ESET ENDPOINT SECURITY для ANDROID

Руководство пользователя

(для программы версии 2.0 и выше)

Щелкните здесь, чтобы загрузить актуальную версию этого документа

ESET **ENDPOINT SECURITY**

Служба поддержки клиентов: www.eset.com/support

Испр. 03.01.2017

Содержание

1. Введение

Новое поколение программы ESET Endpoint Security для Android (EESA) предназначено для работы с ESET Remote Administrator (ERA) 6 — новой консолью управления, с помощью которой можно удаленно управлять всеми решениями для обеспечения безопасности ESET. Приложение ESET Endpoint Security для Android 2 совместимо только с ERA 6 и более поздними версиями.

<%Приложение PRODUCTNAME%> для Android предназначено для защиты корпоративных мобильных устройств от новейших угроз, а также для защиты данных даже в случае потери или кражи устройства. Также оно помогает системным администраторам обеспечивать соответствие устройств корпоративным политикам безопасности.

<%Приложение PRODUCTNAME%> может также применяться компаниями малого и среднего размера без необходимости в удаленном управлении с помощью ESET Remote Administrator. ИТ-специалист, системный администратор или пользователь приложения Endpoint может просто предоставить конфигурацию ESET Endpoint Security для использования другими коллегами. Этот процесс полностью устраняет необходимость в активации продукта и ручной настройке каждого модуля программы, которые в ином случае следует выполнять сразу же после установки приложения ESET Endpoint Security.

1.1 Новые возможности версии 2

Контроль приложений

С помощью функции «Контроль приложений» администраторы могут отслеживать установленные приложения, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалять некоторые программы. Дополнительные сведения см. в разделе Контроль приложений данного руководства.

Безопасность устройства

Функция «Безопасность устройства» позволяет администраторам применять основные политики безопасности на нескольких мобильных устройствах. Например, администратор может:

- задать минимальные уровень безопасности и сложность кодов разблокировки экрана;
- указать максимальное количество неудачных попыток разблокировки;
- указать максимальный срок действия для кода разблокировки экрана;
- настроить таймер блокировки экрана;
- ограничить использование камеры.

Дополнительные сведения см. в разделе Безопасность устройства данного руководства.

Импорт и экспорт параметров

Чтобы с легкостью обеспечить передачу параметров между двумя мобильными устройствами, которые не управляются решением ERA, ESET Endpoint Security 2 дает возможность экспортировать и импортировать параметры программы. Администратор может вручную экспортировать параметры в файл, который затем можно передать по электронной почте и импортировать на любое устройство, на котором запущено клиентское приложение. Когда пользователь принимает файл параметров, все параметры импортируются автоматически и приложение активируется (если в файл были добавлены сведения о лицензии). Все параметры защищены паролем администратора.

Защита от фишинга

Этот компонент предотвращает посещение вредоносных веб-сайтов пользователями, которые используют поддерживаемые веб-браузеры (браузер по умолчанию для ОС Android и Chrome).

Технология защиты от фишинга защищает пользователей от попыток получения паролей, банковских данных и прочей конфиденциальной информации незаконными веб-сайтами, выдающими себя за законные. Когда устройство пытается перейти по URL-адресу, модуль защиты от фишинга ESET сравнивает его с адресами известных фишинговых сайтов из базы данных ESET. При наличии совпадения подключение к такому URL-адресу прерывается и отображается соответствующее предупреждение.

Центр уведомлений

ESET Endpoint Security содержит единый центр уведомлений, в котором есть все уведомления, касающиеся тех функций приложения, на которые нужно обратить внимание. Центр уведомлений предоставляет сведения о разных событиях, о причинах их несоответствия корпоративным политикам и о том, как эту несовместимость устранить. Уведомления упорядочены по приоритету: уведомления с более высоким приоритетом отображаются вверху списка.

Новая система лицензирования

ESET Endpoint Security полностью поддерживает решение ESET License Administrator — новую модель лицензирования, представленную в решении ESET Remote Administrator 6.

Новая система лицензирования упрощает развертывание и долгосрочное использование программ ESET. Когда клиент делает запрос на изменение лицензии, это изменение автоматически отображается во всех продуктах, использующих эту лицензию. Поэтому любой клиент вместо выданного компанией ESET имени пользователя и пароля (как в более старых продуктах) может в качестве учетных данных использовать свои адрес электронной почты и пароль.

Использование лицензионных ключей и автоматическое обновление лицензии (в результате продления или другого действия с лицензией) обеспечивает надежную защиту. Портал ESET License Administrator и возможность назначать права на авторизацию лицензий по электронной почте (указанной в сведениях об учетной записи пользователя) упрощают управление лицензиями и их развертывание. С помощью ESET License Administrator любой владелец лицензии может делегировать управление лицензиями ответственной стороне (даже третьей стороне), не теряя контроль над лицензией.

Управляемое обновление программы до более новой версии

Системные администраторы, которые используют ERA и не хотят, чтобы программа ESET Endpoint Security для Android обновлялась автоматически при появлении обновлений, могут контролировать процесс обновления.

Мастеры настройки

ESET Endpoint Security включает в себя несколько мастеров, которые упрощают настройку определенных функций после установки.

Улучшенная защита от вирусов

- Более быстрое сканирование в реальном времени (сканирование при доступе).
- Интегрированная система ESET Live Grid.
- 2 уровня сканирования: сканирование Smart и тщательное сканирование.
- Улучшенный модуль сканирования по требованию: фоновое сканирование, возможность приостановки сканирования.
- Сканирование по расписанию: администратор может запланировать полное сканирование устройства.
- Сканирование в процессе зарядки:сканирование начинается автоматически, когда устройство находится в состоянии простоя (полностью заряжено и подключено к зарядному устройству).
- Расширенная настройка обновлений базы данных сигнатур вирусов: администратор может указать время выполнения регулярных обновлений и выбрать сервер обновлений, который должно использовать устройство (сервер выпусков, сервер тестовых обновлений, локальное зеркало).

Журналы, содержащие подробные сведения о результатах сканирования, отправляются в решение ERA. ESET Endpoint Security включает в себя функции, которые были доступны в ESET Endpoint Security версии 1, например обнаружение потенциально небезопасных приложений и потенциально нежелательных приложений, а также контроль USSD.

Улучшенный фильтр звонков и SMS

Фильтр звонков и SMS, ранее известный как компонент защиты от спама, защищает пользователей от нежелательных звонков, а также SMS- и MMS-сообщений. В этом компоненте теперь действуют правила двух типов: правила администратора и правила пользователя, при этом правила администратора всегда имеют приоритет.

Есть и другие улучшения:

- блокировка на основе времени (пользователь или администратор может блокировать звонки и сообщения, которые приходят в указанное время);
- блокировка одним касанием (можно заблокировать последнего позвонившего или отправителя сообщения, номер телефона, группу контактов, скрытые или неизвестные номера).

Улучшенный компонент «Антивор»

Компонент «Антивор» позволяет администраторам защитить и отыскать устройство, если его потеряли или украли. Функции модуля Антивор можно активировать из ERAили с помощью удаленных команд.

ESET Endpoint Security 2 использует те же удаленные команды, что и версия 1 («Блокировать», «Очистить» и «Найти»). Кроме того, в новую версию добавлены новые команды.

- **Разблокировать**-разблокирует заблокированное устройство.
- **Расширенный сброс до заводских установок**-все доступные на устройстве данные быстро удаляются (уничтожаются заголовки файлов). Кроме того, на устройстве восстанавливаются заводские настройки по умолчанию.
- **Сирена**-потерянное устройство блокируется и начинает издавать очень громкий звук, даже если звук на устройстве отключен.

В целях увеличения безопасности удаленных команд администратор при выполнении такой команды будет получать на свой мобильный телефон уникальный SMS-код с ограниченным сроком действия (на номер, значащийся в списке контактов администратора). Этот код используется для проверки определенной команды.

Отправка команд модуля Антивор из решения ERA

Теперь команды модуля Антивор также можно отправлять из ERA. Новые функции управления мобильными устройствами позволяют администраторам быстро выполнить любую команду компонента «Антивор». Средство подключения для мобильных устройств теперь стало частью инфраструктуры ERA и позволяет быстро передавать задачи на выполнение.

Контакты администратора

Речь идет о списке, который включает в себя номера телефонов администратора и который защищен администраторским паролем. Команды компонента «Антивор» можно отправлять только с доверенных номеров.

Отображение сообщений из решения ERA

При удаленном управлении устройствами администратор может отправить пользовательское сообщение на устройство или группу устройств. Таким образом пользователям управляемых устройств можно передать срочное сообщение. На пользовательском устройстве такое сообщение отображается как всплывающий элемент, поэтому его нельзя будет не заметить.

Пользовательская информация на экране блокировки

Администратор может указать, какая информация может отображаться на экране заблокированного устройства (имя компании, адрес электронной почты, сообщение). При этом можно включить звонок одному из предварительно заданных контактов администратора.

Улучшенное удаленное управление с помощью ESET Remote Administrator **6**

Теперь с помощью удаленной политики можно настроить все параметры приложения, от параметров защиты от вирусов, фильтра звонков и SMS и безопасности устройства до ограничений контроля приложений.

ESET Endpoint Security для Android версии 2 дает возможность просматривать в веб-консоли ERA значительно улучшенные отчеты. Это позволяет администраторам оперативно выявлять проблемные устройства и источники проблемы.

Теперь управление устройствами Android — это неотъемлемая часть решения ESET Remote Administrator 6, причем почти со всеми такими же функциями, как в продуктах ESET для настольных ПК, таких как ESET Endpoint Antivirus 6 и ESET Endpoint Security 6.

Локальное администрирование

ESET Endpoint Security для Android дает администраторам возможность настраивать конечные точки и управлять ими локально, если не используется решение ESET Remote Administrator. Все параметры приложения защищены администраторским паролем, поэтому администратор всегда и всецело контролирует приложение.

Улучшенное распространение и установка программы

В дополнение к традиционным способам установки (загрузка и установка с веб-сайта ESET, отправка пакета установки по электронной почте) администраторы и пользователи могут загрузить и установить приложение из интернет-магазина Google Play.

Улучшенная активация продукта

Чтобы активировать программу после ее загрузки и установки, нужно выполнить одно из следующих действий:

- вручную ввести лицензионный ключ или учетные данные к учетной записи администратора безопасности;
- перейти по ссылке, полученной по электронной почте от администратора. Программа сама настроит подключение к серверу ERA, и сведения о лицензии будут переданы с сервера на устройство;
- ввести (если вы — администратор) данные для подключения к ERA вручную;
- импортировать файл с параметрами приложениями, в который добавлены сведения о лицензии (приложение будет активировано несколько позже).

Улучшенная идентификация мобильного устройства в ERA

Когда выполняется регистрация, устройства Android добавляются в «белый» список. Это делается для того, чтобы к ERA подключались только авторизованные устройства. Благодаря этому повышается безопасность и упрощается идентификация — мобильное устройство идентифицируется по имени, описанию и номеру IMEI. Устройства с возможностью подключения только к сетям Wi-Fi идентифицируются по MAC-адресам адаптера Wi-Fi.

Улучшенный графический интерфейс

ESET Endpoint Security обеспечивает улучшенные условия работы пользователей, подобные тем, которые обеспечивают другие решения ESET для бизнес-клиентов.

Простота использования

Благодаря новому графическому интерфейсу программой стало легче пользоваться. Графический интерфейс имеет такую же структуру, как в решениях ESET Endpoint нового поколения и в решении ESET Remote Administrator.

1.2 Минимальные требования к системе

Чтобы установить приложение ESET Endpoint Security на устройство под управлением ОС Android, оно должно соответствовать следующим минимальным требованиям к системе.

- Операционная система: Android 4 (Ice Cream Sandwich) и более поздние версии.
- Разрешение сенсорного экрана: 480 x 800 пкс.
- Процессор: ARM с набором инструкций ARMv7 или x86 Intel Atom.
- Свободное место для хранения данных: 20 МБ.
- Подключение к Интернету.

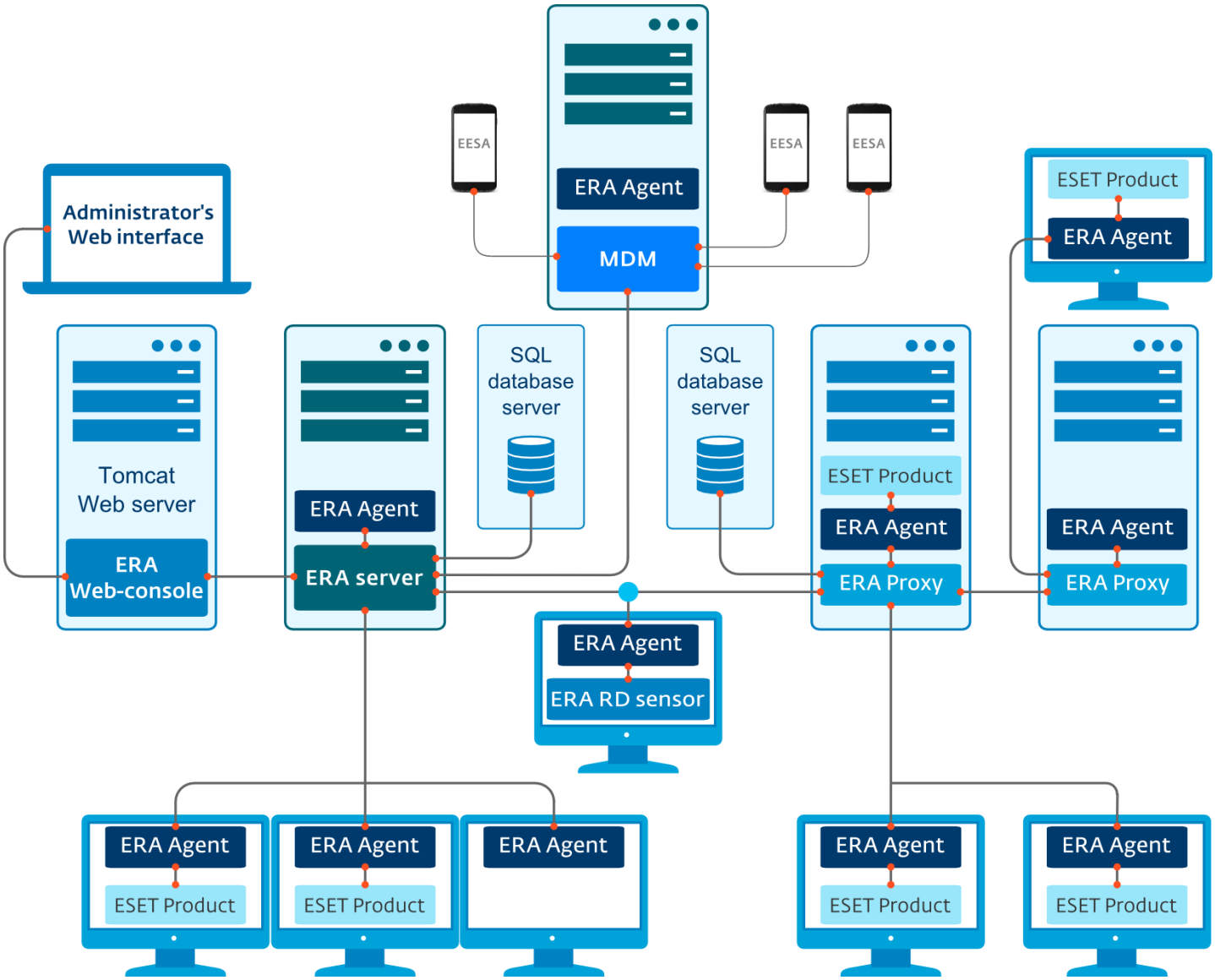
ПРИМЕЧАНИЕ. Не поддерживаются устройства с двумя SIM-картами и устройства, на которых выполнен рутинг. Некоторые возможности (например, модуль Антивор и фильтр звонков и SMS) недоступны на планшетах, которые не поддерживают телефонные звонки и обмен сообщениями.

