Руководство по работе с клиентом Symantec™ Endpoint Protection 14.3 RU1 для Mac

Ноябрь 2020 г.

Как Symantec Endpoint Protection обеспечивает защиту на компьютере Mac

Symantec Endpoint Protection — сочетание нескольких уровней защиты компьютера от атак вирусов и программ-шпионов, а также попыток вторжения.

В таблице Типы защиты описываются все уровни защиты.

Table 1: Типы информации

Защита	Описание
Защита от вирусов и программ-шпионов	Symantec Endpoint Protection включает плановые сканирования на наличие вирусов, сканирования по запросу и выполняемую в фоновом режиме автоматическую защиту, осуществляющую проверку на наличие вирусов. При обнаружении вируса Symantec Endpoint Protection избавляется от него. Принципы обеспечения защиты от вирусов и программ-шпионов на компьютерах Mac
Защита от сетевых угроз	Symantec Endpoint Protection перехватывает данные на сетевом уровне. Для сканирования пакетов или их потоков оно использует сигнатуры. Каждый пакет сканируется индивидуально и сверяется с шаблонами, соответствующими атакам на сеть или браузер. Защита от сетевых угроз включает в себя следующее: • Функцию предотвращения вторжений, которая обнаруживает атаки на уровнях приложений и компонентов операционной системы. Когда Symantec Endpoint Protection обнаруживает сетевую угрозу, осуществляется ее блокировка. • Брандмауэр, который пропускает или блокирует сетевой трафик на основании политик и правил. (Начиная с версии 14.2.) Принцип работы функции защиты от сетевых угроз на компьютерах Mac
Управление устройствами	Администраторы Symantec Endpoint Protection Manager настраивают политику управления устройствами. Политика позволяет настроить условия блокировки и разблокировки устройств по имени, поставщику, модели или серийному номеру устройства. В управляемом клиенте на вкладке **Дополнительно** находятся параметры для управления устройствами. Управление устройствами недоступно для неуправляемых клиентов. Сведения об управлении устройствами на клиенте Symantec Endpoint Protection для Mac
Endpoint Detection and Response	Администраторы Symantec Endpoint Protection Manager настраивают политику Activity Recorder, которая помогает обнаруживать подозрительную сетевую активность и сообщать о ней.

Клиент автоматически загружает на компьютер пользователя определения вирусов, определения IPS и обновления продукта.

Обновление описаний вирусов, описаний угроз для функции предотвращения вторжений, а также программного обеспечения клиента

Принципы обеспечения защиты от вирусов и программ-шпионов на компьютерах Mac

Symantec Endpoint Protection использует описания вирусов для обнаружения известных вирусов во время плановых сканирований и сканирований, выполняемых вручную. Автоматическая защита использует описания вирусов для постоянного сканирования компьютера.

Symantec Endpoint Protection отправляет пользователю уведомления в случае обнаружения вируса или другой угрозы безопасности. Обнаружение вирусов и угроз безопасности происходит в следующих случаях:

- Автоматическая защита обнаруживает вирус во время мониторинга безопасности компьютера.
- Автоматическая защита обнаруживает вирус во время планового сканирования или сканирования вручную.

По умолчанию Symantec Endpoint Protection автоматически пытается исправить найденные вирусы. Если исправление невозможно, клиент помещает файл в карантин, чтобы он вирус мог причинить вред компьютеру. Обычно для исправления не требуется никаких действий со стороны пользователя. Можно настроить отправку сведений о найденных вирусах в Symantec.

В некоторых ситуациях клиент предлагает пользователю выбрать одно из следующих действий: исправить, удалить или восстановить зараженный файл. Затем клиент обрабатывает зараженный файл соответствующим образом.

Реагирование на сообщения об обнаружении заражений и угроз

Включение и отключение отправки сведений о безопасности в Symantec

Принцип работы функции защиты от сетевых угроз на компьютерах Mac

Защита от сетевых угроз включает в себя следующие технологии:

- Предотвращение вторжений
- Брандмауэр

Предотвращение вторжений

Система предотвращения вторжений автоматически выявляет и блокирует атаки на сеть. Предотвращение вторжений — это внутренний уровень защиты клиентских компьютеров. Функцию предотвращения вторжений иногда называют системой предотвращения вторжений (IPS).

Предотвращение вторжений перехватывает данные на сетевом уровне. Для сканирования пакетов или их потоков оно использует сигнатуры. Каждый пакет сканируется индивидуально и сверяется с шаблонами, соответствующими атакам на сеть или браузер. Функция предотвращения вторжений обнаруживает атаки на уровнях приложений и операционной системы.

Для идентификации атак на клиентские компьютеры система предотвращения вторжений использует сигнатуры. Для известных атак система предотвращения вторжений автоматически отбрасывает пакеты, соответствующие сигнатурам.

Брандмауэр

Брандмауэр отслеживает сетевой трафик и блокирует потенциально вредоносный трафик для защиты Mac. Брандмауэр Symantec Endpoint Protection недоступен на неуправляемом клиенте.

Брандмауэр Symantec Endpoint Protection отслеживает трафик на транспортном и межсетевом уровнях. Встроенный брандмауэр Mac отслеживает трафик на более высоком уровне — уровне приложений — после брандмауэра Symantec Endpoint Protection, поэтому можно настроить параллельную работу обоих брандмауэров.

Для разрешения или блокирования сетевого трафика в брандмауэре служат следующие типы правил.

