Symantec™ Endpoint Protection 14.3 RU1: заметки о выпуске

Обновлено: декабрь 2020 г.

Table of Contents

Заявление об авторском праве

Заявление об авторском праве

Broadcom относится к компании Broadcom Inc. и (или) ее дочерним компаниям. Для получения дополнительной информации посетите веб-сайт www.broadcom.com.

Broadcom оставляет за собой право вносить изменения без дополнительного уведомления в любые продукты или данные, приведенные в настоящем документе, для повышения надежности, функциональности или дизайна. Информация, предоставляемая компанией Broadcom, считается точной и надежной. Тем не менее, компания Broadcom не несет никакой ответственности, возникающей в связи с применением или использованием этой информации, а также в связи с применением или использованием любого продукта или схемы, приведенных в данном документе, а также не передает никаких лицензий в соответствии со своими патентными правами или правами других лиц.

Новые возможности Symantec Endpoint Protection 14.3 RU1

В этом разделе описаны новые компоненты этого выпуска.

Компоненты защиты

- Включает новые агенты Symantec для Mac и для Linux, которые можно установить и настроить из локального экземпляра Symantec Endpoint Protection Manager или из интегрированной облачной консоли Cyber Defense Manager.
  Установка клиента Symantec Endpoint Protection for Mac
  Установка Symantec Agent for Linux 14.3 RU1
- Предотвращает новые и неизвестные угрозы на macOS, отслеживая почти 1400 шаблонов поведения файлов в режиме реального времени. Новый агент для Mac включает в себя эти возможности защиты на основе анализа поведения. Защита на основе анализа поведения (SONAR) использует искусственный интеллект и современные технологии машинного обучения для защиты от угроз нулевого дня.
  Управление SONAR
- Блокирует ненадежные непереносимые исполняемые файлы (PE), например PDF-файлы и сценарии, которые еще не определены как угроза. В политике исключений нажмите **Исключения Windows** > **Доступ к файлам**.
- Предотвращает веб-угрозы на основе оценки репутации веб-страницы. Политика предотвращения вторжений включает фильтрацию URL-адресов, которая блокирует веб-страницы с оценкой репутации ниже определенного порогового значения. Оценки репутации могут варьироваться от -10 (плохая репутация) до +10 (хорошая репутация). Параметр **Включить репутацию URL-адреса** включен по умолчанию.
- Можно настроить в Symantec Endpoint Protection принудительное получение данных о приложении из значения хэша приложения. В политике Исключений нажмите **Исключения Windows** > **Приложение** > **Добавить приложение по идентификационному коду**.
- Защищает конечные точки и пользователей от веб-атак на вредоносных сайтах с использованием функции перенаправления сетевого трафика. Функция перенаправления сетевого трафика перенаправляет весь сетевой трафик (любой порт) или только веб-трафик (порты 80 и 443) в службу Symantec Web Security Service, которая разрешает или блокирует сетевой трафик и доступ к приложениям SaaS на основе корпоративной политики. Политика перенаправления сетевого трафика предусматривает новый метод перенаправления, так называемое туннелирование. При туннелировании весь интернет-трафик автоматически перенаправляется в Symantec WSS, где его передача разрешается или блокируется в зависимости от политик Symantec Web Security Service. Метод туннелирования на данный момент находится на этапе бета-тестирования. Необходимо тщательно протестировать его работу с приложениями при использовании политик WSS. Broadcom предоставляет бета-версию веб-сайта, где доступно руководство по тестированию, а также можно оставить отзывы о новой функции. Войдите на следующий веб-сайт, используя учетные данные Broadcom: Validate.broadcom.com.
  Настройка перенаправления сетевого трафика
- Политика интеграции переименована в политику перенаправления сетевого трафика.
- Обеспечивает поддержку событий с учетом контекста MITRE в Symantec EDR. Используйте систему MITRE ATT&CK, чтобы предоставить контекст происходящего в вашей среде.
- Поддерживает следующие события Symantec EDR, которые обеспечивают расширенную визуализацию конечных точек:
  - События AMSI обеспечивают визуализацию тех методов злоумышленников, которые могут остаться незамеченными при использовании традиционных способов опроса командной строки.
  - События ETW обеспечивают визуализацию событий, происходящих на управляемых конечных точках Windows.
- Включает функцию запуска «Защитника Windows» и Symantec Endpoint Protection на одном компьютере. Сканирование с использованием автоматической защиты запускается вслед за «Защитником Windows»

