

Как зашифровать диск с помощью BitLocker в Windows 10

Шифрование жесткого диска — это один из самых простых и быстрых способов повысить безопасность. В Windows 10 встроена программа шифрования диска. BitLocker - это инструмент полного шифрования диска, доступный для пользователей Windows 10 Pro, Enterprise и Education.

Шифрование диска звучит пугающе. Если вы потеряете свой пароль, ваш диск останется заблокированным навсегда. Тем не менее, безопасность, которую он вам предоставляет, практически не имеет себе равных.

Вот как вы можете зашифровать свой жесткий диск с помощью BitLocker в Windows 10.

Что такое BitLocker?

BitLocker - это инструмент шифрования полного тома, включенный в Windows 10 Pro, Enterprise и Education. Вы можете использовать BitLocker для шифрования тома диска. (Объем диска может означать часть диска, а не весь диск.)

BitLocker предлагает надежное шифрование для обычных пользователей Windows 10. По умолчанию BitLocker использует 128-битное шифрование AES. (также написано как AES-128). Что касается шифрования, это сильно. В настоящее время не существует известного метода грубого форсирования 128-битного ключа шифрования AES. Исследовательская группа разработала одну потенциальную атаку на алгоритм шифрования AES, но взломать ключ потребуются миллионы лет. Вот почему люди называют AES «шифрованием военного уровня».

Таким образом, BitLocker с использованием AES-128 является безопасным. Тем не менее, вы также можете использовать BitLocker с большим 256-битным ключом, что делает его практически невозможным для разблокировки. Сейчас я покажу, как переключить BitLocker на AES-256.

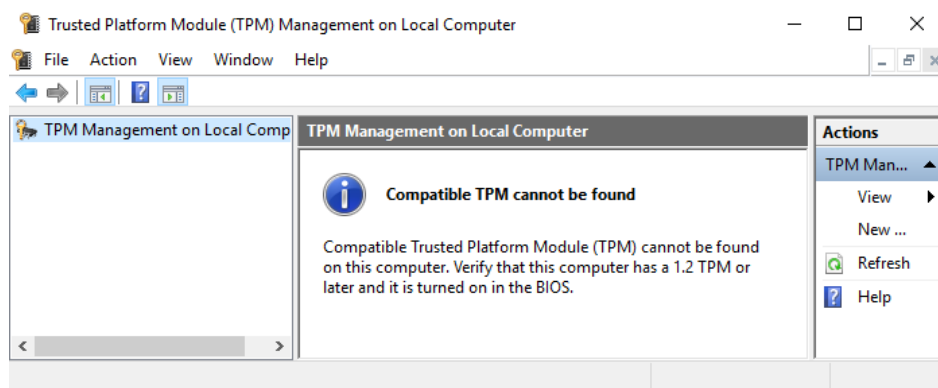
BitLocker имеет три различных метода шифрования:

- Режим аутентификации пользователя. «Стандартный» режим аутентификации пользователя шифрует ваш диск, требуя аутентификацию перед разблокировкой. Аутентификация осуществляется в форме PIN-кода или пароля.
- Прозрачный режим работы. Это немного более продвинутый режим, в котором используется чип доверенного платформенного модуля (TPM). Чип TPM проверяет, что ваши системные файлы не были изменены, так как вы зашифровали диск с помощью BitLocker. Если ваши системные файлы были подделаны, чип TPM не выпустит ключ. В свою очередь, вы не сможете ввести свой пароль для расшифровки диска. Прозрачный режим работы создает дополнительный уровень безопасности над шифрованием вашего диска.
- Режим USB-ключа. В режиме USB Key используется физическое USB-устройство, которое загружается в зашифрованный диск.

Как проверить, есть ли в вашей системе модуль TPM

Не уверены, есть ли в вашей системе модуль TPM? Нажмите Windows Key + R, затем введите *tpm.msc*. Если вы видите информацию о TPM в вашей системе, у вас установлен

модуль TPM. Если вы встречаете сообщение «Не удастся найти совместимый TPM» (как я!), Ваша система не имеет модуля TPM.



Это не проблема, если у вас его нет. Вы все еще можете использовать BitLocker без модуля TPM. Смотрите следующий раздел, чтобы понять, как.

