SSDs Kingston Criptografados

Ativando e Desativando o BitLocker com o eDrive para utilizar a Criptografia de Hardware

Introdução

Este documento descreve como ativar e desativar o recurso eDrive BitLocker da Microsoft para aproveitar a criptografia de hardware em seu SSD Kingston. Este procedimento se aplica a SSDs Kingston compatíveis com o conjunto de recursos TCG OPAL 2.0 e IEEE1667. Se você não possui um SSD Kingston com suporte a TCG OPAL 2.0 e IEEE1667, este processo não funcionará. Se estiver em dúvida, entre em contato com o suporte técnico da Kingston em www.kingston.com/support

Este documento irá se referir ao BitLocker da Microsoft com eDrive como eDrive no restante da explicação passo a passo. Os procedimentos descritos abaixo podem mudar dependendo da versão e atualizações do Windows.

Requisitos do Sistema

-SSD Kingston utilizando o conjunto de recursos de segurança TCG Opal 2.0 e IEEE1667
-Software de Gerenciamento de SSD Kingston https://www.kingston.com/ssdmanager
-Hardware e BIOS do sistema com suporte aos recursos de segurança TCG Opal 2.0 e IEEE1667

Requisitos de Sistema Operacional / BIOS

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

Observação: Todas as unidades de estado sólido criptografas devem acompanhar controladores não RAID para funcionarem adequadamente no Windows 8, 10 e/ou Server 2012

Para usar uma Unidade de Estado Sólido Criptografada no Windows 8, 10 ou Windows Server 2012 como **drives de dados**:

- O drive não deve ter sido inicializado.
- O drive deve estar em estado de segurança inativo.

Para Unidades de Estado Sólido Criptografadas usadas como **unidades de inicialização**:

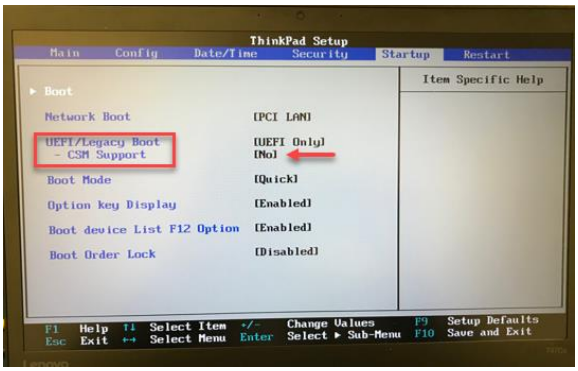
- O drive não deve ter sido inicializado.
- O drive deve estar em estado de segurança inativo.
- O computador deve ser baseado em UEFI 2.3.1 e ter o EFI_STORAGE_SECURITY_COMMAND_PROTOCOL definido. (Este protocolo é usado para permitir a execução dos programas no ambiente de EFI boot services para enviar comandos de protocolo de segurança ao drive).
- O computador deve ter o Módulo de Suporte de Compatibilidade (Compatibility Support Module - CSM) desabilitado no UEFI.
- O computador deve sempre ser inicializado do UEFI nativo.

Para mais informações, consulte o artigo da Microsoft sobre este tópico aqui:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)

Habilitar o eDrive Microsoft em SSD de Inicialização

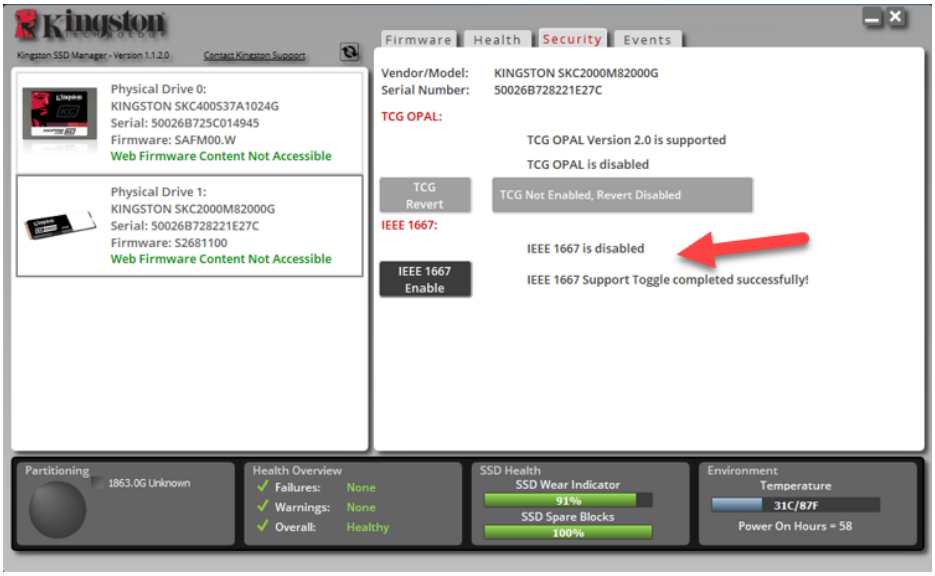
Configuração do BIOS

1. Consulte a documentação do fabricante do seu sistema para confirmar se o BIOS do seu sistema é baseado em UEFI 2.3.1 e possui o EFI_STORAGE_SECURITY_COMMAND_PROTOCOL definido.
2. Entre no BIOS e desative o Módulo de Suporte à Compatibilidade (CSM)

