ESET ENDPOINT SECURITY

ДЛЯ ANDROID

Инструкция по установке и руководство пользователя

Щелкните здесь, чтобы загрузить актуальную версию этого документа.

Содержание

ESET **ENDPOINT SECURITY**

Приложение ESET Endpoint Security разработано компанией ESET, spol. s r.o..
Для получения дополнительных сведений посетите веб-сайт www.eset.com.

Служба поддержки клиентов: www.eset.com/support

Версия 27. 11. 2012

1. Установка ESET Endpoint Security

Установить ESET Endpoint Security для Android на мобильном устройстве можно, если оно соответствует указанным ниже системным требованиям.

	Минимальные системные требования
Операционная система	Android 2.1 (Eclair) и более поздних версий
CPU	600 МГц
RAM	256 МБ
Свободный объем внутренней памяти телефона	5 МБ

ПРИМЕЧАНИЕ. Некоторые функции (например, антиспам и антивор) недоступны в системе Android 3.0 и на планшетных компьютерах, которые не позволяют совершать звонки и отправлять сообщения. Дополнительные сведения представлены в этой статье базы знаний (некоторые статьи могут быть недоступны на вашем языке).

1.1 Установка

Для установки ESET Endpoint Security воспользуйтесь одним из следующих вариантов действий.

- Загрузите установочный файл ESET Endpoint Security *(ees.apk)* с веб-сайта ESET, просканировав показанный ниже QR-код с помощью такого приложения, как QR Droid или Barcode Scanner.

- Загрузите файл *ees.apk* на компьютер с веб-сайта ESET. Скопируйте файл на устройство через Bluetooth или USB. Нажмите значок Launcher на главном экране Android или выберите **Главная** > **Меню** и откройте **Настройки** > **Приложения.** Убедитесь, что выбран параметр **Неизвестные источники**. Найдите файл *ees.apk* с помощью такого приложения, как ASTRO File Manager или ES File Explorer. Откройте этот файл и нажмите **Установить**. После завершения установки приложения нажмите **Открыть**.

- Чтобы установить и активировать ESET Endpoint Security на нескольких устройствах, необходимо создать XML-файл конфигурации при помощи ESET Configuration Editor.

  Откройте ESET Configuration Editor в консоли ERA Console (**Инструменты** > ESET Configuration Editor) или нажмите кнопку **Пуск** Windows > **Все программы** > **ESET** > ESET Remote Administrator **Консоль >** ESET Configuration Editor. В дереве слева выберите **Мобильные устройства** > **Endpoint Security для Android** > **Обновление** > **Настройки** > **Имя пользователя**. Введите имя пользователя (данные лицензии, полученные от ESET после приобретения продукта) в поле **Значение** справа и щелкните **Далее**. Нажмите кнопку **Задать пароль** и введите пароль. Подтвердите, нажав кнопку **OK**. Помимо имени пользователя и пароля, здесь также можно определить дополнительные настройки (например, параметры удаленного администрирования или защиты от вирусов), которые необходимо применить ко всем конечным мобильным устройствам. Завершив изменение настроек, щелкните **Файл** > **Сохранить** (или нажмите сочетание клавиш Ctrl+S) и сохраните файл с именем *settings.xml*.

  Скопируйте этот файл в корневую папку (/mnt/sdcard) SD-карты вместе с установочным файлом ESET Endpoint Security *ees.apk* (который находится здесь). Откройте файл *ees.apk* с помощью такого приложения, как ASTRO File Manager или ES File Explorer и нажмите **Установить**. После установки приложения выберите команду **Открыть**. Активация ESET Endpoint Security будет выполнена автоматически с помощью имени пользователя и пароля, сохраненных в файле *settings.xml*.

Внимание! ESET Endpoint Security необходимо установить во внутреннем хранилище устройства. Некоторые мобильные телефоны позволяют пользователям устанавливать приложения на SD-картах. Если установить ESET Endpoint Security на SD-карте, функции защиты в режиме реального времени, антиспама и антивора не будут работать.

После успешного выполнения установки

активируйте ESET Endpoint Security в соответствии с инструкциями, приведенными в разделе Активация программы 4.

1.2 Удаление приложения

Если нужно удалить ESET Endpoint Security с устройства, воспользуйтесь **мастером удаления**, который можно открыть с главного экрана ESET Endpoint Security, или же выполните описанные далее действия.