и может обнаруживать любые угрозы, которые он пропускает. Параметр **Совместное использование с «Защитником Windows»** гарантирует, что автоматическая защита продолжит работать после отключения «Защитника Microsoft». Чтобы отключить этот параметр, нажмите «Политика защиты от вирусов и программ-шпионов» > **Прочее** > вкладка **Прочее**.

- Обрыв цепочки атаки теперь поддерживается для клиентов с гибридным управлением.

Symantec Endpoint Protection Manager

- В качестве встроенной базы данных теперь используется база Microsoft SQL Express. База данных SQL Server Express хранит политики и события безопасности более эффективно, чем встроенная база данных по умолчанию, и устанавливается автоматически вместе с Symantec Endpoint Protection Manager.

  Рекомендации по замене встроенной базы данных на базу данных Microsoft SQL Server Express
- Во время установки или обновления Symantec Endpoint Protection Manager мастер настройки сервера управления выполняет следующие действия.
  - Автоматически устанавливает содержимое LiveUpdate.
  - Предоставляет возможность использовать сертификат TLS для безопасной связи между SQL Server и Symantec Endpoint Protection Manager.
- LiveUpdate использует в Symantec Endpoint Protection Manager новый модуль, который оптимизирован для выполнения в облачной консоли.

  Примечания к выпуску и новые исправления LiveUpdate Administrator
- Параметр **Автоматическое удаление существующего стороннего программного обеспечения безопасности**, который был недоступен в версии 14.3 MP1, теперь обновлен и добавлен в версию 14.3 RU1. Этот параметр используется для удаления стороннего программного обеспечения безопасности. Чтобы получить доступ к нему, перейдите на страницу **Администратор** > **Пакеты** > **Параметры установки клиента**.

  Удаление стороннего программного обеспечения безопасности в Endpoint Protection 14

  Удаление стороннего программного обеспечения безопасности в Endpoint Protection 14.3 RU1
- Мастер развертывания клиентов, используемый для развертывания клиентских пакетов, должен иметь проверенные учетные данные, а также иметь возможность подключиться к Symantec Endpoint Protection Manager. Если проверка не пройдена, процесс развертывания клиента будет прерван, чтобы не допустить блокировки учетных записей пользователей Active Directory.

  Установка клиентов Symantec Endpoint Protection с помощью принудительной отправки
- Теперь в разделе "Журналы и отчеты о состоянии компьютеров" можно выбрать диапазон для полей **Версия клиента** и **Версия IPS**. Имя фильтра **Версия продукта** изменено на **Версия клиента**.
- Опция **Не показывать значок в области уведомлений** доступна для клиентов, которые работают на сервере терминалов и интенсивно потребляют ресурсы ЦП и памяти. Теперь вы можете отключить показ значка в области уведомлений (на панели задач), чтобы предотвратить запуск нескольких экземпляров процесса пользовательского сеанса (например, SmcGui.exe и ccSvcHost.exe). Включить этот параметр можно в разделе **Клиенты** > вкладка **Политики** > **Параметры безопасности** > вкладка **Общие**.
- Обновлен режим белого списка и черного списка в соответствие с функциями разрешения и блокировки. На странице **Клиенты** > вкладка **Политики** > диалоговое окно **Блокировка системы** списки файлов приложений изменены с **Режим белого списка** и **Режим черного списка** на **Режим разрешенных элементов** и **Режим запрещенных элементов**.
- На странице **Администратор** > вкладка **Серверы** > **Настроить внешние журналы** > вкладка **Общие** параметр **Главный сервер ведения журналов** изменен на **Основной сервер ведения журналов**.
- Журнал **Система** > журнал **Администрирование** и журнал **Аудит** содержат имя компьютера.
- Выполняется сбор данных журналов брандмауэра клиента, чтобы в облачной консоли отображалось меньше уведомлений.
- Oracle Java SE заменен на OpenJDK.
- Сторонние компоненты JQuery заменены на более новые версии.

