kaspersky

Kaspersky Security 10 для мобильных устройств Service Pack 4, Maintenance Release 3

Содержание

Часто задаваемые вопросы

Что нового

Kaspersky Security для мобильных устройств

- О приложении Kaspersky Endpoint Security для Android
- О Kaspersky Device Management для iOS
- О почтовом ящике Exchange
- О плагине управления Kaspersky Endpoint Security для Android
- О плагине управления Kaspersky Device Management для iOS
- Комплект поставки
- Аппаратные и программные требования

Развертывание

- Архитектура решения
- Типовые схемы развертывания комплексного решения
  - Схемы развертывания Kaspersky Endpoint Security для Android
  - Схемы развертывания для iOS MDM-профиля
- Подготовка Консоли администрирования к развертыванию комплексного решения
  - Настройка параметров Сервера администрирования для подключения мобильных устройств
  - Отображение папки "Управление мобильными устройствами" в Консоли администрирования
  - Создание группы администрирования
  - Создание правила автоматического переноса устройств в группу администрирования
  - Создание общего сертификата
- Установка Kaspersky Endpoint Security для Android
  - Разрешения
  - Установка Kaspersky Endpoint Security для Android по ссылке на Google Play
  - Другие способы установки Kaspersky Endpoint Security для Android
    - Установка из Google Play и Huawei AppGallery вручную
    - Создание и настройка инсталляционного пакета
    - Создание автономного пакета установки
  - Настройка параметров синхронизации
- Активация программы
  - Активация приложений в Kaspersky Security Center
  - Активация Kaspersky Endpoint Security для Android без Kaspersky Security Center
- Установка iOS MDM-профиля
  - О режимах управления iOS-устройствами
  - Установка через Kaspersky Security Center
- Установка плагинов управления
- Обновление предыдущей версии программы
  - Обновление предыдущей версии Kaspersky Endpoint Security для Android
  - Установка более ранней версии Kaspersky Endpoint Security для Android
  - Обновление предыдущих версий плагинов управления
- Удаление Kaspersky Endpoint Security для Android
  - Дистанционное удаление приложения
  - Разрешение пользователям удалять приложение
  - Удаление приложения пользователем

Настройка и управление

- Начало работы

- Запуск и остановка программы
- Создание группы администрирования
- Групповые политики для управления мобильными устройствами
  - Создание групповой политики
  - Настройка параметров синхронизации
  - Работа с ревизиями групповых политик
  - Удаление групповой политики
  - Ограничение прав на настройку групповых политик

Защита

- Настройка антивирусной защиты Android-устройств
- Защита Android-устройств в интернете
- Защита данных при потере или краже устройств
  - Отправка команд на мобильное устройство
  - Разблокировка мобильного устройства
  - Шифрование данных
- Настройка надежности пароля разблокировки устройства
  - Настройка надежности пароля разблокировки Android-устройства
  - Настройка надежности пароля разблокировки iOS MDM-устройств
  - Настройка надежности пароля разблокировки EAS-устройств
- Настройка виртуальной частной сети (VPN)
  - Настройка VPN на Android-устройствах (только Samsung)
  - Настройка VPN на iOS MDM-устройствах
- Настройка Сетевого экрана на Android-устройствах (только Samsung)
- Защита Kaspersky Endpoint Security для Android от удаления
- Обнаружение взлома устройства (получение root-прав)
- Настройка глобального HTTP-прокси на iOS MDM-устройствах
- Добавление сертификатов безопасности на iOS MDM-устройства
- Добавление профиля SCEP на iOS MDM-устройства

Контроль

- Настройка ограничений
  - Особые рекомендации для устройств под управлением Android 10 и выше
  - Настройка ограничений для Android-устройств
  - Настройка ограничений для iOS MDM-устройств
  - Настройка ограничений функций для EAS-устройств
- Настройка доступа пользователей к веб-сайтам
  - Настройка доступа к веб-сайтам на Android-устройствах
  - Настройка доступа к веб-сайтам на iOS MDM-устройствах
- Контроль соответствия Android-устройств требованиям корпоративной безопасности
- Контроль запуска приложений
  - Контроль запуска приложений на Android-устройствах
  - Настройка ограничений приложений для EAS-устройств
- Инвентаризация программного обеспечения на Android-устройствах
- Настройка отображения Android-устройств в Kaspersky Security Center

Управление

- Настройка подключения к сети Wi-Fi
  - Подключение Android-устройств к сети Wi-Fi
  - Подключение iOS MDM-устройств к сети Wi-Fi
- Настройка электронной почты

Настройка почтового ящика на iOS MDM-устройствах
Настройка почтового ящика Exchange на iOS MDM-устройствах
Настройка почтового ящика Exchange на Android-устройствах (только Samsung)
Управление сторонними мобильными приложениями
Настройка уведомлений Kaspersky Endpoint Security для Android
Подключение iOS MDM-устройств к AirPlay
Подключение iOS MDM-устройств к AirPrint
Настройка точки доступа (APN)
Настройка APN на Android-устройствах (только Samsung)
Настройка APN на iOS MDM-устройствах
Настройка рабочего профиля Android
О рабочем профиле Android
Настройка рабочего профиля
Добавление учетной записи LDAP
Добавление учетной записи календаря
Добавление учетной записи контактов
Настройка подписки на календарь
Добавление веб-клипов
Добавление шрифтов
Управление приложением с помощью сторонних EMM-систем (только Android)
Начало работы
Как установить приложение
Как активировать приложение
Как подключить устройство к Kaspersky Security Center
Файл AppConfig
Для пользователей мобильных устройств
Возможности приложения
Обзор главного окна
Проверка устройства
Проверка устройства по расписанию
Изменение режима защиты
Обновление антивирусных баз
Обновление баз по расписанию
Действия в случае кражи или потери устройства
Веб-Фильтр
Контроль установленных приложений
Получение сертификата
Синхронизация с Kaspersky Security Center
Обновление приложения
Удаление приложения
Приложения с "портфелем"
Приложение KNOX
Нагрузка на сеть
Участие в Kaspersky Security Network
Обмен информацией с Kaspersky Security Network
Включение и выключение использования Kaspersky Security Network
Предоставление данных в сервисы Google
Обмен информацией с Firebase Cloud Messaging

Обмен информацией с Google Analytics для Firebase
Известные проблемы и рекомендации
Лицензирование программы
О Лицензионном соглашении
О лицензии
О подписке
О ключе
О коде активации
О файле ключа
Принятие дополнительных Положений глобально администратором
Предоставление данных
Samsung KNOX
Установка приложения Kaspersky Endpoint Security для Android с помощью KNOX Mobile Enrollment
Создание профиля KNOX MDM
Добавление устройств в KNOX Mobile Enrollment
Установка приложения
Настройка KNOX-контейнеров
О KNOX-контейнере
Активация Samsung KNOX
Настройка Сетевого экрана в KNOX
Настройка почтового ящика Exchange в KNOX
Обращение в Службу технической поддержки
Способы получения технической поддержки
Получение технической поддержки по телефону
Техническая поддержка через Kaspersky CompanyAccount
Другие источники информации о программе
Глоссарий
Apple Push Notification service (APNs) сертификат
EAS-устройство
IMAP
iOS MDM-профиль
iOS MDM-устройство
Kaspersky Security Network (KSN)
Manifest-файл
POP3
Provisioning-профиль
SSL
Автономный пакет установки
Администратор Kaspersky Security Center
Администратор устройства
Активация программы
Антивирусные базы
Веб-сервер Kaspersky Security Center
Вирус
Группа администрирования
Групповая задача
Запрос Certificate Signing Request
Инсталляционный пакет

- Карантин
- Категории "Лаборатории Касперского"
- Код активации
- Код разблокировки
- Контролируемое устройство
- Контроль соответствия
- Лицензионное соглашение
- Лицензия
- Плагин управления программой
- Подписка
- Политика
- Прокси-сервер
- Рабочее место администратора
- Рабочий профиль Android;
- Сервер iOS MDM
- Сервер администрирования
- Сервер мобильных устройств Exchange
- Серверы обновлений "Лаборатории Касперского"
- Срок действия лицензии
- Файл ключа
- Фишинг

Приложения

- Права на настройку групповых политик
- Категории приложений

Информация о стороннем коде

Уведомления о товарных знаках

Часто задаваемые вопросы

УСТАНОВКА

Как удаленно установить Kaspersky Endpoint Security для Android?

