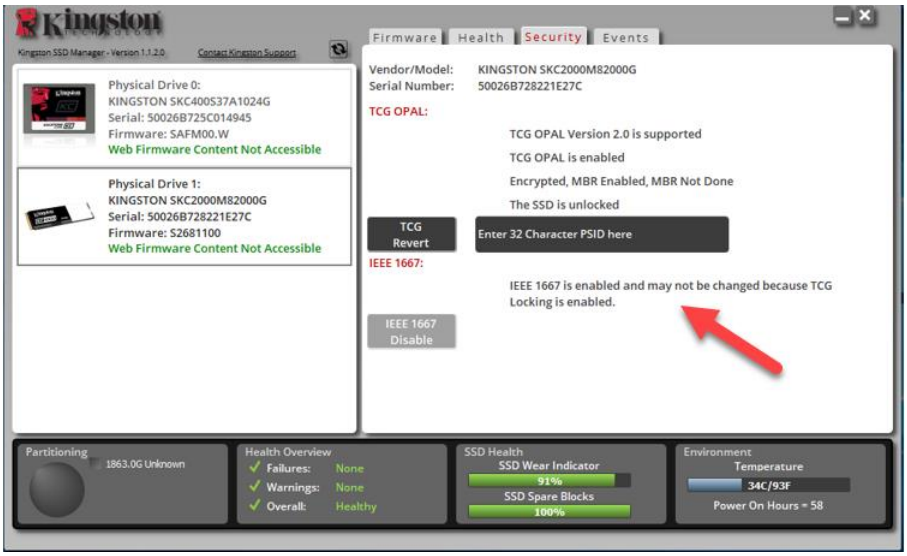


Windows 10 (バージョン 1903+)で、Microsoft dDrive を有効にする場合

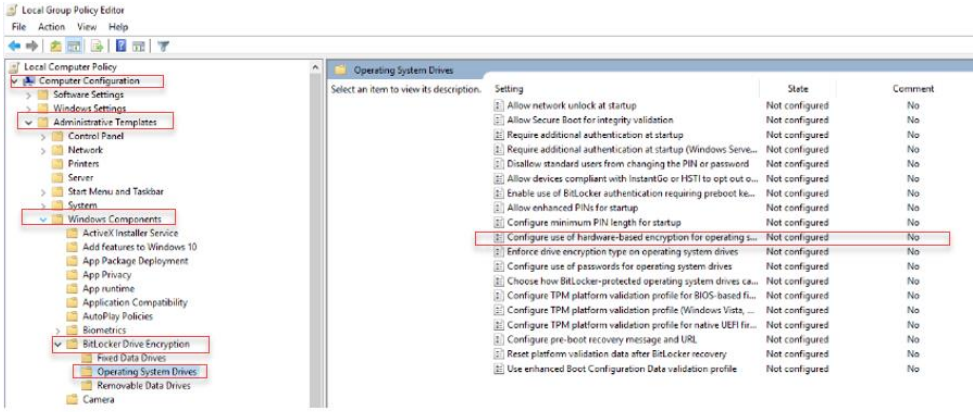
*Microsoft 社は Windows 10 バージョン 1903 のリリースに際し、eDrive 暗号化に関する Windows 10 のデフォルト動作を変更しました。このビルドおよびそれ以降で eDrive を有効にするには、**gpedit** を実行して、ハードウェアの暗号化を有効にする必要があります。*

注：ターゲット SSD に、OS のクローンを作成しないでください。 *ターゲット SSD に OS をクローンすると、eDrive を使用したハードウェア暗号化を有効にできなくなります。 eDrive でハードウェア暗号化を利用するには、ターゲット SSD に新しく OS をインストールしなければなりません。*

1. 対応 OS をターゲット SSD にインストールします。
2. OS のインストール後、Kingston SSD Manager（KSM）をインストールして実行し、アプリケーションの [セキュリティ] (Security) タブに次のメッセージが表示されることを確認します。
   「IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.」（IEEE 1667 が有効になっており、TCG ロックが有効になっているため、変更できません。）

