Symantec™ Endpoint Protection 14.3: заметки о выпуске

Последнее обновление: июнь 2020 г.

Table of Contents

Заявление об авторском праве

Новые возможности Symantec Endpoint Protection 14.3

В этом разделе описаны новые компоненты выпуска 14.3.

Компоненты защиты

- Сторонние разработчики приложений могут защитить своих клиентов от динамических вредоносных программ на основе сценариев и от нетрадиционных способов проведения кибератак. Стороннее приложение вызывает AMSI-интерфейс Windows для запроса сканирования предоставленного пользователем сценария, который направляется клиенту Symantec Endpoint Protection. Клиент отвечает, указывая, является ли поведение сценария вредоносным. Если поведение не является вредоносным, то выполнение сценария продолжается. Если поведение сценария является вредоносным, приложение не выполняет его. В диалоговом окне клиента, где представлены результаты сканирования, отображается статус "Доступ запрещен". В качестве примеров сторонних сценариев можно привести Windows PowerShell, JavaScript и VBScript. Автоматическая защита должна быть включена. Данная функция поддерживается в Windows 10 и на более новых компьютерах.
  Защита от вредоносных программ с помощью интерфейса антивирусного сканирования (AMSI)
  Интерфейс антивирусного сканирования (AMSI)

Symantec Endpoint Protection Manager

- Удаленная консоль Symantec Endpoint Protection теперь поддерживает Java 11, а не Java 8.Чтобы получить доступ к удаленной консоли, откройте поддерживаемый веб-браузер, введите следующий адрес в адресной строке: `http://SEPMServer:9090/symantec.html` и загрузите новый пакет удаленной консоли. Следуйте отображаемым инструкциям. Предыдущая версия Symantec Endpoint Protection Manager более не поддерживается.
  Вход в Symantec Endpoint Protection
- Вы можете настроить один экземпляр Symantec Endpoint Protection Manager на сайте в качестве основного сервера регистрации для передачи журналов на сервер syslog. Если основной сервер регистрации переходит в автономный режим, второй сервер управления берет его функции на себя и направляет журналы на сервер syslog. Когда основной сервер регистрации снова подключается к сети, он возобновляет отправку журналов.
  Настройка резервного сервера на внешнее ведение журнала
- Политика интеграции предусматривает новую функцию для перенаправления трафика WSS, **Включить пользовательский PAC-файл LPS**. Эта функция позволяет заменить PAC-файл по умолчанию, размещенный сервером LPS в клиенте, пользовательским PAC-файлом. Пользовательский PAC-файл решает проблемы совместимости со сторонними приложениями, которые не работают с локальным прокси-сервером, но нужно оставить прослушивающим циклический адаптер.

Настройка перенаправления трафика WSS

- Поддержка базы данных Microsoft SQL Server 2019.
- В процессе антивирусного сканирования теперь используется отдельная служба, которая относится к основной службе, не связанной с безопасностью. Этот новый процесс сканирования обеспечивает более эффективное использование памяти, постоянную защиту и меньшее влияние проблем, возникающих с основной службой.
- Схема базы данных включает в себя новые столбцы, которые относятся к компоненту для будущего выпуска. (Таблицы AGENT_SECURITY_LOG_1, AGENT_SECURITY_LOG_2, SEM_AGENT)
- API Rest имеет следующие поля в ответе API /sepm/api/v1/computers на языке JSON для вызова и загрузки отчета о состоянии компьютера: quarantineStatus, quarantineCode, wssStatus, pskVersion.
- До более поздних версий обновлены следующие сторонние компоненты: Apache Tomcat, Boost C++ Libraries, cURL, Jackson-core, jackson-databind, Jakarta Activation, Java, logback, Microsoft JDBC Driver for SQL Server, OpenSC, OpenSSL, Spring Security, spring-framework, sqlite.
- Чтобы зарегистрировать домен Symantec Endpoint Protection Manager в облачной консоли, необходимо сначала получить маркер регистрации с помощью консоли Symantec Endpoint Security. Ранее маркер регистрации можно было получить, нажав кнопку **Начало работы** на странице **Облако**.

Обновления клиентов и платформы

- Клиент Windows поддерживает Windows 10 20H1 (Windows 10 версия 2004)
- Теперь клиент Linux поддерживает Ubuntu 18.04, RHEL 8 и CentOS 8.
- Инструмент AppRemover был обновлен до более поздней версии. Инструмент AppRemover удаляет сторонние приложения перед установкой клиента Windows. Дополнительные сведения об удаляемых приложениях см. в разделе: Удаление стороннего программного обеспечения для управления безопасностью в Endpoint Protection 14.3

Удаленные компоненты

- В следующих уведомлениях больше не отображаются поля **Серьезность угрозы** и **Тип угрозы**: "Угроза эпидемии", "Одиночное событие угрозы", "Обнаружена новая угроза".