- Правила по умолчанию
- Пользовательские правила
- Встроенные правила
- Правила защиты

Эти правила включают в себя сканирование портов, определение отказов в обслуживании, защиту от имитации MAC-адреса, Smart DHCP и Smart DNS. Настройки брандмауэра полностью контролируются администратором

Symantec Endpoint Protection Manager. Включить или отключить брандмауэр можно, только если администратор разрешил пользователю управление Mac с помощью клиента.

Защита брандмауэра добавлена в версии 14.2.

Управление предотвращением вторжений

Управление защитой клиента Mac с помощью брандмауэра

Совместимость операционной системы с Symantec Endpoint Protection для Mac

Symantec Endpoint Protection для Mac поддерживает следующие версии операционной системы:

- macOS 10.15–10.15.5
- macOS 10.14
- macOS 10.13

Дополнительную информацию о поддержке более ранних версий операционной системы см. в документе Совместимость Mac с клиентом Endpoint Protection.

Сведения об авторизации расширений ядра Symantec Endpoint Protection для macOS 10.13 или более поздней версии

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

Установка клиента Symantec Endpoint Protection для Mac

Если вы не можете или не хотите использовать принудительную отправку, можно установить клиент Symantec Endpoint Protection непосредственно на компьютер Mac. Действия по установке неуправляемых и управляемых клиентов аналогичны.

Единственный способ установить управляемый клиент — это использовать пакет, созданный с помощью Symantec Endpoint Protection Manager. Можно в любое время преобразовать неуправляемый клиент в управляемый клиент. Для этого необходимо импортировать параметры связи клиент-сервер на клиент Mac.

NOTE
Сведения о том, как подготовить клиент Symantec Endpoint Protection для Mac для использования совместно с программным обеспечением сторонних производителей для удаленного развертывания, см. в разделе Экспорт и развертывание клиента Symantec Endpoint Protection с помощью Apple Remote Desktop или Casper.

Table 2: Способы установки клиента для Mac

Если загружен файл установки.	1. Извлеките содержимое в папку на устройстве Mac и откройте ее. 2. Откройте папку `SEP_MAC`. 3. Скопируйте файл `Symantec Endpoint Protection.dmg` на рабочий стол компьютера Mac. 4. Дважды щелкните файл `Symantec Endpoint Protection.dmg`, чтобы смонтировать его в качестве виртуального диска. Затем установите клиент Symantec Endpoint Protection для Mac.
Если есть пакет установки клиента в формате .zip, загруженный с портала поддержки Broadcom.	1. Скопируйте файл на рабочий стол компьютера Mac. Файл может называться `Symantec Endpoint Protection.zip` или `Symantec_Endpoint_Protection_версия_Mac_Client.zip`, гдеверсияобозначает версию продукта. 2. Чтобы извлечь содержимое файла, щелкните его правой кнопкой мыши и выберите пункт **Открыть с помощью > Утилита для работы с архивами**. 3. Откройте папку с распакованным содержимым архива. Затем установите клиент Symantec Endpoint Protection для Mac.

Получившийся в результате образ виртуального диска или папка содержит программу установки приложения и папку с именем Additional Resources. Для успешной установки они должны быть размещены в одном и том же расположении. При копировании программы установки в другое расположение следует также скопировать папку Additional Resources.

Установка клиента Symantec Endpoint Protection для Mac

1. Дважды щелкните `Установить Symantec Endpoint Protection`.
2. Чтобы начать установку, щелкните **Установить**.
3. Чтобы установить вспомогательный инструмент, необходимый для установки клиента Symantec Endpoint Protection, введите имя пользователя и пароль администратора Mac, а затем нажмите **Установить**.
4. После установки нажмите **Продолжить**, чтобы завершить настройку клиента Symantec Endpoint Protection.
5. Для настройки клиента Symantec Endpoint Protection выполните следующие действия.

Выполните авторизацию расширения системы Symantec Endpoint Protection.	В диалоговом окне **Безопасность и конфиденциальность** на вкладке **Общие** выберите в пункте **Загрузка системного ПО программы "Symantec Endpoint Protection" была заблокирована** вариант **Разрешить**. При необходимости нажмите значок блокировки, чтобы внести изменения. Для работы всех функций системного расширения Symantec Endpoint Protection необходима авторизация. Сведения об авторизации расширений системы Symantec Endpoint Protection для macOS 10.15 или более поздней версии
Разрешите полный доступ к диску.	В диалоговом окне **Безопасность и конфиденциальность** на вкладке **Конфиденциальность** проверьте, разрешен ли **системному расширению Symantec** доступ к данным и параметрам администрирования для всех пользователей этого устройства Mac. При необходимости нажмите значок блокировки, чтобы внести изменения.
Разрешите внесение изменений в сетевой профиль.	Когда откроется окно с сообщением **Symantec Endpoint Protection запрашивает разрешение фильтровать сетевой трафик**, нажмите **Разрешить**.

6. Нажмите **Завершить**.

Сведения об авторизации расширений системы Symantec Endpoint Protection для macOS 10.15 или более поздней версии

Запрос авторизации расширений системы — это новый компонент безопасности, добавленный в macOS 10.15.Для работы всех функций системного расширения Symantec Endpoint Protection необходима авторизация.

Чтобы авторизовать расширение системы для Symantec Endpoint Protection, во время настройки клиента Symantec Endpoint Protection в диалоговом окне **Security & Privacy** на вкладке **Общие** в разделе **Загрузка системного ПО программы "Symantec Endpoint Protection" была заблокирована**, нажмите **Разрешить**.