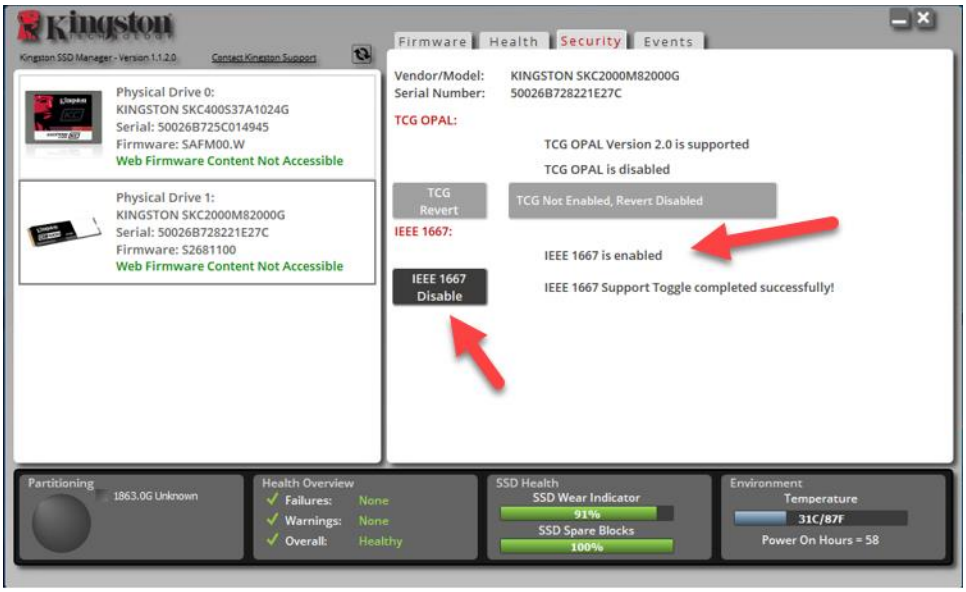


Preparação do Drive

1. Se você ainda não fez o download do SSD Manager da Kingston (KSM), faça-o agora. https://www.kingston.com/ssdmanager
2. Execute um Secure Erase (Apagamento Seguro) do SSD alvo utilizando o software KSM ou outro método padrão do setor.
3. Monte o SSD alvo como um disco secundário para confirmar o status IEEE1667. O drive deve estar no modo **Desativado**.



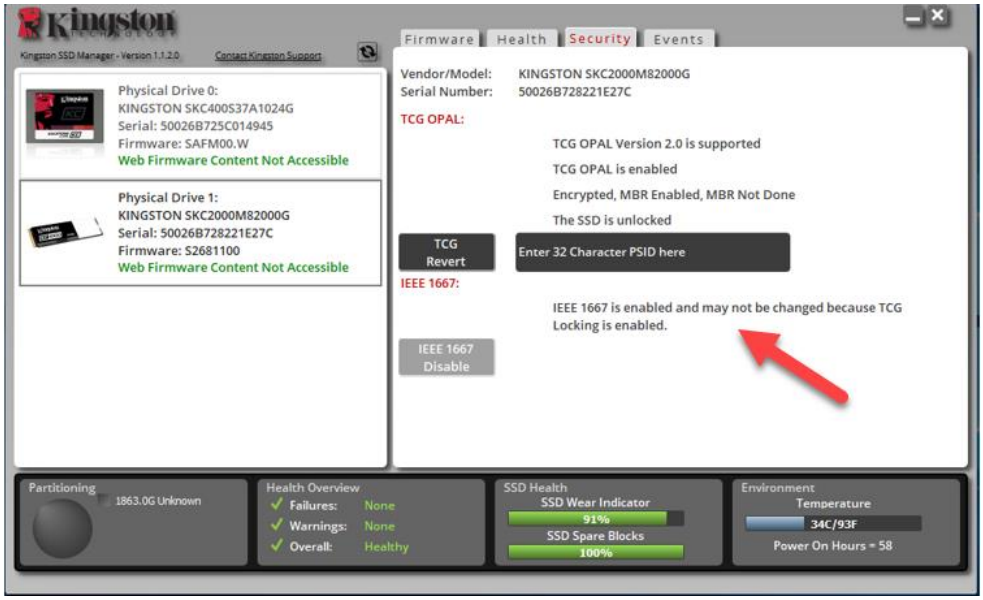
4. Selecione o botão IEEE1667 e **Ative** o recurso. Confirme se o recurso foi alternado com sucesso.