Новые возможности во всех выпусках Symantec Endpoint Protection

Известные проблемы и способы их решения

Информация в этом разделе относится к данному выпуску Symantec Endpoint Protection.

Table 1: Проблемы с обновлением

Проблема	Описание и решение
Не удается обновить SQL Server 2017 до версии 2019, если включен режим FIPS [14.3]	Может появиться сообщение об ошибке: "Произошла следующая ошибка. При установке компонента расширения произошла ошибка и было получено следующее сообщение: Не удалось создать AppContainer с сообщением об ошибке "НЕТ, состояние". Данный компонент не относится к проверенным криптографическим алгоритмам платформы Windows FIPS". Это происходит, если установлено программное обеспечение Symantec Endpoint Protection Manager 14.3 с поддержкой FIPS и выполняется обновление Microsoft SQL Server 2017 до версии 2019. [SEP-61473] Чтобы решить эту проблему, отключите FIPS на уровне операционной системы: 1. В папке `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools` выберите **Локальная политика безопасности** > **Локальные политики** > **Параметры безопасности** и отключите параметр **Системная криптография: использовать FIPS-совместимые алгоритмы для шифрования, хеширования и подписывания**. 2. Обновите SQL Server 2017 до версии 2019. 3. После успешного обновления SQL Server, снова включите FIPS. Не удается обновить SQL 2017 до версии 2019 при включенном режиме FIPS
Пользовательские имена могут помешать обновлению политики брандмауэра при обновлении до 14.2 или более поздней версии	Для обновления до Symantec Endpoint Protection 14.2 или более поздней версии политики брандмауэра не должны включать в себя изменения IPv6, если были изменены некоторые имена по умолчанию. Имена по умолчанию включают имена политик и правил по умолчанию. Если правила не могут быть обновлены во время обновления, параметры IPv6 не отображаются. Любые новые политики или правила, которые создаются после обновления, не затрагиваются. Если возможно, верните все измененные имена к значениям по умолчанию. В противном случае убедитесь, что пользовательские правила, которые вы добавили в политику по умолчанию, не мешают связи через IPv6. Убедитесь в этом для всех новых политик или правил, которые добавляете.

Table 2: Проблемы с Symantec Endpoint Protection Manager

Проблема	Описание и решение
При гибридном управлении и использовании прокси-серверов внесите дополнительные URL-адреса в белый список Symantec Endpoint Security [14.2.2.1 или более поздняя версия]	В связи с тем что компания Broadcom недавно приобрела Symantec Enterprise Security, URL-адреса для взаимодействия между клиентами и облаком изменились в версии 14.2.2.1. [CDM-42467] В следующем случае необходимо обновить клиенты, установив сборку версии 14.2.5569.2100 или более позднюю. • Вы используете Symantec Endpoint Security для управления клиентами и политиками, когда в облачной консоли зарегистрированы локальные домены Symantec Endpoint Protection Manager. • Вы используете прокси-серверы. Для внесения URL-адресов в белый список в клиентах с полностью облачным или гибридным управлением внесите их в белый список Symantec Endpoint Security: 1. в Symantec Endpoint Security выберите **Конечная точка > Политики> [название политики] Политика белого списка**. 2. В разделе "Политика белого списка", рядом с разделом **Исключено доменом**, выберите **Добавить**, добавьте следующие URL-адреса по отдельности и нажмите **Добавить**: `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (добавьте, если у вас есть устройства в Европе). Если вы хотите продолжить управление клиентами с помощью более поздней версии, не удаляйте адрес spoc.norton.com. 3. Выберите **Сохранить политику** и **Да**, чтобы обновить политику и применить ее к существующим группам. См. раздел URL-адреса для внесения в белый список Symantec Endpoint Security. См. раздел Обновление агентов Symantec с облачным управлением до версии 14.2 RU2 MP1 или более поздней до 4 мая 2020 года.
Удаленная консоль Symantec Endpoint Protection Manager больше не поддерживает 32-разрядную платформу Windows [14.3]	Начиная с версии 14.3 невозможно войти в удаленную консоль Symantec Endpoint Protection Manager при использовании 32-разрядной версии Windows. Среда выполнения Oracle Java SE больше не поддерживает 32-разрядные версии Microsoft Windows. [SEP-61106] Если вы видите следующее сообщение, войдите в Symantec Endpoint Protection Manager на локальном устройстве: "Данная версия C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe несовместима с используемой версией Windows. Проверьте информацию о системе вашего компьютера, а затем свяжитесь с разработчиком программного обеспечения". Вход в Symantec Endpoint Protection Manager
Во время установки Symantec Endpoint Protection Manager [14.3] появляется ошибка "Не удалось установить среду выполнения Microsoft Visual C++ "	При установке Symantec Endpoint Protection Manager в Windows 2012 R2 отображается ошибка "Не удалось установить среду выполнения Microsoft Visual C++" [SEP-60396] Чтобы решить эту проблему, активируйте Windows и установите обновления Windows. При обновлении Windows устанавливается распространяемый пакет Visual C++ 2017, который необходим для установки Symantec Endpoint Protection Manager 14.3 в Windows 2012 R2.