Обновления клиентов и платформы

- Клиент Windows поддерживает Windows 10 20H2 (Windows 10 версии 2009).
- Клиент Mac поддерживает версию macOS 10.15.7.
- Устаревшие пакеты установки клиентов Mac перемещены в папку «Дополнительные пакеты».

Удаленные компоненты

- Параметры **Серьезность угрозы** и **Распределение угроз по степени серьезности** удалены из уведомлений и отчетов.
- Вкладка **CASMA** и команда **Анализ** удалены, так как эта функция в версии 14.3 уже не поддерживается.
- Клиент Mac больше не поддерживает macOS 10.13.

Документация

Справка Symantec Endpoint Protection Manager теперь доступна в сети и находится по ссылке Руководство по установке и администрированию Symantec Endpoint Protection.

Схема базы данных

В схему базы данных внесены следующие изменения.

Таблица	Изменение столбца
ПРЕДУПРЕЖДЕНИЯ	Добавлен столбец ENRICHED_DATA.
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	Из каждой таблицы удалены следующие столбцы: RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

Таблица	Изменение столбца
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• Тип столбца CONTENT изменен с image на varbinary • Добавлен индексированный столбец FILESTREAM_ID • Добавлен индекс FILESTREAM_ID. • Удалены следующие столбцы: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	Добавлены следующие столбцы: • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	• Добавлен столбец NTR_MESSAGE. • Удалены следующие столбцы: – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	Добавлены следующие столбцы: • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	Удалены следующие столбцы: • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	Добавлен столбец ENRICHED_DATA.

Новые возможности во всех выпусках Symantec Endpoint Protection

Известные проблемы и их решения для Symantec Endpoint Protection

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

Table 1: Проблемы с обновлением

Проблема	Описание и решение
Symantec Endpoint Protection Manager в даркнете загружает старое содержимое Client Intrusion Detection System (CIDS) в новые клиенты, поскольку LiveUpdate не работает во время обновления [14.3 RU1]	Когда решение Symantec Endpoint Protection Manager 14.3 RU1 не может получить доступ к Интернету или к серверу LiveUpdate Administrator (LUA), оно хранит старое, несовместимое содержимое в кэше. Это старое содержимое обычно доставляется на новые клиенты. Чтобы обновить содержимое в кэше сервера управления, необходимо вручную загрузить сертифицированные определения вирусов и файлы CIDS .jdb. [SEP-69125] Чтобы старое содержимое не предоставлялось на новых клиентах, вручную установите файл CIDS .jdb на SEPM перед установкой новых или обновлением старых клиентов. Скачать файлы .jdb для обновления определений для менеджера по защите конечных точек
Не удается войти в Symantec Endpoint Protection Manager (SEPM), если сетевая карта отключена [14.3 RU1]	Если после установки Symantec Endpoint Protection Manager не удается войти в консоль и появляется следующее сообщение об ошибке: «Неожиданная ошибка сервера» Эта проблема может возникнуть, если сетевая карта была отключена при установке SEPM, что помешало сгенерировать сертификат сервера. [SEP-67040] Чтобы узнать, был ли SEPM установлен с отключенной сетевой картой, посмотрите сертификат сервера. См. Установка SEPM закончится неудачей, если нет сетевого подключения
При удалении SEPM с удалением базы данных по умолчанию и сохранением экземпляра SQL Server Express появляется следующая ошибка: «Произошла ошибка при попытке подключиться к серверу базы данных»	Если вы удаляете Symantec Endpoint Protection Manager и выбираете вариант **Удалить только базу данных и оставить экземпляр SQL Server Express, установленный с SEPM**, может появиться следующее сообщение об ошибке: «Произошла ошибка при попытке подключиться к серверу базы данных». Эта проблема возникает после добавления учетных данных для пользователя по умолчанию (DBA) и может быть связана с привилегиями пользователя. [SEP-68670] Чтобы решить эту проблему, выполните удаление, запустив файл SEPM setup.exe и нажав **Удалить только базу данных и оставить экземпляр SQL Server Express, установленный с SEPM**.