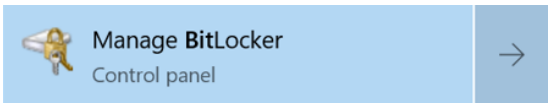
Instalação no sistema operacional (SO)

Observação: Não clone um sistema operacional em seu SSD alvo*. Clonar um sistema operacional no SSD alvo irá impedir que você ative a Criptografia de Hardware usando o eDrive. Você deve instalar um novo sistema operacional no SSD alvo para aproveitar a Criptografia de Hardware com o eDrive.*

1. Instale um sistema operacional compatível no SSD alvo.
2. Após a instalação do sistema operacional, instale o gerenciador de SSD Kingston (KSM), execute o KSM e confirme que a seguinte mensagem esteja presente na guia Segurança do aplicativo:
   "IEEE 1667 está ativado e não pode ser alterado porque o TCG Locking está ativado."

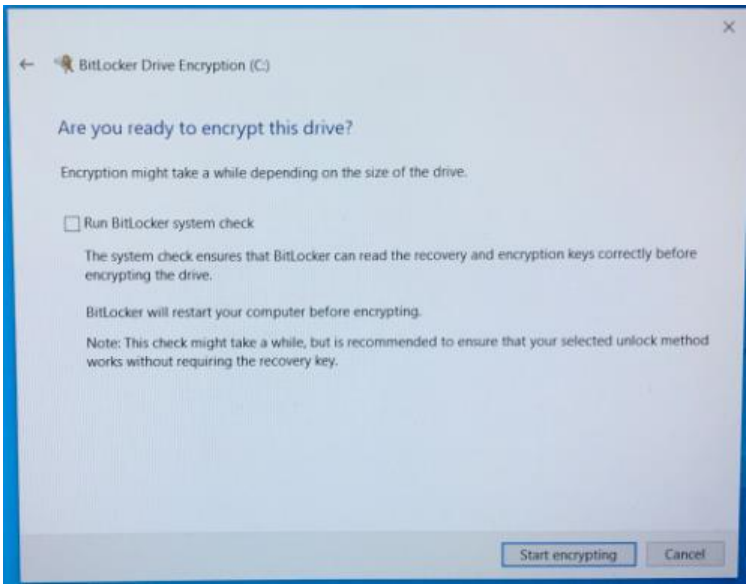


3. Use a Tecla Windows para buscar **Manage BitLocker** e então execute o aplicativo.

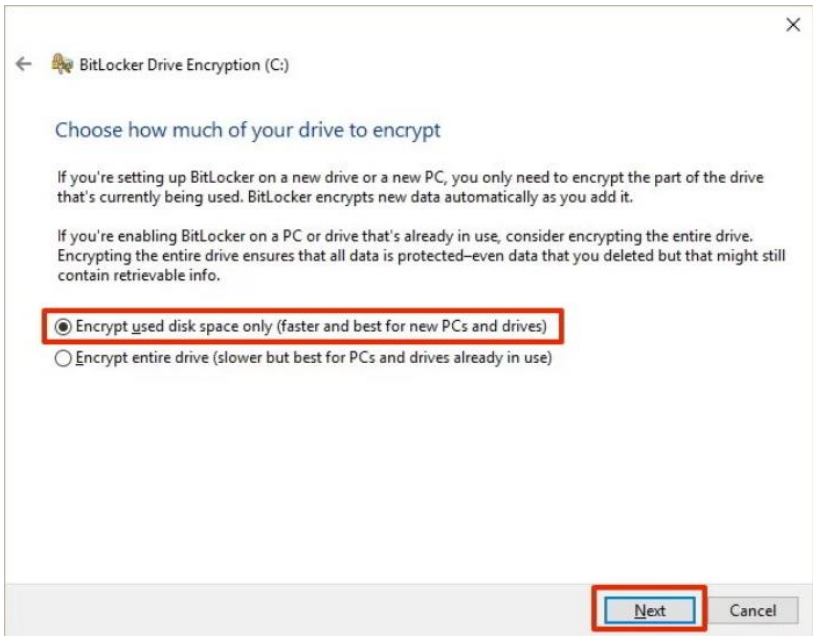


4. Selecione **Ligar BitLocker** na janela do Explorer.

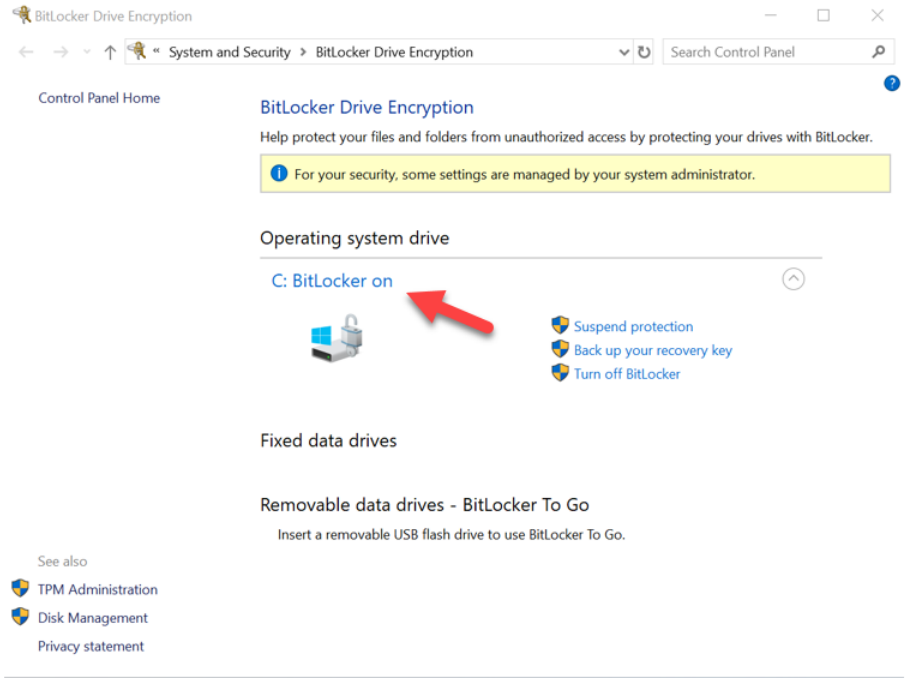