1. Нажмите значок Launcher на главном экране Android (или выберите **Главная** > **Меню**), затем **Настройки** > **Местоположение и защита** > **Выбрать администраторов устройства**, снимите флажок **ESET Security** и нажмите **Отключить**. При появлении запроса введите свой пароль ESET Endpoint Security. (Если вы не выбирали ESET Endpoint Security в качестве администратора устройства, этот шаг можно пропустить.)
2. Вернитесь в раздел **Настройки** и выберите **Приложения** > **Управление приложениями** > **ESET Security** > **Удалить**.

ESET Endpoint Security и папка карантина будут удалены с мобильного устройства без возможности восстановления.

2. Активация программы

После успешного выполнения установки нужно активировать ESET Endpoint Security. Нажмите **Активировать сейчас** на главном экране ESET Endpoint Security.

Активация с помощью имени пользователя и пароля: в соответствующих полях введите имя пользователя и пароль (сведения о лицензии, полученные от ESET после приобретения продукта).

Активация действительна на определенный период времени. По истечении срока действия активации будет предложено продлить лицензию (приложение уведомит об этом заранее).

ПРИМЕЧАНИЕ. Во время активации устройство должно быть подключено к Интернету. При этом на устройство будет загружен небольшой объем данных.

По умолчанию приложение ESET Endpoint Security устанавливается на языке, выбранном на телефоне в качестве системного (в настройках языка и клавиатуры). Если нужно изменить язык всего интерфейса пользователя в приложении, выберите пункт **Язык** на главном экране ESET Endpoint Security и выберите нужный язык.

3. Антивирус

Полное сканирование

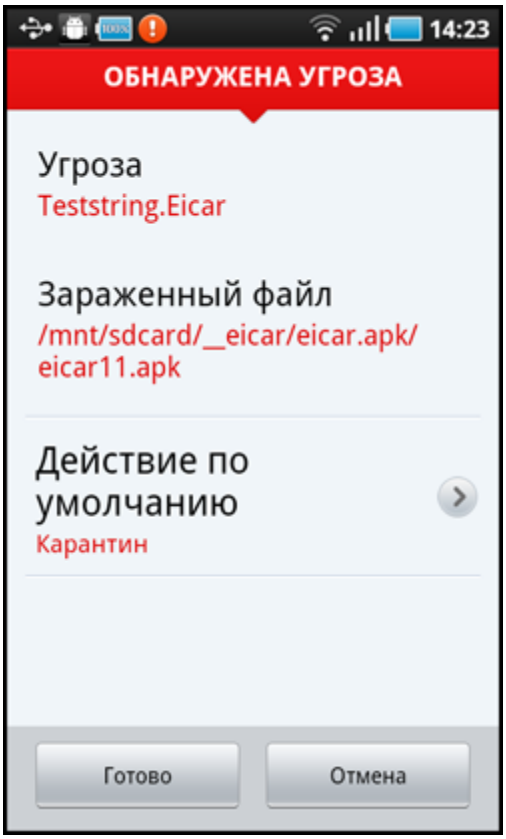
С помощью функции **Полное сканирование** можно проверить, не заражено ли мобильное устройство.

Файлы некоторых предопределенных типов сканируются по умолчанию. В ходе полного сканирования устройства выполняется проверка памяти, запущенных процессов, связанных с ними динамических библиотек и файлов во внутренней памяти и на съемных носителях. После окончания сканирования на экран будет выведена краткая сводка о его результатах (например, о количестве зараженных файлов, количестве просканированных файлов, длительности сканирования и т. д.).

Если нужно прервать выполняемый процесс сканирования, нажмите **Отмена**.

Сканирование папки

Для проверки определенных папок на устройстве выберите команду **Сканирование папки**. Найдите папки, которые нужно сканировать, установите для них флажки в правом столбце и нажмите **Сканировать**.



Угроза, обнаруженная ESET Endpoint Security

Журналы сканирования

Раздел **Журналы сканирования** содержит подробные данные о выполненных задачах сканирования. Журналы создаются после каждого запускаемого вручную (по запросу) сканирования или при обнаружении заражения в процессе сканирования в режиме реального времени.