Как запретить пользователю удалять Kaspersky Endpoint Security для Android?

Как активировать Kaspersky Endpoint Security для Android?

ЗАЩИТА

Как заблокировать устройство, которое потеряно или украдено?

Как защититься от интернет-угроз?

Как запретить установку пустого пароля?

ИСПОЛЬЗОВАНИЕ СТОРОННИХ РЕШЕНИЙ

Android Enterprise (Приложения с "портфелем", Настройка рабочего профиля Android)

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

КОНТРОЛЬ

Как запретить пользователю играть на устройстве?

Как настроить доступ к веб-сайтам на устройстве?

Как обнаружить получение root-прав?

УПРАВЛЕНИЕ

Как настроить почтовый ящик на устройстве?

Как подключить мобильное устройство к Wi-Fi?

Как установить корпоративное приложение?

Что нового

Технический релиз 20

- Пользователям не предлагается принять юридические положения, если администратор принял эти положения глобально.
- Оптимизирована работа приложения.

Технический релиз 19

- Теперь у администратора появилась возможность принимать Положение о Kaspersky Security Network и другие положения в программе Kaspersky Security Center от имени других пользователей.
- Исправлен ряд ошибок, повышена стабильность работы.

Технический релиз 18

- Kaspersky Security для мобильных устройств теперь поддерживает Мобильные службы Huawei (Huawei Mobile Services).
- Kaspersky Endpoint Security для Android теперь можно установить из Huawei AppGallery.

Технический релиз 17

- Kaspersky Endpoint Security теперь поддерживает API уровня 29 и выше, что приводит к определенным изменениям в поведении приложений на устройствах под управлением Android 10 и выше.
- Новые параметры надежности пароля позволяют пользователям устанавливать пароли требуемой сложности.
- Настройка использования отпечатка пальца для разблокировки экрана теперь доступна только для рабочего профиля Android.
- Исправлен ряд ошибок, повышена стабильность работы.

Технический релиз 16

- Kaspersky Endpoint Security для Android теперь поддерживает Android 11.
- В Android 11 введены новые требования к разрешениям для доступа к камере и местоположению устройства. В этом разделе можно подробнее ознакомиться с новыми правилами разрешений для доступа к камере и местоположению устройства.
- Теперь можно указывать корпоративные адреса электронной почты пользователей в сторонней EMM-консоли. Эти адреса электронной почты будут отображаться в Kaspersky Security Center, если настроен новый параметр KscCorporateEmail.

Технический релиз 14

- Каждый раз, когда пользователь предоставляет или отзывает права администратора устройства в приложении, в Консоль управления передается соответствующее событие.

- Параметр KscGroup теперь можно настраивать в сторонних EMM-консолях. При подключении устройства к Kaspersky Security Center, оно автоматически добавляется в подпапку папки "Нераспределенные устройства". Имя подпапки совпадает с названием группы, настроенной в EMM-консоли.

Технический релиз 13

- Обновлен дизайн пользовательского интерфейса Kaspersky Endpoint Security для Android.

- Все разделы справки теперь доступны онлайн.

- IP-адреса управляемых устройств теперь передаются в Kaspersky Security Center, и их можно просмотреть в разделах с информацией об устройстве.

Технический релиз 12

- В Kaspersky Security Center 12.1 добавлена возможность удаленно принимать условия Лицензионного соглашения. Если администратор принял условия Лицензионного соглашения и Политики конфиденциальности в Консоли администрирования, во время установки приложения эти шаги будут пропущены.

- Для пользователей VMware AirWatch реализована возможность изменять название устройства в Kaspersky Security Center. В конфигурационный файл был добавлен новый параметр, используемый для настройки приложения. К названию устройства можно добавить дополнительную информацию (например, серийный номер устройства). Это упрощает поиск и сортировку устройств в Kaspersky Security Center.

Технический релиз 11

Исправлен ряд ошибок, повышена стабильность работы.

Технический релиз 10

- Kaspersky Security для мобильных устройств теперь поддерживает Kaspersky Security Center 12.

- В Kaspersky Security Center 12 прекращена поддержка Kaspersky Safe Browser. Вы можете пользоваться функциями Kaspersky Safe Browser при использовании Kaspersky Security Center 11 или более ранних версий.

- Исправлен ряд ошибок, повышена стабильность работы.

Service Pack 4 Maintenance Release 3

- Проверена поддержка Kaspersky Endpoint Security для Android в среде Microsoft Intune (компонент EMM-решения, enterprise mobility management). Для работы приложения со сторонними EMM-решениями "Лаборатория Касперского" участвует в AppConfig Community.

- Добавлена возможность отключать уведомления и всплывающие сообщения, когда приложение работает в фоновом режиме. Обратите внимание, что выполнение этих действий в фоновом режиме небезопасно. Если уведомления и всплывающие сообщения отключены, когда приложение работает в фоновом

режиме, приложение не уведомляет пользователей об угрозах в реальном времени. Пользователи мобильных устройств узнают о состоянии защиты устройства, только когда откроют приложение.

- Добавлена возможность принимать Лицензионное соглашение и Политику конфиденциальности в VMware AirWatch. Если администратор принял Лицензионное соглашение и Политику конфиденциальности в консоли AirWatch, соответствующий шаг будет пропущен во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android.

- Добавлено Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре). Для использования Веб-Фильтра необходимо принять это положение. Kaspersky Endpoint Security для Android использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN. Положение о Веб-Фильтре можно принять в политике или запросить принятие у пользователя устройства.

- Исправлен ряд ошибок, повышена стабильность работы.

Kaspersky Security для мобильных устройств

Kaspersky Security 10.0 для мобильных устройств Service Pack 4, Maintenance Release 3 (далее "Kaspersky Security для мобильных устройств") – комплексное решение, предназначенное для защиты и настройки корпоративных мобильных устройств, а также личных мобильных устройств сотрудников организации, используемых для корпоративных целей.

Kaspersky Security для мобильных устройств включает в себя следующие компоненты:

- Мобильное приложение Kaspersky Endpoint Security для Android.

  Kaspersky Endpoint Security для Android защищает мобильные устройства от веб-угроз, вирусов и других программ, представляющих угрозы.

- Плагин управления Kaspersky Endpoint Security для Android

  Плагин управления Kaspersky Endpoint Security для Android обеспечивает интерфейс управления мобильными устройствами и установленными на них мобильными приложениями через Консоль администрирования Kaspersky Security Center.

- Плагин управления Kaspersky Device Management для iOS.

  Плагин управления Kaspersky Device Management для iOS позволяет настраивать конфигурационные параметры устройств, подключенных к Kaspersky Security Center по протоколу iOS MDM (далее iOS MDM-устройств) и Exchange ActiveSync (далее EAS-устройств), без использования iPhone Configuration Utility и консоли управления Exchange.

Плагины управления интегрируются в *систему удаленного администрирования Kaspersky Security Center*. С помощью единой Консоли администрирования Kaspersky Security Center администратор может управлять всеми мобильными устройствами организации, а также клиентскими компьютерами и виртуальными системами. После подключения мобильных устройств к Серверу администрирования они становятся управляемыми. Администратор может дистанционно контролировать управляемые устройства.

Мобильное приложение Kaspersky Endpoint Security для Android может также работать в составе *системы удаленного администрирования Kaspersky Endpoint Security Cloud*. Подробная информация о работе с приложениями с помощью Kaspersky Endpoint Security Cloud приведена в *онлайн-справке Kaspersky Endpoint Security Cloud*.

Мобильное приложение Kaspersky Endpoint Security для Android также может работать в составе сторонних EMM-решений участников AppConfig Community.

О приложении Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android защищает мобильные устройства от веб-угроз, вирусов и других программ, представляющих угрозы.

Kaspersky Endpoint Security для Android включает в себя следующие компоненты:

- **Антивирус**. Позволяет обнаруживать и устранять угрозы на мобильном устройстве, используя антивирусные базы приложения и дополнительно облачную службу Kaspersky Security Network. В состав Антивируса входят следующие компоненты:

  - Защита. Позволяет обнаруживать угрозы в открытых файлах, а также проверять новые приложения и предотвращать заражение устройства в режиме реального времени.