5. Continue seguindo os prompts para configurar o SSD alvo. Quando solicitado, selecione **Iniciar criptografia.** Por padrão, **Executar verificação do sistema BitLocker**está selecionado. É aconselhável prosseguir com essa configuração ativada. Entretanto, quando estiver desmarcada, você poderá confirmar se a criptografia de hardware está ativada sem precisar reinicializar o sistema.



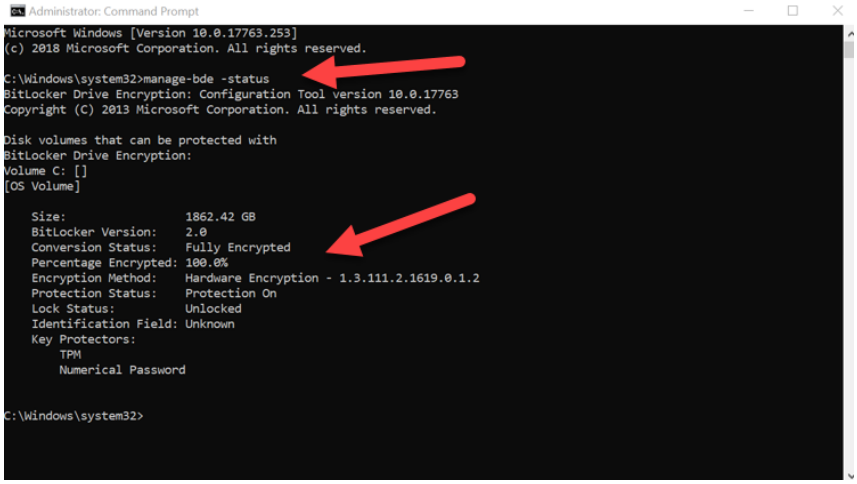
Observação: Se aparecer uma tela que solicite a você "Escolher o quanto criptografar de seu drive", frequentemente significa que o SSD alvo NÃO irá habilitar a criptografia de hardware, mas, em vez disso, utilizar a criptografia de software.



6. Se necessário, reinicialize o sistema e depois abra novamente **Gerenciar BitLocker** para confirmar o status da criptografia do SSD alvo.



7. Você também pode verificar o status da criptografia do SSD alvo abrindo **cmd.exe** e digitando: **manage-bde -status**

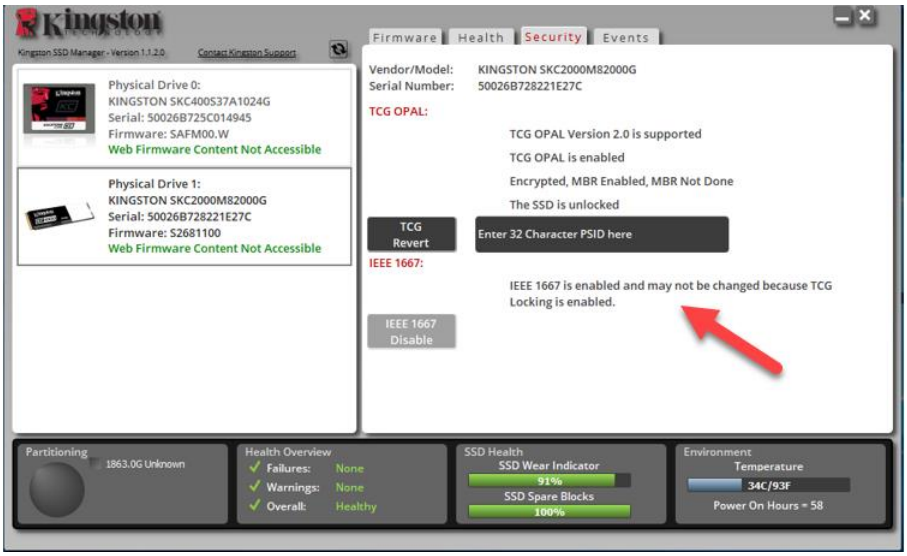


Ativar o eDrive Microsoft com Windows 10 (versão 1903+)