В каждом журнале содержится следующая информация:

- дата и время события;
- количество просканированных файлов;
- количество зараженных файлов;
- имя и полный путь для зараженных файлов;
- длительность сканирования;
- действия, выполненные в ходе сканирования, и возникшие ошибки.

Карантин

Карантин предназначен в первую очередь для безопасного хранения зараженных файлов. Файлы следует помещать на карантин, если их нельзя очистить или безопасно удалить, а также если они по ошибке отнесены программой ESET Endpoint Security к зараженным.

Информация о файлах, помещенных на карантин, записывается в журнал. Она включает имя и исходное местоположение зараженного файла, дату и время помещения файла на карантин.

Если нужно восстановить помещенный на карантин файл в исходное местоположение, нажмите его и выберите команду **Восстановить**. Этой возможностью пользоваться не рекомендуется.

Для удаления помещенного на карантин файла с устройства без возможности восстановления нажмите его и выберите команду **Удалить**. Для удаления всех помещенных на карантин файлов нажмите кнопку **МЕНЮ** и выберите команду **Удалить все**.

Настройки

Настройки в разделе **По запросу** позволяют изменить параметры запускаемого вручную (по запросу) сканирования.

Параметр **Показывать предупреждения** позволяет выводить на экран уведомления при обнаружении новой угрозы модулем сканирования по запросу.

Если нужно просканировать все приложения (файлы *.apk*), установленные на устройстве, выберите параметр **Сканировать приложения**.

Проактивная защита — это алгоритмический метод обнаружения, основанный на анализе кода и поиске типичных признаков поведения вирусов. Основным преимуществом этого метода является возможность обнаружения вредоносных программ, не распознаваемых с использованием текущей версии базы данных сигнатур вирусов. При активации проактивной защиты время сканирования будет увеличено.

Параметр **Глубина сканирования архивов** позволяет задать уровень вложенности архивов (файлов с расширением *.zip*), подлежащих сканированию. Чем больше это число, тем глубже сканирование.

Параметр **История проверок** позволяет задать максимальное количество журналов, сохраняемых в разделе **Журналы сканирования** 5.

В поле **Действие по умолчанию** можно указать действие по умолчанию, автоматически выполняемое при обнаружении зараженных файлов. Доступны указанные ниже варианты.

- **Игнорировать**: с зараженным файлом не будут выполняться никакие действия (этот вариант использовать не рекомендуется).
- **Удалить**: зараженный файл будет удален.
- **Карантин** (вариант по умолчанию): зараженный файл будет помещен на **карантин** 5.

Настройки раздела **Расширения** показывают наиболее распространенные типы файлов, подвергаемые заражениям на платформе Android. Выберите типы файлов, которые нужно сканировать, или отмените выбор расширений, если выполнять сканирование файлов соответствующих типов не нужно. Эти настройки применяются и к сканированию по запросу, и к сканированию в режиме реального времени.

- При выборе параметра **Сканирование с исключениями** сканирование будет выполняться только в отношении файлов с расширениями указанных типов, при этом скорость сканирования будет выше. Рекомендуется по возможности отключить эту функцию, чтобы дать возможность программе ESET Endpoint Security выполнить сканирование на все возможные типы угроз, включая заражения, скрытые ложными расширениями файлов.
- **DEX (системные файлы)** — формат исполняемых файлов, которые содержат компилированный код, написанный для ОС Android.
- **SO (библиотеки)** — общие библиотеки, сохраненные в указанных местоположениях в файловой системе и связанные с программами, которым нужны их функции.
- **Архивы (сжатые файлы)** — сжатые файлы Zip.
- **Другие** — другие известные типы файлов.

В разделе настроек **Реальное время** можно сконфигурировать параметры сканирования для модуля сканирования при доступе. Модуль сканирования при доступе проверяет файлы, к которым обращается пользователь, в режиме реального времени. Он автоматически сканирует папку *Загрузка* на карте памяти, файлы из числа установочных файлов с расширением *.apk* и файлы на карте памяти после ее подключения (если активирован параметр **Сканировать карту памяти**). Модуль сканирования при доступе автоматически запускается при загрузке системы.