- Проверка. Запускается по требованию для всей файловой системы, только для установленных приложений, выбранного файла или папки.

- Обновление. Позволяет загружать новые антивирусные базы приложения.

- **Анти-Вор.** Защищает информацию на устройстве от несанкционированного доступа в случае потери или кражи устройства. Позволяет отправлять на устройство следующие команды:

  - **Поиск**, чтобы получить координаты местоположения устройства.

  - **Сигнал**, чтобы устройство издало громкий сигнал тревоги.

  - **Фото**, чтобы устройство сделало фотоснимки на фронтальную камеру, если кто-то попытается его разблокировать.

  - **Удаление корпоративных данных, чтобы защитить конфиденциальную информацию компании.**

- **Веб-Фильтр.** Позволяет блокировать вредоносные веб-сайты, цель которых – распространить вредоносный код. Веб-Фильтр также блокирует поддельные (фишинговые) веб-сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Фильтр проверяет веб-сайты до открытия, используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Фильтр разрешает загрузку веб-сайтов, признанных надежными, и блокирует веб-сайты, признанные вредоносными. Веб-Фильтр также поддерживает фильтрацию веб-сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Это позволяет администратору ограничить доступ пользователей к некоторым категориям веб-страниц (например, к веб-страницам из категории "Азартные игры, лотереи, тотализаторы" или "Общение в сети").

- **Контроль приложений.** Позволяет вам устанавливать на устройство рекомендованные и обязательные приложения с помощью прямой ссылки на дистрибутив или ссылки на Google Play. С помощью Контроля приложений вы можете удалять запрещенные приложения, которые не удовлетворяют требованиям корпоративной безопасности.

- **Контроль соответствия.** Этот компонент позволяет проверять управляемые устройства на соответствие требованиям корпоративной безопасности и накладывать ограничения на определенные функции несовместимых устройств.

О Kaspersky Device Management для iOS

Kaspersky Device Management для iOS обеспечивает защиту и контроль мобильных устройств, подключенных к Kaspersky Security Center, и включает следующие функции управления устройствами:

- **Защита паролем**. Эта функция позволяет установить требования к сложности пароля, чтобы пользователи использовали сложные пароли, соответствующие корпоративной политике паролей.

- **Управление сетями**. Эта функция позволяет добавлять утвержденные сети VPN и Wi-Fi или ограничивать доступ к другим сетям.

- **Удаление корпоративных данных**. В случае потери или кражи устройства вы можете отправить на устройство команду "Очистить", чтобы защитить конфиденциальную информацию компании.

- **Веб-Фильтр**. Позволяет блокировать вредоносные веб-сайты, цель которых – распространить вредоносный код. Веб-Фильтр также блокирует поддельные (фишинговые) веб-сайты, цель которых – украсть конфиденциальные данные пользователя (например, пароли от интернет-банка или платежных систем) и получить доступ к его финансовым счетам. Веб-Фильтр проверяет веб-сайты до открытия,

используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Фильтр разрешает загрузку веб-сайтов, признанных надежными, и блокирует веб-сайты, признанные вредоносными. Веб-Фильтр также поддерживает фильтрацию веб-сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Это позволяет администратору ограничить доступ пользователей к некоторым категориям веб-страниц (например, к веб-страницам из категории "Азартные игры, лотереи, тотализаторы" или "Общение в сети").

- **Ограничения программ.** Этот компонент позволяет контролировать, можно ли использовать собственные приложения устройства, такие как iTunes, Safari или Game Center, на управляемом устройстве.

- **Ограничения функций.** Этот компонент позволяет проверять управляемые устройства на соответствие требованиям корпоративной безопасности и накладывать ограничения на определенные функции несовместимых устройств.

О почтовом ящике Exchange

Почтовый ящик Exchange – клиентское приложение службы Exchange ActiveSync. Приложение предназначено для работы корпоративных пользователей с почтой, календарем, контактами и задачами. Почтовый ящик Exchange позволяет подключить мобильное устройство к серверу Microsoft Exchange. Подробные сведения о службе Exchange ActiveSync приведены на *веб-сайте технической поддержки Microsoft*.

Для управления мобильными устройствами по протоколу Exchange ActiveSync на сервере Microsoft Exchange должен быть развернут Сервер Exchange. Подробная информация об установке Exchange Server приведена в *Справке Kaspersky Security Center*. На мобильных устройствах дополнительная настройка не требуется.

С помощью почтового ящика Exchange вы можете удаленно настраивать EAS-устройства с использованием групповых политик и отправлять команду удаления данных. Протокол Exchange ActiveSync поддерживают следующие операционные системы:

- Windows Mobile;
- Windows CE;
- Windows Phone;
- Android;
- Bada;
- BlackBerry 10;
- iOS;
- Symbian.

Набор параметров управления устройством Exchange ActiveSync зависит от операционной системы мобильного устройства. С особенностями поддержки протокола Exchange ActiveSync для конкретной операционной системы можно ознакомиться в документации для этой операционной системы.

О плагине управления Kaspersky Endpoint Security для Android

Плагин управления Kaspersky Endpoint Security для Android обеспечивает интерфейс управления мобильными устройствами и установленными на них мобильными приложениями через Консоль администрирования Kaspersky Security Center. С помощью плагина управления Kaspersky Endpoint Security для Android вы можете выполнять следующие действия:

- создавать групповые политики безопасности мобильных устройств;
- удаленно настраивать параметры работы приложения Kaspersky Endpoint Security для Android на мобильных устройствах пользователей;
- получать отчеты и статистику о работе мобильного приложения Kaspersky Endpoint Security для Android на устройствах пользователей.

Плагин управления Kaspersky Endpoint Security для Android устанавливается по умолчанию при развертывании Kaspersky Security Center. Плагин не требует отдельной установки.

О плагине управления Kaspersky Device Management для iOS

Плагин управления Kaspersky Device Management для iOS обеспечивает интерфейс управления мобильными устройствами, подключенными по протоколам iOS MDM и Exchange ActiveSync, через Консоль администрирования Kaspersky Security Center. Плагин управления Kaspersky Device Management для iOS позволяет выполнять следующие действия:

- создавать групповые политики безопасности мобильных устройств;
- удаленно настраивать устройства, подключенные по протоколу Exchange ActiveSync (далее "EAS-устройства");
- удаленно настраивать устройства, подключенные по протоколу iOS MDM (далее "iOS MDM-устройства");
- получать отчеты и статистику о работе мобильных устройств пользователей.

Подробная информация о подключении мобильных устройств к Kaspersky Security Center по протоколам iOS MDM и Exchange ActiveSync приведена в *справке Kaspersky Security Center*.

Плагин управления Kaspersky Device Management для iOS устанавливается по умолчанию при развертывании Kaspersky Security Center. Плагин не требует отдельной установки.

Комплект поставки

В состав комплекта поставки комплексного решения Kaspersky Security для мобильных устройств входят следующие компоненты:

- Самораспаковывающийся архив `sc_package_xx`, который содержит установочные файлы мобильных приложений для основных поддерживаемых систем:
  - `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` – набор файлов, необходимый для установки Kaspersky Endpoint Security для Android;
  - `installer.ini` – конфигурационный файл с параметрами подключения к Серверу администрирования;

    - `KES10_xx_xx_xxx.apk` – установочный файл Kaspersky Endpoint Security для Android;
    - `kmlisten.exe` – утилита доставки инсталляционного пакета приложения через рабочую станцию;
    - `kmlisten.ini` – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
    - `kmlisten.kpd` – файл с описанием программы.
- `Klcfginst_en.exe` – установочный файл плагина управления Kaspersky Endpoint Security для Android, предназначенного для управления программой с помощью системы удаленного администрирования Kaspersky Security Center;
- `Klmdminst.exe` – установочный файл плагина управления Kaspersky Device Management для iOS, предназначенного для управления программой с помощью системы удаленного администрирования Kaspersky Security Center;
- `KES10_xx_xx_xxx.apk` – установочный файл Kaspersky Endpoint Security для Android;
- `licutil.exe` – утилита для активации приложения Kaspersky Endpoint Security для Android, если в вашей организации не развернут Kaspersky Security Center;
- `SigningUtility.zip` – архив, который содержит утилиту для подписания дистрибутива мобильного приложения и контейнеров для iOS-устройств.
- Комплект документации:
    - контекстная справка плагина управления Kaspersky Endpoint Security для Android;
    - контекстная справка плагина управления Kaspersky Device Management для iOS;
    - справка мобильного приложения Kaspersky Endpoint Security для Android.