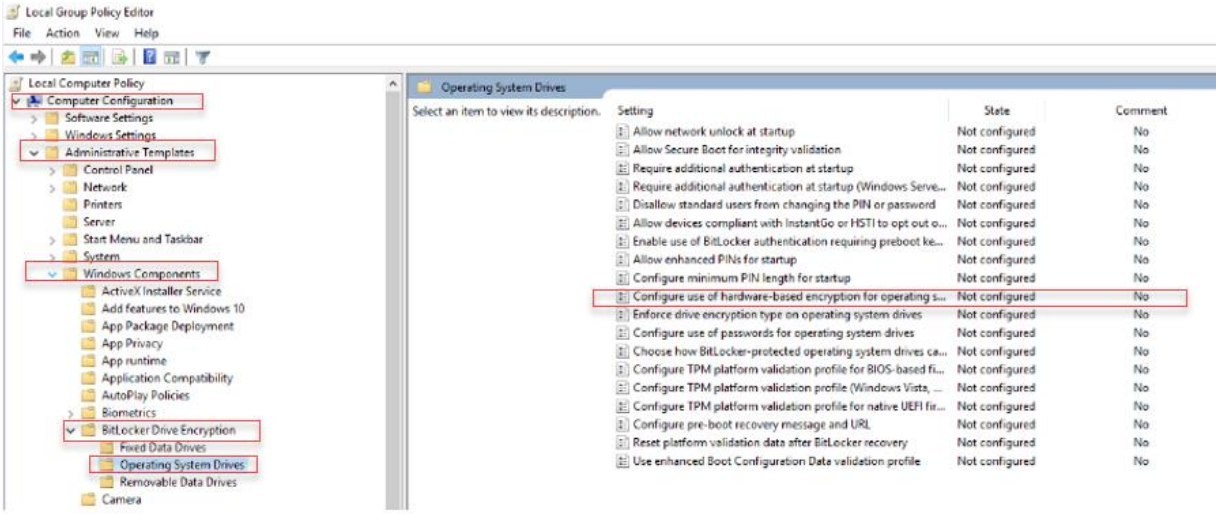
A Microsoft mudou o comportamento padrão do Windows relativo à criptografia eDrive quando lançou o Windows 10 versão 1903. Para ativar o eDrive neste modelo, e possivelmente em modelos posteriores, você precisará executar ***gpedit*** *para habilitar a Criptografia de hardware.*

Observação: Não clone um sistema operacional em seu SSD alvo*. Clonar um sistema operacional no SSD alvo irá impedir que você ative a Criptografia de Hardware usando o eDrive. Você deve instalar um novo sistema operacional no SSD alvo para aproveitar a Criptografia de Hardware com o eDrive.*

1. Instale um sistema operacional compatível no SSD alvo.
2. Após a instalação do sistema operacional, instale o gerenciador de SSD Kingston (KSM), execute o KSM e confirme que a seguinte mensagem esteja presente na guia Segurança do aplicativo: *"IEEE 1667 está ativado e não pode ser alterado porque o TCG Locking está ativado."*

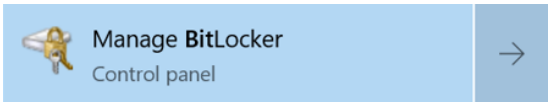


3. Execute gpedit.msc para modificar a configuração da criptografia.
    a. Vá para **Modelos Administrativos> Componentes do Windows> Criptografia BitLocker Drive> Drives do Sistema Operacional**
    b. Em seguida, selecione **Configurar o uso de criptografia com base em hardware para sistemas operacionais**
    c. **Ativar** o recurso e depois **Aplicar** a configuração.



