

Твердотельные накопители SSD Kingston с шифрованием Включение и отключение технологии BitLocker с eDrive для использования аппаратного шифрования



Введение

В данном документе описывается, как включать и отключать функцию BitLocker eDrive, разработанную компанией Microsoft, для оптимального применения аппаратного шифрования на твердотельном накопителе SSD Kingston. Данная процедура применяется к твердотельным накопителям SSD Kingston, поддерживающим группу функций TCG OPAL 2.0 и IEEE1667. Если у вас нет твердотельного накопителя SSD Kingston с поддержкой функций TCG OPAL 2.0 и IEEE1667, этот процесс не будет работать. Если вы не уверены, обратитесь в Службу технической поддержки Kingston по адресу www.kingston.com/support.

Разработанная компанией Microsoft технология шифрования BitLocker с eDrive в данном документе будет именоваться как 'eDrive' на продолжении остальной части этого пошагового описания. Описанные ниже процедуры могут различаться в зависимости от версии (-ий) и обновлений Windows.

Системные требования

-Твердотельный накопитель SSD Kingston с поддержкой группы функций по обеспечению безопасности TCG Opal 2.0 и IEEE1667

-Программное обеспечение по управлению функционалом твердотельного накопителя Kingston SSD Manager <u>https://www.kingston.com/ssdmanager</u>

-Системное аппаратное оборудование и BIOS с поддержкой функций по обеспечению безопасности TCG Opal 2.0 и IEEE1667

Требования к OC/BIOS

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

Примечание. Все зашифрованные твердотельные накопители должны быть подключены к контроллерам, не являющимися контроллерами массивов RAID, для обеспечения правильности их работы в среде Windows 8, 10 и/или Server 2012.

Для использования зашифрованного твердотельного накопителя в среде Windows 8, 10 или Windows Server 2012 в качестве **диска данных**:

- Диск должен находиться в неинициализированном состоянии.
- Диск должен находиться в неактивном состоянии относительно обеспечения безопасности.

Для использования зашифрованного твердотельного накопителя в качествезагрузочного диска:

- Диск должен находиться в неинициализированном состоянии.
- Диск должен находиться в неактивном состоянии относительно обеспечения безопасности.
- Компьютер должен быть оснащен интерфейсом UEFI 2.3.1 и иметь определение протокола команд безопасности EFI_STORAGE_SECURITY_COMMAND_PROTOCOL. (Этот протокол используется для того, чтобы программы, запущенные в среде загрузочных служб EFI, могли отправлять на диск команды протокола безопасности).
- На компьютере в интерфейсе UEFI модуль поддержки совместимости (CSM) должен быть отключен.
- Самозагрузка компьютера должна всегда по умолчанию выполняться из UEFI.

Для получения дополнительной информации обратитесь к статье Microsoft по этой теме, размещенной здесь: <u>https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831627(v=ws.11)</u>



1

Включение функции Microsoft eDrive на загрузочном твердотельном диске SSD

Конфигурация BIOS

- 1. Обратитесь к документации производителя вашей системы для подтверждения того, что BIOS вашей системы основан на интерфейсе UEFI 2.3.1 и имеет определение протокола команд безопасности EFI_STORAGE_SECURITY_COMMAND_PROTOCOL.
- 2. Войдите в BIOS и отключите модуль поддержки совместимости (CSM).



Подготовка диска

- 1. Если вы еще не загрузили приложение SSD Manager компании Kingston (KSM), сделайте это сейчас. https://www.kingston.com/ssdmanager
- 2. Выполните безопасное стирание целевого твердотельного накопителя SSD с помощью программного обеспечения KSM или другого метода, принятого в качестве отраслевого стандарта.
- 3. Смонтируйте целевой твердотельный накопитель SSD в качестве вторичного диска для подтверждения статуса IEEE1667. Диск должен находиться в режиме **Disabled** (Отключен).



4. Выберите кнопку «IEEE1667» и выполните для этой функции команду **Enable** (Включить). Убедитесь, что состояния функции успешно переключаются.