Как проверить, включен ли BitLocker

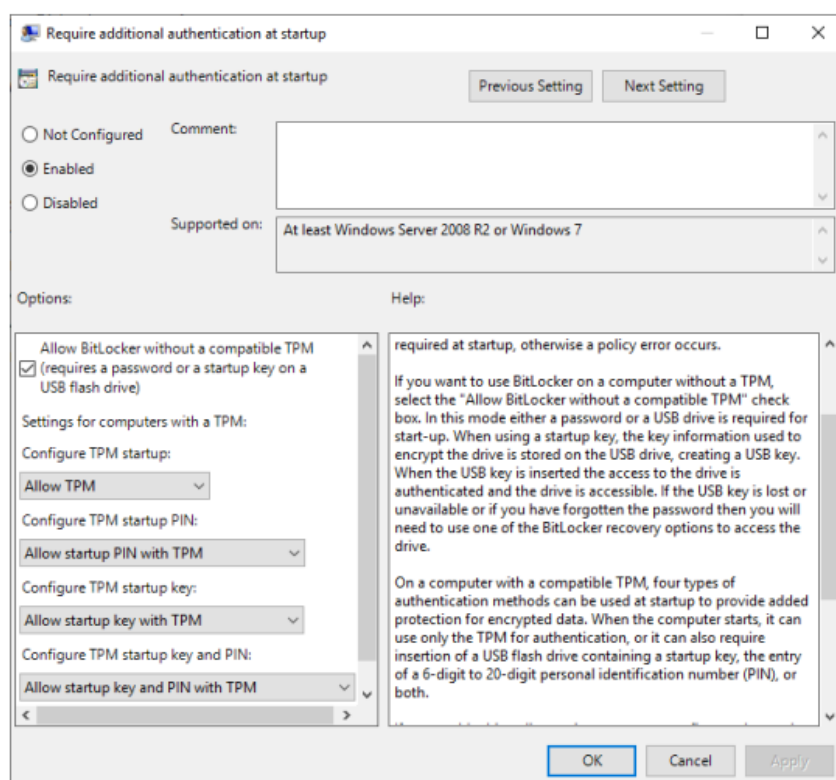
Прежде чем перейти к учебнику по шифрованию диска BitLocker, проверьте, включен ли BitLocker в вашей системе.

Введите gredit в строке поиска в меню «Пуск» и выберите «Лучшее совпадение». Откроется редактор групповой политики.

Перейдите в раздел Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Шифрование диска BitLocker → Диски операционной системы.

Выберите «Требовать дополнительную аутентификацию при запуске», затем «Включено».

Если в вашей системе нет совместимого модуля TPM, установите флажок Разрешить BitLocker без совместимого TPM.



Как использовать шифрование диска BitLocker в Windows 10

Сначала введите bitlocker в строке поиска в меню «Пуск», затем выберите «Лучшее совпадение».

Выберите диск, который нужно шифровать BitLocker, затем выберите «Включить BitLocker».


Теперь вы должны выбрать, как вы хотите разблокировать этот диск. Здесь у вас есть два варианта.



1. Используйте пароль.
2. Используйте смарт-карту.

Выберите первый вариант Использовать пароль, чтобы разблокировать диск.

Выберите пароль BitLocker

Выбор подходящего надежного пароля, который вы также можете запомнить. Как подсказывает мастер BitLocker, ваш пароль должен содержать заглавные и строчные буквы, цифры, пробелы и символы.



  BitLocker Drive Encryption (E:)

Choose how you want to unlock this drive

☐ Use a password to unlock the drive

Passwords should contain upper and lower case letters, numbers, spaces and symbols.

Enter your password

Re-enter your password

☐ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

Next

Cancel

Как только вы создадите подходящий пароль, введите его, а затем введите его еще раз для подтверждения.

Следующая страница содержит параметры для создания ключа восстановления BitLocker. Ключ восстановления BitLocker является уникальным для вашего диска и является

единственным способом безопасного и надежного создания резервной копии. Есть четыре варианта на выбор. Сейчас выберите «Сохранить в файл», затем выберите место для сохранения. После сохранения нажмите «Далее».

На данный момент, вы выбираете, сколько вашего диска для шифрования.

Мастер BitLocker настоятельно рекомендует шифровать весь диск, если вы уже используете его, чтобы обеспечить шифрование всех доступных данных, включая удаленные, но не удаленные с диска. Принимая во внимание, что если вы шифруете новый диск или новый ПК, «вам нужно только зашифровать ту часть диска, которая используется в данный момент», потому что BitLocker будет шифровать новые данные автоматически по мере их добавления.

Наконец, выберите режим шифрования. Windows 10 версии 1511 представила новый режим шифрования диска, известный как XTS-AES. XTS-AES обеспечивает дополнительную поддержку целостности. Тем не менее, он не совместим со старыми версиями Windows. Если диск, который вы шифруете с помощью BitLocker, останется в вашей системе, вы можете спокойно выбрать новый режим шифрования XTS-AES.

Если нет (если вы собираетесь подключить свой диск к отдельной машине), выберите режим совместимости.

Зашифруйте свой диск с помощью BitLocker



Вы попали на последнюю страницу: пришло время зашифровать диск с помощью BitLocker. Выберите Начать шифрование и дождитесь завершения процесса. Процесс шифрования может занять некоторое время, в зависимости от объема данных.

Когда вы перезагружаете свою систему или пытаетесь получить доступ к зашифрованному диску, BitLocker предложит вам ввести пароль диска.