- **Защита в режиме реального времени**: если этот параметр активирован (по умолчанию), модуль сканирования при доступе работает в фоновом режиме.
- Параметр **Показывать предупреждения** позволяет выводить на экран уведомления при обнаружении новой угрозы модулем сканирования при доступе.
- **Сканировать карту памяти**: файлы сканируются до их открытия или сохранения на карту памяти.
- **Проактивная защита**: если выбрать этот параметр, будут использоваться методы эвристического анализа. Эвристический анализ позволяет в упреждающем режиме обнаруживать новые вредоносные программы, еще не обнаруживаемые с помощью базы данных сигнатур вирусов, путем анализа кода и распознавания типичного для вирусов поведения. При активации проактивной защиты время сканирования увеличивается.
- Параметр **Глубина сканирования архивов** позволяет задать уровень вложенности архивов (файлов с расширением *.zip*), подлежащих сканированию. Чем больше это число, тем глубже сканирование.
- **Действие по умолчанию**: этот параметр позволяет указать действие по умолчанию, которое будет выполняться автоматически при обнаружении зараженных файлов модулем сканирования при доступе. Если выбрать вариант **Игнорировать**, то с зараженным файлом не будут выполняться никакие действия (этот вариант использовать не рекомендуется). Вариант **Удалить** позволяет удалить зараженный файл. Если же остановиться на возможности **Карантин**, то зараженный файл будет помещен на **карантин** 5.

ESET Endpoint Security выводит на экран значок уведомления  в левом верхнем углу (строка состояния Android). Если не нужно, чтобы этот значок отображался, перейдите на главный экран ESET Endpoint Security, нажмите кнопку **МЕНЮ**, выберите пункт **Настройки уведомлений** и снимите флажок **Включить виджет**. Имейте в виду, что при этом не будет отключен значок

предупреждения красного цвета с восклицательным знаком, который уведомляет пользователя об угрозе безопасности (например, об отключении сканирования на наличие вирусов в режиме реального времени, согласования SIM и т. д.).

4. Антиспам

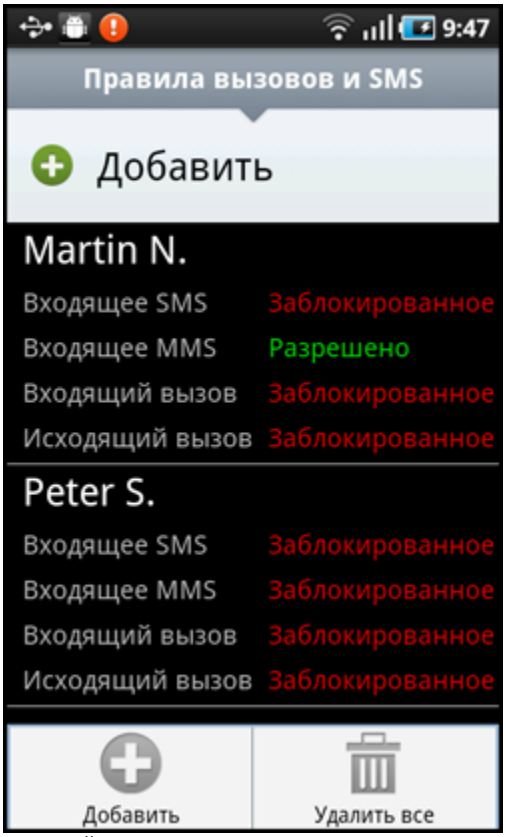
Модуль **Антиспам** блокирует входящие сообщения SMS и MMS, а также входящие и исходящие вызовы на основе ваших правил.

Как правило, нежелательные сообщения содержат рекламные объявления от операторов мобильной связи либо послания от неизвестных или неуказанных пользователей. Под термином *блокировать контакты* понимается автоматическое перемещение входящих сообщений в раздел **Журналы спама** 7. При блокировании входящего сообщения уведомление на экран не выводится. Преимуществом такого подхода является то, что вы не будете отвлекаться на ненужную информацию, но все же всегда сможете проверить журналы на предмет наличия сообщений, которые могли быть заблокированы по ошибке.

Для создания нового правила антиспама нажмите **Правила вызовов и SMS** > **Добавить**. Введите номер телефона, который следует заблокировать, или же нажмите кнопку **+**, чтобы выбрать нужный номер из адресной книги. Настройте правило, разрешив или заблокировав сообщения и вызовы, и нажмите **Готово**.