2. Пользователи, подключенные к серверу ESET Remote Administrator

ESET Remote Administrator (ERA) 6 — это приложение, позволяющее осуществлять централизованное управление установленными в сетевой среде продуктами ESET. Система управления задачами ESET Remote Administrator позволяет установить программы ESET на удаленные компьютеры и мобильные устройства и быстро реагировать на новые проблемы и угрозы. Сама программа ESET Remote Administrator не предоставляет защиту от вредоносного кода — на каждом клиенте защиту предоставляет отдельное решение ESET (если оно установлено).

В программах ESET предусмотрена поддержка сетей, в которых используется несколько операционных платформ. В сети могут сосуществовать операционные системы Microsoft, Linux и OS X, а также системы, работающие на мобильных устройствах (мобильных телефонах и планшетах).

На рисунке ниже представлен пример архитектуры сети, защищенной решениями ESET, которыми управляет приложение ERA.



ПРИМЕЧАНИЕ. Дополнительные сведения см. в интернет-документации по ESET Remote Administrator.

2.1 Сервер ESET Remote Administrator

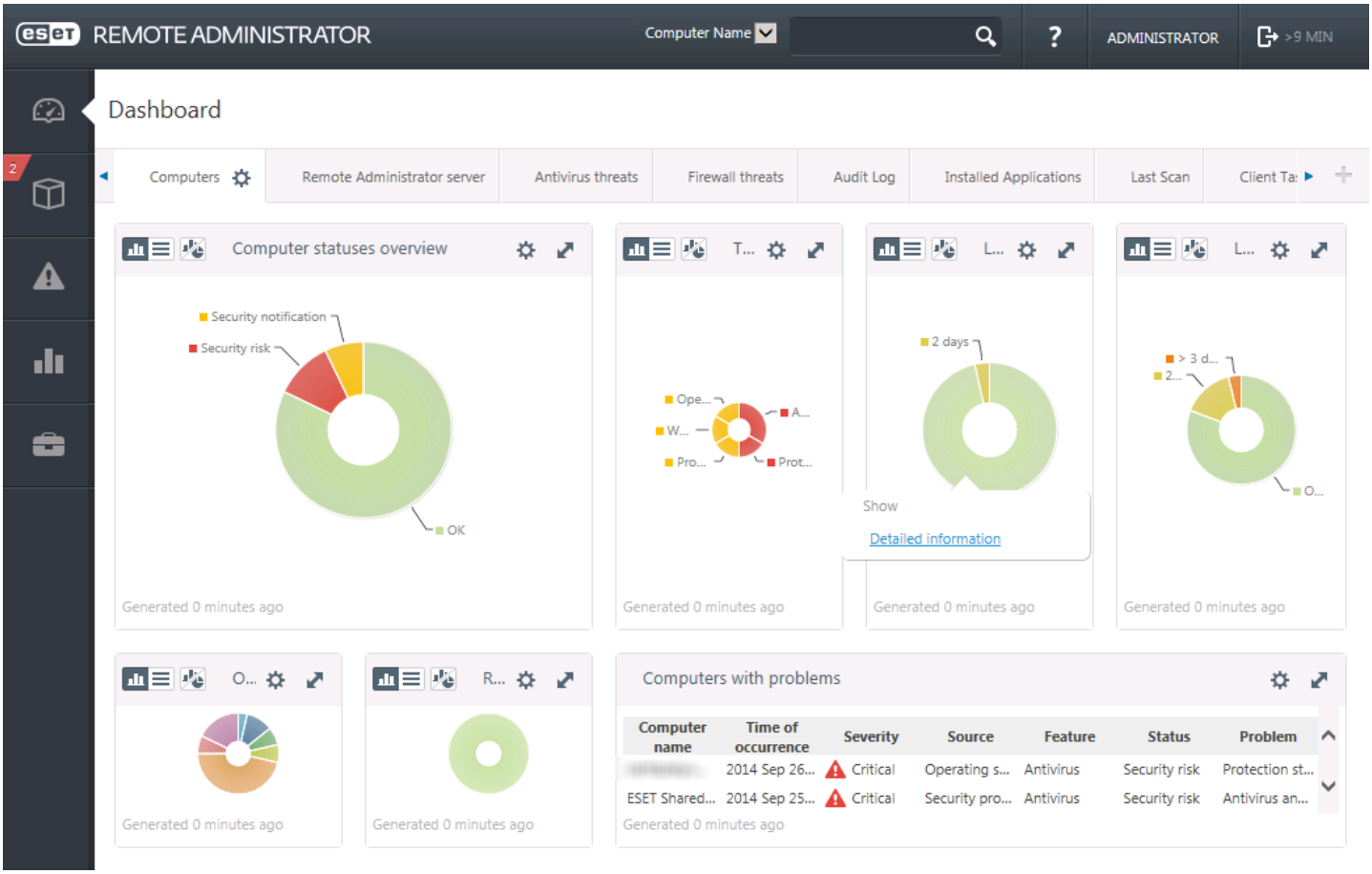
ESET Remote Administrator Server является главным компонентом продукта ESET Remote Administrator. Это приложение обрабатывает все данные, получаемые от клиентов, которые подключены к серверу через агент ERA. Агент ERA упрощает обмен данными между клиентом и сервером. Данные (файлы журналов клиентов, файлы конфигурации, файлы репликации агентов и т. д.) хранятся в базе данных, которой сервер ERA пользуется для создания отчетов.

Для правильной обработки данных серверу ERA требуется стабильное соединение с сервером базы данных. Для оптимальной производительности рекомендуется установить сервер ERA и базу данных на разные серверы. Компьютер, на котором установлен сервер ERA, должен быть настроен на прием всех запросов на подключение от агентов, прокси-сервера и компонента RD Sensor. Такие подключения проходят проверку с использованием сертификатов. После установки сервера ERA можно открыть веб-консоль ERA, позволяющую управлять конечными рабочими станциями, на которых установлены решения ESET.

2.2 Веб-консоль

Веб-консоль ERA — это приложение с веб-интерфейсом, которое отображает данные, полученные с сервера ERA, и позволяет управлять решениями безопасности ESET в сети. Доступ к веб-консоли можно получить с помощью браузера. В ней отображаются общие сведения о статусах клиентов в сети, и ее можно использовать для удаленного развертывания решений ESET на неуправляемых компьютерах. Если разрешить доступ к веб-серверу из Интернета, решение ESET Remote Administrator можно будет использовать практически в любом месте и на любом устройстве.

Панель мониторинга веб-консоли



В верхней части консоли расположено средство **Быстрый поиск**. В раскрывающемся меню выберите пункты **Имя компьютера**, **IPv4- или IPv6-адрес** или **Имя угрозы**, введите в текстовое поле поисковую фразу и щелкните значок лупы (либо нажмите клавишу **ВВОД**), чтобы начать поиск. Вы будете перенаправлены в раздел **Группы**, где будут показаны результаты поиска.

2.3 Прокси-сервер

Прокси-сервер ERA является еще одним компонентом ESET Remote Administrator, который выполняет две основные функции. В сетях среднего размера и корпоративных сетях с большим количеством клиентов (например, от 10 000 клиентов) прокси-сервер ERA может использоваться для распределения нагрузки между несколькими прокси-серверами ERA, снижая таким образом нагрузку на главный сервер ERA. Другим преимуществом прокси-сервера ERA является то, что его можно использовать для подключения к удаленном филиалу со слабой связью. Это означает, что установленные на всех клиентах агенты ERA не подключаются к главному серверу ERA напрямую через прокси-сервер ERA, который находится в локальной сети филиала. Таким образом освобождается канал связи с филиалом. Прокси-сервер ERA принимает подключения от всех локальных агентов ERA, получает от них данные и передает их на главный сервер ERA (или другой прокси-сервер ERA). Это позволяет подключать к сети больше клиентов без ухудшения ее производительности и качества запросов к базе данных.

В зависимости от конфигурации сети прокси-сервер ERA может подключаться к главному серверу ERA через другой прокси-сервер.

Чтобы прокси-сервер ERA работал правильно, на главном компьютере, на который устанавливается прокси-сервер ERA, нужно установить агент ESET, а сам компьютер необходимо подключить к верхнему уровню сети (серверу ERA или прокси-серверу ERA верхнего уровня).

2.4 Агент

Агент ERA является важной частью программы ESET Remote Administrator. Решения по обеспечению безопасности ESET, работающие на клиентских компьютерах (например, ESET Endpoint Security), обмениваются данными с сервером ERA посредством агентов. Это позволяет централизованно управлять решениями по обеспечению безопасности ESET, которые установлены на удаленных клиентах. Агент получает информацию от клиента и отправляет ее на сервер. Когда сервер отправляет задачу клиенту, ее вначале получает агент, который затем направляет ее клиенту. Передача данных по сети происходит между агентом и верхним уровнем сети ERA — сервером и прокси-сервером.

Для связи с сервером агент ESET использует один из трех методов, указанных ниже:

1. Агент клиента напрямую связывается с сервером.
2. Агент клиента связывается с сервером через прокси-сервер.
3. Агент клиента связывается с сервером через несколько прокси-серверов.

Агент ERA обменивается данными с установленными на клиенте решениями ESET, собирает информацию о программах, используемых на таком клиенте, и передает клиенту полученные от сервера сведения о конфигурации.

ПРИМЕЧАНИЕ: Прокси-сервер ESET имеет собственный агент, отвечающий за обмен данными с клиентами, другими прокси-серверами и сервером.

2.5 RD Sensor

RD (Rogue Detection) Sensor — это входящий в состав ESET Remote Administrator инструмент поиска компьютеров в сети. Компонент RD Sensor позволяет с легкостью добавлять новые компьютеры на сервер ESET Remote Administrator, избавляя от необходимости искать и добавлять их вручную. Каждый обнаруженный в сети компьютер отображается в веб-консоли и добавляется в группу по умолчанию «Все». После этого с отдельными клиентскими компьютерами можно выполнять дальнейшие действия.

Компонент RD Sensor пассивно прослушивает сеть, обнаруживая находящиеся в ней компьютеры и направляя информацию о них серверу ERA. Затем сервер ERA проверяет, являются ли обнаруженные ПК неизвестными или уже находятся под его управлением.

3. Удаленная установка

Чтобы установить программу ESET Endpoint Security с сервера ERA удаленно, требуется выполнить следующие действия:

- установить средство подключения для мобильных устройств;
- зарегистрировать мобильное устройство.

Есть два способа установки программы ESET Endpoint Security.

1. Администратор отправляет конечному пользователю по электронной почте ссылку для регистрации, установочный APK-файл и краткие инструкции по установке. Ссылка открывается в стандартном веб-браузере Android, после чего программа ESET Endpoint Security регистрируется и подключается к серверу ERA. Если программа ESET Endpoint Security на устройстве не установлена, пользователь автоматически будет перенаправлен в интернет-магазин Google Play, откуда ее можно загрузить. За этим последует стандартная установка.
2. Администратор отправляет конечному пользователю по электронной почте файл параметров приложения, установочный APK-файл и краткие инструкции по установке. Пользователю также можно предложить загрузить APK-файл из интернет-магазина Google Play, отправив ссылку на файл. После установки пользователь откроет файл параметров приложения, и все параметры будут импортированы, а приложение — активировано (если импортируемые данные содержали сведения о лицензии).

4. Локальная установка на устройство

ESET Endpoint Security дает администратору возможность настраивать это приложение и управлять им локально, если не используется ESET Remote Administrator. Все параметры приложения защищены администраторским паролем, поэтому администратор всегда и всецело контролирует приложение.

Если администратор небольшой компании не использует ESET Remote Administrator и при этом ему необходимо обеспечивать защиту корпоративных устройств и применять базовые политики безопасности, ему будут доступны два варианта локального управления устройствами.

1. Получить к каждому устройству компании физический доступ и настроить параметры вручную.
2. Администратор может подготовить необходимую конфигурацию на своем устройстве Android (на котором установлена программа ESET Endpoint Security) и экспортировать эти настройки в файл. Дополнительные сведения см. в разделе Импорт и экспорт параметров данного руководства.). Администратор может передать экспортированный файл конечным пользователям (например, по электронной почте), чтобы они могли импортировать его на любое устройство, на котором установлена программа ESET Endpoint Security. Когда пользователь открывает и принимает файл параметров, все параметры импортируются автоматически и приложение активируется (если в файл были включены сведения о лицензии). Все параметры будут защищены паролем администратора.