Установка клиента Symantec Endpoint Protection for Mac

Запрос обновления для клиента Symantec Endpoint Protection для Mac

Администраторы Symantec Endpoint Protection Managerмогут назначить автоматическое обновление управляемых клиентских компьютеров с помощью пакета установки клиента при использовании параметров для установки клиента.

При выполнении входа на Mac вы можете получить запрос на перезагрузку для завершения установки. Можно отложить перезагрузку компьютера на основании параметров установки клиента.

Если вход на Mac не выполнен, компьютер Mac будет автоматически перезагружен в ходе установки.

Начало работы с клиентом Symantec Endpoint Protection

Если нет проблем, требующих действий пользователя, при открытии клиента Symantec Endpoint Protection в верхней части страницы отображается сообщение **Защита активирована**. При наличии неполадок нажмите кнопку **Исправить**.

В клиенте Symantec Endpoint Protection отображаются основные задачи, которые можно выполнить.

Table 3: Страницы клиента Symantec Endpoint Protection

Параметр	Описание
Безопасность	Отображение состояния системы защиты компьютера.
Сканирование	Сканирование компьютера. Можно выбрать тип сканирования: быстрое или полное. Можно также перетащить файл или папку для сканирования. Выполнение сканирования вручную
LiveUpdate	Запускает LiveUpdate для обновления описаний и файлов Symantec Endpoint Protection. Немедленное обновление содержимого в Symantec Endpoint Protection
Дополнительно	Позволяет настроить дополнительные параметры защиты от вирусов и программ-шпионов, защиты от сетевых угроз и LiveUpdate.

Управление защитой компьютера Mac с помощью Symantec Endpoint Protection

Настройки по умолчанию в клиенте Symantec Endpoint Protection обеспечивают защиту компьютера от многих типов вредоносных программ. Клиент обрабатывает вредоносные программы автоматически либо предоставляет пользователю возможность выбрать нужное действие.

В зависимости от настроек администратора, пользователю могут быть доступны следующие задачи для управления защитой.

NOTE
Администратор может разрешить или запретить пользователям выполнять эти задачи.

Table 4: Защита компьютера

Шаги	Описание
Шаг 1. Убедитесь, что на компьютере включены оба компонента: защита от вирусов и программ-шпионов и защита от сетевых угроз.	Если защита активна, на странице **Безопасность** будут показаны зеленая галочка и сообщение **Защита активирована**. Включение и выключение защиты от вирусов и программ-шпионов Включение и отключение защиты от сетевых угроз
Шаг 2. Убедитесь, что на компьютере установлены последние версии программного обеспечения и описаний.	На странице **Безопасность** отображается время последнего обновления описаний для компонентов защиты от вирусов и программ-шпионов и защиты от сетевых угроз. Время последнего обновления файлов продукта отображается в разделе **LiveUpdate**. Чтобы увидеть номер версии программного обеспечения, нажмите **Справка > О программе**.
Шаг 3. При необходимости обновите программное обеспечение или описания.	Для немедленного обновления ПО и описаний перейдите в клиент Symantec Endpoint Protection и нажмите **LiveUpdate**. Обновление описаний вирусов, описаний угроз для функции предотвращения вторжений, а также программного обеспечения клиента
Шаг 4. Выполните сканирование.	Сканирование можно запустить немедленно или настроить расписание через регулярные промежутки времени. Настройка плановых сканирований Выполнение сканирования вручную

Параметры защиты от вирусов и программ-шпионов

Продление лицензии на продукт

Под значком клиента Symantec Endpoint Protection в строке меню может появиться сообщение о том, что срок действия лицензии на Symantec Endpoint Protection истек. Клиент Symantec Endpoint Protection использует лицензию для обновления следующих компонентов:

- Клиентское программное обеспечение
- Файлы описания защиты для сканирования на наличие вирусов и шпионских программ и предотвращения вторжений

В клиенте можно использовать лицензии двух типов: пробные и оплаченные. Если срок действия какой-либо из лицензий истекает, клиент не может обновить описания и программное обеспечение.

При любом типе лицензии следует обратиться к администратору для ее обновления или продления.

Реагирование на сообщения об обнаружении заражений и угроз

Включение и отключение управления устройством Mac в клиенте Symantec Endpoint Protection

Администраторы Symantec Endpoint Protection Manager могут настроить управляемые клиенты с помощью политики управления устройствами. Политика позволяет настроить условия блокировки и разблокировки устройств по имени, поставщику, модели или серийному номеру устройства.

Действия по управлению устройствами можно просмотреть на странице **Дополнительно**, нажав **Операции > Журнал безопасности**.

С помощью настроек управления устройствами, доступных в клиенте Symantec Endpoint Protection, можно включить или отключить **управление устройствами**. Если управление устройствами включено, можно дополнительно включить уведомления о блокировке или разблокировке устройств.

Для изменения параметров необходимо ввести учетные данные администратора Mac. Если параметры отображаются серым цветом, это означает, что администратор запретил пользователям включать и отключать данную функцию.

Добавление или изменение устройств для блокировки и разблокировки невозможно через интерфейс клиента Symantec Endpoint Protection.

> **NOTE**
> Параметры управления устройствами контролируются соответствующей политикой Symantec Endpoint Protection Manager. Со следующим контрольным сигналом все изменения, внесенные в эти параметры, будут переопределены текущими значениями политики.

Управление устройствами недоступно для неуправляемых клиентов.