Аппаратные и программные требования

В этом разделе содержатся аппаратные и программные требования к компьютеру администратора, который используется для развертывания приложений на мобильных устройствах, а также перечень операционных систем для мобильных устройств, работу с которыми поддерживает Kaspersky Security для мобильных устройств.

Аппаратные и программные требования к компьютеру администратора

Для развертывания комплексного решения Kaspersky Security для мобильных устройств компьютер администратора должен соответствовать аппаратным требованиям Kaspersky Security Center. Подробная информация об аппаратных требованиях для Kaspersky Security Center приведена в *справке Kaspersky Security Center*.

Для работы плагина управления Kaspersky Endpoint Security для Android на компьютере администратора должна быть установлена Консоль администрирования Kaspersky Security Center версии 10.0 Service Pack 3 или выше.

Для работы плагина управления Kaspersky Device Management для iOS компьютер администратора должен удовлетворять следующим программным требованиям:

- Консоль администрирования Kaspersky Security Center 10 Service Pack 3 или выше;
- компонент Сервер Exchange;
- компонент Сервер iOS MDM;
- набор инструкций SSE2 или более новой версии.

Для развертывания мобильного приложения Kaspersky Endpoint Security для Android через Сервер администрирования компьютер администратора должен удовлетворять следующим программным требованиям:

- Kaspersky Security Center 10 Service Pack 3 или выше;
- плагин управления Kaspersky Endpoint Security для Android.

Для развертывания мобильного приложения Kaspersky Endpoint Security для Android из соответствующих интернет-магазинов к компьютеру администратора программных требований не предъявляется.

Мобильное приложение Kaspersky Endpoint Security для Android может также работать в составе системы удаленного администрирования Kaspersky Endpoint Security Cloud версии 6.0 и выше. Подробная информация о работе с приложениями с помощью Kaspersky Endpoint Security Cloud приведена в *справке Kaspersky Endpoint Security Cloud*.

Также мобильное приложение Kaspersky Endpoint Security для Android может работать в составе сторонних EMM-систем:

- VMWare AirWatch 9.3 и выше.
- MobileIron 10.0 и выше.
- IBM Maas360 10.68 и выше.
- Microsoft Intune 1908 и выше.
- SOTI MobiControl 14.1.4 (1693) и выше.

Аппаратные и программные требования к мобильному устройству пользователя для Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android имеет следующие аппаратные и программные требования:

- смартфон или планшет с разрешением экрана от 320x480 пикселей;
- 65 МБ свободного места в основной памяти устройства;
- Android 4.2 – 11.0 (за исключением версии Go Edition для устройств Samsung);
- архитектура процессора x86, x86-64, ARM5, ARM6, ARM7, ARM8.

Приложение устанавливается только в основную память устройства.

Аппаратные и программные требования к мобильному устройству пользователя для iOS MDM-профиля

iOS MDM-профиль имеет следующие аппаратные и программные требования:

- iOS 10.0 – 14.0 или iPadOS;
- подключение к интернету.

Развертывание

Этот раздел справки адресован специалистам, которые осуществляют установку Kaspersky Security для мобильных устройств, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security для мобильных устройств.

Архитектура решения

Kaspersky Security для мобильных устройств включает в себя следующие компоненты:

- Мобильное приложение Kaspersky Endpoint Security для Android.

  Kaspersky Endpoint Security для Android защищает мобильные устройства от веб-угроз, вирусов и других программ, представляющих угрозы. Осуществляет взаимодействие между мобильным устройством и Сервером администрирования Kaspersky Security Center с помощью Firebase Cloud Messaging.

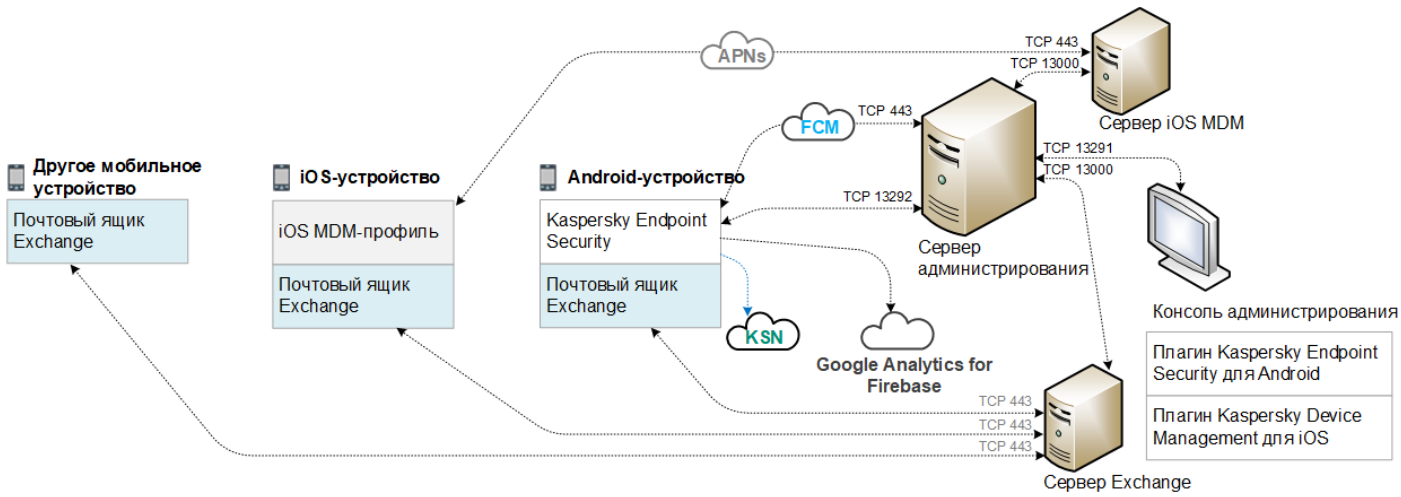
- Плагин управления Kaspersky Endpoint Security для Android

  Плагин управления Kaspersky Endpoint Security для Android обеспечивает интерфейс управления мобильными устройствами и установленными на них мобильными приложениями через Консоль администрирования Kaspersky Security Center.

- Плагин управления Kaspersky Device Management для iOS.

  Плагин управления Kaspersky Device Management для iOS обеспечивает интерфейс управления мобильными устройствами, подключенными по протоколам iOS MDM и Exchange ActiveSync, через Консоль администрирования Kaspersky Security Center.

Архитектура комплексного решения Kaspersky Security для мобильных устройств представлена на рисунке ниже.



Архитектура Kaspersky Security для мобильных устройств

Подробная информация о Консоли администрирования, Сервере администрирования, Сервере Exchange и Сервере iOS MDM приведена в *справке Kaspersky Security Center*.

Типовые схемы развертывания комплексного решения

В этом разделе описаны типовые схемы развертывания комплексного решения Kaspersky Security для мобильных устройств.

Развертывание комплексного решения на Android-устройствах и iOS-устройствах выполняется по разным схемам. Если в организации используются мобильные устройства под управлением различных операционных систем, следует выполнять установку приложений для каждой операционной системы отдельно по соответствующей схеме развертывания.

Схемы развертывания Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android можно разворачивать на мобильных устройствах в сети организации несколькими способами. Вы можете выбрать наиболее подходящий для вашей организации способ развертывания, а также использовать несколько способов развертывания одновременно.

Подробная информация о развертывании Kaspersky Endpoint Security для Android в Kaspersky Endpoint Security Cloud приведена в *справке Kaspersky Endpoint Security Cloud*.

Схемы развертывания Kaspersky Endpoint Security для Android через Kaspersky Security Center

Развертывание Kaspersky Endpoint Security для Android через Kaspersky Security Center может быть выполнено следующими способами:

- С помощью рассылки сообщений со ссылкой на Google Play (рекомендуется).
- С помощью рассылки сообщений со ссылкой на автономный пакет приложения.