4.1 Загрузка с веб-сайта ESET

Загрузите <%PRODUCTNAME,%> просканировав находящийся ниже QR-код с помощью мобильного устройства и приложения для сканирования QR-кодов.

Кроме того, APK-файл для установки ESET Endpoint Security можно загрузить с веб-сайта ESET.

1. Загрузите установочный файл с веб-сайта ESET.
2. Откройте этот файл из области уведомлений Android или найдите его с помощью приложения для работы с файлами. Обычно файл сохраняется в папку загрузок.
3. Убедитесь, что приложения, полученные из неизвестных источников разрешены на вашем устройстве. Для этого коснитесь значка запуска на главном экране Android или последовательно выберите **Главный экран** > **Меню**. Нажмите **Параметры** > **Безопасность**. Использование **неизвестных источников** должно быть разрешено.
4. Открыв файл, нажмите **Установить**.

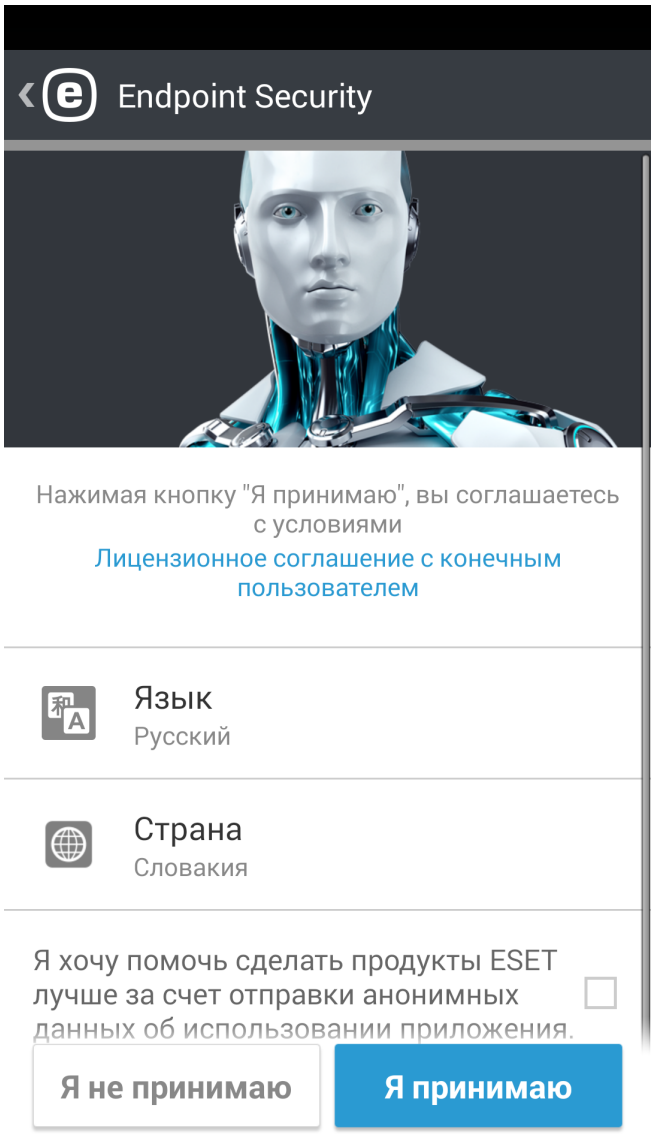
4.2 Загрузка из интернет-магазина Google Play

Откройте приложение магазина Google Play на устройстве Android и найдите программу ESET Endpoint Security (или просто ESET).

Кроме того, можно загрузить программу, воспользовавшись этой ссылкой или просканировав QR-код ниже:

https://play.google.com/store/apps/details?id=com.eset.endpoint

4.3 Мастер начальной настройки



После установки приложения нажмите **Настройки администратора** и следуйте подсказкам мастера начальной настройки. Эта процедура предназначена только для администраторов:

1. Выберите **язык,** который следует использовать в ESET Endpoint Security.
2. Выберите **страну,** в которой вы работаете или находитесь в настоящее время.
3. Если вы хотите помочь улучшить продукты ESET путем отправки анонимных данных об использовании приложения, установите соответствующий флажок.
4. Нажмите **Я принимаю**. Это будет означать, что вы принимаете условия лицензионного соглашения с конечным пользователем.
5. Нажмите **Я принимаю,** чтобы подтвердить согласие пользователя.
6. Выберите, что необходимо сделать: подключить ESET Endpoint Security к ESET Remote Administrator или выполнить настройку вручную.
7. Для настройки вручную необходимо активировать программу.
8. Создайте пароль администратора.
9. **Защита от удаления программы** не дает пользователям, которые не имеют соответствующего разрешения, удалить ESET Endpoint Security. Нажмите **Включить** и затем **Активировать** в сообщении **Администратор устройства** .
10. Выберите, нужно ли участвовать в системе ESET LiveGrid. Дополнительные сведения о системе ESET LiveGrid приведены в этом разделе..
11. Выберите, нужно ли программе ESET Endpoint Security обнаруживать потенциально нежелательные приложения. Дополнительные сведения о таких приложениях приведены в этом разделе..

5. Удаление

Программу ESET Endpoint Security можно удалить с помощью мастера удаления. Чтобы запустить его, в главном меню программы последовательно щелкните элементы **Параметры** > **Удалить**. Если включена защита от удаления программы, вам предложат ввести пароль администратора.

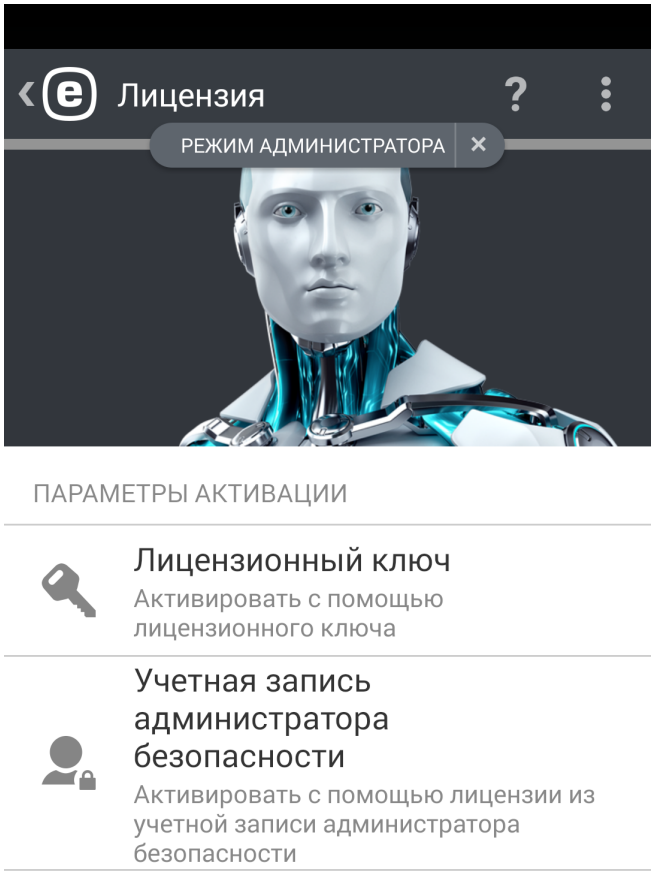
Программу можно удалить также и вручную. Для этого выполните следующие действия:

1. На главном экране ОС Android коснитесь значка запуска (или откройте **Основной экран** > **Меню**) и последовательно выберите элементы **Настройки** > **Безопасность** > **Администраторы устройства**. Снимите флажок рядом с программой ESET Endpoint Security и коснитесь элемента **Отключить**. Коснитесь элемента **Разблокировать** и введите пароль администратора. Если программа ESET Endpoint Security не указана в качестве администратора устройства, пропустите этот этап.
2. Вернитесь на экран **Настройки** и последовательно коснитесь элементов **Приложения** > ESET Endpoint Security > **Удалить**.

6. Активация продукта

Есть несколько способов активации ESET Endpoint Security. Доступность того или иного способа зависит от страны и того, как продукт был получен (с веб-страницы ESET и т. д.).

Чтобы активировать ESET Endpoint Security непосредственно на устройстве Android, нажмите значок **Меню** на главном экране программы ESET Endpoint Security (или нажмите кнопку **МЕНЮ** на устройстве) и выберите элемент **Лицензия**.



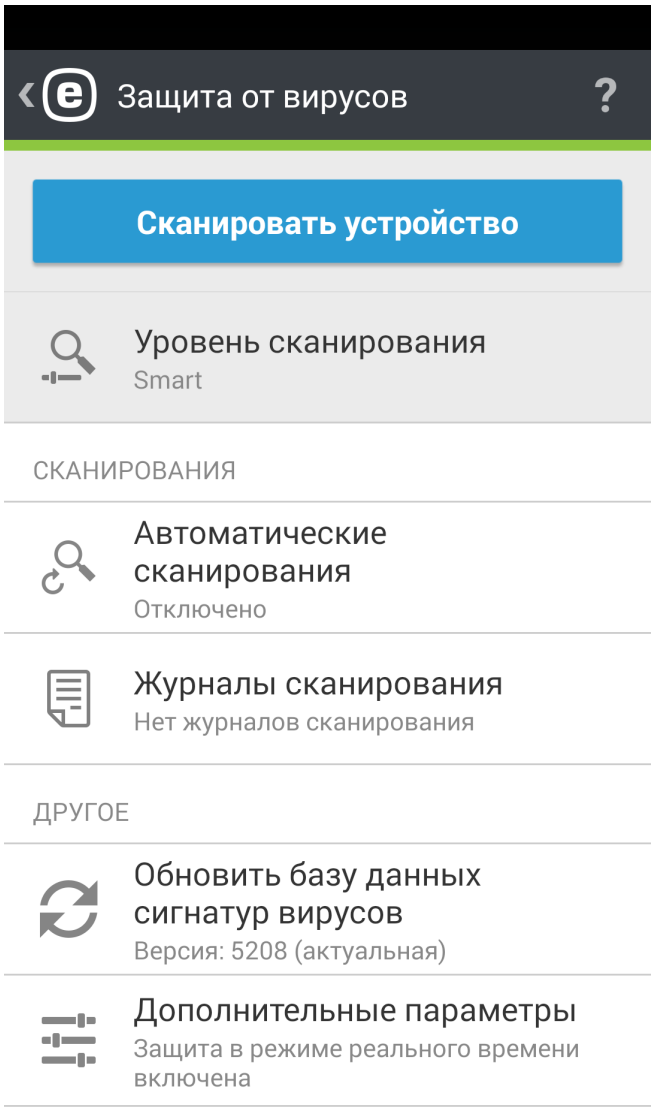
Можно воспользоваться любым из перечисленных ниже способов для активации ESET Endpoint Security:

- **Лицензионный ключ**-уникальная строка в формате XXXX-XXXX-XXXX-XXXX-XXXX, которая используется для идентификации владельца лицензии и активации лицензии.
- **Учетная запись администратора безопасности**-учетная запись, созданная на портале ESET License Administrator с указанием учетных данных (адреса электронной почты и пароля). Этот способ позволяет централизовано управлять несколькими лицензиями.

ПРИМЕЧАНИЕ: ESET Remote Administrator может активировать клиентские устройства в автоматическом режиме, используя предоставленные администратором лицензии.

7. Защита от вирусов

Модуль защиты от вирусов защищает устройство от вредоносного кода, блокируя угрозы и затем удаляя их или перемещая в карантин.



Сканирование устройства

Функцию «Сканировать устройство» можно использовать для проверки устройства на наличие заражений.

Некоторые предварительно заданные типы файлов сканируются по умолчанию. Во время полного сканирования проверяются память, запущенные процессы, зависимые от них динамические библиотеки, а также файлы, находящиеся на съемных носителях и во внутреннем хранилище. Сводные сведения о результатах сканирования сохраняются в файл журнала в разделе «Журналы сканирования».

Чтобы прервать запущенное сканирование, коснитесь значка .

Уровень сканирования

Доступны два уровня сканирования.

- **Сканирование Smart**. Во время сканирования Smart проверяются установленные приложения, DEX-файлы (исполняемые файлы для ОС Android), SO-файлы (библиотеки), ZIP-файлы (максимальная глубина сканирования — три уровня вложения в архиве) и содержимое SD-карт.
- **Тщательное сканирование**. В этом режиме проверяются файлы всех типов с любыми расширениями, находящиеся во внутреннем хранилище и на SD-карте.

Автоматические сканирования

Кроме сканирования по требованию, приложение ESET Endpoint Security выполняет автоматическое сканирование. Сведения об использовании функций «Сканирование при зарядке» и «Запланированное сканирование» см. в этом разделе.

Журналы сканирования

В области интерфейса «Журналы сканирования» находятся файлы журналов, содержащие подробные сведения о выполненных сканированиях. Дополнительные сведения см. в разделе этого документа Журналы сканирования средства защиты от вирусов.

Обновление базы данных сигнатур вирусов

По умолчанию программа ESET Endpoint Security регулярно загружает и устанавливает обновления. Это происходит автоматически. Чтобы обновить ее вручную, коснитесь элемента **Обновление базы данных сигнатур вирусов**.

ПРИМЕЧАНИЕ. Чтобы не загружать напрасно полосу пропускания, обновления выпускаются только тогда, когда в базу данных добавляется новая угроза. Обновления для активированного продукта предоставляются бесплатно, но за передачу данных в мобильной сети может взиматься плата.

Подробные сведения о дополнительных параметрах защиты от вирусов можно найти в разделе Дополнительные параметры этого документа.

7.1 Автоматические сканирования

Уровень сканирования

Доступны два уровня сканирования. Этот параметр применяется во время сканирования в процессе зарядки и сканирования по расписанию.