Проблема	Описание и решение
Обновление с целью включения TLS 1.1 и TLS 1.2 в WinHTTP в качестве протоколов безопасности Windows по умолчанию [14.3]	После обновления или установки программного обеспечения Symantec Endpoint Protection Manager 14.3, которое зарегистрировано в облачной консоли, сервер управления перестает успешно загружать журналы в облако. В uploader.log можно видеть следующую ошибку: `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` Эта проблема вызвана отсутствием обновления Microsoft, которое обеспечивает поддержку протоколов TLS 1.1 и 1.2. Чтобы решить проблему, установите обновление Microsoft: KB3140245. Дополнительные сведения см. в: Обновление с целью включения TLS 1.1 и TLS 1.2 в WinHTTP в качестве протоколов безопасности Windows по умолчанию
Сообщение "Выполняется развертывание" по-прежнему появляется в Symantec Endpoint Protection Manager после того, как клиент получает обновленную политику для Endpoint Threat Defense for AD [14.2 RU1 MP1 и более поздняя версия]	Такое поведение является нормальным. Политики Endpoint Threat Defense for AD 3.3 поддерживаются в клиентах только начиная с версии 14.2 RU1 MP1. Политика для Symantec Endpoint Threat Defense for Active Directory 3.3 применяется к группе. В этой группе находится несколько клиентов с работающим программным обеспечением Symantec Endpoint Protection 14.2 RU1 или более ранней версии. Эти клиенты получают и применяют политику должным образом, но в Symantec Endpoint Protection Manager по-прежнему отображается сообщение "Выполняется развертывание".

Table 3: Проблемы с клиентами Windows, Mac и Linux

Проблема	Описание и решение
Установка клиента Symantec Endpoint Protection 14.3 для Windows может оказаться невозможной, если предварительно не установлена поддержка SHA-2 [14.3]	При использовании устаревших версий операционной системы (Windows 7 RTM или SP1, Windows Server 2008 R2, R2 SP1 или R2 SP2) необходимо, чтобы на устройстве была установлена поддержка подписания кода SHA-2, чтобы установить обновления Windows, выпущенные в июле 2019 года или после. Без поддержки SHA-2 установка клиента Windows иногда заканчивается неудачей. Проблемы с установкой могут возникнуть не только при первой установке клиента, но и при автоматическом обновлении предыдущего выпуска. [SEP-61175/61403] Сведения о том, как получить принудительную поддержку подписания кода SHA-2 Microsoft, см. в разделе: Требования по поддержке подписания кода 2019 SHA-2 для Windows и WSUS Попытка установить клиент Symantec Endpoint Protection 14.3 для Windows может быть неудачной, если не установлена поддержка SHA-2
Клиент Symantec Endpoint Protection Windows не работает при установке в Windows 10 1803 с поддержкой UWF [14.3]	Если клиент Symantec Endpoint Protection работает в 32-разрядной операционной системе Windows 10 RS4 1803, и при этом включен объединенный фильтр записи (UWF), который защищает диск с установленным клиентом Windows, клиент не работает должным образом. Эта операционная система Windows содержит дефект UWF, который мешает запуску клиента Windows. Решение проблемы • Обновите операционную систему до другой версии, в которой отсутствует данный дефект. • Отключите объединенный фильтр записи. См. раздел: Проблемы при работе Endpoint Protection после установки в Windows 10 1803 с включенным объединенным фильтром записи

Проблема	Описание и решение
Клиенты Mac, которые активируют перенаправление трафика WSS, не принимают пользовательские настройки прокси-сервера для LiveUpdate [14.2 RU1 MP1 или более поздняя версия]	Вы настроили управляемые клиенты Mac для Symantec Endpoint Protection 14.2 RU1 MP1 или более поздней версии, чтобы применить пользовательские параметры прокси-сервера к LiveUpdate с помощью внешних параметров связи. Однако после включения перенаправления трафика WSS (WTR) для клиентов Mac через политику Symantec Endpoint Protection Manager трафик LiveUpdate больше не принимает пользовательские параметры прокси-сервера. Вместо этого LiveUpdate предпринимает попытку прямого подключения. В качестве временного решения этой проблемы используйте только пользовательские параметры прокси-сервера для LiveUpdate при отключении перенаправления трафика WSS.
Microsoft Edge неожиданно разрешает загрузки файлов PDF при включенном усилении защиты [14.2 RU1 MP1 или более поздняя версия]	Когда в клиенте Symantec Endpoint Protection включена функция усиления защиты, вы неожиданно получаете возможность загружать PDF-файлы при использовании браузера Microsoft Edge. Предотвращение загрузки PDF-файлов работает ожидаемым образом в других браузерах. Исправление этой неполадки запланировано в будущих выпусках.