Для изменения или удаления существующего правила нажмите и удерживайте соответствующий элемент, после чего выберите нужное действие. Если следует удалить все правила антиспама, нажмите кнопку **МЕНЮ** и выберите пункт **Удалить все**.

ПРИМЕЧАНИЕ. Номер телефона должен включать международный код и собственно номер (например, +761O2OO2OOO).



Настройка антиспама

Настройки

Блокировать скрытые номера: установите этот флажок, если следует блокировать вызовы от абонентов, намеренно скрывающих свои номера с помощью функции запрета определения телефонного номера.

Блокировать известные контакты: этот параметр позволяет блокировать сообщения и вызовы от контактов из адресной книги.

Блокировать неизвестные контакты: блокируются сообщения и вызовы от контактов, отсутствующих в адресной книге. Этот параметр можно использовать, чтобы блокировать нежелательные телефонные звонки (например, рекламные) или предотвращать набор детьми неизвестных номеров. (Для предотвращения этого рекомендуется защитить настройки антиспама **паролем** 11.)

В разделе **Журналы спама** можно просмотреть вызовы и сообщения, заблокированные модулем защиты от спама. В каждом журнале содержатся имя события, соответствующий номер телефона, дата и время события. Для заблокированных SMS-сообщений также приводится тело сообщения.

5. Антивор

Функция **антивора** предотвращает несанкционированный доступ к мобильному телефону.

Если вы потеряете телефон или кто-то украдет его и заменит вашу SIM-карту на новую (не являющуюся доверенной), ESET Endpoint Security автоматически заблокирует телефон. На указанные пользователем телефонные номера будет тайно отправлено SMS-сообщение с предупреждением. Оно будет включать телефонный номер текущей SIM-карты, номер IMSI и номер IMEI телефона. Неавторизованный пользователь не узнает об отправке сообщения, поскольку оно будет автоматически удалено из диалогов раздела **Сообщения**. Кроме того, вы также можете запросить координаты GPS своего потерянного мобильного телефона или удаленно очистить все данные, имеющиеся на устройстве.

Доверенные SIM-карты

Этот раздел недоступен на устройствах, в которых не используется SIM-карта (планшетные компьютеры и телефоны стандарта CDMA).

Если SIM-карту, которая в данный момент вставлена в мобильный телефон, следует запомнить в качестве доверенной, нажмите кнопку **Добавить**. Если используется несколько SIM-карт, можно воспользоваться пунктом **Введите имя SIM-карты**, указав имя для каждой из них (например, *Рабочая*, *Домашняя* и т. д.).

Чтобы **Изменить** или **Удалить** SIM-карту, нажмите и удерживайте ее, после чего выберите соответствующую команду. Если следует удалить все пункты из списка, нажмите кнопку **МЕНЮ** и выберите пункт **Удалить все**.

Админ. контакты

В списке **Админ. контакты** нажмите **Добавить**, чтобы указать номера телефонов, на которые будет отправлено SMS-сообщение с предупреждением после вставки в устройство SIM-карты, не являющейся доверенной. Введите имя в поле **Имя контакта** и заполните поле **Номер телефона** или нажмите кнопку **+**, чтобы выбрать контакт из адресной книги. Если у контакта несколько номеров телефона, SMS-сообщение с предупреждением будет отправлено на все эти номера.

Чтобы **Изменить** или **Удалить** карту, нажмите и удерживайте ее, после чего выберите соответствующую команду. Если следует удалить все пункты из списка, нажмите кнопку **МЕНЮ** и выберите пункт **Удалить все**.

ПРИМЕЧАНИЕ. Номер телефона должен включать международный код и собственно номер (например, +161O1OO1OO).

Настройки

Если не нужно использовать функцию согласования SIM, выберите параметр **Не определять SIM-карту**. При этом будут отключены обозначенные красным цветом предупреждения *Угроза безопасности!* (*Согласование SIM отключено* и *Не задана доверенная SIM-карта*) на главном экране ESET Endpoint Security. Параметр «Не определять SIM-карту» неактивен на устройствах стандарта CDMA.

Чтобы включить автоматическую проверку вставляемых SIM-карт (и отправку SMS-сообщений с предупреждением), установите флажок **Определять SIM-карту**.