- **Сканирование Smart**. Во время сканирования Smart проверяются установленные приложения, DEX-файлы (исполняемые файлы для ОС Android), SO-файлы (библиотеки), ZIP-файлы (максимальная глубина сканирования — три уровня вложения в архиве) и содержимое SD-карт.
- **Тщательное сканирование**.В этом режиме проверяются файлы всех типов с любыми расширениями, находящиеся во внутреннем хранилище и на SD-карте.

Сканирование в процессе зарядки

Если выбран этот параметр, сканирование начинается автоматически, когда устройство находится в состоянии простоя (полностью заряжено и подключено к зарядному устройству).

Сканирование по расписанию

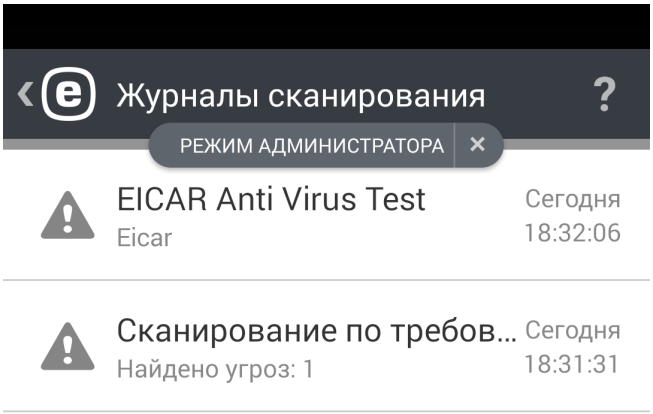
Этот параметр позволяет указывать время, когда устройство будет сканироваться автоматически. Чтобы запланировать сканирование, коснитесь значка  рядом с элементом **Сканирование по расписанию** и укажите дату и время начала сканирования. По умолчанию начало запланировано на понедельник в 4:00.

7.2 Журналы сканирования

Журналы сканирования создаются после каждого запланированного или запущенного вручную сканирования.

Каждый журнал содержит такие сведения:

- дата и время события;
- продолжительность сканирования;
- количество просканированных файлов;
- результаты сканирования или ошибки, обнаруженные во время сканирования.



7.3 Правила игнорирования

Если управление приложением ESET Endpoint Security осуществляется удаленно с помощью ERA, у пользователя есть возможность указать файлы, которые не будут отнесены к разряду вредоносных. Файлы, добавленные в разделе **Правила игнорирования**, при будущих сканированиях будут игнорироваться. Чтобы создать правило, необходимо указать следующее.

- имя файла с надлежащим расширением apk;
- имя пакета приложения, например *uk.co.extorian.EICARAntiVirusTest*;
- имя угрозы, определяемое антивирусными программами, например *Android/MobileTX.A* (это поле является обязательным).

ПРИМЕЧАНИЕ. Эта функция недоступна в приложении ESET Endpoint Security.

7.4 Дополнительные параметры

Защита в режиме реального времени

Этот параметр позволяет включать и отключать модуль сканирования в режиме реального времени. Модуль автоматически начинает проверку при запуске системы и сканирует файлы, с которыми работает пользователь. Он автоматически сканирует папки загрузок, установочные APK-файлы и содержимое SD-карты.

ESET LiveGrid

Система ESET LiveGrid, основанная на современной системе своевременного обнаружения ThreatSense.Net, предназначена для повышения уровня безопасности компьютера. Она непрерывно отслеживает запущенные на компьютере программы и процессы и сравнивает их с новейшими сведениями, полученными от миллионов пользователей ESET по всему миру. Кроме того, по мере увеличения базы данных ESET LiveGrid увеличивается скорость и точность сканирования. Это позволяет обеспечивать более качественную упреждающую защиту и более высокую скорость сканирования для всех пользователей ESET. Рекомендуется активировать эту функцию. Благодарим за поддержку.

Обнаружение потенциально нежелательных приложений

Нежелательное приложение отличается тем, что содержит рекламу, устанавливает панели инструментов и выполняет другие неясные функции. В некоторых ситуациях может показаться, что преимущества такого приложения перевешивают риски. Поэтому компания ESET помещает эти приложения, в отличие от других вредоносных программ, в категорию незначительного риска.

Обнаружение потенциально опасных приложений

Существует множество надежных программ, которые упрощают администрирование подключенных к сети компьютеров. Однако злоумышленники могут использовать их для причинения вреда. С помощью параметра «Определять потенциально опасные приложения» можно отслеживать и, если нужно, блокировать такие приложения. *Потенциально опасными приложениями* считаются нормальные коммерческие программы. В эту категорию входят такие программы, как средства удаленного доступа, приложения для взлома паролей и клавиатурные шпионы.

Блокировать неразрешенные угрозы

С помощью этого параметра определяется действие, которое будет выполняться после того, как сканирование завершено и обнаружены угрозы. Если включить этот параметр, ESET Endpoint Security будет блокировать доступ к файлам, классифицированным как угрозы.

Обновления базы данных сигнатур вирусов

Этот параметр позволяет задать период времени, в соответствии с которым автоматически загружаются обновления базы данных угроз. Эти обновления выпускаются, когда в базу данных добавляется новая угроза. Рекомендуется оставить значение по умолчанию (ежедневно).

Пользовательское значение макс. возраста базы данных

С помощью этого параметра задается период между обновлениями базы данных сигнатур вирусов, после которого пользователь получает уведомление о необходимости обновить ESET Endpoint Security.

Сервер обновлений

С помощью этого параметра устройство можно обновлять с **сервера тестовых обновлений**. Тестовые обновления — это обновления, которые уже прошли полное внутреннее тестирование и в ближайшее время будут доступны всем пользователям. Их преимущество заключается в том, что у вас появляется доступ к новейшим исправлениям и способам обнаружения. Однако иногда такие обновления могут быть недостаточно стабильны. Список доступных модулей можно просмотреть в области интерфейса **О программе**. Щелкните значок меню  на главном экране ESET Endpoint Security, а затем выберите **О программе** > ESET Endpoint Security. Неопытным пользователям рекомендуется для параметра **Сервер выпусков** оставить значение по умолчанию.

Программа ESET Endpoint Security дает возможность создавать копии файлов обновления, которые могут использоваться для обновления других устройств в сети. Использование **локального зеркала** (копии файлов обновления в локальной сети) позволяет избежать загрузки одних и тех же файлов обновления с сервера поставщика всеми мобильными устройствами. Подробная информация о том, как настроить сервер зеркала, используя продукты ESET Endpoint для Windows, приведена в этом документе.

8. Антивор

Компонент **Антивор** защищает мобильное устройство от несанкционированного доступа.

Если устройство потеряется или его украдут и заменят в нем SIM-карту на новую (недоверенную), приложение ESET Endpoint Security автоматически заблокирует его и на указанные пользователем номера будут отправлены SMS-оповещения. В этом оповещении будет указан телефонный номер новой SIM-карты, идентификатор IMSI (International Mobile Subscriber Identity — международный идентификатор абонента мобильной связи) и идентификатор IMEI (International Mobile Equipment Identity — международный идентификатор мобильного оборудования) телефона. Неавторизованный пользователь не узнает об отправке этого сообщения, поскольку оно будет незамедлительно удалено из потоков сообщений на устройстве. Кроме того, вы можете запросить GPS-координаты потерянного устройства или удаленно уничтожить все сохраненные на устройстве данные.

ПРИМЕЧАНИЕ. Некоторые возможности компонента «Антивор» (доверенные SIM-карты и текстовые команды через SMS) недоступны на планшетах, которые не поддерживают обмен сообщениями.

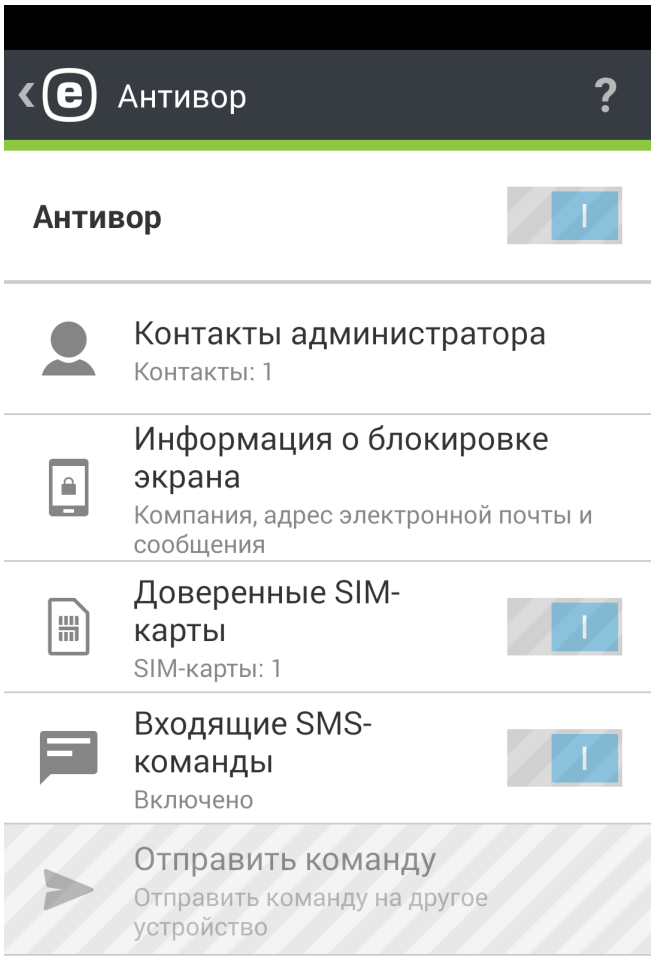
Возможности компонента «Антивор» помогают администраторам защитить и найти пропавшее устройство. Выполнение действий можно инициировать с сервера ERA или посредством SMS-команд.

В решении ESET Endpoint Security 2 используются те же SMS-команды, что и в версии 1 («Блокировать», «Очистить» и «Найти»). Кроме того, в новую версию добавлены новые команды.

- **Разблокировать**. Если выполнить эту команду, устройство будет разблокировано.
- **Расширенный сброс до заводских установок**. Все доступные на устройстве данные будут удалены (заголовки файлов будут уничтожены). Кроме того, на телефоне будут восстановлены заводские настройки по умолчанию.
- **Сирена**. Потерянное устройство блокируется и начинает издавать очень громкий звук, даже если звук на устройстве отключен.

В целях увеличения безопасности SMS-команд администратор при выполнении SMS-команды будет получать на свой мобильный телефон уникальный и ограниченный по времени SMS-код (на номер, значащийся в списке контактов администратора). Этот код используется для проверки определенной команды.

Отправив на управляемое устройство (например, потерянный мобильный телефон) SMS-сообщение с текстом *eset lock,* администратор получит SMS-сообщение с кодом проверки для этой команды. После этого администратор должен на этот же номер телефона отправить SMS-сообщение с текстом *eset lock* и кодом подтверждения после него. И только теперь, после этой проверки, команда будет выполнена. SMS-команду можно отправить с любого мобильного телефона и с любого номера, указанного в контактах администратора.



Выполняя команду через SMS, администратор получает SMS-подтверждение отправки команды. Выполняя команду на сервере ERA, администратор получает подтверждение на сервере.

Сведения о расположении, которые получает администратор, выполняя команду «Найти» (если при этом используется решение ESET Remote Administrator), отображаются в виде GPS-координат. Если команда выполняется через SMS, сведения о расположении (GPS-координаты и ссылка на карты Google) приходят тоже через SMS. Если для выполнения SMS-команд используется графический интерфейс (функция **Отправить команду**), информация о расположении отображается также в соответствующем интерфейсе.

Команды компонента «Антивор» можно выполнять и с сервера ERA. Новые функции управления мобильными устройствами позволяют администраторам быстро выполнить любую команду компонента «Антивор». Новый компонент передачи и обработки команд (средство подключения для мобильных устройств), ставший частью инфраструктуры ERA, позволяет без задержек передавать задачи на выполнение.

8.1 Контакты администратора

Речь идет о списке, который включает в себя номера телефонов администратора и который защищен администраторским паролем. Команды компонента «Антивор» можно отправлять только с доверенных номеров. Кроме того, на них приходят уведомления о действиях этого компонента.

8.1.1 Добавление контактов администратора

Имя и номер телефона администратора нужно вводить, когда работает мастер запуска компонента «Антивор». Если контакт содержит более одного номера телефона, то учитываться будут все номера.

Контакты администратора можно добавить или изменить в разделе **Антивор** > **Контакты администратора**.

8.2 Информация на заблокированном экране

Администратор может указать, какая информация может отображаться на экране заблокированного устройства (имя компании, адрес электронной почты, сообщение). При этом можно включить звонок одному из предварительно заданных контактов администратора.

Отображаться может следующая информация:

- имя компании (необязательно);
- адрес электронной почты (необязательно);
- пользовательское сообщение.

8.3 Доверенные SIM-карты

В области интерфейса **Доверенная SIM-карта** отображается список SIM-карт, которые приложение ESET Endpoint Security считает доверенными. Если вставить SIM-карту, которой в списке нет, экран будет заблокирован и администратору будет отправлено SMS-оповещение.

Чтобы добавить новую SIM-карту, коснитесь значка ✚. Введите **имя** SIM-карты (например, «Дом», «Работа») и ее идентификатор IMSI (International Mobile Subscriber Identity — международный идентификатор абонента мобильной связи). Идентификатор IMSI обычно нанесен на SIM-карту и состоит из 15 цифр. Иногда он может быть короче.

Чтобы удалить SIM-карту, коснитесь имени карты и задержите на нем палец, а затем коснитесь значка  .

ПРИМЕЧАНИЕ. Функция «Доверенная SIM-карта» недоступна на устройствах CDMA и WCDMA, а также на устройствах, в которых используется только WiFi.

8.4 Удаленные команды

Существует три способа запуска удаленных команд:

- непосредственно в консоли ERA;
- с помощью функции **Отправить команду** в программе ESET Endpoint Security, установленной на устройстве Android администратора;
- путем отправки текстовых сообщений (SMS) с устройства администратора.