После недавнего заявления компании Broadcom об официальном присоединении к ней Symantec Enterprise Protection вся документация Symantec была перенесена на портал Broadcom Symantec Security Tech Docs Portal.

Чтобы найти документацию по Endpoint Protection, перейдите на вкладку **Symantec Security Software** и выберите **Endpoint Security and Management** > **Endpoint Protection**.

Table 4: Проблемы с документацией

Проблема	Описание и решение
Истек срок действия статей практического руководства.	Статьи практического руководства (HOWTO), которые дублировали разделы Справки по Symantec Endpoint Protection Manager, были заново опубликованы на сайте Endpoint Protection и теперь имеют другой URL-адрес. Чтобы найти статью, используйте **поле поиска**.
PDF-файлы	Symantec опубликовала все файлы PDF к статьям DOC. Срок действия этих страниц истек. Чтобы найти последнюю версию файла PDF, перейдите на страницу Related Documents (Связанные документы). В будущем Broadcom будет добавлять на сайт устаревшие и переведенные файлы PDF.

Сведения об устраненных проблемах см. в разделе Новые исправления и компоненты Symantec Endpoint Protection 14.3

Требования к системе для Symantec Endpoint Protection (SEP)

Обычно требования к системе для следующих продуктов аналогичны требованиям поддерживаемых операционных систем.

> **NOTE**
> Более ранняя версия Symantec Endpoint Protection Manager может оказаться не в состоянии правильно управлять клиентом с более поздней версией. Могут возникнуть проблемы с обновлением содержимого и управлением клиентами. Например, Symantec Endpoint Protection Manager 14.0.1 или более ранней версии не может должным образом предоставить моникеры, используемые в данной версии, клиенту с версией 14.2. Symantec Endpoint Protection Manager версии до 14 MP2 не может должным образом предоставить моникеры, используемые в данной версии, клиенту с версией после 14.0.1.

В следующих таблицах представлены требования к программному и аппаратному обеспечению для Symantec Endpoint Protection.

Table 5: Требования к системе для программного обеспечения Symantec Endpoint Protection Manager (SEPM)

Компонент	Требования
Операционная система	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** Операционные системы для настольных ПК не поддерживаются. **Note:** Версия Windows Server Core не поддерживается. Windows Server Core не включает в себя браузер Internet Explorer, который требуется для работы Symantec Endpoint Protection Manager.
Веб-браузер	Для доступа веб-консоли к Symantec Endpoint Protection Manager и просмотра справочного раздела Symantec Endpoint Protection Manager поддерживаются следующие браузеры: • Microsoft Edge Примечание. В 32-разрядной версии Windows 10 не поддерживается доступ к веб-консоли через браузер Edge. • Microsoft Internet Explorer 11 • Mozilla Firefox версии 5.x–68.x • Google Chrome 75.x

Компонент	Требования
База данных	**Symantec Endpoint Protection Manager содержит встроенную базу данных. Кроме того, можно выбрать базу данных из следующих версий Microsoft SQL Server:** • SQL Server 2008, SP4 • SQL Server 2008 R2, SP3 • SQL Server 2012, RTM - SP4 • SQL Server 2014, RTM - SP3 • SQL Server 2016, RTM, SP1, SP2 • SQL Server 2017, RTM • SQL Server 2019, RTM (начиная с версии 14.3) **Note:** База данных SQL Server Express Edition не поддерживается. Поддерживаются базы данных SQL Server, размещенные на Amazon RDS (начиная с версии 14.0.1 MP2). **Note:** Если Symantec Endpoint Protection использует базу данных SQL Server, а ваша среда использует только TLS 1.2, убедитесь, что SQL Server поддерживает TLS 1.2. Может потребоваться установить исправление для SQL Server. Данная рекомендация относится к SQL Server 2008, 2012 и 2014. Необходимо установить исправление SQL Server для поддержки TLS 1.2, в противном случае могут возникнуть проблемы при обновлении Symantec Endpoint Protection 12.1 до версии 14. **Note:** Поддержка TLS 1.2 для сервера Microsoft SQL Server
Другие требования к среде	В сетях, использующих только IPv6, по-прежнему необходимо установить и отключить стек IPv4. Если стек IPv4 удален, Symantec Endpoint Protection Manager не будет работать.