В поле **Текст SMS-оповещения** можно изменить текстовое сообщение, отправляемое на указанные телефонные номера после вставки в устройство SIM-карты, не являющейся доверенной. Если приложение ESET Endpoint Security приобретено в магазине Google Play, автоматически будет вставлен адрес электронной почты из учетной записи Google. Можно также ввести другой адрес электронной почты или альтернативный контактный номер.

SMS-команды

Удаленные SMS-команды (на очистку, блокирование и поиск) будут работать только в том случае, если установлен флажок **Включить SMS-команды**.

Параметр **Включить SMS-сброс пароля** позволяет осуществить сброс пароля безопасности, отправив SMS-сообщение с номера мобильного телефона, указанного в списке **Админ. контакты**, на свой номер. Такое SMS-сообщение должно быть в следующем формате:
eset remote reset

Если вы потеряли свой телефон и хотели бы заблокировать его, отправьте SMS-сообщение для выполнения удаленной блокировки с любого мобильного устройства на свой номер телефона в таком виде:
eset lock пароль
Замените *пароль* на собственный пароль, заданный в разделе **Пароль** 11. Незаконный пользователь вашего телефона не сможет им воспользоваться, так как нужно будет ввести ваш пароль.

Если нужно запросить координаты GPS своего мобильного устройства, отправьте SMS-сообщение удаленного поиска на свой номер мобильного телефона или номер телефона незаконного пользователя (в зависимости от того, была ли уже заменена SIM-карта):
eset find пароль
Вы получите SMS-сообщение с координатами GPS и ссылкой на карту Google Maps, показывающими точное местонахождение вашего мобильного устройства. Обратите внимание на то, что для получения координат GPS модуль GPS вашего телефона должен быть активирован заранее.

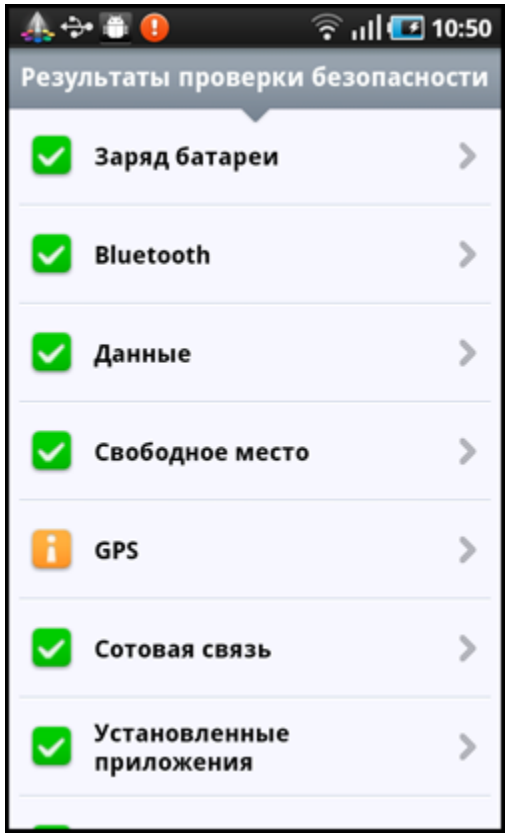
Если нужно удалить все данные на устройстве и подключенных к нему в настоящий момент съемных носителях, отправьте SMS-сообщение для удаленной очистки:
eset wipe пароль
Все контакты, сообщения, электронная почта, установленные приложения, учетная запись Google и содержимое карты памяти будут удалены с устройства без возможности восстановления. Если приложение ESET Endpoint Security не выбрано в качестве администратора устройства, удалены будут только контакты, сообщения и содержимое карты памяти.

ПРИМЕЧАНИЕ. Вводить пароль нужно с учетом регистра. Обязательно нужно вводить пароль именно так, как он указан в разделе «Пароль».

6. Проверка безопасности

Функция **Проверка безопасности** позволяет проверять состояние телефона: уровень заряда аккумулятора, состояние Bluetooth, объем свободного места и т. д.

Чтобы запустить проверку безопасности вручную, выберите команду **Проверка**. На экран будет выведен подробный отчет.



Результаты проверки безопасности

Зеленая отметка рядом с элементом указывает, что его значение выше порогового или он не представляет угрозы для безопасности.