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
Некоторые события EDR не отображаются в клиенте [14.3 RU1]	Клиент Symantec Endpoint Protection должен запустить Windows 10 (сборка 14393) или более поздней версии, чтобы выполнить сбор результатов трассировки событий Symantec EDR в Windows (ETW). [SEP-67175]
Политика перенаправления сетевого трафика предполагает ряд ограничений (14.3 RU1)	• Служба Web Security Service предоставляется по протоколу IPv4, а не IPv6. (SEP-68700) • Способ перенаправления с использованием туннелирования: – Доступен только в 64-разрядной версии Windows 10 1703 и более поздних версиях (Semi-Annual Servicing Channel). Этот метод не поддерживает все остальные операционные системы Windows и клиенты Mac. [SEP-67927] – Не поддерживает устройства с 64-разрядной версией Windows 10 с поддержкой HVCI [SEP-67648] – Исходящий трафик с клиента Symantec Endpoint Protection перенаправляется в службу WSS, прежде чем он будет проанализирован брандмауэром клиента либо на основе правил репутации URL-адресов. Этот трафик анализируется брандмауэром WSS и на основе правил URL-адресов WSS. Например, если правило брандмауэра клиента SEP блокирует сайт google.com, а правило WSS его разрешает, клиент разрешает пользователям доступ к google.com. Входящий локальный трафик к клиенту в этом случае по-прежнему обрабатывается брандмауэром Symantec Endpoint Protection. [SEP-67488] – Невозможно подключиться к порталу WSS Captive Portal методом туннелирования, и клиент игнорирует контрольные учетные данные. В будущем выпуске аутентификация SAML в WSS Agent заменит Captive Portal и будет доступна в клиенте Symantec Endpoint Protection. – Если клиентский компьютер подключается к WSS методом туннелирования и размещает виртуальные машины, каждый гость должен установить SSL-сертификат, представленный на портале WSS. – Перенаправление трафика локальной сети, например трафика аутентификации домашнего каталога или Active Directory, не выполняется. Метод туннелирования на данный момент находится на этапе бета-тестирования.
Дубликаты записей о регистрации агента после обновления версии 14.2.x до 14.3 MP1 и более поздних (14.3 RU1)	При обновлении версии клиентов Symantec Endpoint Protection 14.2.x до версии 14.3 MP1 образуются дубликаты записей о регистрации агента для этих клиентов на странице **Устройства** в Symantec Endpoint Protection Manager. На работу программы это не влияет. Вы можете продолжать работать с новыми записями для клиентов версии 14.3 RU1. Symantec Endpoint Protection Manager удаляет старые записи агента.
Разрешите использовать URL-адреса в Symantec Endpoint Security, если вы используете гибридное управление, прокси-серверы или брандмауэр периметра [14.3]	В связи с тем, что компания Broadcom приобрела Symantec Enterprise Security, URL-адреса для взаимодействия между клиентами и облаком в версии 14.2.2.1 изменились. [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. Разрешить URL-адреса можно в агентах с полностью облачным или гибридным управлением, на прокси-сервере и (или) в брандмауэре периметра. См. URL-адреса, которые разрешают SEP и SES подключаться к серверам Symantec См. раздел Обновление агентов Symantec с облачным управлением до версии 14.2 RU2 MP1 или более поздней.

Проблема	Описание и решение
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".
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.
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 следующей статье базы знаний: 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
Некорректные сообщения в журнале программы установки агента Symantec для Linux. [14.3 RU1]	В некоторых случаях прогрмама установки агента регистрирует некорректные сообщения, связанные с несоответствием версий драйвера или необходимостью перезагрузки. Эти сообщения не влияют на работоспособность агента.
На устройстве SuSe Linux команда zypper удаляет пакеты клиентов SEP для Linux при удалении пакета "at". [14.3 RU1]	На устройстве SuSe Linux команда "zypper remove at" удаляет пакеты клиента SEP Linux, поскольку пакет "at" добавляется в качестве обязательного зависимого пакета, а команды zypper автоматически пытаются удалить пакеты клиентов SEP "sdcss-kmod" и "sdcss-sepagent" как пакеты с неиспользованными зависимостями. **Решение:** чтобы удалить пакет "at", выполните следующую команду: rpm -e --nodeps at