Table 6: Системные требования к аппаратному обеспечению для Symantec Endpoint Protection Manager

Компонент	Требования
Процессор	Минимум Intel Pentium Dual-Core или аналогичный, рекомендуется 8-ядерный или выше. **Note:** Процессоры Intel Itanium IA-64 не поддерживаются.
Физическое ОЗУ	2 ГБ ОЗУ (минимум); 8 ГБ ОЗУ или более (рекомендуется) **Note:** Для сервера Symantec Endpoint Protection Manager может понадобиться дополнительная оперативная память в зависимости от требований уже установленных приложений к оперативной памяти. Например, если продукт Microsoft SQL Server установлен на сервере Symantec Endpoint Protection Manager, то на этом сервере требуется как минимум 8 ГБ свободного пространства.
Экран	1024 x 768 или выше
Жесткий диск при установке на системный диск	**Со встроенной базой данных или локальной базой данных Microsoft SQL Server:** • Минимум 40 ГБ свободного места (рекомендуется 200 ГБ) для сервера управления и базы данных **С удаленный базой данных SQL Server:** • Минимум 40 ГБ свободного места (рекомендуется 100 ГБ) для сервера управления. • Дополнительное доступное дисковое пространство на удаленном сервере для базы данных
Жесткий диск при установке на другой диск	**Со встроенной базой данных или локальной базой данных Microsoft SQL Server:** • Системный диск требует 15 ГБ свободной памяти (минимум); 100 ГБ (рекомендуется) • Диск установки требует 25 ГБ свободной памяти (минимум); 100 ГБ (рекомендуется) **С удаленный базой данных SQL Server:** • Системный диск требует 15 ГБ свободной памяти (минимум); 100 ГБ (рекомендуется) • Диск установки требует 25 ГБ свободной памяти (минимум); 100 ГБ (рекомендуется) • Дополнительное доступное дисковое пространство на удаленном сервере для базы данных

Если вы используете базу данных SQL Server, необходимо иметь больше доступного дискового пространства. Объем и расположение дополнительного пространства зависит от диска, используемого SQL Server, требований обслуживания базы данных и других параметров.

Table 7: Системные требования к ПО клиента Symantec Endpoint Protection для Windows

Компонент	Требования
Операционная система (настольная)	• Windows 7 (32-разрядная, 64-разрядная; RTM и пакет обновления SP1) • Windows Embedded 7 Standard, POSReady и Корпоративная (32- и 64-разрядная) • Windows 8 (32- или 64-разрядная) • Windows Embedded 8 Standard (32- и 64-разрядная) • Windows 8.1 (32- или 64-разрядная), включая Windows To Go • Windows 8.1 с обновлением от апреля 2014 г. (32- и 64-разрядная) • Windows 8.1 с обновлением от августа 2014 г. (32- и 64-разрядная) • Windows Embedded 8.1 Pro, Industry Pro, Industry Enterprise (32- и 64-разрядная) • Windows 10 (версия 1507) (32-разрядная, 64-разрядная), включая Windows 10 Enterprise 2015 LTSB • Windows 10 с ноябрьским обновлением 1511 (32- или 64-разрядный выпуск) • Windows 10 с юбилейным обновлением (версия 1607) (32-разрядная, 64-разрядная), включая Windows 10 Enterprise 2016 LTSB • Windows 10 Creators Update 1703 (32- или 64-разрядный выпуск) • Windows 10 Fall Creators Update 1709 (32- или 64-разрядный выпуск) • Windows 10 с апрельским обновлением 1803 (32- или 64-разрядный выпуск) • Windows 10 с обновлением обновления за октябрь 2018 г. (версия 1809) (32-разрядная, 64-разрядная), включая Windows 10 Enterprise 2019 LTSC. • Windows 10 с обновлением за май 2019 г. (версия 1903) (32-разрядная, 64-разрядная) • Windows 10 с обновлением за ноябрь 2019 г. (версия 1909) (32-разрядная, 64-разрядная) (14.2 RU1 и более поздние версии) • Windows 10 20H1 (Windows 10 версия 2004) (начиная с версии 14.3)
Операционная система (серверная)	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 с обновлением от апреля 2014 г. • Windows Server 2012 R2 с обновлением от августа 2014 г. • Windows Server 2016 • Windows Server 2019 • Windows Server, версия 1803 (основные серверные компоненты) (14.2 и более поздние версии) • Windows Server, версия 1809 (основные серверные компоненты) • Windows Server, версия 1903 (основные серверные компоненты) (14.2 RU1 и более поздние версии) • Windows Server, версия 1909 (основные серверные компоненты) (14.2 RU1 и более поздние версии)
Система предотвращения вторжений для браузера	Возможность поддержки системы предотвращения вторжений для браузера зависит от версии модуля системы обнаружения вторжений для клиента (CIDS). См. раздел Поддерживаемые браузеры с системой предотвращения вторжений в Endpoint Protection.