Для удобства администраторов, не использующих сервер ERA, SMS-команды можно запускать из программы ESET Endpoint Security, установленной на устройстве Android администратора. Вместо того чтобы вручную набирать текст сообщения и подтверждать команду с помощью кода проверки, администратор может воспользоваться функцией **Отправить команду** (доступна только в режиме администрирования). Администратор может ввести номер телефона или выбрать контакт, а затем в раскрывающемся меню указать команду, которую необходимо отправить. ESET Endpoint Security автоматически выполнит все необходимые действия в фоновом режиме.

При отправке SMS-команд номер телефона администратора должен быть сохранен на целевом устройстве как контакт администратора. Администратор получит код проверки, действительный в течение одного часа, который можно использовать для выполнения любых перечисленных далее команд. Этот код добавляется в сообщение с командой в следующем формате: `eset find код`. После того как команда будет выполнена на целевом устройстве, администратор получит подтверждение. Можно отправить следующие SMS-команды.

Найти
SMS-команда: `eset find`
Вы получите текстовое сообщение, содержащие GPS-координаты целевого устройства и ссылку на его расположение на картах Google. Через 10 минут устройство отправит еще одно сообщение, если появятся более точные координаты местонахождения.

Заблокировать
SMS-команда: `eset lock`
Эта команда заблокирует устройство. Впоследствии вы сможете разблокировать его с помощью пароля администратора или удаленной команды разблокировки. При отправке этой SMS-команды можно добавить свое сообщение, которое будет отображаться на экране заблокированного устройства. Используйте следующий формат: `eset lock код сообщение`. Если оставить этот параметр сообщения пустым, отобразится сообщение из раздела Информация о блокировке экрана.

Разблокировать
SMS-команда: `eset unlock`
Устройство будет разблокировано, а используемая в устройстве SIM-карта будет сохранена как доверенная.

Сирена
SMS-команда: `eset siren`
Громкий звук сирены будет воспроизводиться, даже если на устройстве отключен звук.

Расширенный сброс до заводских установок
SMS-команда: `eset enhanced factory reset`
На устройстве будут восстановлены заводские настройки. Все доступные данные будут удалены, а заголовки файлов будут уничтожены. Процесс может занять несколько минут.

Очистить
SMS-команда: `eset wipe`
С устройства будут безвозвратно удалены контакты, SMS-сообщения, сообщения электронной почты, учетные записи, содержимое SD-карты, изображения, музыка и видеофайлы, хранящиеся в папках по умолчанию. Приложение ESET Endpoint Security останется.

ПРИМЕЧАНИЕ. SMS-команды можно вводить без учета регистра.

9. Контроль приложений

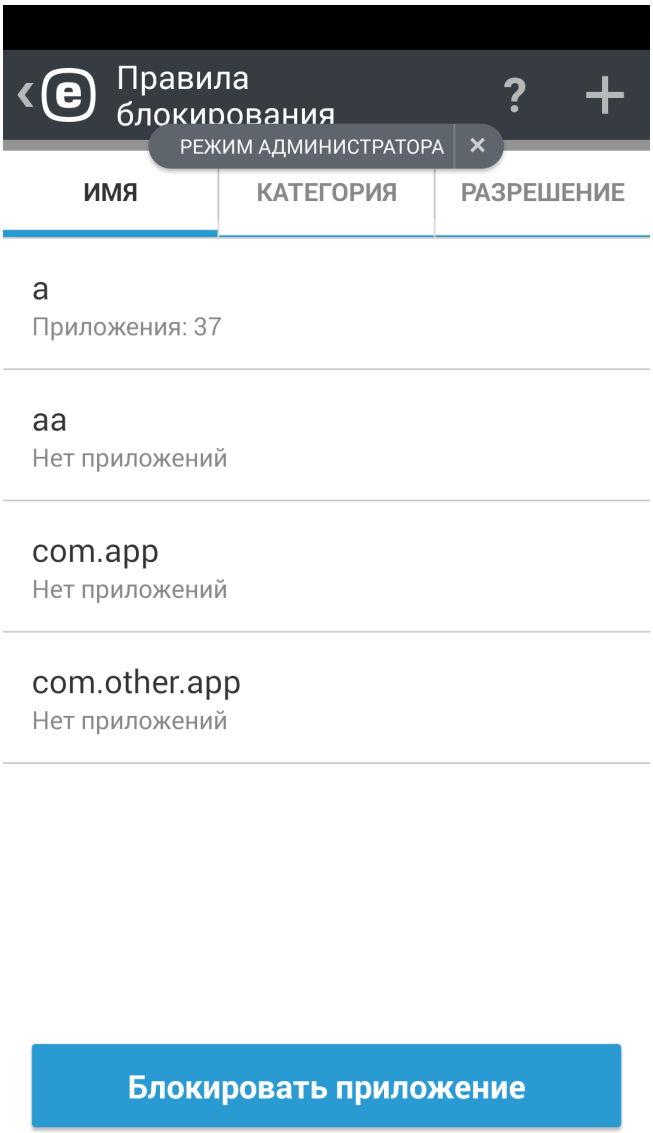
Контроль приложений позволяет администраторам отслеживать установленные приложения, блокировать доступ к определенным приложениям и снижать степень риска, предлагая пользователям удалить некоторые программы. Администратору доступны следующие способы фильтрации приложений:

- блокировка приложений, указанных вручную;
- блокировка приложений по категориям (например, игры или программы для общения);
- блокировка на основе разрешений (например, программы, которые отслеживают расположение пользователя);
- блокировка по источникам (например, приложений, установленных не из магазина Google Play).

9.1 Правила блокирования

В области интерфейса **Контроль приложений** > **Блокирование** > **Правила блокирования** можно создавать правила блокирования приложений на основании следующих критериев:

- имя приложения или пакета;
- категория;
- разрешения.



9.1.1 Блокировка по имени приложения

С помощью ESET Endpoint Security администратор может блокировать приложения по их имени или по имени пакета. В разделе **Правила блокирования** представлены общие сведения о созданных правилах и список заблокированных приложений.

Для изменения существующего правила коснитесь и удерживайте его, а затем выберите пункт **Изменить**  . Чтобы удалить из списка несколько записей с правилами, коснитесь одного правила и задержите на нем палец, а затем выделите остальные правила, которые нужно удалить, после чего выберите команду **Удалить**  .

Чтобы удалить все правила в списке, коснитесь элемента **ВЫДЕЛИТЬ ВСЕ** и выберите команду **Удалить**  .

Блокируя приложение по имени, ESET Endpoint Security будет искать точное соответствие с именем запущенного приложения. При изменении языка интерфейса программы ESET Endpoint Security необходимо повторно ввести имя приложения для этого языка, чтобы продолжить его блокировку.

Во избежание возможных проблем, связанных с локализованными именами приложений, рекомендуется блокировать такие приложения по имени пакета — уникальному идентификатору, который не может быть изменен во время выполнения или повторно использован другим приложением.

При наличии прав локального администратора пользователь может найти имя пакета приложения, выбрав **Контроль приложений** > **Отслеживание** > **Разрешенные приложения**. Если коснуться значка приложения, отобразится экран **Подробности**, содержащий имя пакета приложения. Чтобы заблокировать приложение, выполните следующие действия.

9.1.1.1 Блокировка приложений по имени

1. Последовательно коснитесь элементов **Контроль приложений** > **Блокирование** > **Блокировать приложение** > **Блокировать по имени**.
2. Укажите, по какому свойству нужно блокировать приложения: по имени приложения или по имени пакета.
3. Введите слова, которые должны присутствовать в имени, чтобы приложение было заблокировано. Для разделения нескольких слов используйте запятую (,).

Например, если в поле **Имя приложения** ввести слово «*poker*», будут заблокированы все приложения, имена которых содержат слово «*poker*». Если в поле **Имя пакета** ввести «*com.poker.game*», программа ESET Endpoint Security заблокирует только одно приложение.

9.1.2 Блокировка по категории приложений

Приложение ESET Endpoint Security позволяет администратору блокировать приложения, относящиеся к тем или иным предварительно заданным категориям. В разделе **Правила блокирования** доступны сводные сведения о созданных правилах и список заблокированных приложений.

Если нужно изменить существующее правило, коснитесь его имени и задержите на нем палец, а затем коснитесь команды **Изменить**  .

Чтобы удалить несколько правил из списка, коснитесь одного правила и задержите на нем палец, затем выберите остальные правила, которые нужно удалить, и выберите команду **Удалить**  . Чтобы удалить все правила в списке, коснитесь элемента **ВЫДЕЛИТЬ ВСЕ**.

9.1.2.1 Блокировка приложений по категориям

1. Последовательно коснитесь элементов **Контроль приложений** > **Блокировка** > **Блокировать приложение** > **Блокировать по категории**.
2. Установите флажки напротив предварительно заданных категорий и нажмите кнопку **Блокировать**.

9.1.3 Блокировка приложений по типу разрешений

Программа ESET Endpoint Security позволяет администратору блокировать приложения на основании их разрешений. В разделе **Правила блокирования** доступны сводные сведения о созданных правилах и список заблокированных приложений.

Если нужно изменить существующее правило, коснитесь его имени и задержите на нем палец, а затем коснитесь команды **Изменить** .

Чтобы удалить несколько правил из списка, коснитесь одного правила и задержите на нем палец, затем выберите остальные правила, которые нужно удалить, и выберите команду **Удалить** . Чтобы удалить все правила в списке, коснитесь элемента **ВЫДЕЛИТЬ ВСЕ**.

9.1.3.1 Блокировка приложений по типу разрешений

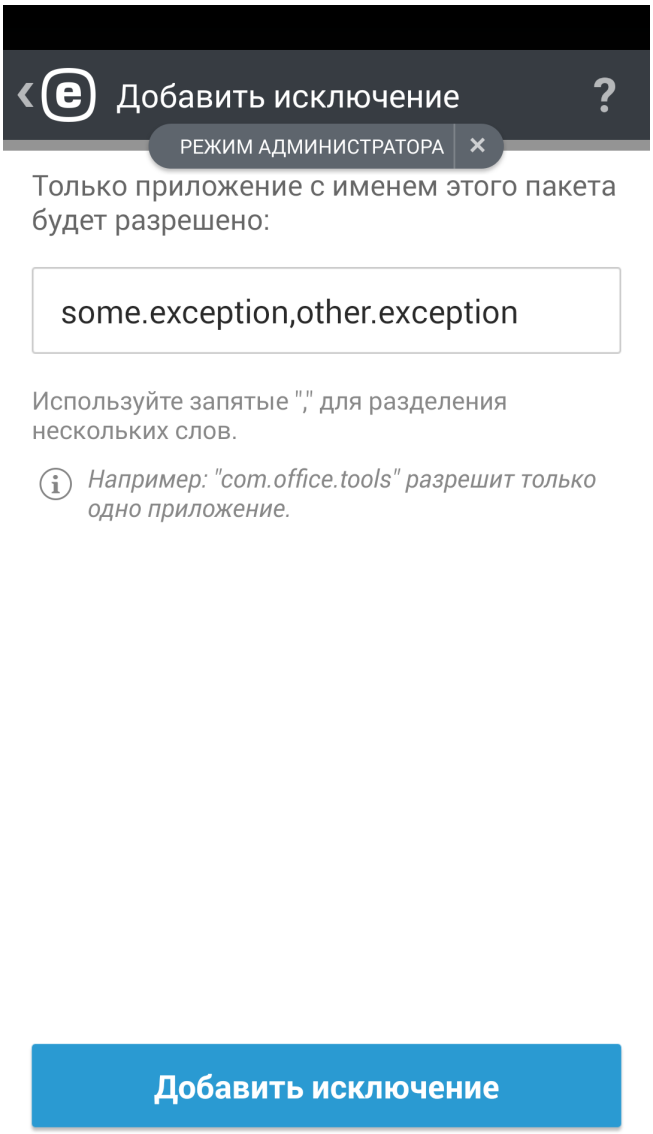
1. Последовательно коснитесь элементов **Контроль приложений** > **Блокирование** > **Блокировать приложение** > **Блокировать по типу разрешений**.
2. Установите флажки напротив разрешений и нажмите кнопку **Блокировать**.

9.1.4 Блокировка неизвестных источников

По умолчанию ESET Endpoint Security не блокирует приложения, полученные из Интернета или любого другого источника, кроме магазина Google Play. В области интерфейса **Заблокированные приложения** доступны сводные сведения о заблокированных программах (имя пакета, применяемое правило), а также возможность удалить приложение или добавить его в «белый» список (находящийся в области интерфейса **Исключения**).

9.2 Исключения

Чтобы удалить ту или иную программу из списка заблокированных приложений, можно создать исключения. Администраторы, управляющие приложением ESET Endpoint Security удаленно, могут с помощью этой новой функции определять, соответствует ли то или иное устройство корпоративной политике по установленным приложениям.



9.2.1 Добавление исключений

Приложение можно не только исключить (путем ввода имени пакета приложения), но и добавить в «белый» список, удалив его из списка **Заблокированные приложения**.