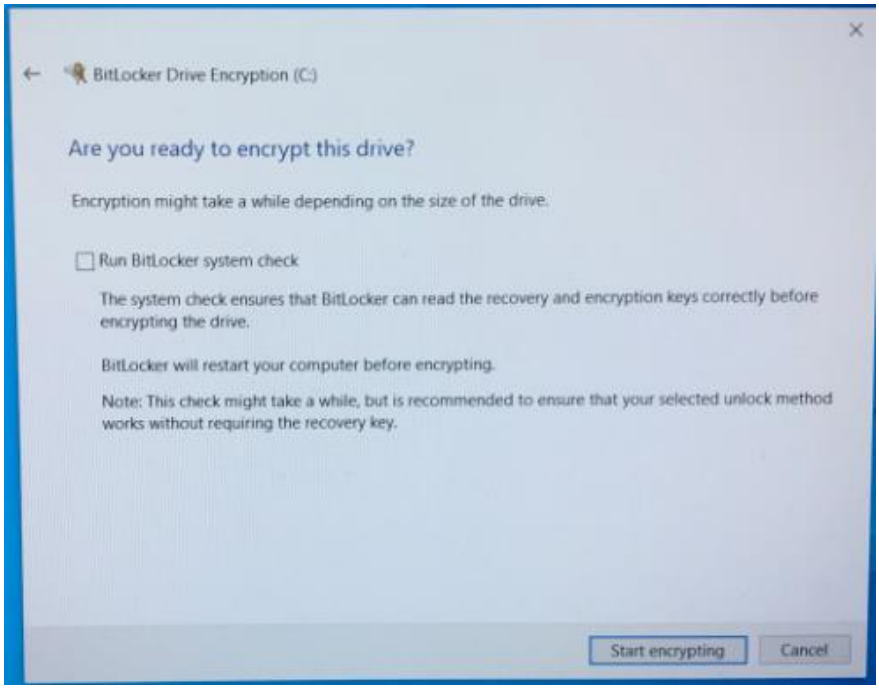
Observação: Para ativar o eDrive em outros drives que não sejam o drive do Sistema Operacional, você pode aplicar as mesmas configurações selecionando: **Modelos Administrativos> Componentes do Windows> Criptografia BitLocker Drive> Drives de Dados Fixos> Configurar o uso de criptografia com base em hardware para drives de dados fixos (Ativar e Aplicar)**

4. Use a Tecla Windows para buscar **Manage BitLocker e então execute o aplicativo.**

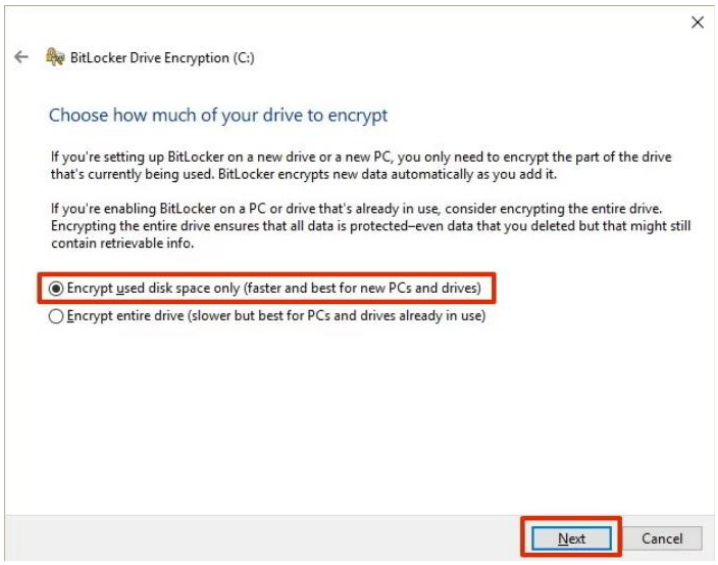


5. Selecione **Ligar BitLocker na janela do Explorer.**

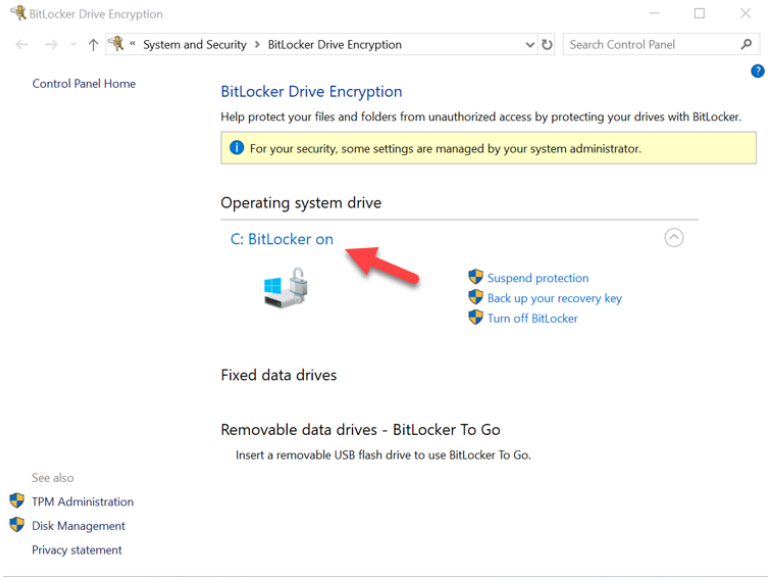
6. Continue seguindo os prompts para configurar o SSD alvo. Quando solicitado, selecione **Iniciar criptografia.** Por padrão, **Executar verificação do sistema BitLocker**está selecionado. É aconselhável prosseguir com essa configuração ativada. Entretanto, quando estiver desmarcada, você poderá confirmar se a criptografia de hardware está ativada sem precisar reinicializar o sistema.