О перенаправлении трафика WSS для клиентов Mac

С помощью перенаправления трафика (WTR) Web Security Service (WSS) можно автоматизировать перенаправление веб-трафика в Symantec Web Security Service и защитить веб-трафик на каждой конечной точке, которая использует Symantec Endpoint Protection.

Администратор управляет параметрами, которые использует перенаправление трафика WSS, включая URL-адрес конфигурации прокси-сервера и дополнительный корневой сертификат службы Symantec Web Security Service. Только администратор Symantec Endpoint Protection Manager может настроить эти параметры, которые не отображаются в интерфейсе клиента Symantec Endpoint Protection. Вы можете просмотреть URL файла конфигурации прокси-сервера на компьютере Mac в меню **Системные настройки > Сеть** в разделе **Прокси**. Сертификат облачных служб отображается в **цепочке ключей**.

Перенаправление трафика WSS поддерживается в веб-браузерах Safari, Chrome и Firefox версии 65 и более поздних. Версии Symantec Endpoint Protection, предшествующие 14.2 RU1, поддерживают только Safari и Chrome.

Удаление клиента Symantec Endpoint Protection для Mac

Для удаления клиента Symantec Endpoint Protection для Mac необходимо нажать значок клиента в строке меню. Клиент Symantec Endpoint Protection для Mac можно удалить при наличии прав администратора.

> **NOTE**
> После удаления клиента Symantec Endpoint Protection будет предложено перезапустить клиентский компьютер для завершения процедуры удаления. Перед началом процедуры сохраните все открытые файлы и закройте запущенные приложения.

Как удалить клиент Symantec Endpoint Protection для Mac

1. Откройте клиент Symantec Endpoint Protection на клиентском компьютере Mac и нажмите **Symantec Endpoint Protection > Удалить Symantec Endpoint Protection**.
2. Нажмите кнопку **Удалить** еще раз, чтобы начать удаление.
3. Чтобы установить вспомогательный инструмент, необходимый для удаления клиента Symantec Endpoint Protection, введите имя пользователя и пароль администратора Mac, а затем нажмите **Установить**.
4. В диалоговом окне **Symantec Endpoint Protection is trying to modify a System Extension** введите имя пользователя и пароль администратора Mac и нажмите **ОК**.

   Возможно, потребуется ввести пароль для удаления клиента. Этот пароль может отличаться от пароля администратора на вашем компьютере Mac.
5. После завершения процедуры удаления нажмите **Перезагрузить**.

В случае сбоя удаления, возможно, потребуется использовать другой способ удаления. См. следующую статью базы знаний:

Удаление Symantec Endpoint Protection

Обновление описаний вирусов, описаний угроз для функции предотвращения вторжений, а также программного обеспечения клиента

Чтобы продукты Symantec обеспечивали защиту компьютера от всех новых типов атак, им необходимо регулярно предоставлять свежую информацию. Компания Symantec предоставляет эту информацию Symantec Endpoint Protection с помощью функции LiveUpdate. Функция LiveUpdate загружает обновления продуктов и описаний на компьютер по соединению с Интернетом.

Обновления описаний — это файлы, обеспечивающие использование в продуктах Symantec новейших технологий защиты от угроз. LiveUpdate извлекает новые сигнатуры для предотвращения вторжений или файлы описаний вирусов с веб-сайта Symantec и затем заменяет ими старые файлы.

Обновления продуктов — это усовершенствования для установленного клиента. Обычно обновления продуктов применяются для улучшения совместимости с операционной системой и оборудованием, повышения производительности или исправления ошибок. Обновления продукта выпускаются по мере необходимости. Клиент получает обновления напрямую с сервера LiveUpdate. Обновления продуктов и описаний вместе называются обновлениями содержимого.

Table 5: Способы обновления содержимого на компьютере

Задача	Описание
Немедленное обновление содержимого	Запустить LiveUpdate можно немедленно. Немедленное обновление содержимого в Symantec Endpoint Protection

Управление защитой компьютера Mac с помощью Symantec Endpoint Protection

Немедленное обновление содержимого в Symantec Endpoint Protection

Функция LiveUpdate позволяет немедленно обновлять описания и файлы продукта. В следующих ситуациях LiveUpdate требуется запускать вручную:

- Клиентское ПО установлено недавно.
- Прошло много времени с момента последнего сканирования.
- Предполагается наличие вируса или другого вредоносного ПО.

Как выполнить немедленное обновление содержимого в Symantec Endpoint Protection

Запустите LiveUpdate одним из следующих способов:

- Нажмите значок Symantec Endpoint Protection на панели меню и выберите **LiveUpdate**.
- Откройте клиент Symantec Endpoint Protection и нажмите **LiveUpdate**.

Программа LiveUpdate подключается к заданному серверу Symantec, проверяет наличие обновлений, а затем автоматически загружает и устанавливает их. Ход загрузки отображается в строке состояния.

Обновление описаний вирусов, описаний угроз для функции предотвращения вторжений, а также программного обеспечения клиента

Обновление содержимого Symantec Endpoint Protection по расписанию

Расписания на управляемых клиентах Mac

По умолчанию управляемые клиенты Mac получают расписание из Symantec Endpoint Protection Manager, согласно которому LiveUpdate запускается каждые четыре часа. Расписание настраивается администратором Symantec Endpoint Protection Manager. Управляемые клиенты не могут создать новое расписание, а также не могут удалить, изменить или просмотреть расписание, созданное администратором.

Расписания на неуправляемых клиентах Mac

Сеансы LiveUpdate можно выполнять автоматически по заданному расписанию. Запуск LiveUpdate можно запланировать на то время, когда компьютер не используется.