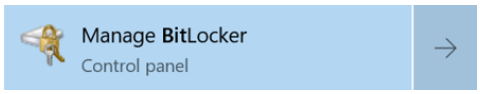


3. gpedit.msc を実行して、暗号化の設定を変更します。
   a. **Administrative Templates （管理用テンプレート）> Windows Components （Windows のコンポーネント）> BitLocker Drive Encryption （BitLocker ドライブの暗号化）> Operating System Drives （OS ドライブ）を順次選択します**
   b. 次に、「**Configure use of hardware-based encryption for operating systems**」（OS のハードウェアベース暗号化の利用設定）を選択します。
   c. 機能を「Enable」（**有効**）にし、次に設定内容に「Apply」（**適用**） します。



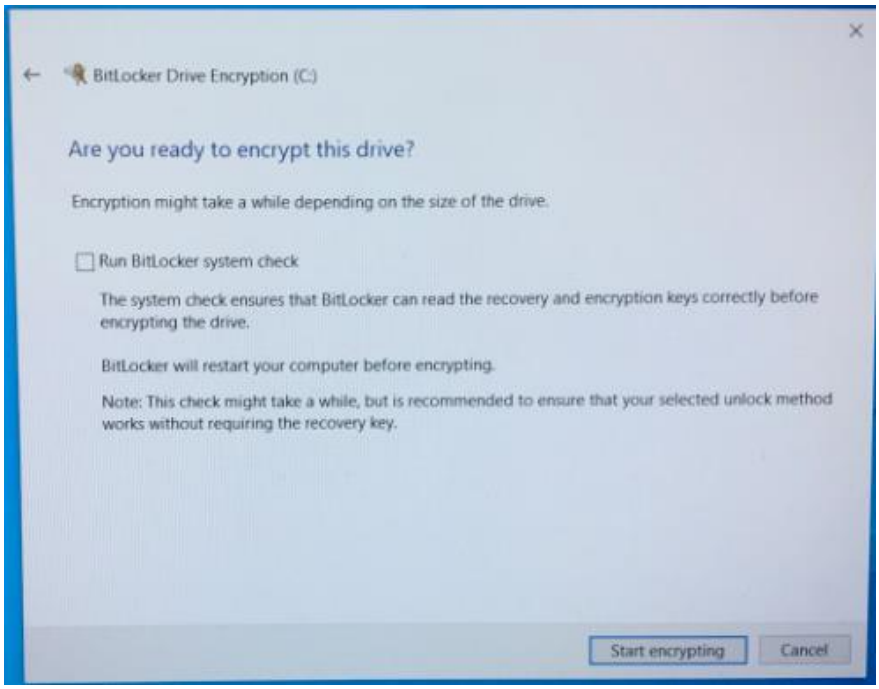
注：OS のドライブ以外のドライブで eDrive を有効にするには、以下を順番に選択し、同じ設定内容を適用できます。ナビゲーション： **Administrative Templates （管理用テンプレート）> Windows Components （Windows コンポーネント）> BitLocker Drive Encryption （BitLocker ドライブ暗号化）> Fixed Data Drives （固定データ ドライブ）> Configure use of hardware-based encryption for fixed data drives （固定データ ドライブのハードウェアベース暗号化の利用設定）(Enable、次に Apply)**