Проблема	Описание и решение
Проблема с обновлением в macOS 10.15 и более поздних версиях (14.3 MP1)	В macOS 10.15 и более поздних версий функция **Установить Symantec Endpoint Protection на удаленные компьютеры** в мастере развертывания клиентов не позволяет обновить старые версии клиента Symantec Endpoint Protection до версии 14.3 MP1. **Решение:** используйте функцию **Автообновление Symantec Endpoint Protection Manager** для обновления клиента Symantec Endpoint Protection в macOS 10.15 и более поздних версиях.
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
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.

Описание устраненных проблем см. в разделах:

Новые исправления и компоненты Symantec Endpoint Protection Manager 14.3 RU1

Новые исправления и компоненты Symantec Endpoint Protection Manager 14.3 MP1

Новые исправления и компоненты Symantec Endpoint Protection Manager 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 предоставить соответствующие моникеры клиенту версии 14.2. Symantec Endpoint Protection Manager версий, предшествующих 14 MP2, не может предоставить соответствующие моникеры клиентам версии 14.0.1 и выше.

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 в 14.2x и более ранних версиях.
Веб-браузер	Для доступа веб-консоли к Symantec Endpoint Protection Manager и просмотра справочного раздела Symantec Endpoint Protection Manager поддерживаются следующие браузеры: • Браузер на базе Microsoft Edge Chromium (версия 14.3 и более поздние) • Microsoft Edge Примечание. В 32-разрядной версии Windows 10 не поддерживается доступ к веб-консоли через браузер Edge. • Microsoft Internet Explorer 11 (14.2.x и более ранние версии) • Mozilla Firefox версий 5.x–83 • Google Chrome 87

Компонент	Требования
База данных	Symantec Endpoint Protection Manager содержит базу данных по умолчанию: • Microsoft SQL Server Express 2014 (для Windows Server 2008 R2) • Microsoft SQL Server Express 2017 • Встроенная база данных Sybase (только 14.3 MP.x и более ранние версии) 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 (14.3 и более поздние версии) **Note:** Поддерживаются базы данных SQL Server, размещенные на Amazon RDS (на момент выхода 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	С локальной базой данных 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

Компонент	Требования
Жесткий диск при установке на другой диск	С локальной 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) 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
Другие	Включенная сетевая карта

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) (14.3 и более поздние версии) • Windows 10 20H2 (Windows 10 версия 2004) (начиная с 14.3 RU1)
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 (Server Core) (14.2 RU1 и более поздние версии) • Windows Server, версия 2004 • Windows Server, версия 20H2 (14.3 RU1)
Система предотвращения вторжений для браузера	Возможность поддержки системы предотвращения вторжений для браузера зависит от версии модуля системы обнаружения вторжений для клиента (CIDS). См. 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. **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
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.

Компонент	Требования
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	1 ГБ свободного пространства на жестком диске для установки
Экран	800 x 600
Операционная система	• macOS 10.14 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. • macOS 10.15–10.15.7 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 • 500 МБ ОЗУ • 2 ГБ дискового пространства, если для /var, /opt и /tmp используется одна и та же файловая система/том • 500 МБ дискового пространства для каждого /var, /opt и /tmp, если они находятся в разных томах
Операционные системы	Поддерживаемые операционные системы начиная с версии 14.3 RU1: • Amazon Linux 2 • CentOS 6.x, 7.x, 8.x • Oracle Enterprise Linux 6.x, 7.x, 8.x • Red Hat Enterprise Linux 6.x, 7.x, 8.x • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Поддерживаемые операционные системы для версии 14.3 и более ранних: • 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 поддерживаемых ядер операционной системы для предыдущих выпусков см. в разделе Список дистрибутивов Linux и ядер с предварительно скомпилированными драйверами или модулями автоматической защиты для Symantec Endpoint Protection для Linux 14.x.
Графические настольные среды	Для отображения клиента Symantec Endpoint Protection для Linux можно использовать следующие графические настольные среды: • KDE • Gnome • Единица В агенте Symantec для Linux 14.3 RU1 нет графического пользовательского интерфейса.