Желтый значок является признаком того, что хотя бы у одного элемента значение ниже порогового или он может угрожать безопасности. Нажмите соответствующий элемент, чтобы просмотреть подробные результаты.

Красный восклицательный знак показывает, что значение элемента ниже порогового или он представляет угрозу для безопасности и должен быть исправлен.

Если вы хотите исправить состояние выделенного красным элемента, нажмите его и подтвердите свое решение, выбрав **Да**.

Настройки

По умолчанию проверка безопасности выполняется периодически каждые сутки. Если нужно отключить периодическую проверку, снимите флажок **Проверять периодически**.

Если включен параметр **Исправлять автоматически**, приложение ESET Endpoint Security будет автоматически пытаться устранить факторы риска (связанные, например, с состоянием Bluetooth) без вмешательства пользователя. Этот параметр распространяется только на периодические (запланированные) проверки.

Параметр **История проверок** позволяет задать максимальное количество журналов, сохраняемых в разделе **Результаты проверки**.

Параметр **Период проверки** дает возможность указать частоту выполнения периодической (запланированной) проверки.

Для изменения пороговых значений, при которых объем свободного места и заряд батареи будут считаться низкими, можно воспользоваться параметрами **Минимальный объем памяти** и **Минимальный заряд батареи**.

На вкладке **Элементы для проверки** можно выбрать элементы, которые будут проверяться в процессе периодических (запланированных) проверок.

В разделе **Результаты проверки** можно найти журналы, в которых содержатся все данные о выполненных по расписанию или запущенных вручную проверках. В каждом таком журнале содержатся дата и время события и подробные результаты для каждого элемента.

Диспетчер задач предоставляет общие сведения обо всех процессах, службах и задачах, запущенных на устройстве. ESET Endpoint Security позволяет останавливать процессы, службы и задачи, не выполняемые системой. Такие элементы обозначаются красным значком (**x**).

7. Удаленное администрирование

ESET Remote Administrator (ERA) позволяет управлять программой ESET Endpoint Security в сетевой среде непосредственно из одного централизованного местоположения.

Администраторы могут удаленно выполнять следующие действия:

- создание задач конфигурации в ERA и перенос настроек на ESET Endpoint Security;
- запуск сканирования по запросу;
- установка обновлений для базы данных сигнатур вирусов;
- проверка файлов журнала;
- отправка уведомлений от администратора на мобильные устройства.

Использование ERA не только способствует повышению уровня безопасности, но и обеспечивает простоту администрирования всех продуктов безопасности ESET, установленных на клиентских рабочих станциях и мобильных устройствах. Для связи между ERA и ESET Endpoint Security требуется соединениеWi-Fi или USB (или внешнее соединение VPN), а также правильная конфигурация обеих конечных точек.

Настройки

Параметры настройки удаленного администрирования доступны на главном экране ESET Endpoint Security. Откройте раздел **Удаленное администрирование** > **Настройки**.

Активируйте функцию удаленного администрирования, выбрав параметр **Подключиться к серверу удаленного администрирования**.

Параметр **Интервал между подключениями к серверу** указывает на частоту, с которой ESET Endpoint Security пытается подключиться к серверу ERA Server для отправки данных.

Основной сервер, **Дополнительный сервер**: обычно настройка требуется только для основного сервера. Если в сети запущено несколько серверов ERA, можно добавить соединение с дополнительным сервером ERA Server. Это можно использовать в качестве резервного решения. Если основной сервер станет недоступным, ESET Endpoint Security автоматически установит связь с дополнительным сервером ERA Server. Параллельно будут выполняться попытки восстановления соединения с основным сервером. Когда это соединение снова станет активным, ESET Endpoint Security снова переключится на основной сервер. Настройка двух профилей сервера удаленного администрирования больше всего подходит для клиентов, которые подключаются как из локальной сети, так и из-за ее пределов.

Адрес сервера: укажите DNS-имя или IP-адрес сервера, на котором запущен сервер ERA Server.

В поле **Порт** указан предопределенный порт сервера, который используется для соединения. Рекомендуется установить порт по умолчанию (2222).

Если ESET Remote Administrator требует выполнить проверку пароля, выберите параметр **Для сервера Remote Administrator Server требуется аутентификация** и введите свой пароль в поле **Пароль**.