Развертывание Kaspersky Endpoint Security для Android с помощью Google Play заключается в рассылке пользователям устройств сообщений со ссылкой на Google Play из Консоли администрирования.

Развертывание Kaspersky Endpoint Security для Android с помощью рассылки автономного пакета состоит из следующих действий администратора:

1. Создание инсталляционного пакета приложения.
2. Настройка параметров инсталляционного пакета.
3. Создание автономного пакета установки.
4. Рассылка пользователям Android-устройств сообщений со ссылкой на загрузку автономного пакета установки. Доступна массовая рассылка.

Установку Kaspersky Endpoint Security для Android на мобильное устройство выполняет пользователь после получения сообщения со ссылкой на Google Play или ссылкой на загрузку дистрибутива с Веб-сервера Kaspersky Security Center. Дополнительной подготовки приложения к работе не требуется.

Схема развертывания Kaspersky Endpoint Security для Android из Google Play

Рекомендуется применять схему развертывания из Google Play, если провести удаленную установку невозможно.

Установку Kaspersky Endpoint Security для Android из Google Play пользователи устройств выполняют самостоятельно. Пользователь загружает дистрибутив мобильного приложения из Google Play и устанавливает его на устройство. После установки приложения на мобильное устройство требуется дополнительная подготовка к работе: настройка параметров подключения к Серверу администрирования и установка общего сертификата.

Схема развертывания Kaspersky Endpoint Security для Android через KNOX Mobile Enrollment

Развертывание Kaspersky Endpoint Security для Android заключается в добавлении профиля KNOX MDM на мобильные устройства. Профиль KNOX MDM содержит ссылку на приложение, размещенное на Веб-сервере Kaspersky Security Center или другом сервере. После установки приложения на мобильном устройство дополнительно требуется установить общий сертификат.

Информация об установке с помощью KNOX Mobile Enrollment приведена в разделе Samsung KNOX.

Схемы развертывания для iOS MDM-профиля

iOS MDM-профиль – это профиль, который содержит параметры подключения мобильных устройств под управлением операционной системы iOS к Kaspersky Security Center. После установки iOS MDM-профиля и синхронизации с Kaspersky Security Center устройство становится управляемым. Управление мобильными устройствами осуществляется с помощью Apple Push Notification service (APNs). Подробная информация об установке iOS MDM-профиля и работе с APNs приведена в *справке Kaspersky Security Center*.

С помощью iOS MDM-профиля можно выполнять следующие действия:

- Удаленно настраивать параметры iOS MDM-устройств с помощью групповых политик.
- Отправлять команды блокирования и удаления данных.
- Удаленно устанавливать приложения "Лаборатории Касперского", а также другие сторонние приложения.

iOS MDM-профиль можно разворачивать на мобильных устройствах в сети организации несколькими способами. Вы можете выбрать наиболее подходящий для вашей организации способ развертывания, а также использовать несколько способов развертывания одновременно.

Перед развертыванием iOS MDM-профиля администратор должен выполнить следующие действия:

1. Установить Сервер iOS MDM.
2. Получить сертификат Apple Push Notification Service (APNs-сертификат).
3. Установить APNs-сертификат на Сервер iOS MDM.

Подробная информация об установке Сервера iOS MDM и работе с APNs-сертификатом приведена в *справке Kaspersky Security Center*.

Подробная информация о развертывании iOS MDM-профиля в Kaspersky Endpoint Security Cloud приведена в *справке Kaspersky Endpoint Security Cloud*.

Схема развертывания iOS MDM-профиля через Kaspersky Security Center

Развертывание iOS MDM-профиля через Kaspersky Security Center может быть выполнено с помощью рассылки сообщений со ссылкой на загрузку iOS MDM-профиля. Доступна массовая рассылка.

Установку iOS MDM-профиля на мобильное устройство выполняет пользователь после получения сообщения со ссылкой на Веб-сервер Kaspersky Security Center. Дополнительной подготовки iOS MDM-профиля к работе не требуется.

Подробная информация о создании iOS MDM-профиля приведена в *справке Kaspersky Security Center*.

Подготовка Консоли администрирования к развертыванию комплексного решения

Этот раздел содержит инструкции по подготовке Консоли администрирования к развертыванию комплексного решения.

Настройка параметров Сервера администрирования для подключения мобильных устройств

Чтобы мобильные устройства могли подключиться к Серверу администрирования, перед установкой мобильного приложения Kaspersky Endpoint Security настройте параметры подключения мобильных устройств в свойствах Сервера администрирования.

Чтобы настроить параметры Сервера администрирования для подключения мобильных устройств, выполните следующие действия:

1. В контекстном меню Сервера администрирования выберите пункт **Свойства**.

   Откроется окно свойств Сервера администрирования.

2. Выберите раздел **Параметры подключения к Серверу** → **Дополнительные порты**.

3. Установите флажок **Открывать порт для мобильных устройств**.

4. В поле **Порт для мобильных устройств** укажите порт, по которому к Серверу администрирования будут подключаться мобильные устройства.

   По умолчанию указан порт 13292. Если флажок **Открывать порт для мобильных устройств** снят или порт для подключения указан неверно, мобильные устройства не смогут подключаться к Серверу администрирования.

5. В поле **Порт активации мобильных клиентов** укажите порт для подключения мобильных устройств к Серверу администрирования для активации приложения Kaspersky Endpoint Security для Android. По умолчанию указан порт 13292.

6. Нажмите кнопку **ОК**.

Отображение папки "Управление мобильными устройствами" в Консоли администрирования

Отображение папки **Управление мобильными устройствами** в Консоли администрирования позволяет просматривать перечень мобильных устройств, находящихся под управлением Сервера администрирования, настраивать параметры управления мобильными устройствами и устанавливать сертификаты на мобильные устройства пользователей.

*Чтобы включить отображение папки **Управление мобильными устройствами** в Консоли администрирования, выполните следующие действия:*

1. В контекстном меню Сервера администрирования выберите пункт **Вид** → **Настройка интерфейса**.
2. В открывшемся окне установите флажок **Отображать Управление мобильными устройствами**.
3. Нажмите кнопку **ОК**.

Папка **Управление мобильными устройствами** будет отображаться в дереве Консоли администрирования после перезапуска Консоли администрирования.

Создание группы администрирования

Централизованная настройка параметров приложения Kaspersky Endpoint Security для Android, установленного на мобильных устройствах пользователей, выполняется посредством применения к этим устройствам групповых политик.

Для того чтобы применить политику к группе устройств, перед установкой мобильных приложений на устройства пользователей рекомендуется создать для этих устройств отдельную группу администрирования в папке **Управляемые устройства**.

После создания группы администрирования рекомендуется настроить автоматическое перемещение в эту группу устройств, на которые вы хотите установить приложения. Затем необходимо задать общие для всех устройств параметры с помощью групповой политики.

Чтобы создать группу администрирования, выполните следующие действия:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** или вложенной папки выберите закладку **Устройства**.
3. Нажмите на кнопку **Создать группу**.

   Откроется окно создания новой группы.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **ОК**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем. Подробная информация о работе с группами администрирования приведена в *справке Kaspersky Security Center*.

Создание правила автоматического переноса устройств в группу администрирования

Централизованное управление параметрами приложения Kaspersky Endpoint Security для Android, установленного на мобильных устройствах пользователей, возможно, только если эти устройства находятся в созданной ранее группе администрирования, для которой назначена групповая политика.

Если правило автоматического перемещения обнаруженных в сети мобильных устройств в группу администрирования не задано, то при первой синхронизации устройства с Сервером администрирования устройство автоматически попадает в Консоль администрирования в папку **Дополнительно → Опрос сети → Домены → KES10**. Групповая политика к этому устройству не применяется.

Чтобы создать правило автоматического перемещения мобильных устройств в группу администрирования, выполните следующие действия:

1. В дереве консоли выберите папку **Нераспределенные устройства**.
2. В контекстном меню папки **Нераспределенные устройства** выберите пункт **Свойства**.

   В результате откроется окно **Свойства: Нераспределенные устройства**.
3. В разделе **Перемещение устройств** нажмите на кнопку **Добавить**, чтобы запустить процесс создания правила автоматического перемещения устройств в группу администрирования.