Table 8: Системные требования к аппаратному обеспечению для клиентаSymantec Endpoint Protection для Windows

Компонент	Требования
Процессор (для физических компьютеров)	• 32-разрядный процессор: минимум Intel Pentium 4 2 ГГц или аналогичный (рекомендуется Intel Pentium 4 или аналогичный процессор) • 64-разрядный процессор: минимум Pentium 4 с тактовой частотой 2 ГГц и поддержкой разрядности x86-64 или аналогичный процессор **Note:** Процессоры Itanium не поддерживаются.
Процессор (для виртуальных компьютеров)	Один виртуальный сокет и одно ядро на каждый сокет с минимальной частотой 1 ГГц (рекомендуется один виртуальный сокет и два ядра на каждый сокет с частотой 2 ГГц) **Note:** Необходимо включить резервирование ресурсов гипервизора.
Физическое ОЗУ	1 ГБ (рекомендуется 2 ГБ) или более, в зависимости от требований ОС
Экран	800 x 600 или выше
Жесткий диск	Требования дискового пространства зависят от типа устанавливаемого клиента, диска установки и расположения файла данных о программе. Папка с данными о программе находится на системном диске в расположении по умолчанию C:\ProgramData. На системном диске всегда должно быть доступное дисковое пространство, независимо от того, какой диск установки вы выбираете. **Системные требования к жесткому диску:** • В таблице Имеющиеся системные требования к жесткому диску при установке на системный диск для клиента Symantec Endpoint Protection описываются системные требования к жесткому диску при установке Symantec Endpoint Protection на системный диск. • В таблице Имеющиеся системные требования к жесткому диску при установке на другой диск для клиента Symantec Endpoint Protection для Windows описываются системные требования к жесткому диску при установке Symantec Endpoint Protection на другой диск. **Note:** Требования к дисковому пространству указаны для файловых систем NTFS. Дополнительное свободное пространство также требуется для обновлений содержимого и журналов.

Table 9: Имеющиеся системные требования к жесткому диску при установке на системный диск для клиента Symantec Endpoint Protection для Windows

Тип клиента	Требования
Standard	**Если папка с данными о программе находится на системном диске:** • 395 МБ* **Если папка с данными о программе находится на другом диске:** • Системный диск: 180 МБ • Другой диск установки: 350 МБ
Встроенный или VDI	**Если папка с данными о программе находится на системном диске:** • 245 МБ* **Если папка с данными о программе находится на другом диске:** • Системный диск: 180 МБ • Другой диск установки: 200 МБ

Тип клиента	Требования
Даркнет	**Если папка с данными о программе находится на системном диске:** • 545 МБ* **Если папка с данными о программе находится на другом диске:** • Системный диск: 180 МБ • Другой диск установки: 500 МБ

* В ходе установки дополнительно требуется 135 МБ.

Table 10: Имеющиеся системные требования к жесткому диску при установке на другой диск для клиента Symantec Endpoint Protection для Windows

Тип клиента	Требования
Standard	**Если папка с данными о программе находится на системном диске:** • Системный диск: 380 МБ • Другой диск установки: 15 МБ* **Если папка с данными о программе находится на другом диске:**** • Системный диск: 30 МБ • Диск с данными программы: 350 МБ • Другой диск установки: 150 МБ
Встроенный или VDI	**Если папка с данными о программе находится на системном диске:** • Системный диск: 230 МБ • Другой диск установки: 15 МБ* **Если папка с данными о программе находится на другом диске:**** • Системный диск: 30 МБ • Диск с данными программы: 200 МБ • Другой диск установки: 150 МБ
Даркнет	**Если папка с данными о программе находится на системном диске:** • Системный диск: 530 МБ • Другой диск установки: 15 МБ* **Если папка с данными о программе находится на другом диске:**** • Системный диск: 30 МБ • Диск с данными программы: 500 МБ • Другой диск установки: 150 МБ

* В ходе установки дополнительно требуется 135 МБ.

** Если папка с данными о программе совпадает с альтернативным (или дополнительным) диском для установки, добавьте 15 МБ на диск с данными программы. Однако для программы установки все еще требуется, чтобы на другом диске установки в ходе установки были доступны 135 МБ.