Как настроить обновление содержимого Symantec Endpoint Protection по расписанию

1. В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Настройки продукта**, а затем значок настроек **Scheduled LiveUpdate**.

   Будет показано текущее расписание.

2. Выберите интервал времени в раскрывающемся меню Расписание LiveUpdate.

   По умолчанию программа выполняется каждые **4** часа. Помимо стандартного значения можно выбрать **Ежедневно** или **Еженедельно** и указать время или день и время соответственно.

3. Нажмите кнопку **Применить изменения**.

Немедленное обновление содержимого в Symantec Endpoint Protection

Обновление описаний вирусов, описаний угроз для функции предотвращения вторжений, а также программного обеспечения клиента

Сведения о подключении к серверу управления через прокси-сервер

Вам может быть предложено разрешить Symantec Endpoint Protection использовать учетные данные для подключения к серверу управления через прокси-сервер. Сообщение содержит запрос на разрешение процессу `symdaemon` использовать ваши учетные данные.

Нажмите **Всегда разрешать** в этом сообщении. В противном случае это сообщение будет отображаться при каждом подключении клиента к серверу LiveUpdate. Если нажать кнопку **Запретить**, клиент не сможет получать обновления программного обеспечения и описаний.

Обновление описаний вирусов, описаний угроз для функции предотвращения вторжений, а также программного обеспечения клиента

Параметры защиты от вирусов и программ-шпионов

По умолчанию Symantec Endpoint Protection обеспечивает защиту от вирусов и угроз безопасности, включая сетевые угрозы, сразу после запуска компьютера. Автоматическая защита, входящая в состав системы защиты от вирусов и программ-шпионов, проверяет программы на наличие вирусов во время их работы. Кроме того, она регистрирует все операции, которые могут указывать на наличие вируса или угрозы безопасности. Автоматическая защита препятствует заражению компьютера, поэтому ее не следует отключать.

Для управляемых клиентов объем вашего контроля над этими параметрами зависит от того, как администратор настроил клиент. Кроме того, все изменения, внесенные в эти параметры, могут быть переопределены текущими значениями политики со следующим контрольным сигналом.

В разделе Управление защитой от вирусов и программ-шпионов описываются задачи, помогающие управлять защитой Mac от соответствующих угроз.

Table 6: Управление защитой от вирусов и программ-шпионов

Шаги	Описание
Шаг 1. Включите или отключите защиту от вирусов и программ-шпионов	Выключить/отключить защиту от вирусов и программ-шпионов очень просто. Компания Symantec рекомендует оставить эту функцию включенной. Включение и выключение защиты от вирусов и программ-шпионов
Шаг 2. Настройте параметры автоматической защиты	Автоматическая защита является важным компонентом системы защиты от вирусов и программ-шпионов. Эти параметры можно настроить на странице **Дополнительно**. Настройка параметров автоматической защиты и параметров зоны сканирования
Шаг 3. Настройте сканирование компьютера на наличие вирусов	Можно настроить расписание сканирования или запустить сканирование немедленно. Настройка плановых сканирований Приостановка, перенос и остановка сканирований Выполнение сканирования вручную
Шаг 4. Выполните необходимые действия при обнаружении вируса программой Symantec Endpoint Protection	Во время выполнения сканирования компьютера Symantec Endpoint Protection может: • Сообщать о действиях, которые вы можете предпринять. • Сообщать о мерах защиты, предпринятых программой. Реагирование на сообщения об обнаружении заражений и угроз

Включение и выключение защиты от вирусов и программ-шпионов

По умолчанию защита от вирусов и программ-шпионов включена, как и автоматическая защита.

Настроив нужные параметры, можно добиться более точного управления автоматической защитой.

Если защита от вирусов и программ-шпионов выключена, то на странице **Состояние** показывается красный крестик и сообщение **Защита от вирусов и программ-шпионов выключена**. Если защита отключена, ее следует включить как можно быстрее.

> **NOTE**
> Запланированные сканирования будут выполняться вне зависимости от состояния защиты от вирусов и программ-шпионов. Администратор может ограничить доступ к некоторым параметрам Symantec Endpoint Protection. Так, вам может быть недоступно отключение этих параметров, планирование

сканирований или настройка параметров защиты.Для изменения любого из этих параметров может потребоваться указать пароль администратора Mac.

Как включить или отключить защиту от вирусов и программ-шпионов

1. Чтобы включить защиту от вирусов и программ-шпионов, в клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Protect My Mac** и включите **Автоматическое сканирование**.
2. Чтобы отключить защиту от вирусов и программ-шпионов, в клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Protect My Mac** и выключите **Автоматическое сканирование**.

Настройка параметров автоматической защиты и параметров зоны сканирования

Параметры защиты от вирусов и программ-шпионов

Реагирование на сообщения об обнаружении заражений и угроз

Настройка параметров автоматической защиты и параметров зоны сканирования

На управляемых клиентах, если администратор позволяет вам, можно настроить способ контроля за вирусами и исправления зараженных файлов функцией автоматической защиты.

Настройки автоматической защиты отображаются в качестве опций в разделе **Protect My Mac**. Для использования автоматической защиты нужно включить **Автоматическое сканирование**.

Scan Zone Settings позволяют указать файлы, которые необходимо включить в сканирование или исключить из него.