ПРИМЕЧАНИЕ. Для получения дальнейшей информации по управлению сетью при помощи ESET Remote Administrator см. Инструкцию по установке и руководство пользователя ESET Remote Administrator (этот документ может быть недоступен на вашем языке).

8. Обновление

По умолчанию при установке приложения ESET Endpoint Security настраивается задача обновления, обеспечивающая регулярное выполнение этой процедуры. Для запуска обновления вручную нажмите **Обновление**.

Настройки

Параметр **Автоматическое обновление** позволяет настроить интервал автоматической загрузки обновлений базы данных сигнатур вирусов.

ПРИМЕЧАНИЕ. Чтобы предотвратить ненужное использование пропускной способности сети, обновления выпускаются по мере необходимости при появлении новых угроз. Сами обновления предоставляются при наличии активной лицензии бесплатно, но при этом поставщик услуг мобильной связи может взимать плату за передачу данных.

9. Пароль

Пароль безопасности предотвращает неразрешенное внесение изменений в настройки. Пароль нужен в таких ситуациях:

- доступ к защищенным паролем функциям ESET Endpoint Security (антивирус, антиспам, антивор и проверка безопасности);
- доступ к телефону в случае, если он был заблокирован;
- отправка SMS-команд на свое устройство;
- удаление ESET Endpoint Security.

ПРИМЕЧАНИЕ. Защита от удаления доступна только для ОС Android 2.2 и более поздних версий.

Для выбора нового пароля безопасности введите его в поля **Пароль** и **Повторите ввод пароля**. Параметр **Подсказка** (если настроен) позволяет получить подсказку, когда не удается вспомнить пароль.

ВНИМАНИЕ! Пароль следует выбирать тщательно, поскольку он понадобится, чтобы разблокировать устройство или удалить ESET Endpoint Security.

На вкладке **Применить к** можно указать, какие модули будут защищены паролем.

Если вы забудете пароль, то сможете отправить SMS-сообщение с номера мобильного телефона, сохраненного в списке **Админ. контакты**, на номер своего телефона. Такое SMS-сообщение должно быть в следующем формате:
eset remote reset
Пароль будет сброшен.

10. Устранение проблем и поддержка

10.1 Устранение проблем

ESET Endpoint Security поддерживает передовые функции ведения журнала, помогающие диагностировать потенциальные технические проблемы. Прежде чем обращаться в службу поддержки клиентов ESET, рекомендуется сначала попытаться найти решение в базе знаний ESET. Если все же нужно обратиться в службу поддержки клиентов ESET, выполните указанные ниже действия.

1. На главном экране ESET Endpoint Security нажмите кнопку **МЕНЮ** и выберите пункт **Настройки журнала**.
2. Выберите компонент программы, с которым связана проблема.
3. Воспроизведите проблему. Сведения о проблеме будут записаны в файл журнала приложения.
4. На главном экране ESET Endpoint Security нажмите кнопку **МЕНЮ** и выберите пункт **Служба поддержки клиентов**.
5. Если найти решение в нашей базе знаний не удастся, выберите команду **Продолжить**.
6. Введите нужные сведения и выберите команду **Отправить** в нижней части экрана. Убедитесь, что выбран параметр **Журнал приложения** (выбран по умолчанию).

10.2 Техническая поддержка

По административным и техническим вопросам, связанным с ESET Endpoint Security или другими продуктами безопасности ESET, обращайтесь к специалистам нашей службы поддержки клиентов.

Ответы на часто задаваемые вопросы можно найти в базе знаний ESET по адресу:
http://kb.eset.com/android

База знаний содержит большой объем полезной информации об устранении наиболее распространенных проблем, которую легко найти с помощью категорий и удобных средств поиска.

Для обращения в службу поддержки клиентов ESET можно использовать форму запроса по адресу:
http://eset.com/support/contact

Чтобы отправить запрос в службу поддержки непосредственно с мобильного телефона, перейдите на главный экран ESET Endpoint Security, нажмите кнопку **МЕНЮ** и выберите пункт **Служба поддержки клиентов**. Заполните необходимые поля. Чтобы включить в запрос полный **журнал приложения**, выполните действия, описанные в разделе Устранение проблем 12.