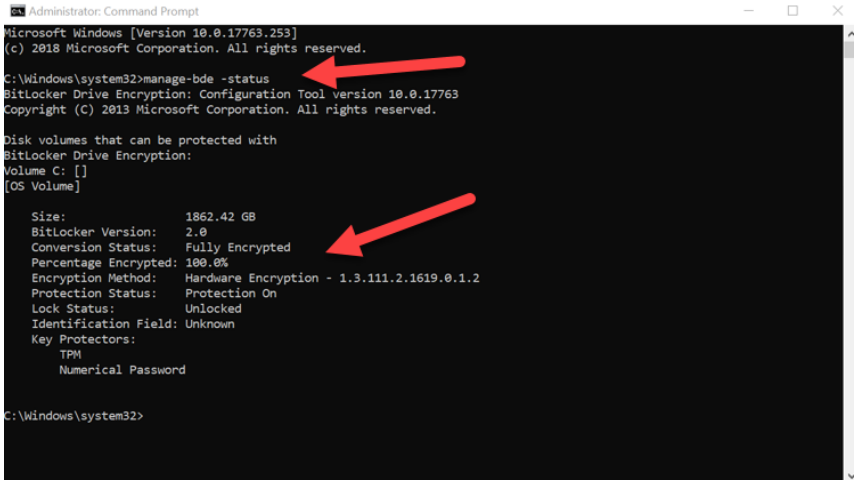
Observação: Se aparecer uma tela que solicite a você "Escolher o quanto criptografar de seu drive", frequentemente significa que o SSD alvo NÃO irá habilitar a criptografia de hardware, mas, em vez disso, utilizar a criptografia de software.



7. Se necessário, reinicialize o sistema e depois abra novamente **Gerenciar BitLocker para confirmar o status da criptografia do SSD alvo.**



8. Você também pode verificar o status da criptografia do SSD alvo abrindo **cmd.exe** e digitando: **manage-bde -status**



Para Desativar o Suporte do eDrive Microsoft

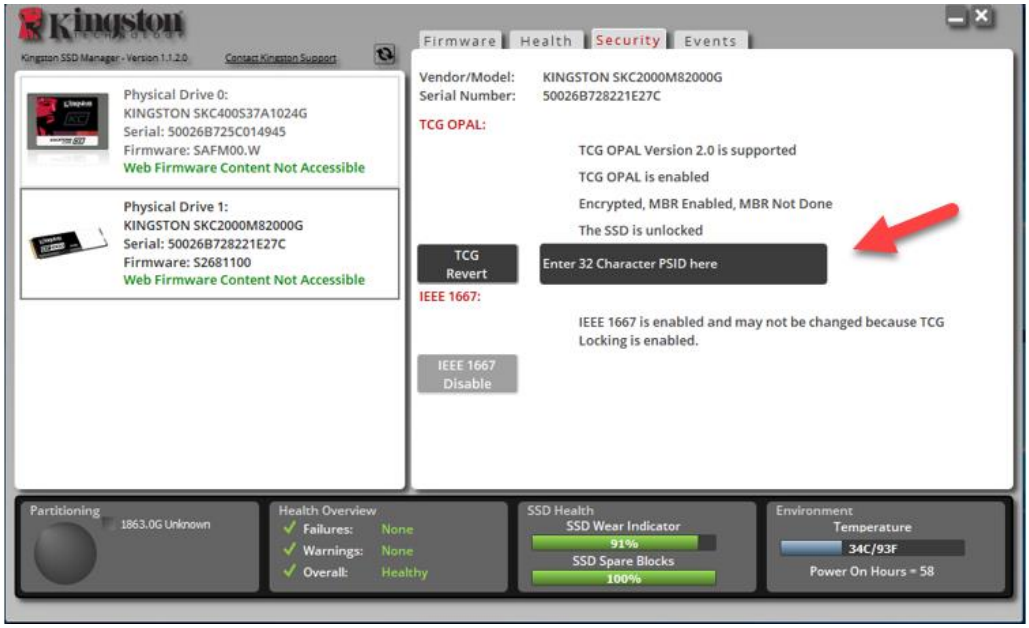
Para apagar os dados dos seus SSDs alvo e remover o suporte ao eDrive Microsoft do drive, siga os passos a seguir.

Observação: Este processo irá redefinir seu SSD Alvo e TODOS OS DADOS PRESENTES NO DRIVE SERÃO PERDIDOS.