Как настроить параметры автоматической защиты

1. В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Protect My Mac**, а затем значок настроек **Автоматическое сканирование**.
2. Внесите изменения для одного из следующих параметров:

Поместить в карантин автоматически	Можно автоматически помещать в карантин все файлы, которые не удается исправить.
Исправить автоматически	Найденные зараженные файлы будут исправляться автоматической защитой.
Сканирование	Можно выбрать **Data Disks** или **All other disks**.
Сканировать сжатые файлы	Сканирование автоматической защиты может включать также сжатые файлы. В сканирование будут включены сжатые файлы и файлы внутри сжатых файлов.

WARNING
Если параметр **Исправить автоматически** не выбран, то зараженные файлы не будут помещаться в карантин, даже если включен параметр **Поместить в карантин автоматически**. Программа спросит, требуется ли исправить зараженный файл. Если файл не будет исправлен, то он останется на компьютере. Если параметр **Исправить автоматически** выбран, а параметр **Поместить в карантин автоматически** не выбран, зараженные файлы будут удаляться.

3. Нажмите кнопку **Готово**.

Как настроить параметры зоны сканирования

1. В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Protect My Mac**, а затем значок **Scan Zone Settings**.
2. Внесите изменения для одного из следующих параметров:

Сканировать все	Все файлы и процессы на вашем компьютере сканируются по мере доступа к ним.
Только сканирование	При сканировании проверяются только указанные пользователем файлы и папки.
Не сканировать	При сканировании проверяются все указанные пользователем файлы и папки кроме тех, что были исключены из сканирования.
Использовать по умолчанию	При выборе этого параметра производится сканирование всех разделов.

3. Нажмите кнопку **ОК**.

Принципы обеспечения защиты от вирусов и программ-шпионов на компьютерах Mac

Включение и выключение защиты от вирусов и программ-шпионов

Работа с файлами, помещенными в карантин

Настройка плановых сканирований

При использовании управляемого клиента Symantec Endpoint Protection автоматически выполняет сканирование по умолчанию. Если это разрешено администратором, можно настроить дополнительные плановые сканирования.

> **NOTE**
> На неуправляемых клиентах необходимо запускать пользовательские сканирования. Symantec рекомендует как можно скорее вручную запустить полное сканирование, а затем настроить обычное плановое сканирование. Вы можете приостановить или отложить любые сканирования, включая плановые и сканирования вручную.

На управляемых клиентах сканирование по умолчанию запускается ежедневно в 20:00 с включенной функцией автоматического исправления.

Выполнение сканирования вручную

Как настроить плановые сканирования

1. В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Protect My Mac**, а затем значок настроек **Плановые сканирования**.
2. В диалоговом окне нажмите **Добавить плановое сканирование** или выберите текущее плановое сканирование и нажмите **Изменить**, чтобы настроить его параметры.
3. На вкладке **Элементы сканирования** можно настроить следующие параметры:

Диски	Можно указать, включать **жесткие диски** и **съемные носители** в сканирование или нет.
Папки	Для сканирования можно выбрать следующие папки файлов: **Домашняя папка (активный пользователь)**, **Приложения** и **Библиотека**. Если на момент планового сканирования папки «Личное» в систему компьютера не вошел ни один пользователь, сканирование не будет выполнено.

Параметры сканирования	Можно выбрать один из следующих вариантов. • **Сканировать сжатые файлы** • **Исправить автоматически** • **Поместить в карантин автоматически** • **Включить сканирование во время простоя**

4. На вкладке **Расписание сканирования** можно настроить следующие параметры:

Расписание сканирования	Сканирование можно настроить таким образом, чтобы оно выполнялось с определенными временными интервалами: ежедневно, еженедельно или ежемесячно. Параметр **Выполнять через регулярные промежутки времени** выбирается по умолчанию при внесении нового сканирования в расписание.
Частота запуска	Этот параметр доступен, если в разделе **Расписание сканирования** установлен флажок **Выполнять через регулярные промежутки времени**.
Время начала	Доступно при выборе одного из вариантов расписания сканирования: **Ежедневно**, **Еженедельно** или **Ежемесячно**. Позволяет выбрать время суток для выполнения сканирования. Рекомендуется выбирать время, когда компьютер не используется, так как сканирование может снижать быстродействие системы.
Вкл.	Доступно при выборе одного из следующих вариантов расписания сканирования: **Еженедельно** или **Ежемесячно**. Позволяет выбрать день недели или месяца для выполнения сканирования. Рекомендуется выбирать время, когда компьютер не используется, так как сканирование может снижать быстродействие системы.

5. На вкладке **Настройка** можно настроить оптимизацию производительности сканирования.
6. Нажмите кнопку **ОК**.
7. Нажмите кнопку **Готово**.

Приостановка, перенос и остановка сканирований

Управление защитой компьютера Mac с помощью Symantec Endpoint Protection

Реагирование на сообщения об обнаружении заражений и угроз

Включение и отключение отправки сведений о безопасности в Symantec

Выполнение сканирования вручную

Может возникнуть необходимость просканировать некоторые файлы вручную. Например, вам может потребоваться просканировать файлы, сохраненные на ваш компьютер до установки Symantec Endpoint Protection. Или же вы решите, что какой-то файл, который был исключен из планового сканирования, необходимо просканировать.

> **NOTE**
> Вы можете приостановить или отложить любое сканирование, включая плановые сканирования и сканирования вручную.