Table 11: Требования к системе для клиента Symantec Endpoint Protection для Windows Embedded

Компонент	Требования
Процессор	Intel Pentium, 1 ГГц
Физическое ОЗУ	256 МБ **Note:** Это значение для установки встроенного клиента Symantec Endpoint Protection. При внедрении дополнительных компонентов из интегрированного решения, такого как EDR, потребуется дополнительная физическая оперативная память.
Жесткий диск	Встроенному клиенту или клиенту VDI Symantec Endpoint Protection необходимо следующее свободное дисковое пространство: • Установлено на системный диск: 245 МБ • Установлено на другой диск: 230 МБ на системный диск и 15 МБ на другой диск В ходе установки дополнительно требуется 135 МБ. Исходя из этих данных папка с данными о программе находится на системном диске. Чтобы получить более подробные сведения или требования к другим типам клиентов, см. Системные требования к клиенту Symantec Endpoint Protection для Windows.
Встроенная операционная система	• Windows Embedded Standard 7 (32- и 64-разрядная) • Windows Embedded POSReady 7 (32- и 64-разрядная) • Windows Embedded Enterprise 7 (32- и 64-разрядная) • Windows Embedded 8 Standard (32- и 64-разрядная) • Windows Embedded 8.1 Industry Pro (32- и 64-разрядная) • Windows Embedded 8.1 Industry Enterprise (32- и 64-разрядная) • Windows Embedded 8.1 Pro (32- и 64-разрядная)
Минимально требуемые компоненты	• Диспетчер фильтров (FltMgr.sys) • Модуль поддержки данных производительности (pdh.dll) • Служба установщика Windows
Шаблоны	• Совместимость приложений (по умолчанию) • Цифровая вывеска • Промышленная автоматизация • Internet Explorer, медиапроигрыватель, протокол удаленного рабочего стола • Телевизионная абонентская приставка • Тонкий клиент Шаблон минимальной конфигурации не поддерживается. Расширенный фильтр записи (EWF) и объединенный фильтр записи (UWF) не поддерживаются. Рекомендованным фильтром записи является файловый фильтр записи (FBWF), устанавливаемый вместе с фильтром реестра.

Table 12: Требования к системе для клиента Symantec Endpoint Protection для Mac

Компонент	Требования
Процессор	64-разрядный Intel Core 2 Duo или более поздней версии
Физическое ОЗУ	2 ГБ ОЗУ
Жесткий диск	500 МБ свободного дискового пространства для установки
Экран	800 x 600

Компонент	Требования
Операционная система	• macOS 10.13 • macOS 10.14 • macOS 10.15–10.15.5 macOS 10.14.5 и более поздние версии поддерживают требования по заверению расширения ядра. См. статью Endpoint Protection 14.2 RU1 и проверка подлинности kext для macOS 10.14.5. Список операционных систем, поддерживаемых предыдущими выпусками, см. в разделе: Совместимость Mac с клиентом Endpoint Protection

Table 13: Требования к системе для клиента Symantec Endpoint Protection для Linux

Компонент	Требования
Аппаратное обеспечение	• Процессор Intel Pentium 4 (2 ГГц) или новее • 1 ГБ ОЗУ • 7 ГБ свободного дискового пространства
Операционные системы	• Amazon Linux • CentOS 6U3–6U9, 7–7U7, 8; 32- и 64-разрядная • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32- и 64-разрядные версии • Fedora 16, 17; 32- и 64-разрядные • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2–6U9, 7–7U8, 8–8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1–11 SP4, 32- и 64-разрядные версии; 12, 12 SP1–12 SP3, 64-разрядные версии • SUSE Linux Enterprise Desktop (SLED) 11 SP1–11 SP4, 32- и 64-разрядные версии; 12 SP3, 64-разрядные версии • Ubuntu 12.04, 14.04, 16.04, 18.04 (по состоянию на 14.3); 32- и 64-разрядная Список ядер операционных систем, поддерживаемых предыдущими версиями, см. в разделе Ядра Linux, поддерживаемые Symantec Endpoint Protection.
Графические настольные среды	Для отображения клиента Symantec Endpoint Protection для Linux можно использовать следующие графические настольные среды: • KDE • Gnome • Единица

Компонент	Требования

Другие требования к среде	• Glibc
	Ни одна операционная система под управлением glibc с версией ранее 2.6 не поддерживается.
	• Зависимые пакеты на основе i686 на 64-разрядных компьютерах
	Многие исполняемые файлы в клиенте Linux представляют собой 32-разрядные программы. На 64-разрядных компьютерах перед установкой клиента для Linux необходимо установить зависимые пакеты на основе i686.
	Если зависимые пакеты на основе i686 еще не установлены, их можно установить с помощью командной строки. Для этой установки необходимы привилегии суперпользователя, как в следующих командах `sudo`:
	– Для распределений на основе Red Hat: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Для распределений на основе Debian: `sudo apt-get install ia32-libs`
	– Для распределений на основе Ubuntu:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• net-tools или iproute2
	Symantec Endpoint Protection использует одно из этих средств в зависимости от того, что уже установлено на компьютер.
	• Инструменты разработчика
	Автоматическая и ручная компиляции для модуля ядра автоматической защиты требуют установки определенных инструментов разработчика. Такие инструменты разработчика включают gcc, а также исходные и заголовочные файлы ядра. Подробнее о процессе и элементах для установки в определенных версиях Linux см.:
	Ручная компиляция модуля ядра автоматической защиты для Endpoint Protection для Linux

Заметки о выпуске и требования к системе для всех версий Symantec Endpoint Protection

Поддерживаемые пути обновления до последней версии Symantec Endpoint Protection 14.x

NOTE

Как правило, все версии Symantec Endpoint Protection, предшествующие последней версии, поддерживаются. Однако это следует уточнить в заметках о выпуске вашей конкретной версии.