4. Windows キーを使用して 「**Manage BitLocker** 」（BitLocker 管理）を検索し、次にアプリケーションを実行します。

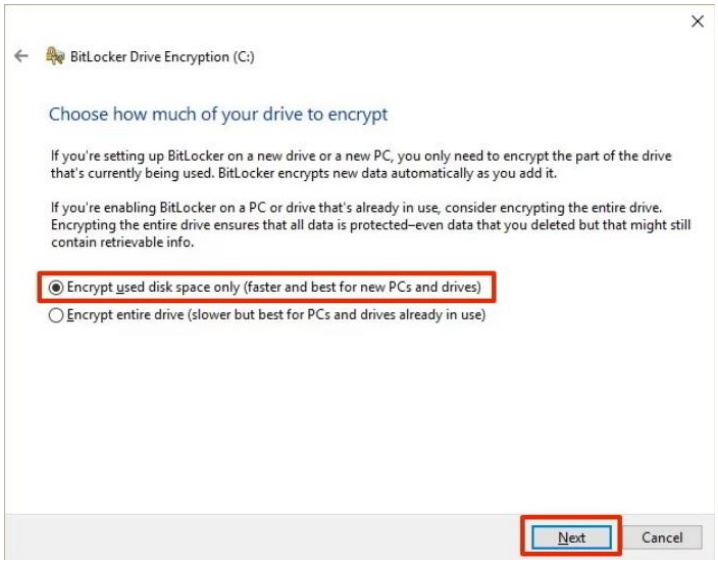


5. エクスプローラ ウィンドウ内で、「**Turn on BitLocker**」（BitLocker をオンにする）を選択します。

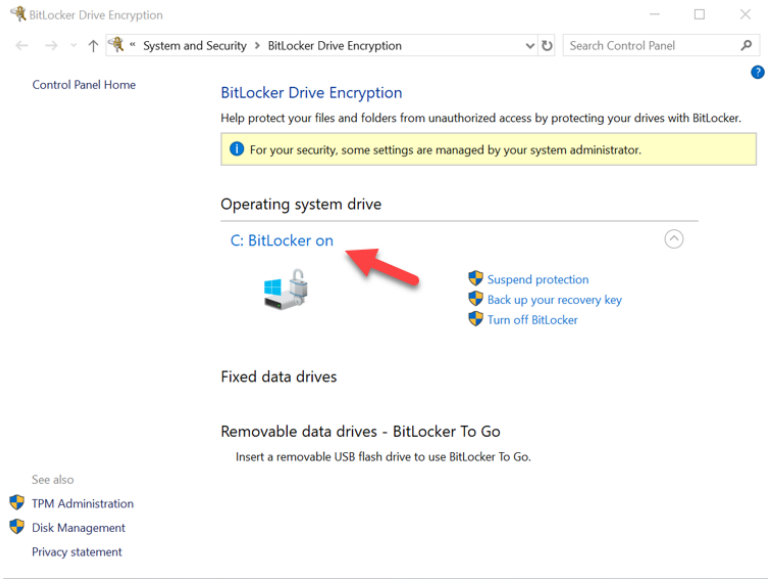
6. プロンプトメッセージに従って続行し、ターゲット SSD を構成します。プロンプトが示されたら、**「Start encrypting」（暗号化を開始する） を選択します。** デフォルトで、**「Run BitLocker system check」**（BitLocker システムチェックを実行） が選択されています。 この設定を有効にして続行するように推奨します。しかしこのチェックを外すと、システムの再起動を必要とせずに、ハードウェア暗号化が有効かどうかを確認できます。



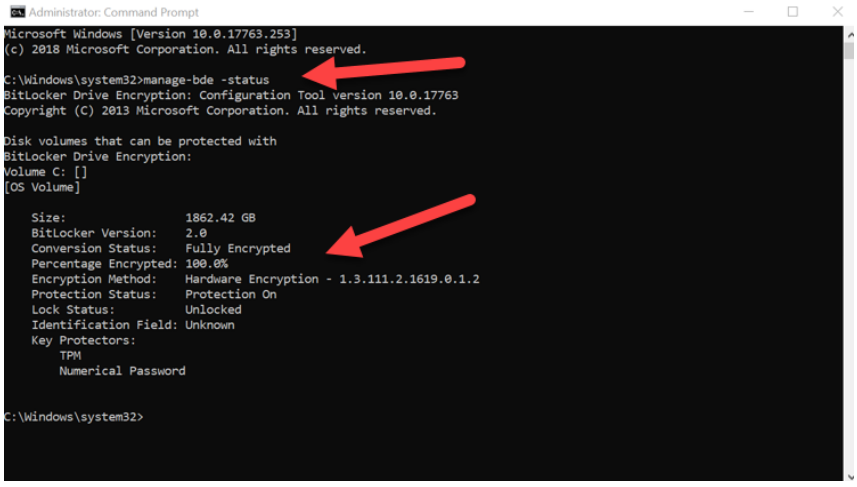
注：「Choose how much of your drive to encrypt」（暗号化するドライブの数を選択してください）という画面が表示されたら、多くの場合、ターゲット SSD がハードウェアの暗号化を有効にせず、代わりにソフトウェア暗号化を使うことを意味します。