Компонент	Требования

Другие требования к среде (14.3 MP1 и более ранние версии)	• Glibc
	Ни одна операционная система под управлением glibc с версией ранее 2.6 не поддерживается.
	• net-tools или iproute2
	Symantec Endpoint Protection использует одно из этих средств в зависимости от того, что уже установлено на компьютер.
	• OpenSSL 1.0.2k-fips или более поздние версии
	• 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
	• 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`

Версии выпусков, примечания, исправления и системные требования для Endpoint Security и всех версий Endpoint Protection

Поддерживаемые и неподдерживаемые варианты обновления до последней версии Symantec Endpoint Protection 14.x

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

Версии выпусков, примечания, исправления и системные требования для Endpoint Security и всех версий Endpoint Protection

Поддерживаемые варианты обновления

- Symantec Endpoint Protection Manager версии 12.1.6 MP10 и более поздних со встроенной базой данных поддерживает свободный переход на базу данных Microsoft SQL Server Express версии 14.3 RU1. Обновление с 12.1.6 MP9 и более ранних версий до версии 14.3 RU1 заблокировано.
- Версии 12.1.x легко обновить до Symantec Endpoint Protection Manager 14.x за иключением тех компонентов, поддержка которых прекращена, например Windows Server 2003, операционные системы для настольных ПК, 32-разрядные ооперационные системы, а также некоторые версии SQL Server.
- Клиент Symantec Endpoint Protection 14.x поддерживает обновление всех предыдущих версий клиента 12.1 и 11, установленных в поддерживаемых операционных системах. Исключением является клиент Mac версий, предшествующих 12.1.4, который необходимо обновить до версии 12.1.4 или более поздней, или удалить.

Рекомендации по миграции Symantec Endpoint Protection 14

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 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 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 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 MP1

NOTE

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

Клиент Linux

NOTE
Агент Symantec для Linux 14.3 RU1 обнаруживает и удаляет более ранние версии клиента Symantec Endpoint Protection для Linux, а затем выполняет установку новой версии. Старые конфигурации не сохраняются.

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.t
- 14, 14 MP1, 14 MP2
- 14 RU1, 14 RU1 MP1, 14 RU1 MP2
- 14.2, 14.2 MP1
- 14.2 RU1, 14.2 RU1 MP1
- 14.2 RU2, 14.2 RU2 MP1
- 14.3, 14.3 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:

- Symantec AntiVirus и Symantec Client Security (не поддерживаются)
- Все продукты Norton компании Symantec
- Symantec Endpoint Protection для Windows XP Embedded 5.1
- Все версии Symantec Endpoint Protection для клиента Mac, предшествующие 12.1.4. Кроме того, его можно обновить до версии 12.1.4 или более поздней.

Примечания.

- Миграция всех версий клиентов Symantec Endpoint Protection, предшествующих 12.1.x, не поддерживается.
- Нельзя обновить Symantec Endpoint Protection Manager 11.0.x или Symantec Endpoint Protection Manager Small Business Edition 12.0.x напрямую до любой версии Symantec Endpoint Protection Manager 14. Сначала

необходимо удалить эти версии или обновить продукты до версии 12.1.x, а затем обновить их до последней 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.
- В 14.0.x прекращена поддержка Windows XP, Server 2003 и всех операционных систем Windows Embedded на базе Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 может управлять этими компьютерами как устаревшими клиентами версии 12.1.x, хотя в действительности такие клиенты больше не предоставляются. Для этих клиентов можно использовать продукты Symantec, которые по-прежнему поддерживают эти устаревшие операционные системы, например Data Center Security (DCS).
- 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 12.1.6 MP10, необходимо сначала удалить Symantec Endpoint Protection 14.2.1.
- Если у вас есть номер сборки, но вы не уверены, как он соотносится с выпущенной версией, см.: Типы и версии выпусков Endpoint Protection

Источники дополнительной информации

В следующей таблице приведен 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)
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