   Откроется окно **Новое правило**.
4. Введите имя правила.
5. Укажите группу администрирования, в которую должны помещаться устройства после установки на них мобильного приложения Kaspersky Endpoint Security для Android. Для этого нажмите на кнопку **Обзор** справа от поля **Группа, в которую следует перемещать устройства** и в открывшемся окне выберите группу.
6. В блоке **Выполнение правила** выберите вариант **Выполняется один раз для каждого устройства**.
7. Установите флажок **Перемещать только устройства, не размещенные в группах администрирования** для того чтобы в результате применения правила мобильные устройства, уже распределенные в другие группы администрирования, не были перемещены в выбранную группу.
8. Установите флажок **Включить правило**, чтобы правило применялось для только что обнаруженных устройств.
9. Откройте раздел **Программы** и выполните следующие действия:

   a. Установите флажок **Версия операционной системы**.

   b. Выберите один или несколько типов операционной системы устройств, которые будут перемещаться в указанную группу: Android или iOS.
10. Нажмите кнопку **ОК**.

Созданное правило отображается в списке правил перемещения устройств в разделе **Перемещение устройств** окна свойств папки **Нераспределенные устройства**.

В результате выполнения правила Kaspersky Security Center переносит все устройства, соответствующие заданным условиям, из папки **Нераспределенные устройства** в указанную вами группу администрирования. Мобильные устройства, ранее распределенные в папку **Нераспределенные устройства**, также могут быть перемещены в нужную группу администрирования папки **Управляемые устройства** вручную. Подробная информация об управлении группами администрирования и работе с нераспределенными устройствами приведена в *справке Kaspersky Security Center*.

Создание общего сертификата

Для идентификации пользователя мобильного устройства в Консоли администрирования необходимо создать общий сертификат.

Чтобы создать общий сертификат, выполните следующие действия:

1. В дереве консоли выберите папку **Управление мобильными устройствами → Сертификаты**.
2. В рабочей области папки **Сертификаты** по ссылке **Добавить сертификат** запустите мастер установки сертификатов.
3. В окне мастера **Тип сертификата** выберите вариант **Общий сертификат**.
4. В окне мастера **Выбор пользователя** укажите пользователей, для которых вы хотите создать общий сертификат.
5. В окне мастера **Источник сертификата** укажите способ создания общего сертификата.
   - Чтобы создать общий сертификат автоматически средствами Сервера администрирования, выберите вариант **Выписать сертификат средствами Сервера администрирования**.
   - Чтобы назначить пользователю сертификат, созданный ранее, выберите вариант **Указать файл сертификата**. По кнопке **Задать** откройте окно **Сертификат** и укажите в нем файл сертификата.

     Снимите флажок **Опубликовать сертификат**, если вы не хотите указывать тип мобильного устройства и способ уведомления пользователя о создании сертификата.
6. В окне мастера **Способ уведомления пользователей** настройте параметры уведомления пользователя мобильного устройства о создании сертификата с помощью SMS-сообщения или по электронной почте.
7. В окне мастера **Генерация сертификата** нажмите на кнопку **Готово** для завершения работы мастера установки сертификатов.

В результате работы мастера установки сертификатов будет создан общий сертификат, который пользователь сможет установить на мобильное устройство. Для получения сертификата необходимо запустить синхронизацию мобильного устройства с Сервером администрирования. Подробная информация о создании сертификатов и настройке правил их выпуска приведена в *справке Kaspersky Security Center*.

Установка Kaspersky Endpoint Security для Android

В этом разделе описаны способы развертывания Kaspersky Endpoint Security для Android в сети организации.

Разрешения

Для работы всех функций приложений Kaspersky Endpoint Security для Android запрашивает у пользователя необходимые разрешения. Kaspersky Endpoint Security для Android запрашивает обязательные разрешения во время прохождения мастера установки, а также после установки перед использованием отдельных функций приложений. Без предоставления обязательных разрешений Kaspersky Endpoint Security для Android установить невозможно.

На некоторых устройствах (например, Huawei, Meizu, Xiaomi) требуется вручную, в настройках устройства, добавить Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы. Если приложение не добавлено в список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства.

Поддержка Фильтра вызовов и SMS и SIM-Контроля (отправка сообщений с новым номером телефона) прекращена в Kaspersky Endpoint Security для Android Service Pack 4 Update 4 (сборка 10.8.0.103). В этом случае Kaspersky Endpoint Security для Android не запрашивает у пользователя разрешение Управление SMS. Для работы Фильтра вызовов и SMS и всех функций SIM-Контроля используйте Kaspersky Endpoint Security для Android более ранних версий.

Разрешения, запрашиваемые Kaspersky Endpoint Security для Android

Разрешение	Функция приложения
Телефон (обязательно только для Android 4.2 – 9.X)	Подключение к Kaspersky Security Center (идентификатор устройства)
Память (обязательно)	Антивирус
Администратор устройства (обязательно)	Анти-Вор – блокировка устройства (только для Android 4.2 – 6.X)
	Анти-Вор – выполнение снимка фронтальной камерой
	Анти-Вор – воспроизведение звукового сигнала
	Анти-Вор – сброс настроек до заводских
	Защита паролем
	Защита приложения от удаления
	установка сертификатов безопасности;
	Контроль установленных приложений
	Управление KNOX (только для Samsung-устройств)
	настройка Wi-Fi;
	настройка Exchange ActiveSync;
	ограничение использования камеры, Bluetooth, Wi-Fi.
Камера	Анти-Вор – выполнение снимка фронтальной камерой На устройствах с операционной системой Android 11.0 и выше необходимо при появлении запроса предоставить разрешение "При использовании приложения".
Местоположение	Анти-Вор – определение местоположения устройства На устройствах с операционной системой Android 10.0 и выше необходимо при появлении запроса предоставить разрешение "Всегда".
Специальные	Анти-Вор – блокировка устройства (только для Android 7.0 и выше)

возможности	Веб-Фильтр (только для Android 5.0 и выше)
	Контроль установленных приложений
	Защита приложения от удаления (только для Android 7.0 и выше)
	Отображение предупреждений Kaspersky Endpoint Security для Android (только для Android 10.0 и выше)

Установка Kaspersky Endpoint Security для Android по ссылке на Google Play

Установка Kaspersky Endpoint Security для Android выполняется на мобильные устройства пользователей, учетные записи которых добавлены в Kaspersky Security Center. Подробная информация о работе с учетными записями пользователей в Kaspersky Security Center приведена в справке Kaspersky Security Center.

Kaspersky Security для мобильных устройств позволяет установить приложение с помощью Kaspersky Security Center по ссылке на Google Play (рекомендуемый способ).

Пользователь получит ссылку на Google Play. Установка выполняется обычным способом, принятым для платформы Android. Дополнительной настройки Kaspersky Endpoint Security для Android после установки не требуется.

> У некоторых устройств Huawei и Honor отсутствуют сервисы Google и, следовательно, доступ к приложениям в Google Play. Если пользователям устройств Huawei и Honor не удается установить приложение из Google Play, им следует установить приложение из Huawei AppGallery.

Ссылка содержит следующие данные:

- Параметры синхронизации с Kaspersky Security Center.
- Общий сертификат.
- Индикатор принятия условий и положений Лицензионного соглашения для Kaspersky Endpoint Security для Android и дополнительных Положений. Если администратор принял условия Лицензионного соглашения и дополнительных Положений в Консоли администрирования, во время установки приложения Kaspersky Endpoint Security для Android соответствующий шаг будет пропущен.

Чтобы установить Kaspersky Endpoint Security для Android с помощью Kaspersky Security Center по ссылке на Google Play, выполните следующие действия:

1. В дереве консоли выберите папку **Управление мобильными устройствами** → **Мобильные устройства**.
2. В рабочей области папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.

   Запустится мастер подключения нового мобильного устройства. Следуйте его указаниям.
3. В окне мастера **Операционная система** выберите **Android**.