Как выполнить сканирование вручную

На клиенте Symantec Endpoint Protection на странице **Сканирования** выполните одно из следующих действий:

- Чтобы начать быстрое сканирование, нажмите **Быстрое сканирование**, а затем **Начать быстрое сканирование**.
- Чтобы начать полное сканирование, нажмите **Полное сканирование**, а затем **Начать полное сканирование**.
- Чтобы сканировать файл или папку, нажмите **Сканирование файлов**, а затем **Выбрать файл**.Откроется программа Finder, где можно выбрать **Show Hidden Files** или **Scan Compressed Files**. Можно также включить параметры **Исправить автоматически** и **Поместить в карантин автоматически**.

Приостановка, перенос и остановка сканирований

Настройка плановых сканирований

Включение и отключение отправки сведений о безопасности в Symantec

Приостановка, перенос и остановка сканирований

Функция приостановки позволяет остановить сканирование в любой момент, чтобы продолжить его позже. Любое сканирование можно остановить или отменить по выбору пользователя. Для использования этих функций не требуются права администратора.

После возобновления сканирование будет продолжено с того же места.

> **NOTE**
> Если сканирование приостанавливается в момент проверки сжатого файла, то клиент может выполнить запрос о приостановке с задержкой в несколько минут.

Если включена команда Отложить, сканирование можно отложить, но только до того, как оно начнется. Невозможно отложить сканирование в процессе его выполнения.

Как приостановить или остановить плановое сканирование

1. В диалоговом окне хода сканирования выберите пункт **Приостановить**.
2. Для продолжения сканирования выберите в диалоговом окне хода выполнения пункт **Возобновить**, а для остановки сканирования — пункт **Остановить**. Чтобы закрыть окно, можно нажать **Готово**.

Как приостановить или остановить сканирование, выполняемое вручную

1. В диалоговом окне хода сканирования выберите пункт **Приостановить**.
2. Нажмите **Отмена**, чтобы остановить сканирование, запущенное вручную, или **Возобновить**, чтобы продолжить сканирование.

Как отложить сканирование, которое скоро начнется

1. В появившемся окне нажмите на раскрывающееся меню, чтобы выбрать значение для команды «Отложить». Минимальное время, на которое можно отложить сканирование, составляет 15 минут, максимальное — сутки.
2. Нажмите **ОК**, чтобы отложить сканирование.

   Для выполнения плановых сканирований от вас не требуется никаких действий.

Настройка плановых сканирований

Выполнение сканирования вручную

Реагирование на сообщения об обнаружении заражений и угроз

Можно проверить, заражен ли компьютер, и выполнить ряд дополнительных задач, чтобы повысить уровень безопасности или быстродействие.

Вы можете использовать клиент, который управляется администратором, или неуправляемый клиент. Задачи защиты, которые вы можете выполнять, зависят от степени контроля вашего администратора над клиентом.

Если продукт Symantec Endpoint Protection обнаружит вирус или угрозу безопасности, от вас могут потребоваться определенные действия по их устранению. Исходя из выбираемых администратором настроек вы можете получать уведомление о действиях, выполняемых клиентом автоматически.

Table 7: Реагирование на сообщения о заражениях

Содержимое сообщения	Требуется действие
Исправлен зараженный файл	Нет
Запрашивает подтверждение на исправление зараженного файла	Утвердить исправление. Этот параметр зависит от настроек автоматической защиты. Параметры защиты от вирусов и программ-шпионов Если параметр автоматического исправления зараженных файлов не выбран, необходимо исправить файл вручную. Исправление зараженных файлов
Исправление зараженного файла невозможно	Управляйте заражениями в карантине. Работа с файлами, помещенными в карантин

Принципы обеспечения защиты от вирусов и программ-шпионов на компьютерах Mac

Исправление зараженных файлов

Если зараженный файл не заменяется или не помещается в карантин автоматически, можно исправить файл в списке результатов сканирования. Можно исправить файлы на жестком диске компьютера или съемном носителе вручную.

Как исправлять зараженные файлы

1. В списке результатов сканирования выберите файл для исправления и нажмите **Исправить**.

   Можно также щелкнуть правой кнопкой мыши любой файл в меню Mac **Finder** или **Поиск**.
2. Повторите по мере необходимости.
3. Выполните еще одно сканирование для проверки на другие зараженные файлы.
4. Проверьте исправленные файлы, чтобы убедиться в правильности их работы.

Параметры защиты от вирусов и программ-шпионов

Работа с файлами, помещенными в карантин

Работа с файлами, помещенными в карантин

По умолчанию клиент пытается удалить найденный вирус. Если удалить файл не удается, файл помещается в карантин локального компьютера. Когда Symantec Endpoint Protection обнаруживает угрозу безопасности, файл сразу же помещается в карантин. Затем выполняются действия по устранению всех побочных эффектов угрозы.

После обновления описаний вирусов клиент автоматически проверяет файлы в карантине. Файлы в карантине можно просканировать повторно. Новые описания могут содержать средства очистки или исправления файлов, уже находящихся в карантине.

Как работать с файлами, помещенными в карантин

1. В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Операции > Журнал безопасности > Карантин**.
2. Выберите требуемый файл, затем выберите действие:

Исправить	Позволяет исправить файл, помещенный в карантин. Убедитесь, что описания вирусов были созданы позднее, чем файл был помещен в карантин.
Удалить	Позволяет удалить из карантина файлы, которые больше не нужны.
Восстановить	Позволяет восстановить файл, в безопасности которого вы уверены, в исходном расположении на компьютере. При этом ни сканирование, ни исправление не выполняются.