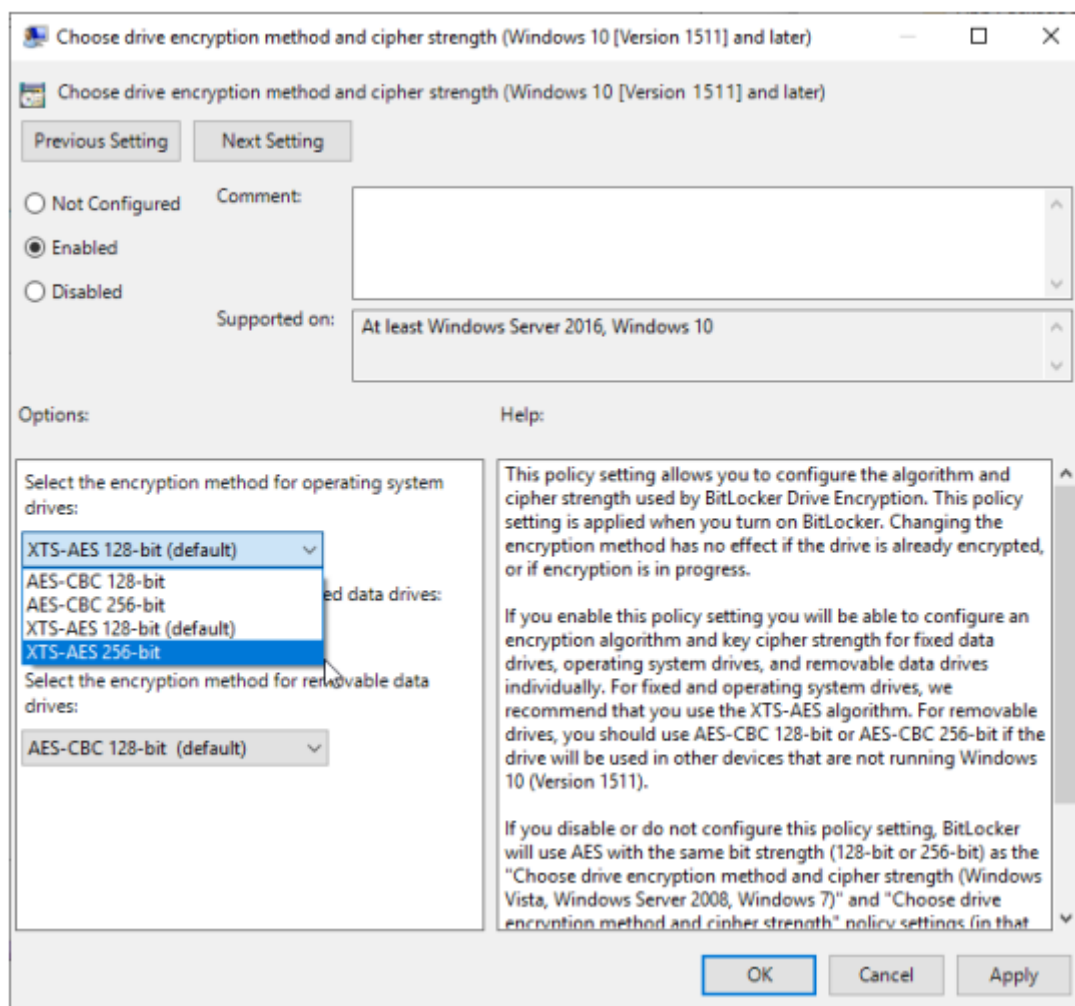
Использование AES-256 с BitLocker

Вы можете заставить BitLocker использовать гораздо более надежное 256-битное шифрование AES вместо 128-битного AES. Несмотря на то, что 128-битное AES-шифрование будет длиться вечно, вы всегда можете сделать это навсегда и день, используя дополнительную силу.

Основной причиной использования AES-256 вместо AES-128 является защита от роста квантовых вычислений в будущем. Квантовые вычисления смогут сломать наши текущие стандарты шифрования более легко, чем наше текущее оборудование.

Откройте редактор групповой политики, затем выберите «Конфигурация компьютера» → «Административные шаблоны» → «Компоненты Windows» → «Шифрование диска BitLocker».

Выберите «Выбрать метод шифрования диска и силу шифра». Выберите Enabled, затем используйте выпадающие списки, чтобы выбрать XTS-AES 256-bit. Нажмите Применить, и ВЫ ГОТОВЫ.



Сделайте резервную копию вашего пароля Windows BitLocker!

Теперь вы знаете, как зашифровать диск Windows 10 с помощью BitLocker. BitLocker - это фантастический инструмент шифрования, интегрированный в Windows 10. Вам не нужно беспокоиться о стороннем инструменте шифрования.