9.3 Обязательные приложения

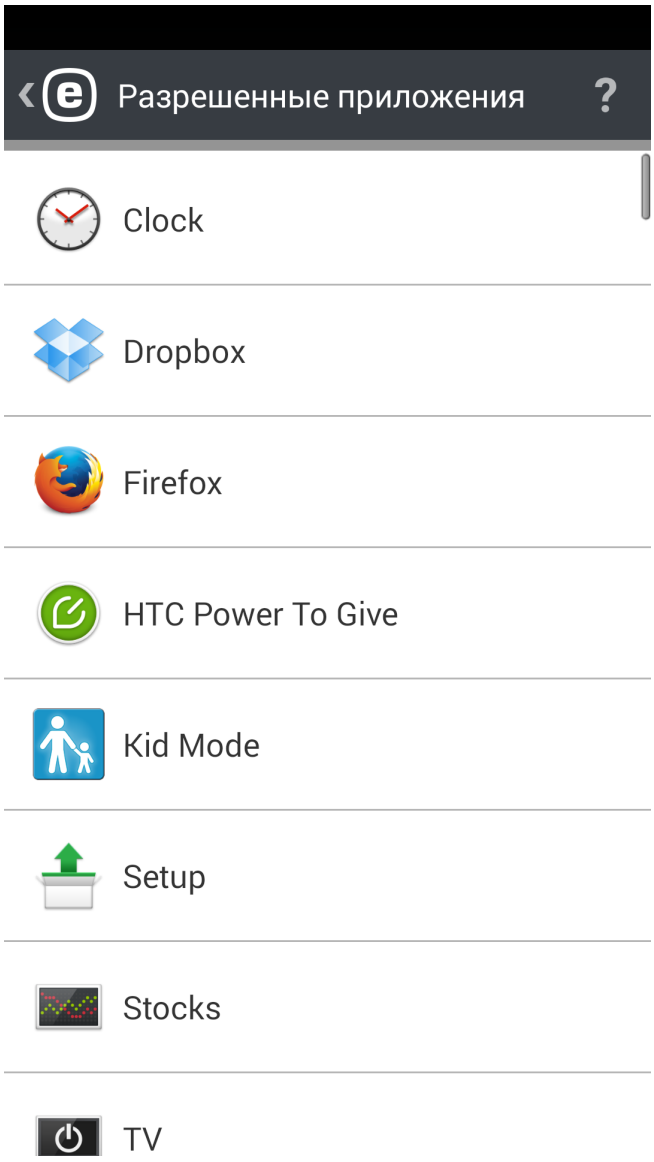
Если управление приложением ESET Endpoint Security осуществляется удаленно с помощью ERA, у пользователя есть возможность указать приложения, которые должны быть установлены на целевых устройствах. Необходимо указать следующие сведения:

- имя приложения, отображаемое для пользователя;
- уникальное имя пакета приложения, например *com.eset.ems2.gp*;
- URL-адрес, по которому пользователь может найти ссылку для загрузки. Можно также использовать ссылки Google Play, например *https://play.google.com/store/apps/details?id=com.eset.ems2.gp*.

ПРИМЕЧАНИЕ. Эта функция недоступна в приложении ESET Endpoint Security.

9.4 Разрешенные приложения

Этот раздел содержит информацию об установленных приложениях, которые не блокируются согласно правилам блокирования.

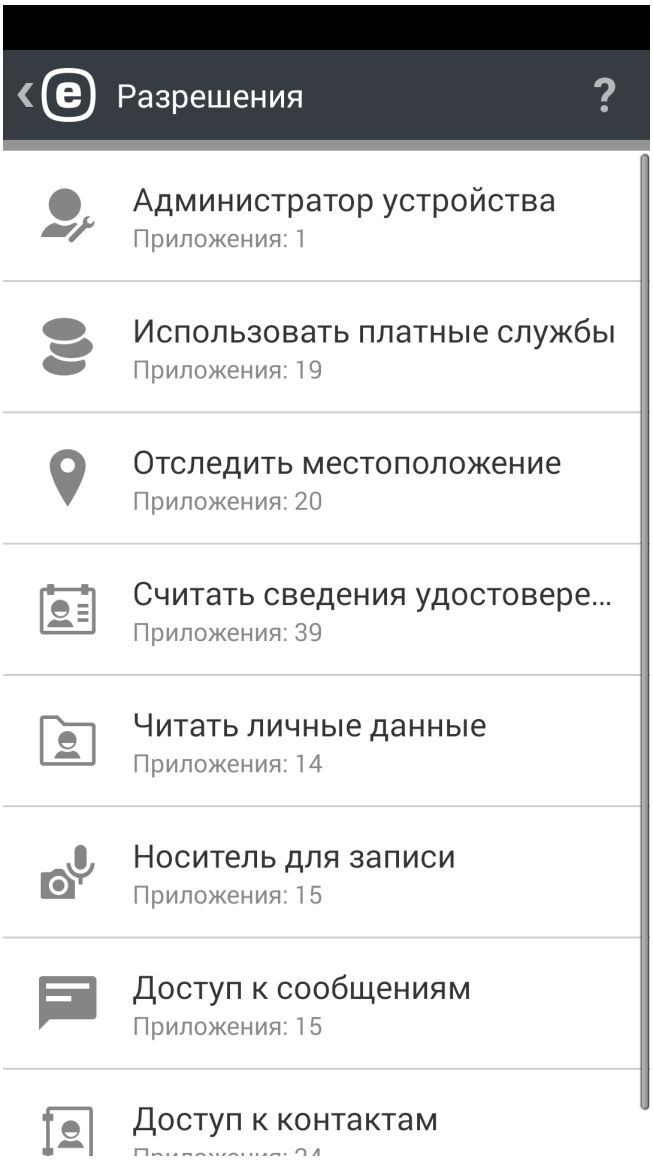


9.5 Разрешения

Эта функция отслеживает поведение приложений, у которых есть доступ к личным или корпоративным данным. Кроме того, используя предварительно заданные категории разрешений, администраторы могут контролировать, к каким данным приложения получают доступ.

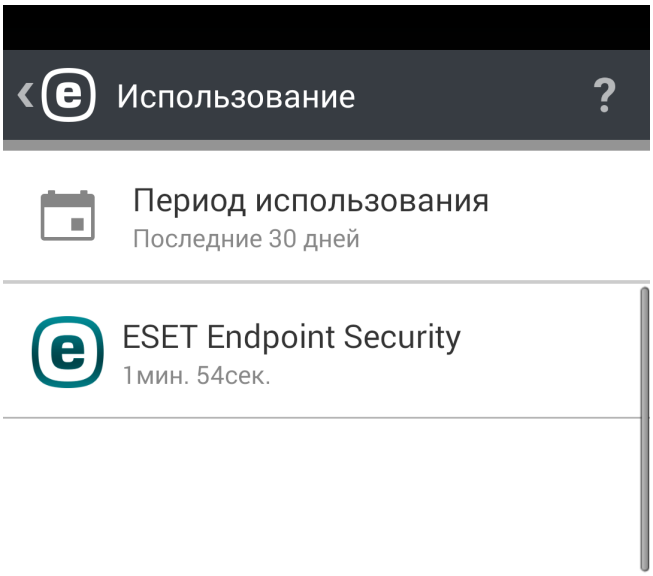
Некоторые приложения, установленные на вашем устройстве могут иметь доступ к платным услугам, отслеживать ваше местоположение либо считывать ваши идентификационные данные, контакты или текстовые сообщения. ESET Endpoint Security проводит аудит таких приложений.

Этот раздел содержит список приложений, отсортированных по категориям. Выберите категорию, чтобы увидеть ее подробное описание. Сведения о разрешениях отдельного приложения можно получить, нажав на это приложение.



9.6 Использование

В этой области интерфейса администратор может отслеживать, сколько времени пользователь работает с тем или иным приложением. Чтобы отфильтровать общие сведения по периоду использования, используйте параметр **Интервал**.

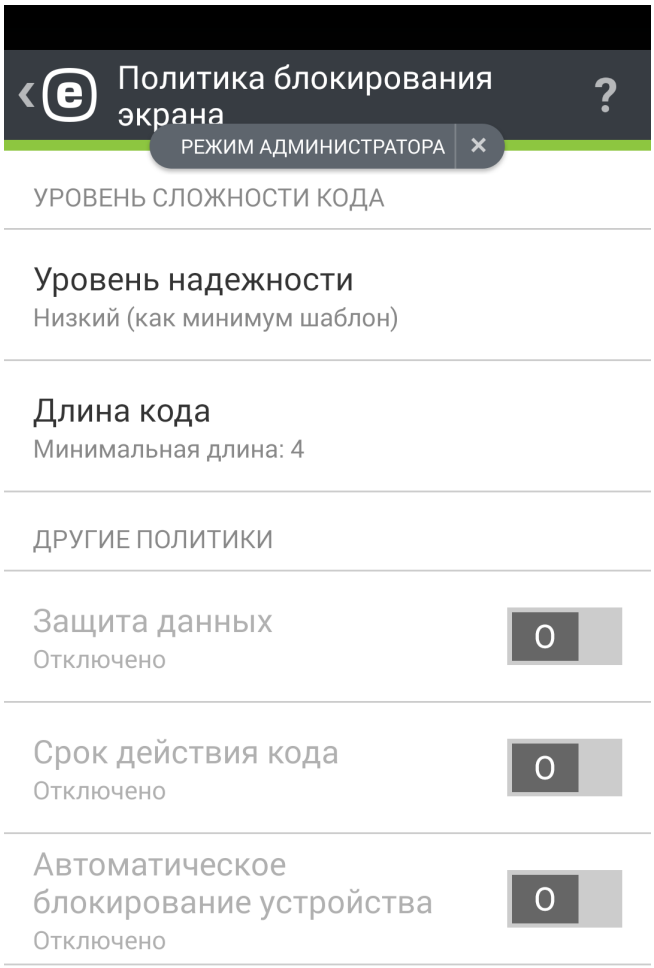


10. Безопасность устройства

В разделе **Безопасность устройства** администратор может:

- выполнять базовые политики безопасности на мобильных устройствах и определять политики, касающиеся важных параметров устройства;
- указывать необходимый уровень сложности разблокировки экрана;
- ограничивать использование встроенной камеры.

10.1 Политика блокирования экрана



В этой области интерфейса администратор может выполнить следующие действия:

- задать минимальный уровень безопасности (разблокировка экрана с помощью графического ключа, PIN-кода или пароля) и настроить сложность кода разблокировки экрана (например, минимальную длину);
- указать максимальное количество неудачных попыток разблокировки, после которых настройки устройства будут сброшены до заводских;
- указать максимальный возраст кода блокировки экрана;
- настроить таймер блокировки экрана.

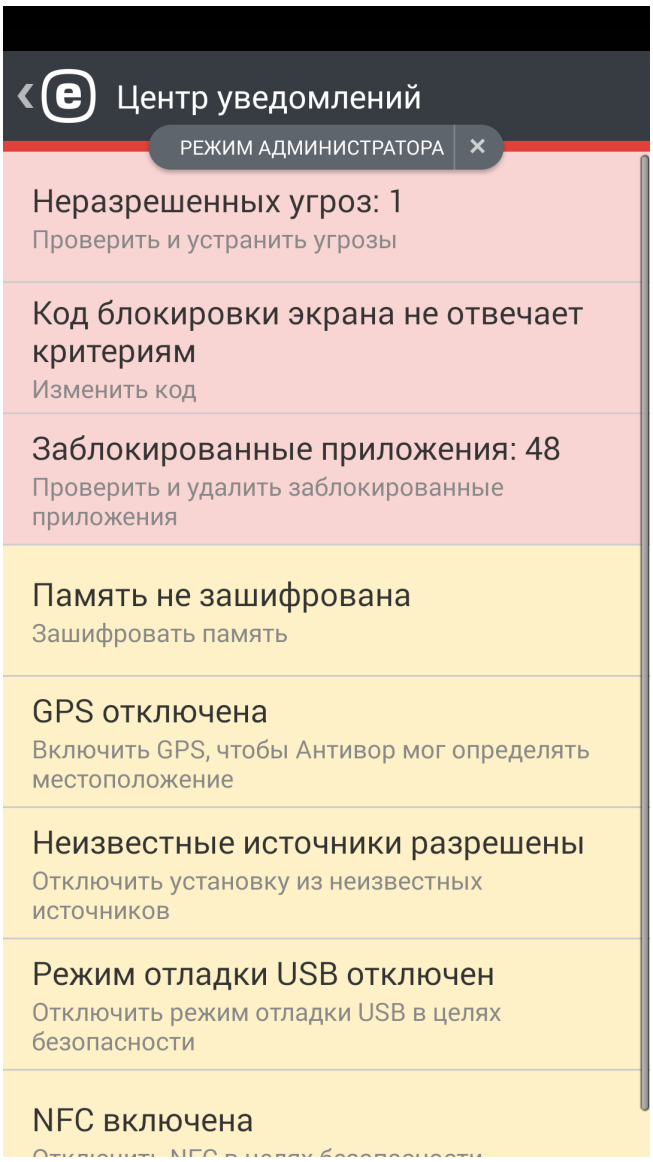
Решение ESET Endpoint Security автоматически уведомляет пользователя и администратора, соответствуют ли текущие параметры устройства корпоративным политикам безопасности. Если устройство политикам не соответствует, приложение автоматически предлагает пользователю возможное решение проблемы.

10.2 Политика настроек устройства

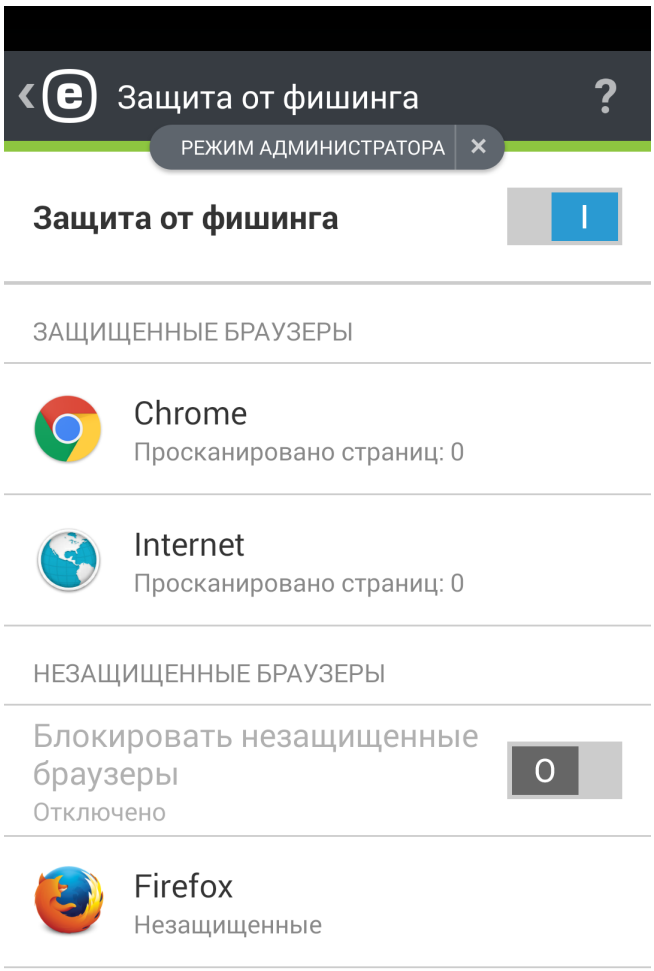
Компонент «Безопасность устройства» включает также возможность использования **политики настроек устройства** (раньше входила в компонент «Аудит безопасности»). С помощью этой политики системный администратор может контролировать предварительно заданные настройки устройства.