7. 必要な場合は、システムを再ブートし、**Manage BitLocker** を再起動して、ターゲット SSD の暗号化の状態を確認してください。



8. また、**cmd.exe** を開いて **manage-bde -status** をキー入力し、ターゲット SSD の暗号化の状態をチェックできます。



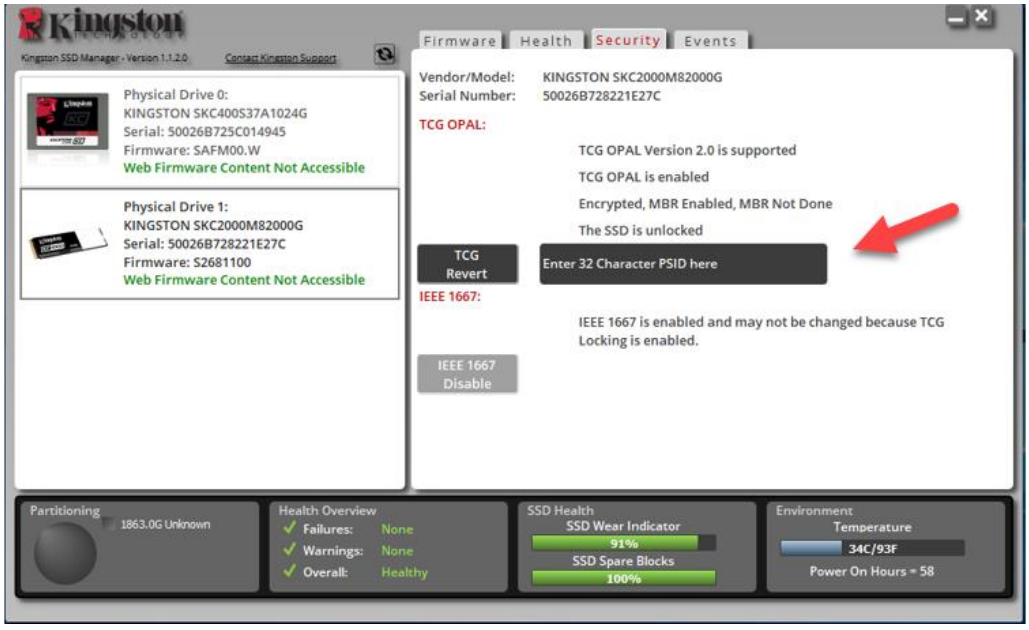
Microsoft eDrive のサポートを無効にする場合
ターゲットの SSD を消去し、ドライブから BitLocker eDrive のサポートを削除するには、以下の各手順に従ってください。

注：このプロセスによりターゲット SSD がリセットされます。また、ドライブに存在するすべてのデータが失われます。

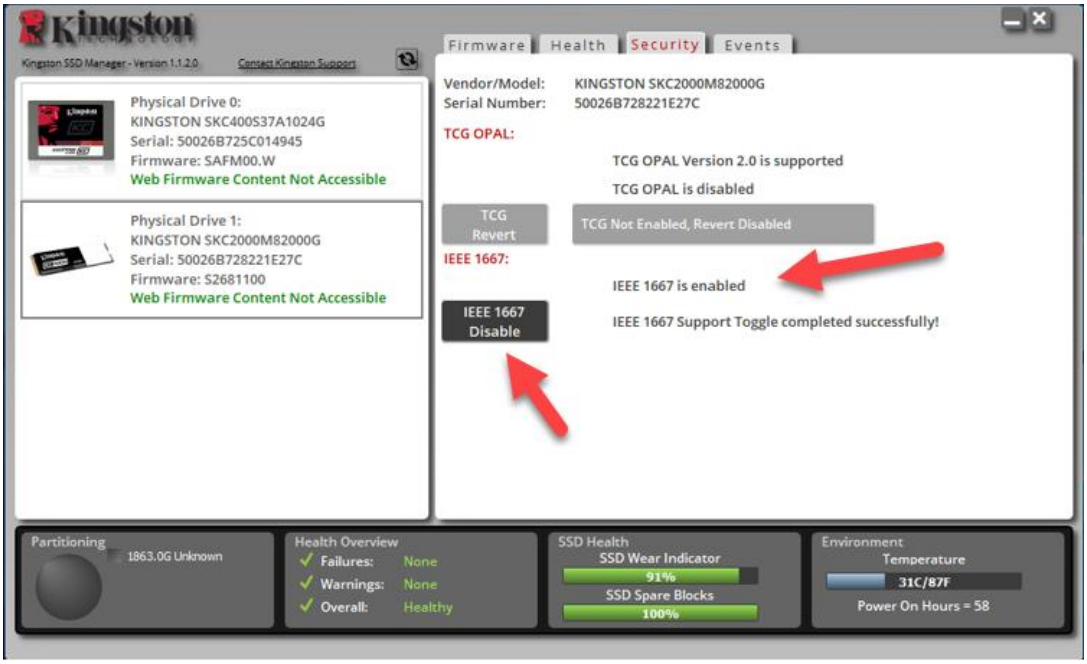
1. ターゲット SSD の PSID 値を、書き留めてください。この値はラベルに印刷されています。