Kaspersky Security Center проверяет наличие обновлений плагина управления. При обнаружении обновлений программой Kaspersky Security Center, можно установить новую версию плагина администрирования. После обновления плагина управления можно принять условия и положения Лицензионного соглашения (EULA) и дополнительных Положений для Kaspersky Endpoint Security для Android. Если администратор принял условия Лицензионного соглашения и дополнительных Положений в Консоли администрирования, во время установки приложения Kaspersky Endpoint Security для Android соответствующий шаг будет пропущен. Эта функция доступна в Kaspersky Security Center версии 12.

4. На странице **Способ установки Kaspersky Endpoint Security для Android** выберите способ установки приложения **По ссылке на Google Play**.

5. На странице **Выбор пользователей** выберите пользователей, чтобы установить Kaspersky Endpoint Security для Android на их мобильные устройства.

   Если пользователя нет в списке, можно добавить новую учетную запись, не выходя из мастера подключения нового мобильного устройства.

6. На странице **Источник сертификата** выберите источник сертификата для защиты обмена данными между Kaspersky Endpoint Security для Android и Kaspersky Security Center:

   - **Выписать сертификат средствами Сервера администрирования.** В этом случае сертификат будет создан автоматически.

   - **Указать файл сертификата**. В этом случае требуется предварительно подготовить собственный сертификат и выбрать его в окне мастера. Этот вариант невозможно использовать, если вы хотите установить Kaspersky Endpoint Security для Android на несколько мобильных устройств. Для каждого пользователя должен быть создан отдельный сертификат.

7. На странице **Способ уведомления пользователей** выберите канал передачи ссылки для установки приложения:

   - Для передачи ссылки по электронной почте выберите **Отправить ссылку на Kaspersky Endpoint Security** и настройте параметры в блоке **По электронной почте**. Убедитесь, что в параметрах учетных записей пользователей указан адрес электронной почты.

   - Для передачи ссылки с помощью SMS-сообщения выберите **Отправить ссылку на Kaspersky Endpoint Security** и настройте параметры в блоке **С помощью SMS**. Убедитесь, что в параметрах учетных записей пользователей указан номер телефона.

   - Для установки Kaspersky Endpoint Security для Android с помощью QR-кода выберите **Показать ссылку на инсталляционный пакет** и выполните сканирование QR-кода с помощью камеры мобильного устройства.

   - Если вам не подошел ни один из перечисленных способов, выберите **Показать ссылку на инсталляционный пакет → Скопировать**, чтобы сохранить ссылку для установки Kaspersky Endpoint Security для Android в буфер обмена. Передайте ссылку для установки приложения любым доступным способом. Вы также можете использовать другие способы установки Kaspersky Endpoint Security для Android.

8. Нажмите на кнопку **Завершить**, чтобы завершить работу мастера подключения нового мобильного устройства.

После установки Kaspersky Endpoint Security для Android на мобильные устройства пользователей вы сможете настраивать параметры устройств и приложений с помощью групповых политик. Вы также сможете отправлять на мобильные устройства команды для защиты данных в случае потери или кражи устройств.

Другие способы установки Kaspersky Endpoint Security для Android

Вы можете установить Kaspersky Endpoint Security для Android, используя ссылку на собственный веб-сервер, или попросить пользователей установить приложение вручную.

Установка из Google Play и Huawei AppGallery вручную

Пользователи могут вручную установить Kaspersky Endpoint Security для Android из Google Play или Huawei AppGallery. Установка выполняется обычным способом, принятым для платформы Android. Для установки приложения пользователь использует свою личную учетную запись Google.

Подробнее о процедуре установки Kaspersky Endpoint Security для Android из Google Play см. на сайте технической поддержки Google.

Подробная информация о процедуре установки Kaspersky Endpoint Security для Android из Huawei AppGallery приведена на сайте технической поддержки HUAWEI.

У некоторых устройств Huawei и Honor отсутствуют сервисы Google и, следовательно, доступ к приложениям в Google Play. Если пользователям устройств Huawei и Honor не удается установить приложение из Google Play, им следует установить приложение из Huawei AppGallery.

После установки Kaspersky Endpoint Security для Android из Google Play или Huawei AppGallery требуется выполнить подготовку приложения к работе. Подготовка приложения к работе состоит из следующих этапов:

1. Администратор отправляет пользователю параметры синхронизации мобильного устройства с Сервером администрирования (адрес сервера и порт) любым доступным способом (например, в сообщении электронной почты).

2. Пользователь настраивает параметры синхронизации мобильного устройства с Сервером администрирования во время работы мастера первоначальной настройки или в настройках Kaspersky Endpoint Security для Android.

3. Администратор создает общий сертификат для пользователя мобильного устройства.

4. Пользователь получает автоматическое уведомление с предложением установить общий сертификат. После подтверждения общий сертификат устанавливается на мобильное устройство.

Для синхронизации с Сервером администрирования на мобильном устройстве должен быть включен доступ в интернет.

Подробная информация о настройке параметров синхронизации мобильного устройства с Сервером администрирования и получении общего сертификата приведена в справке Kaspersky Security Center.

При следующей синхронизации мобильного устройства с Сервером администрирования мобильное устройство пользователя, на котором установлено приложение Kaspersky Endpoint Security для Android, помещается в папку **Дополнительно** → **Опрос сети** → **Домены** в группу администрирования, указанную при установке приложения (по умолчанию используется группа **KES10**). Вы можете переместить мобильное устройство в папку Управляемые устройства в созданную вами группу администрирования вручную или с помощью правил автоматического перемещения.

Этот способ установки удобен, если вы хотите установить определенную версию Kaspersky Endpoint Security для Android.

Для установки Kaspersky Endpoint Security для Android по ссылке на собственный Веб-сервер требуется выполнить следующие действия:

1. Создайте инсталляционный пакет и настройте его параметры.

   Инсталляционный пакет – набор файлов, сформированный для удаленной установки приложения "Лаборатории Касперского" с помощью Kaspersky Security Center.

2. Создайте автономный пакет установки.

   Автономный пакет установки – установочный файл мобильного приложения, содержащий параметры подключения приложения к Серверу администрирования и индикатор принятия условий и положений Лицензионного соглашения для Kaspersky Endpoint Security для Android. Создается на основе инсталляционного пакета для Kaspersky Endpoint Security для Android. Автономный пакет установки является частным случаем пакета мобильных приложений.

Пользователь получит ссылку на Веб-сервер, на котором расположен автономный пакет установки Kaspersky Endpoint Security для Android. Для установки приложения пользователю необходимо запустить apk-файл. Дополнительной настройки Kaspersky Endpoint Security для Android после установки не требуется.

Для установки Kaspersky Endpoint Security для Android по ссылке на собственный Веб-сервер на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников.

Создание и настройка инсталляционного пакета

Инсталляционный пакет Kaspersky Endpoint Security для Android представляет собой самораспаковывающийся архив `sc_package.exe`. В состав архива входят файлы, необходимые для установки мобильного приложения на устройства:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll` – набор файлов, необходимый для установки Kaspersky Endpoint Security для Android;
- `installer.ini` – конфигурационный файл с параметрами подключения к Серверу администрирования;
- `KES10_xx_xx_xxx.apk` – установочный файл Kaspersky Endpoint Security для Android;
- `kmlisten.exe` – утилита доставки инсталляционного пакета приложения через рабочую станцию;
- `kmlisten.ini` – конфигурационный файл с параметрами для утилиты доставки инсталляционного пакета;
- `kmlisten.kpd` – файл с описанием программы.

Чтобы создать инсталляционный пакет Kaspersky Endpoint Security для Android, выполните следующие действия:

1. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. В рабочей области папки **Инсталляционные пакеты** нажмите на кнопку **Создать инсталляционный пакет**.

   Запустится мастер создания инсталляционного пакета. Следуйте его указаниям.

3. В окне мастера **Выбор типа инсталляционного пакета** нажмите на кнопку **Создать инсталляционный пакет для программы "Лаборатории Касперского"**.

4. В окне мастера **Определение имени инсталляционного пакета** введите имя инсталляционного пакета для отображения в рабочей области папки **Инсталляционные пакеты**.

5. В окне мастера **Выбор дистрибутива программы для установки** выберите самораспаковывающийся архив `sc_package.exe`, который входит в комплект поставки.

   Если архив был распакован ранее, то вы можете выбрать входящий в состав архива файл с описанием приложения `kmlisten.kpd`. В результате в поле ввода отобразится название приложения и номер версии.