Настраивать в устройстве можно следующее:

- Wi-Fi
- спутники GPS,
- службы определения местоположения,
- память,
- передача данных в роуминге,
- вызовы в роуминге,
- неизвестные источники,
- режим отладки,
- NFC,
- шифрование памяти.
- На устройстве получены права суперпользователя root



11. Защита от фишинга



Термином *фишинг* обозначается преступная деятельность с использованием методов социотехники (манипулирование пользователями для получения конфиденциальной информации). Фишинг часто используется для получения доступа к такой конфиденциальной информации, как номера банковских счетов, номера кредитных карт, PIN-коды или имена пользователей и пароли.

Рекомендуется оставить функцию **защиты от фишинга** включенной. ESET Endpoint Security сканирует URL-адреса — все потенциальные фишинговые атаки с веб-сайтов или доменов, занесенных компанией ESET в базу данных вредоносных объектов, блокируются, а для пользователя отображается уведомление об атаке.

ВНИМАНИЕ! Компонент защиты от фишинга интегрируется с самыми распространенными веб-браузерами, доступными в ОС Android. В большинстве случаев защита от фишинга доступна для браузеров Chrome, Firefox, Opera, Opera Mini, Dolphin, Samsung и стандартных браузеров, предварительно устанавливаемых на устройствах Android. Другие браузеры будут отображаться в списке незащищенных, и доступ к ним можно заблокировать, переключив кнопку .

Для надлежащей работы модуля ESET по защите от фишинга в настройках системы Android необходимо включить параметр **Доступность**.

12. Фильтр звонков и SMS

Фильтр звонков и SMS блокирует входящие SMS- и MMS-сообщения в соответствии с пользовательскими правилами.

Нежелательные сообщения обычно содержат рекламные объявления от поставщиков услуг мобильной связи или приходят от неизвестных либо неуказанных пользователей. Заблокировать сообщение — значит автоматически переместить его в раздел **История**. При блокировке сообщения уведомление не отображается. Благодаря этому вас не будет отвлекать нежелательная информация. При этом вы всегда сможете проверить журналы на наличие сообщений, которые могли быть заблокированы по ошибке.

ПРИМЕЧАНИЕ. Фильтр звонков и SMS недоступен на планшетах, которые не поддерживают телефонные звонки и обмен сообщениями. Фильтрация SMS- и MMS-сообщений не работает на устройствах под управлением ОС Android 4.4 и более поздних версий и будет отключена на устройствах, где основным приложением для обмена SMS является Google Hangouts.

Чтобы блокировать звонки и сообщения с последнего входящего номера телефона, коснитесь элемента **Заблокировать последнего звонящего** или **Блокировать последнего отправителя SMS**. В результате этого действия будет создано правило.

12.1 Правила

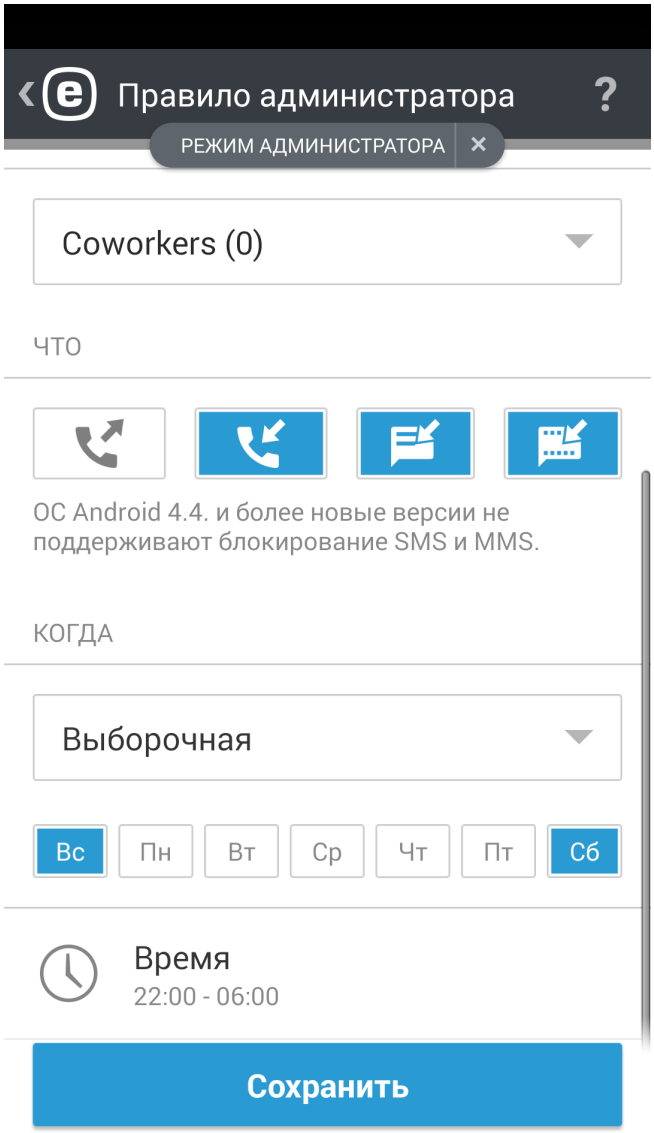
Пользователь может создавать пользовательские правила, не вводя пароль администратора. Правила администратора можно создавать только в режиме администратора. Пользовательские правила переопределяются правилами администратора.

Дополнительные сведения о создании правил можно найти в этом разделе.

Если нужно удалить существующее правило из списка **Правила**, коснитесь имени правила и задержите на нем палец, а затем коснитесь значка **Удалить**  .

12.1.1 Добавление нового правила

Чтобы добавить новое правило, в правом верхнем углу экрана **Правила** коснитесь значка ➕.



Укажите, как нужно обрабатывать звонки и сообщения: разрешить или блокировать.

Выберите контакт или группу телефонных номеров. Приложение ESET Endpoint Security распознает сохраненные на телефоне группы контактов (например, «Семья», «Друзья» или «Сотрудники»). Параметр **Все неизвестные номера** относится ко всем телефонным номерам, не сохраненным в списке контактов. С помощью этого параметра можно заблокировать нежелательные телефонные звонки (например, рекламные) или запретить сотрудникам звонить на неизвестные номера. Параметр **Все известные номера** относится ко всем телефонным номерам, сохраненным в списке контактов. Параметр **Скрытые номера** относится к абонентам, которые намеренно скрывают свои номера с помощью услуги «антиопределитель номера».

Укажите, что нужно разрешать или блокировать:

- исходящие звонки,
- входящие звонки,
- входящие текстовые сообщения (SMS),
- входящие мультимедийные сообщения (MMS).

Чтобы применить правило только на указанный период времени, последовательно коснитесь элементов **Всегда** > **Выборочная** и укажите дни недели и промежуток времени. По умолчанию выбраны суббота и воскресенье. Эта функция может пригодиться, например, если вы не хотите, чтобы вас беспокоили во время совещаний, командировок, ночью или на выходных.

ПРИМЕЧАНИЕ. Если вы находитесь за границей, все телефонные номера в списке должны включать международный телефонный (например, +1610100100).

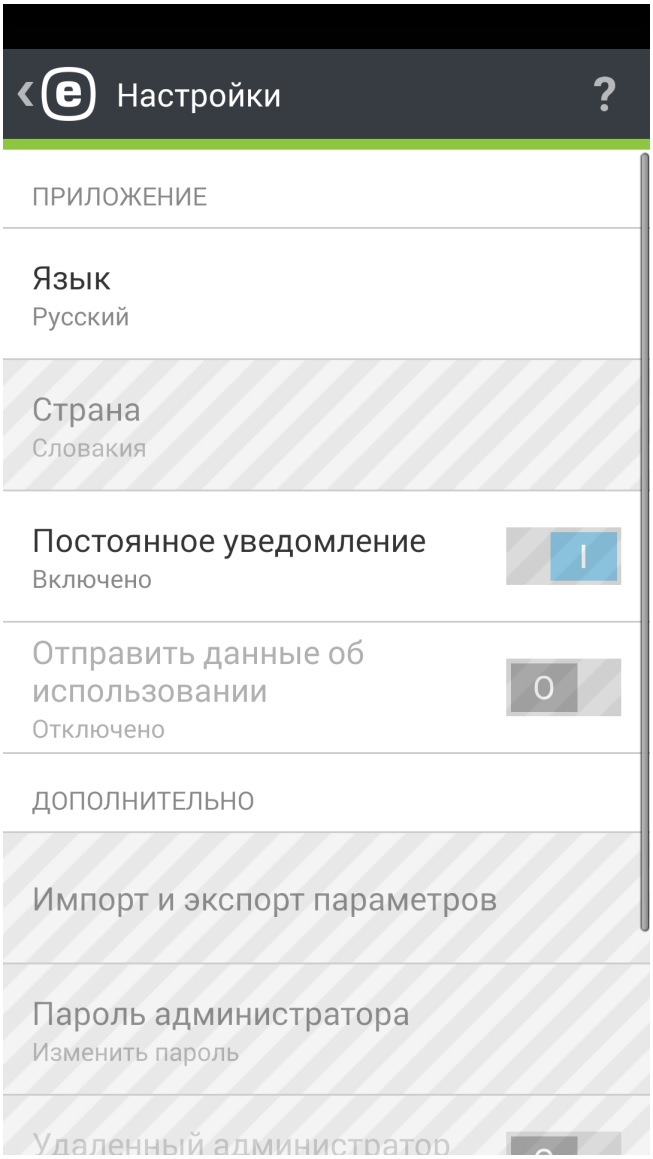
12.2 История

В области интерфейса **История** отображаются звонки и сообщения, которые заблокировал или разрешил фильтр звонков и SMS. Каждый журнал содержит следующие сведения: имя события, соответствующий номер телефона, дата и время события. Журналы SMS- и MMS-сообщений содержат также тексты сообщений.

Если нужно изменить правило, связанное с заблокированным номером телефона или контактом, коснитесь записи в списке, чтобы выбрать ее, а затем коснитесь значка  .

Чтобы удалить запись из списка, выберите ее и коснитесь значка  . Чтобы удалить несколько записей, коснитесь одной из них и задержите на ней палец, выберите остальные ненужные записи и коснитесь значка  .

13. Параметры



Язык
По умолчанию приложение ESET Endpoint Security устанавливается на языке, который выбран в качестве языка системы на устройстве (настройки языка и клавиатуры в ОС Android). Чтобы изменить язык интерфейса приложения, коснитесь элемента «Язык» и выберите язык.

Страна
Выберите страну, в которой вы работаете или находитесь в настоящий момент.

Обновление
Чтобы обеспечить максимальную защиту, важно использовать самую последнюю версию ESET Endpoint Security. Нажмите **Обновление,** чтобы узнать, доступна ли более новая версия для загрузки на веб-сайте ESET. Эта возможность недоступна, если программа ESET Endpoint Security была загружена из магазина Google Play. В этом случае продукт обновляется из магазина Google Play.

Постоянное уведомление

ESET Endpoint Security отображает значок уведомления  в верхнем левом углу экрана (строка состояния Android). Если отображать этот значок не нужно, снимите флажок **Постоянное уведомление**.

Уведомления о разрешениях
См. раздел Управление разрешениями.

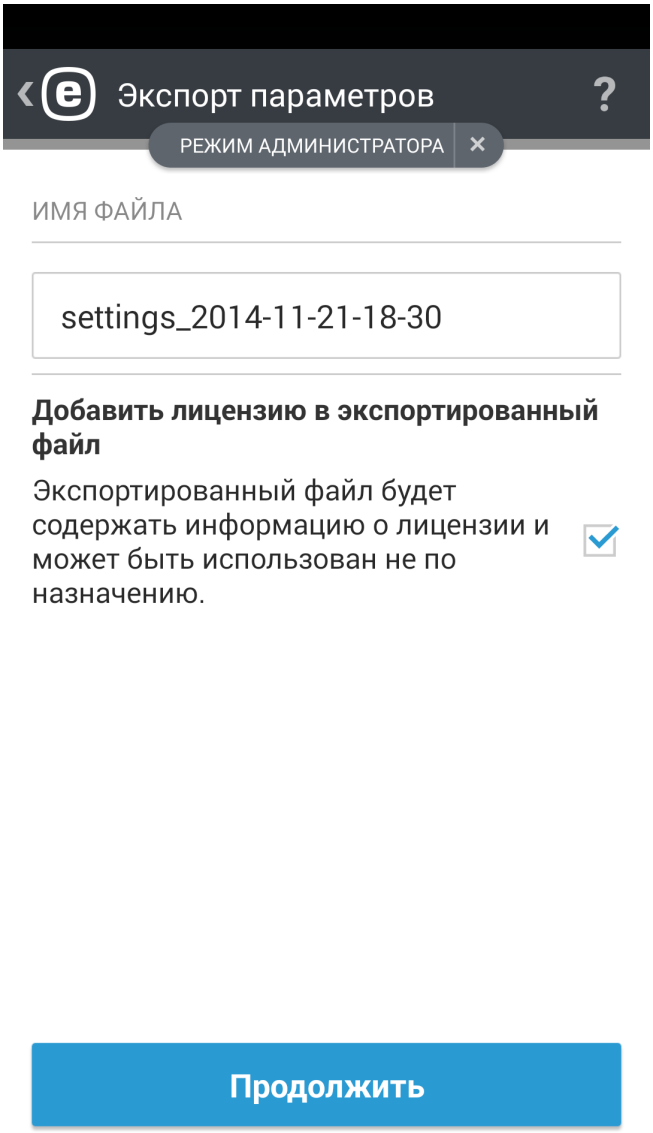
Отправить данные об использовании
Этот параметр помогает улучшать продукты ESET путем отправки анонимных данных об использовании приложения. Конфиденциальная информация не отправляется. Если этот параметр не был включен с помощью мастера начальной настройки на этапе установки, это можно сделать в разделе **Параметры** .