Заметки о выпуске, новые исправления и системные требования для всех версий Endpoint Protection

Symantec Endpoint Protection Manager и клиент Windows

Следующие версии Symantec Endpoint Protection Manager и клиента Windows Symantec Endpoint Protection можно обновить непосредственно до текущей версии:

- 11.x и Small Business Edition 12.0 (только клиенты Symantec Endpoint Protection для поддерживаемых операционных систем)
- 12.1.x до 12.1.6 MP10
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU2 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Клиент Mac

Следующие версии клиента Symantec Endpoint Protection для Mac можно обновить непосредственно до текущей версии:

- 12.1.4 - 12.1.6 MP9
  Клиент Mac не был обновлен для версии 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

Клиент Symantec Endpoint Protection для Mac не был обновлен для 14.0.1 MP2.

Клиент Linux

Следующие версии клиента Symantec Endpoint Protection для Linux можно обновить непосредственно до текущей версии:

- 12.1.x - 12.1.6 MP9
  Клиент Linux не был обновлен для версии 12.1.6 MP10.
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU2 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Symantec AntiVirus for Linux 1.0.14 — это единственная версия, для которой возможна миграция непосредственно на Symantec Endpoint Protection. Сначала необходимо удалить все другие версии Symantec AntiVirus for Linux. Нельзя выполнить миграцию управляемого клиента на неуправляемый клиент.

Неподдерживаемые способы обновления

Миграцию на Symantec Endpoint Protection можно выполнить не со всех продуктов Symantec. Перед установкой клиента Symantec Endpoint Protection необходимо удалить следующие продукты:

- Неподдерживаемые продукты Symantec, такие как Symantec AntiVirus и Symantec Client Security
- Все продукты Symantec Norton ™
- Symantec Endpoint Protection для Windows XP Embedded 5.1
- Версии Symantec Endpoint Protection для Mac, предшествующие 12.1.4

Версию Symantec Endpoint Protection Manager 11.0.x или Symantec Endpoint Protection Manager Small Business Edition 12.0.x невозможно обновить непосредственно до Symantec Endpoint Protection Manager 14. Сначала необходимо удалить эти версии или обновить продукты до версии 12.1.x, а затем обновить их до версии 14.x.

Невозможно обновить Symantec Endpoint Protection Manager 12.1.6 MP7 до версии 14, так как версия схемы базы данных в 12.1.6 MP7 старше версии в 14. Вместо этого выполните обновление 12.1.6 MP7 до 14 MP1 или более поздней версии.

Обновление с 14 MP1 (14.0.2332.0100) до 14 MP1 Refresh Build (14.0.2349.0100) не поддерживается.

Переход на более старые версии не поддерживается. Например, чтобы перейти с Symantec Endpoint Protection 14.2.1.1 на версию 12.1.6 10, необходимо сначала удалить Symantec Endpoint Protection MP14.2.1.1.

Если у вас есть номер сборки, но вы не уверены, как он соотносится с выпущенной версией, см.:

- Выпущенные версии Symantec Endpoint Protection
- Типы и версии выпусков Endpoint Protection

Источники дополнительной информации

В разделе Endpoint Protection:информация содержится перечень веб-сайтов, на которых можно найти рекомендации, сведения об устранении неполадок и другие ресурсы, которые помогут в работе с продуктом.

Table 14: Сведения о веб-сайтах Endpoint Protection

Тип информации	Ссылка на веб-сайт
Пробные версии	Свяжитесь с менеджером по работе с клиентами.
Обновления руководств и документации	• Руководства по последним выпускам продуктов (на английском языке) • Руководства по последним выпускам продуктов (на других языках) • Руководства по всем версиям Symantec Endpoint Protection 14.x (на английском языке) **Другие языки:**
Техническая поддержка	Техническая поддержка Endpoint Protection Включает в себя статьи базы знаний, сведения о выпуске продукта, обновления и исправления, а также варианты обращения для получения поддержки.
Сведения об угрозах и обновления	Центр безопасности Symantec
Обучение	Услуги обучения Доступ к обучающим курсам, электронной библиотеке и другим ресурсам.
Форумы Symantec Connect	Endpoint Protection


Symantec
A Division of Broadcom