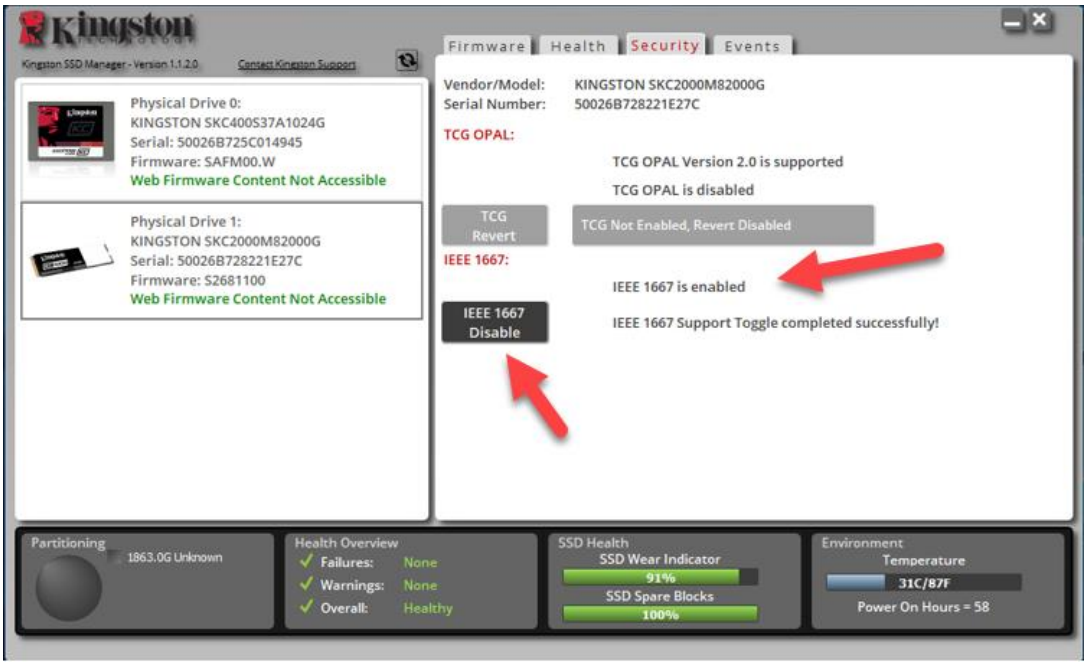
1. Anote o valor PSID do SSD alvo. Isso será impresso na etiqueta.

Ex: Valor PSID do KC2000

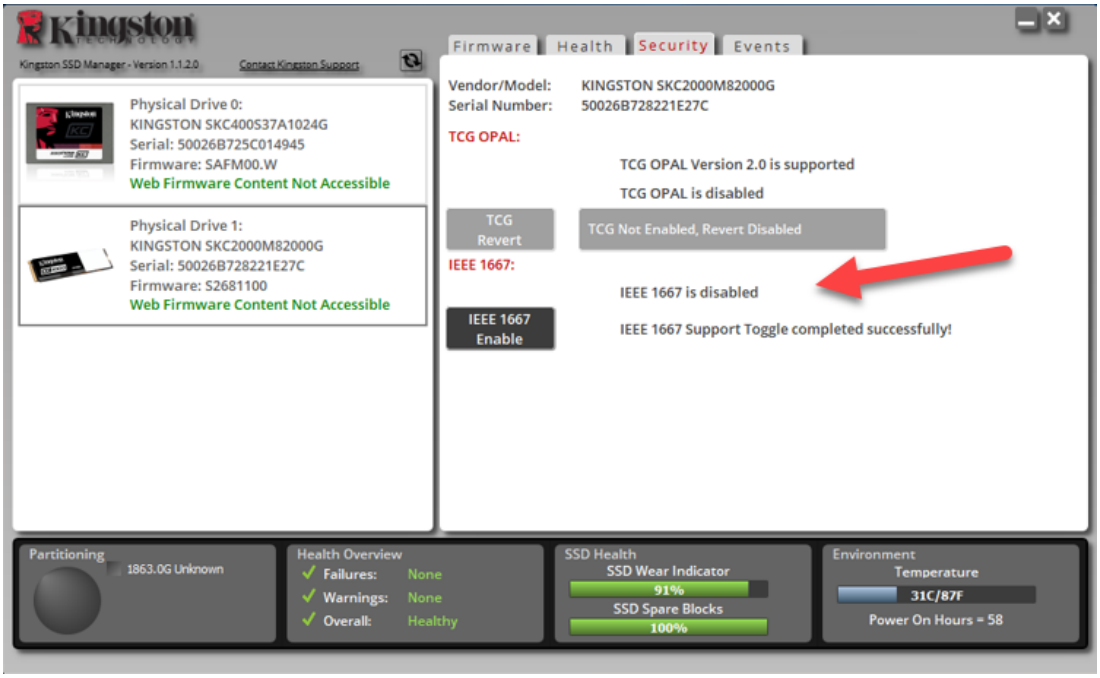
2. Monte o SSD alvo como um drive secundário e execute o Gerenciador de SSD da Kingston (KSM).
3. Selecione a guia **Segurança** e execute um **TCG Revert** inserindo o valor PSID de 32 dígitos do passo 1 e selecionando **TCG Revert.** Quando concluído, você verá a mensagem **TCG Revert concluído com sucesso**. Se esta mensagem não aparecer, insira novamente seu valor PSID e tente reverter novamente.



4. Quando a reversão do drive tiver sido bem-sucedida, você terá a opção de desativar o suporte IEEE1667. Selecione **IEEE1667 Desativar** e aguarde a mensagem “Alternar suporte de IEEE1667 concluído com sucesso”.



5. Confirme que o suporte IEEE1667 está desativado.



6. Seu SSD alvo está pronto para ser usado novamente.