Пароль администратора
Этот параметр позволяет создать пароль администратора или изменить существующий. Дополнительные сведения см. в разделе Пароль администратора данного документа.

Удалить
Если запустить мастер удаления, приложение ESET Endpoint Security и папки карантина будут безвозвратно удалены с устройства. Если перед этим была включена защита от удаления приложения, вам будет предложено ввести **пароль администратора**.

13.1 Импорт и экспорт параметров

Чтобы с легкостью обеспечить передачу параметров между двумя мобильными устройствами, которые не управляются решением ERA, ESET Endpoint Security 2 дает возможность экспортировать и импортировать параметры программы. Администратор может вручную экспортировать параметры в файл, который затем можно передать по электронной почте и импортировать на любое устройство, на котором запущено клиентское приложение. Когда пользователь принимает файл параметров, все параметры импортируются автоматически и приложение активируется (если в файл были добавлены сведения о лицензии). Все параметры будут защищены паролем администратора.



13.1.1 Экспорт параметров

Чтобы экспортировать текущие параметры приложения ESET Endpoint Security, укажите имя файла параметров (текущие дата и время будут вставлены автоматически). В экспортируемый файл можно добавить также сведения о лицензии (лицензионный ключ или адрес электронной почты и пароль к учетной записи администратора безопасности), однако помните, что эта информация не будет зашифрована и может быть использована в преступных целях.

На следующем этапе выберите способ передачи файла:

- по сети Wi-Fi,
- через Bluetooth,
- по электронной почте,
- через приложение Gmail,
- через диспетчер файлов (например, ASTRO File Manager или ES File Explorer).

13.1.2 Импорт параметров

Чтобы импортировать параметры из файла, который находится на устройстве, используйте диспетчер файлов, например ASTRO File Manager или ES File Explorer, найдите файл параметров и выберите ESET Endpoint Security.

Также параметры можно импортировать, выбрав файл в разделе **История.**

13.1.3 История

История отображает список импортированных файлов с параметрами. Тут эти файлы можно передавать другим пользователям, импортировать и удалять.

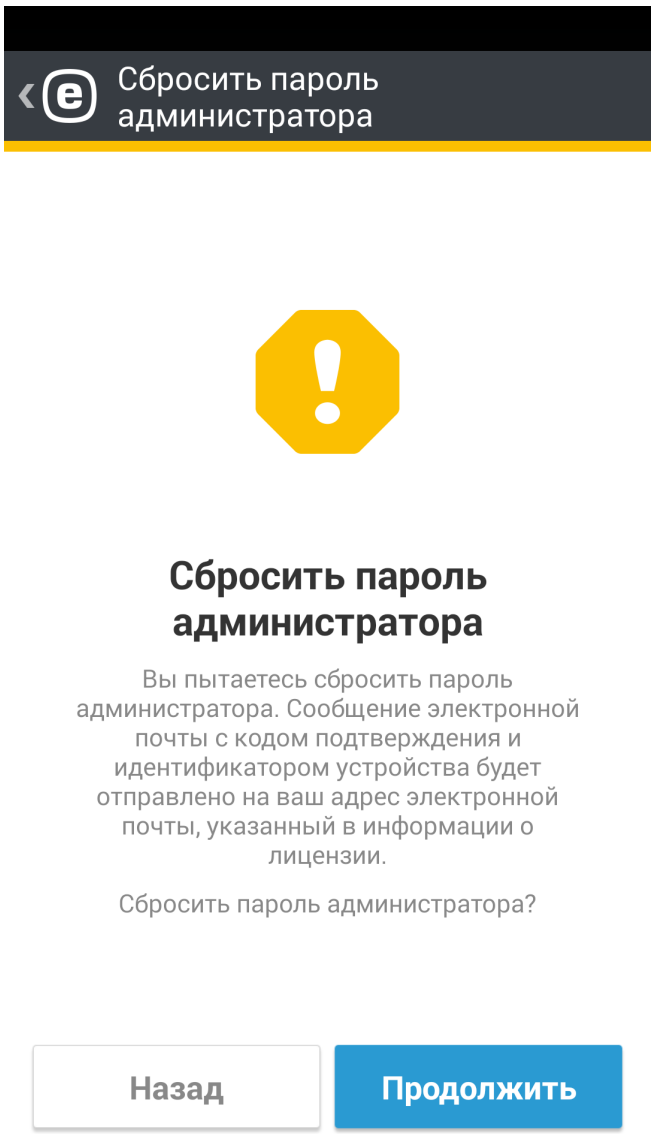
13.2 Пароль администратора

Пароль **администратора** требуется для разблокировки устройства, отправки команд модуля Антивор, доступа к защищенным паролем функциям и удаления ESET Endpoint Security.

ВНИМАНИЕ! Подойдите к вопросу выбора пароля со всей серьезностью. Чтобы улучшить безопасность и надежность пароля, используйте сочетание цифр, строчных и прописных букв.

Чтобы сбросить пароль администратора на устройстве с заблокированным экраном, выполните такие действия:

1. Нажмите **Восстановление пароля** > **Продолжить** > **Запросить код проверки**. Если устройство не подключено к Интернету, вместо этого нажмите ссылку **выбрать сброс в автономном режиме** и свяжитесь со службой поддержки клиентов ESET.
2. Проверьте вашу электронную почту. Сообщение с кодом проверки и идентификатором устройства будет отправлено на адрес электронной почты, связанный с лицензией ESET. Срок действия кода проверки — семь дней после получения.
3. Введите код проверки и новый пароль на заблокированном экране вашего устройства.



13.3 Remote administrator

ESET Remote Administrator (ERA) позволяет централизовано управлять приложением ESET Endpoint Security в сетевой среде.

Использование ERA не только повышает уровень безопасности, но и упрощает администрирование всех программ ESET, установленных на клиентских рабочих станциях и мобильных устройствах. Устройства, на которых установлено приложение <%PRODUCTNAME,%> могут подключаться к ERA, используя любой тип подключения к Интернету — по сетиWi-Fi, локальной сети, беспроводной локальной сети, сети сотовой связи (3G, 4G LTE, HSDPA, GPRS) и т. д. При этом требуется, чтобы подключение к Интернету было обычным (без использования прокси-сервера или файервола) и чтобы обе конечные точки были правильно настроены.

Успешное подключение к ERA по сотовой сети зависит от поставщика услуг мобильной связи и требует полноценного Интернет-соединения.

Чтобы подключить устройство к ERA, добавьте устройство в список **Компьютеры** в веб-консоли ERA, зарегистрируйте устройство с помощью задачи **Регистрация устройства** и введите **адрес сервера средства подключения для мобильных устройств**.

Ссылка для регистрации (адрес сервера средства подключения для мобильных устройств) имеет стандартный формат `https://MDCserver:port/token` в ERA 6.4 и более поздних версиях. В более ранних версиях ERA параметр маркера не используется, поэтому ссылка для регистрации имеет формат `https://MDCserver:порт`. Ссылка содержит следующие значения:

- **MDCserver** — полное DNS-имя или общедоступный IP-адрес сервера, на котором запущено средство подключения для мобильных устройств (MDC). Имя хоста может использоваться только в том случае, если подключение выполняется через внутреннюю сеть Wi-Fi.
- **Port** — номер порта, который используется для подключения к средству подключения для мобильных устройств.
- **Token** — строка, содержащая набор символов, генерируемый администратором в веб-консоли ERA (используется только в ERA 6.4 и более поздних версиях).

Дополнительные сведения о том, как управлять сетью с помощью решения ESET Remote Administrator, доступны в следующих разделах интернет-справки:

- Управление политиками
- Создание клиентских задач
- Сведения об отчетах

13.4 ИД устройства

ИД устройства поможет администратору идентифицировать устройство, если оно потеряется или его украдут.

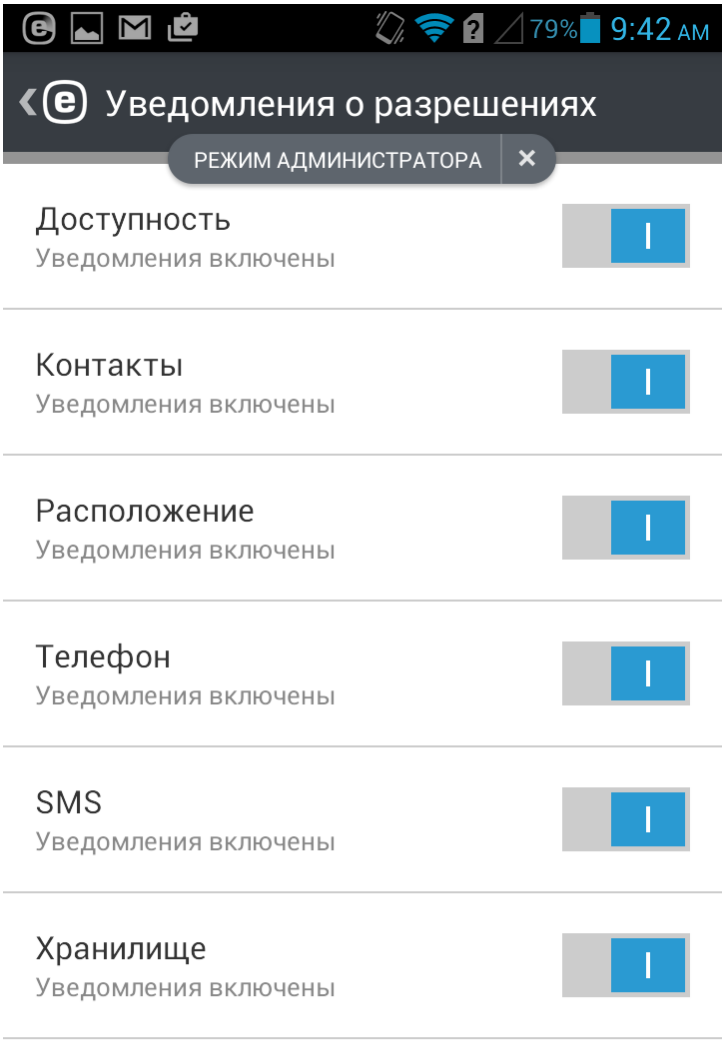
13.5 Управление разрешениями

В ОС Android 6 (Marshmallow) компания Google представила новую функцию управления разрешениями. Приложение ESET Endpoint Security совместимо с этой функцией. Приложения, предназначенные для Android 6.0, будут запрашивать разрешения, как только вы попытаетесь запустить их. Вместо предоставления приложению доступа во время установки пользователь получает запрос при первой попытке доступа приложения к определенной функции устройства.

ESET Endpoint Security запрашивает разрешение на доступ к следующим функциям.

- **Доступность** — это разрешение необходимо для надлежащей работы функции защиты от фишинга ESET.
- **Контакты** — требуется для модуля Антивор и фильтра звонков и SMS.
- **Расположение** — требуется для модуля Антивор.
- **Телефон** — для модуля Антивор и фильтра звонков и SMS.
- **SMS** — для модуля Антивор и фильтра звонков и SMS.
- **Хранилище** — требуется для функции защиты от вирусов и модуля Антивор.

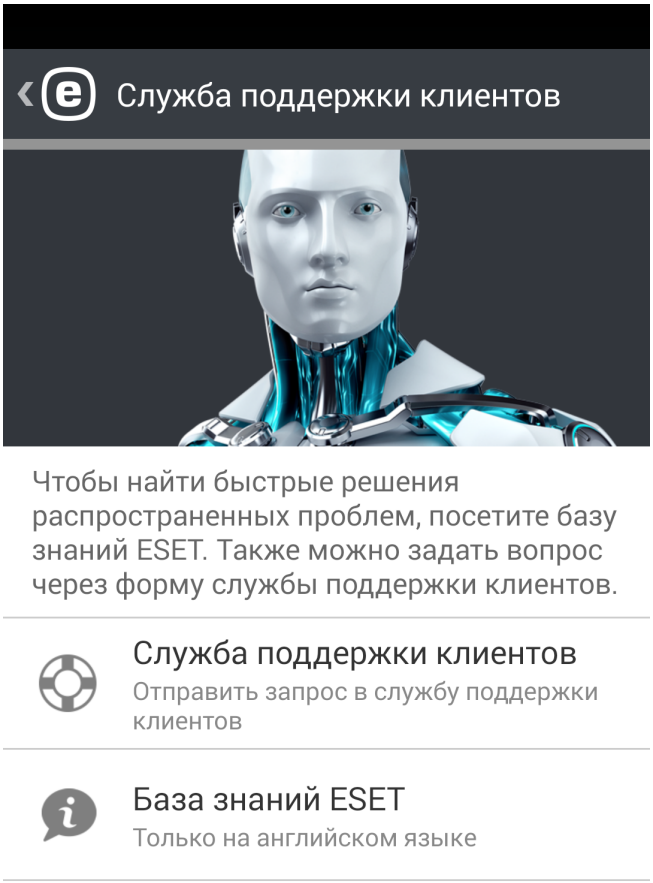
Администратор может отключить мониторинг этих разрешений в разделе **Параметры** > **Уведомления о разрешениях**.



14. Служба поддержки клиентов

Сотрудники службы поддержки клиентов ESET с радостью помогут вам в решении административных и технических вопросов, возникающих при работе с приложением ESET Endpoint Security или любыми другими продуктами ESET.

Чтобы отправить запрос в службу поддержки со своего устройства, коснитесь значка меню на главном экране ESET Endpoint Security (или нажмите кнопку меню на устройстве), последовательно щелкните элементы **Служба поддержки клиентов** > **Служба поддержки клиентов** и заполните все обязательные поля.



В приложении ESET Endpoint Security улучшены функции ведения журналов, что позволяет лучше диагностировать потенциальные технические проблемы. Для предоставления специалистам ESET подробного журнала приложения убедитесь, что выбран параметр **Отправить журнал приложения** (по умолчанию). Нажмите **Отправить**, чтобы отправить запрос. Специалист службы поддержки клиентов ESET свяжется с вами по указанному адресу электронной почты.