Реагирование на сообщения об обнаружении заражений и угроз

Включение и отключение отправки сведений о безопасности в Symantec

Symantec Endpoint Protection может отправлять псевдонимизированную информацию об обнаруженных угрозах в Symantec. Symantec использует эти сведения для защиты клиентских компьютеров от новых, целенаправленных и меняющихся угроз. Все переданные пользователем данные расширяют возможности Symantec в борьбе с угрозами и оптимизируют защиту компьютера пользователя.

Данные, собираемые телеметрией Symantec, могут содержать псевдонимизированные элементы, которые не являются личными сведениями. Symantec не использует данные телеметрии для определения личности пользователя.

Клиентский компьютер по умолчанию отправляет информацию об обнаруженных угрозах в Symantec. Отправку сведений можно отключить, однако Symantec не рекомендует отключать данную функцию.

Отправляются только сведения о найденных вирусах.

NOTE
Компания Symantec рекомендует оставить эту функцию включенной.

Как включить или отключить отправку псевдонимизированных сведений о безопасности в Symantec

В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Настройки продукта** и включите/выключите параметр **Security Info Submission**.

Настройка плановых сканирований

Выполнение сканирования вручную

Управление предотвращением вторжений

Параметры предотвращения вторжений по умолчанию обеспечивают защиту клиента Mac. Однако при необходимости систему предотвращения вторжений можно настроить как компонент защиты от сетевых угроз.

Table 8: Управление предотвращением вторжений

Шаги	Описание
Шаг 1. Изучите информацию о предотвращении вторжений.	Изучите принципы, используемые системой предотвращения вторжений для обнаружения и блокирования атак на сеть. Принцип работы функции защиты от сетевых угроз на компьютерах Mac
Шаг 2. Загрузите актуальные сигнатуры IPS.	По умолчанию в клиент загружаются самые актуальные сигнатуры. Однако загрузку сигнатур можно выполнить немедленно. Немедленное обновление содержимого в Symantec Endpoint Protection
Шаг 3. Включите или выключите систему предотвращения вторжений.	Выключение системы предотвращения вторжений может потребоваться во время устранения неполадок или в случае чрезмерного количества ложных срабатываний защиты на клиентских компьютерах. В общем случае рекомендуется не отключать систему предотвращения вторжений. Включение и отключение защиты от сетевых угроз
Шаг 4. Включите уведомления системы предотвращения вторжений.	Можно настроить показ уведомлений при обнаружении атаки в Symantec Endpoint Protection. Включение и отключение уведомлений системы защиты от сетевых угроз

Управление защитой клиента Mac с помощью брандмауэра

Брандмауэр Symantec Endpoint Protection для Mac обеспечивает полную интеграцию с возможностями Symantec Endpoint Protection, включая события, политики и команды. Брандмауэр Symantec Endpoint Protection доступен только для управляемых клиентов.

NOTE
Брандмауэр Symantec Endpoint Protection для Mac не интегрируется со встроенным брандмауэром операционной системы. Вместо этого он работает параллельно. Брандмауэр операционной системы выполняет проверку на уровне приложения, а брандмауэр Symantec Endpoint Protection выполняет проверку на более низких уровнях (IP и транспортном).Брандмауэр Symantec Endpoint Protection для Mac не обеспечивает выполнение правил блокировки одноранговых узлов, но их можно частично настроить с помощью пользовательских правил брандмауэра.

Table 9: Управление защитой с помощью брандмауэра

Шаги	Описание
Шаг 1. Изучите документацию по защите с помощью брандмауэра.	Узнайте, как средства защиты брандмауэра отслеживают трафик и защищают от распространенных атак. Принцип работы функции защиты от сетевых угроз на компьютерах Mac
Шаг 2. Включите или отключите брандмауэр.	Возможно, потребуется отключить брандмауэр для устранения неполадок, например, если блокируется трафик, который должен быть разрешен. В остальных случаях брандмауэр не следует отключать. Включение и отключение защиты от сетевых угроз

Включение и отключение защиты от сетевых угроз

Обычно выключение компонентов защиты от сетевых угроз снижет уровень безопасности компьютера. Но можно отключить функцию предотвращения вторжения, чтобы избежать ложных срабатываний, или отключить брандмауэр, чтобы избежать проблем, вызванных блокировкой трафика. Предотвращение вторжений и брандмауэр — это компоненты системы защиты от сетевых угроз.

Для управляемых клиентов объем вашего контроля над этими параметрами зависит от того, как администратор настроил клиент. Кроме того, все изменения, внесенные в эти параметры, могут быть переопределены текущими значениями политики со следующим контрольным сигналом.

Брандмауэр нельзя использовать в неуправляемых клиентах.

Как включить или отключить защиту от сетевых угроз

1. В клиенте Symantec Endpoint Protection на странице **Дополнительно** нажмите **Защита от сетевых угроз**.
2. Включить или отключить функцию **Предотвращение вторжений** можно с помощью соответствующего параметра.
3. Используйте параметр **Брандмауэр**, чтобы включить или отключить соответствующую функцию.
4. Чтобы включить или отключить уведомления о предотвращении вторжений и работе брандмауэра, нажмите значок настроек в разделе **Защита от уязвимостей**, а затем в диалоговом окне поставьте или снимите флажок рядом с параметром **Display Vulnerability Protection Notifications**.
5. Нажмите кнопку **Готово**.

Если вы выключили эти компоненты, необходимо включить их как можно скорее, чтобы обеспечить надежную защиту компьютера.

Управление предотвращением вторжений

Управление защитой клиента Mac с помощью брандмауэра


Symantec
A Division of Broadcom