Kingson SSD Manager-Version 1.120 Contact Kingston Support	Firmware Health Security Events	
Physical Drive 0: KINGSTON SKC400537A1024G Serial: 500268725C014945 Firmware: SAFMOO.W 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	
Physical Drive 1: KINGSTON SKC2000M82000G Serial: 500268728221E27C Firmware: S2681100 Web Firmware Content Not Accessible	TCG Revert IEEE 1667: IEEE 1667 is enabled IEEE 1667 Disable IEEE 1667 Support Toggle completed successfully!	
Partitioning 1863.0G Unknown ✓ Failures: Non- ✓ Warnings: Non- ✓ Overall: Heal	SSD Health SSD Wear Indicator 91% SSD Spare Blocks 100% Power On Hours = 58	

Установка операционной системы (ОС)

Примечание. Не выполняйте клонирование операционной системы на целевой твердотельный накопитель SSD. Клонирование ОС на целевой накопитель SSD не позволит вам активировать технологию аппаратного шифрования с использованием eDrive. Чтобы воспользоваться преимуществами аппаратного шифрования с использованием eDrive, необходимо заново установить ОС на целевой твердотельный накопитель SSD.

- 1. Установите поддерживаемую ОС на целевой твердотельный накопитель SSD.
- 2. После установки ОС установите приложение Kingston SSD Manager (KSM), запустите KSM и убедитесь, что на вкладке Security (Безопасность) в приложении имеется следующее сообщение: «IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.» (IEEE 1667 активирован и не может быть изменен, поскольку включена блокировка TCG.)





3. Используйте клавишу Windows для поиска приложения **Manage BitLocker**, а затем запустите данное приложение.



4. В окне Проводника выберите функцию Turn on BitLocker (Включить BitLocker).

RitLocker Drive Encryption				-		\times
🔶 🚽 🕆 🕆 👫 * System	and Security > BitLocker Drive Encryption	~ D	Search Contro	ol Panel		p
Control Panel Home	BitLocker Drive Encryption					-
	Help protect your files and folders from unaut	horized access by p	protecting your d	lrives wit	th BitLoc	ker.
	Operating system drive					
	C: BitLocker off			C		
		🗣 Turn an BitLo	cker			
	Fixed data drives					
	Removable data drives - BitLocker	To Go				
	Insert a removable USB flash drive to use Bi	tLocker To Go.				

5. Следуйте указаниям в запросах на ввод для настройки целевого твердотельного накопителя SSD. При появлении соответствующего сообщения с запросом на ввод выберите операцию Start encrypting (Начать шифрование). По умолчанию выбрана функция Run BitLocker system check (Запуск проверки системы посредством BitLocker). Рекомендуется продолжать работу, когда эта настраиваемая функция остается включенной. Однако, если этот флажок снят, вы сможете проверить, включено ли аппаратное шифрование, без необходимости перезагрузки системы.



Примечание. Если появится экран с запросом «Choose how much of your drive to encrypt» (Выберите, сколько объема диска нужно зашифровать), это зачастую означает, что целевой твердотельный накопитель SSD НЕ будет активировать технологию аппаратного шифрования, а вместо него будет использовать программное шифрование.



6. При необходимости перезагрузите систему, а затем перезапустите приложение **Manage BitLocker**, чтобы подтвердить состояние шифрования целевого накопителя SSD.



7. Вы также можете проверить состояние шифрования целевого накопителя SSD, открыв **cmd.exe** и введя: **manage-bde -status**

🔤 Administrator: Command Pro	mpt	_	\times
Microsoft Windows [Versic (c) 2018 Microsoft Corpor	n 10.0.17763.253] ation. All rights reserved.		î
C:\Windows\system32>manag BitLocker Drive Encryptic Copyright (C) 2013 Micros	e-bde -status n: Configuration Tool version 10.0.17763 oft Corporation. All rights reserved.		
Disk volumes that can be BitLocker Drive Encryptic Volume C: [] [OS Volume]	protected with n:		
Size: BitLocker Version: Conversion Status: Percentage Encrypted: Encryption Method: Protection Status: Lock Status: Identification Field: Key Protectors: TPM Numerical Passwor	1862.42 GB 2.0 Fully Encrypted 180.8% Hardware Encryption - 1.3.111.2.1619.0.1.2 Protection On Unlocked Unknown		
C:\Windows\system32>			