例：KC2000 PSID 値

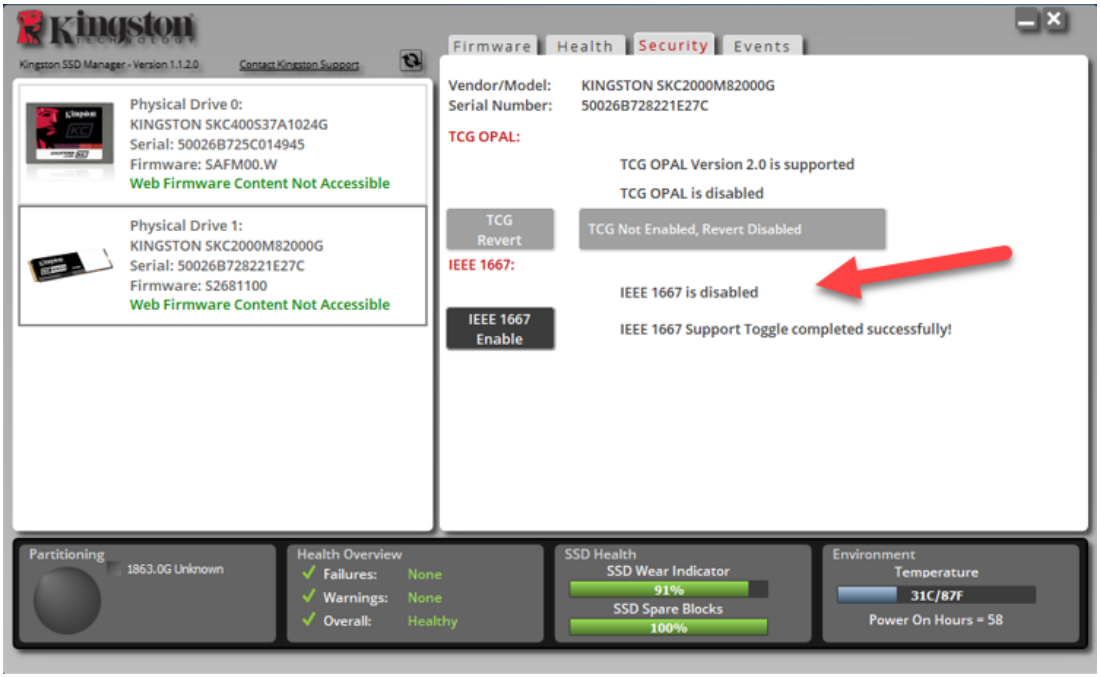
2. ターゲット SSD をセカンダリドライブとしてマウントし、Kingston SSD Manager (KSM) を実行します。
3. **Security** （セキュリティ）タブを選択し、ステップ 1 で取得した 32 ビットの PSID 値を入力して **TCG Revert** を実行します。完了すると、「**TCG Revert completed successfully** 」（TCG Revert が完了しました）のメッセージが表示されます。 このメッセージが表示されない場合は、PSID 値を再入力して、TCG Revert を再試行してください。



4. ドライブが正常に復帰すると、IEEE1667 のサポートを無効にするオプションが表示されます。**IEEE1667 Disable**（IEEE1667 を無効にする）を選択し、「IEEE1667 Support Toggle completed successfully」（IEEE1667 のサポートがトグルされました）のメッセージが表示されるまで待ちます。



5. IEEE1667 のサポートが無効になっているか確認します。



6. これでターゲット SSD は再使用の準備ができました。