Включение функции Microsoft eDrive в ОС Windows 10 (версия 1903+)

Компания Microsoft изменила задаваемый по умолчанию характер работы Windows 10 в отношении шифрования с eDrive, когда выпустила Windows 10 версии 1903. Чтобы включить функцию eDrive в этой сборке, а возможно и в последующих сборках, вам нужно будет запустить редактор локальных групповых политик **gpedit**, чтобы включить технологию аппаратного шифрования.

Примечание. Не выполняйте клонирование операционной системы на целевой твердотельный накопитель SSD. Клонирование OC на целевой накопитель SSD не позволит вам активировать технологию аппаратного шифрования с использованием eDrive. Чтобы воспользоваться преимуществами аппаратного шифрования с использованием eDrive, необходимо заново установить OC на целевой твердотельный накопитель SSD.

- 1. Установите поддерживаемую ОС на целевой твердотельный накопитель SSD.
- После установки ОС установите приложение Kingston SSD Manager (KSM), запустите KSM и убедитесь, что на вкладке Security (Безопасность) в приложении имеется следующее сообщение: «IEEE 1667 is enabled an may not be changed because TCG Locking is enabled.» (IEEE 1667 активирован и не может быть изменен, поскольку включена блокировка TCG.)

Compared Statement 1:20 Control Statement Statement Control Statement Statement Control Statement Statement Control Statement Statement Control Stateme	Firmware Health Security Events Vendor/Model: KINGSTON SKC2000M82000G Serial Number: 500268728221E27C TCG OPAL: TCG OPAL is enabled TCG OPAL: TCG OPAL is enabled Encrypted, MBR Enabled, MBR Not Done The SSD is unlocked TCG Enter 32 Character PSID here IEEE 1667: IEEE 1667 is enabled. IEEE 1667 Locking is enabled.
Partitioning 1863.05 Urknown ✓ Failures: Non- ✓ Warnings: Non- ✓ Overall: Heal	s SSD Health SSD Wear Indicator 91% SSD Spare Blocks thy 100% Power On Hours = 58

- 3. Запустите gpedit.msc, чтобы изменить данную настройку шифрования.
 - перейдите в Administrative Templates> Windows Components> BitLocker Drive Encryption> Operating System Drives (Административные шаблоны> Компоненты Windows> Шифрование диска посредством BitLocker> Диски операционной системы)
 - b. Затем выберите Configure use of hardware-based encryption for operating systems (Настроить использование аппаратного шифрования для операционных систем).
 - с. Включите эту функцию, а затем выполните команду Apply (Применить) для данной настройки.



Примечание. Чтобы включить функцию eDrive на дисках, отличных от диска операционной системы, можно применить те же самые настройки, выбрав параметр: Administrative Templates> Windows Components> BitLocker Drive Encryption> Fixed Data Drives> Configure use of hardware-based encryption for fixed data drives (Административный шаблоны> Компоненты Windows> Шифрование диска посредством BitLocker> Фиксированные диски данных> Настроить использование аппаратного шифрования для фиксированных дисков данных) (Enable (Включить), и затем Apply (Применить))

4. Используйте клавишу Windows для поиска приложения **Manage BitLocker**, а затем запустите данное приложение.



5. В окне Проводника выберите функцию Turn on BitLocker (Включить BitLocker).

Control Panel Home	Ritlaskar Drive Formation			
	BILLOCKEF UNVE Encryption Help protect your files and folders from unauthorized access by protecting your drives with BitLock			
	Operating system drive			
	C: BitLocker off		0	
	S Tur	n on BitLocker		
	Fixed data drives			
	Removable data drives - BitLocker To Go			
	leaved a segmentable USP flack down to use Bittenber T	- E -		

6. Следуйте указаниям в запросах на ввод для настройки целевого твердотельного накопителя SSD. При появлении соответствующего сообщения с запросом на ввод выберите операцию Start encrypting (Начать шифрование). По умолчанию выбрана функция Run BitLocker system check (Запуск проверки системы посредством BitLocker). Рекомендуется продолжать работу, когда эта настраиваемая функция остается включенной. Однако, если этот флажок снят, вы сможете проверить, включено ли аппаратное шифрование, без необходимости перезагрузки системы.



Примечание. Если появится экран с запросом «Choose how much of your drive to encrypt» (Выберите, сколько объема диска нужно зашифровать), это зачастую означает, что целевой твердотельный накопитель SSD НЕ будет активировать технологию аппаратного шифрования, а вместо него будет использовать программное шифрование.

	×
-	RitLocker 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)
	O Encrypt entire drive (slower but best for PCs and drives already in use)
	<u>N</u> ext Cancel



7. При необходимости перезагрузите систему, а затем перезапустите приложение **Manage BitLocker**, чтобы подтвердить состояние шифрования целевого накопителя SSD.



8. Вы также можете проверить состояние шифрования целевого накопителя SSD, открыв **cmd.exe** и введя: **manage-bde -status**



Отключение функции поддержки Microsoft eDrive

Чтобы стереть данные с целевых твердотельных накопителей SSD и удалить с них функцию поддержки BitLocker eDrive, выполните следующие действия.

Примечание. При выполнении этого процесса происходит сброс настроек целевого твердотельного накопителя SSD и BCE ДАННЫЕ, НАХОДЯЩИЕСЯ НА ДИСКЕ, БУДУТ УТЕРЯНЫ.

1. Запишите значение PSID целевого твердотельного накопителя SSD. Оно будет напечатано на этикетке.



Например: KC2000 PSID Value

- 2. Смонтируйте целевой твердотельный накопитель SSD в качестве вторичного диска и запустите приложение Kingston SSD Manager (KSM).
- Выберите вкладку Security (Безопасность) и выполните TCG Revert (Возврат исходных настроек TCG), введя состоящее из 32 цифр значение PSID, полученное на первом этапе, и затем выберите TCG Revert (Возврат исходных настроек TCG). После завершения вы увидите сообщение, что TCG Revert (Возврат исходных настроек TCG) был успешно завершен. Если данное сообщение отсутствует, введите значение PSID повторно и повторите попытку возврата настроек.

Consert Kineston Support Consert Kineston Support Consert Kineston Support Physical Drive 0: KingSTON SKC4000537A1024G Serial: S00268725C014945 Erroware: SAFM00.W Web Firmware Content Not Accessible Physical Drive 1: KINGSTON SKC2000M82000G Serial: S0026872521E27C Erroware: S2681100 Web Firmware Content Not Accessible	Firmware Health Security Events Vendor/Model: KINGSTON SKC2000M82000G Serial Number: 50026B728221E27C TCG OPAL! TCG OPAL Version 2.0 is supported TCG OPAL is enabled Encrypted, MBR Not Done The SSD is unlocked The SSD is unlocked TEEE 1667: Enter 32 Character PSID here IEEE 1667: IEEE 1667 is enabled and may not be changed because TCG Locking is enabled. IEEE 1667 Disable
Partitioning 1863.0G Unknown V Failures: None V Warnings: None V Overall: Healt	SSD Health SSD Wear Indicator 91% SSD Spare Blocks thy 100% SSD Spare Blocks Power On Hours = 58

 После успешного возврата диска в исходное состояние у вас будет возможность отключить функцию поддержки IEEE1667. Выберите IEEE1667 Disable (Отключить IEEE1667) и дождитесь появления сообщения «IEEE1667 Support Toggle completed successfully» (Переключение состояния функции поддержки IEEE1667 выполнено успешно).



5. Подтвердите, что функция поддержки IEEE1667 отключена.



6. Ваш целевой твердотельный накопитель SSD готов к повторному использованию.



©2019 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708. Все права защищены. Все товарные марки и зарегистрированные товарные знаки являются собственностью своих законных владельцев.