6. В окне мастера **Принятие Лицензионное соглашение** прочитайте и примите условия Лицензионного соглашения.

   Условия Лицензионного соглашения необходимо принять для создания инсталляционного пакета. Если вы приняли условия Лицензионного соглашение в Консоли администрирования, во время установки приложения Kaspersky Endpoint Security для Android шаг принятия Лицензионного соглашения будет пропущен.

   Если вы решите прекратить защиту мобильных устройств, можно удалить приложение Kaspersky Endpoint Security для Android и отозвать согласие с условиями Лицензионного соглашения для этого приложения. Дополнительная информация об отзыве Лицензионного соглашения приведена в *справке Kaspersky Security Center*.

После завершения работы мастера созданный инсталляционный пакет будет отображаться в рабочей области папки **Инсталляционные пакеты**. На Сервере администрирования инсталляционные пакеты хранятся в заданной папке общего доступа в служебной папке Packages.

Чтобы настроить параметры инсталляционного пакета, выполните следующие действия:

1. В дереве консоли выберите папку **Дополнительно → Удаленная установка → Инсталляционные пакеты**.

2. В контекстном меню инсталляционного пакета Kaspersky Endpoint Security для Android выберите пункт **Свойства**.

3. На закладке **Параметры** укажите параметры подключения мобильных устройств к Серверу администрирования и имя группы администрирования, в которую будут автоматически добавлены мобильные устройства после первой синхронизации с Сервером администрирования. Для этого выполните следующие действия:

   - В блоке **Подключение к Серверу администрирования** в поле **Адрес сервера** укажите имя Сервера администрирования для подключения мобильных устройств в том формате, в каком он был указан при установке компонента **Поддержка мобильных устройств** во время развертывания Сервера администрирования.

     В зависимости от формата имени Сервера администрирования для компонента **Поддержка мобильных устройств** укажите DNS-имя или IP-адрес Сервера администрирования. В поле **Номер SSL-порта** укажите номер порта, открытого на Сервере администрирования для подключения мобильных устройств. По умолчанию указан порт 13292.

   - В блоке **Размещение компьютеров по группам** в поле **Имя группы** введите имя группы, в которую будут добавлены мобильные устройства после первой синхронизации с Сервером администрирования (по умолчанию **KES10**).

     Указанная группа будет создана автоматически в папке **Дополнительно → Опрос сети → Домены**.

   - В блоке **Действия при установке** установите флажок **Запрашивать адрес электронной почты**, чтобы при первом запуске приложение запрашивало у пользователя его адрес корпоративной электронной почты.

Адрес электронной почты пользователя используется для формирования имени мобильных устройств при добавлении их в группу администрирования.

4. Чтобы применить указанные параметры, нажмите на кнопку **Применить**.

Создание автономного пакета установки

Чтобы создать автономный пакет установки, выполните следующие действия:

1. В дереве консоли выберите папку **Дополнительно** → **Удаленная установка** → **Инсталляционные пакеты**.
2. Выберите инсталляционный пакет приложения Kaspersky Endpoint Security для Android.
3. В контекстном меню инсталляционного пакета выберите пункт **Создать автономный пакет установки**.

   В результате запустится мастер создания автономного пакета установки. Следуйте его указаниям.
4. Настройте способы распространения автономного пакета установки:

   - Чтобы распространить путь к сформированному автономному пакету установки среди пользователей по электронной почте, в блоке **Дальнейшие действия** перейдите по ссылке **Разослать ссылку на автономный пакет установки по электронной почте**.

     Откроется окно создания сообщения, текст которого содержит путь к папке общего доступа с автономным пакетом установки.

   - Чтобы разместить ссылку на сформированный автономный пакет установки на веб-сайте своей компании, перейдите по ссылке **Пример HTML-кода для размещения ссылки на веб-сайте**.

     Откроется tmp-файл, содержащий HTML_RJL ссылки.
5. Чтобы опубликовать сформированный автономный пакет установки на Веб-сервере Kaspersky Security Center, а также просмотреть весь список автономных пакетов для выбранного инсталляционного пакета, в окне мастера **Мастер создания автономного пакета установки успешно завершил работу** установите флажок **Открыть список автономных пакетов**.

После завершения работы мастера откроется окно **Список автономных пакетов для инсталляционного пакета <Имя инсталляционного пакета>**.

Окно **Список автономных пакетов для инсталляционного пакета <Имя инсталляционного пакета>** содержит следующую информацию:

- список автономных пакетов установки;
- сетевой путь к папке общего доступа в поле **Путь**;
- адрес автономного пакета на Веб-сервере Kaspersky Security Center в поле **Веб-адрес**.

При рассылке по электронной почте вы можете указать в качестве ресурса для загрузки пользователями установочного файла приложения как адрес, содержащийся в поле **Веб-адрес**, так и адрес, указанный в поле **Путь**. При рассылке SMS-сообщений пользователям следует указать ссылку для загрузки, содержащуюся в поле **Веб-адрес**.

Рекомендуется скопировать адрес подготовленного автономного пакета в буфер обмена, чтобы затем добавить ссылку для загрузки нужного установочного файла в сообщение электронной почты или SMS-сообщение для пользователей.

Настройка параметров синхронизации

Для управления мобильными устройствами и получения отчетов или статистик от мобильных устройств пользователей требуется настроить параметры синхронизации. Синхронизация мобильного устройства с Kaspersky Security Center может быть выполнена следующими способами:

- **По расписанию**. Синхронизация по расписанию выполняется с помощью протокола HTTP. Вы можете настроить расписание синхронизации в параметрах групповой политики. Изменения параметров групповой политики, команды и задачи будут выполнены во время синхронизации устройства с Kaspersky Security Center по расписанию, т. е. с задержкой. По умолчанию мобильные устройства автоматически синхронизируются с Kaspersky Security Center каждые шесть часов.

- **Принудительно**. Принудительная синхронизация выполняется с помощью push-уведомлений сервиса FCM (Firebase Cloud Messaging). Принудительная синхронизация, в первую очередь, предназначена для своевременной доставки команд на мобильное устройство. Если вы хотите использовать принудительную синхронизацию, убедитесь что в Kaspersky Security Center настроены параметры GSM. Дополнительная информация приведена в справке Kaspersky Security Center.

Чтобы настроить параметры синхронизации мобильных устройств с Kaspersky Security Center, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Синхронизация**.

5. Выберите периодичность запуска синхронизации в раскрывающемся списке **Запускать синхронизацию**.

6. Чтобы запретить синхронизацию устройства с Kaspersky Security Center в роуминге, установите флажок **Выключить синхронизацию в роуминге**.

   Пользователь устройства может выполнять синхронизацию вручную в настройках приложения (→ **Настройки** → **Синхронизация** → **Синхронизировать**).

7. Чтобы скрыть от пользователя параметры синхронизации (адрес сервера, порт и группа администрирования) в настройках приложения, снимите флажок **Показывать параметры синхронизации на устройстве**. Изменить скрытые параметры невозможно.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Вы можете принудительно синхронизировать мобильное устройство с помощью специальной команды. Подробная информация о работе с командами для мобильных устройств приведена в справке *Kaspersky Security Center*.

Активация программы

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования Kaspersky Security для мобильных устройств необходимо, чтобы приобретенная организацией лицензия на Kaspersky Security Center распространялась на функциональность **Управление мобильными устройствами**. Функциональность **Управление мобильными устройствами** предназначена для подключения мобильных устройств к Kaspersky Security Center и управления ими.

Подробная информация о лицензировании Kaspersky Security Center и вариантах лицензирования приведена в *справке Kaspersky Security Center*.

Особенность активации приложения Kaspersky Endpoint Security для Android состоит в том, что информация о лицензии передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

Если активация приложения не произошла в течение 30 дней с момента установки на мобильное устройство, то приложение автоматически переключается в режим работы с ограниченной функциональностью. В этом режиме работы большинство компонентов приложения не работает. При переходе в режим работы с ограниченной функциональностью приложение прекращает выполнять автоматическую синхронизацию с Kaspersky Security Center. Поэтому, если по каким-то причинам активация приложения не произошла в течение 30 дней с момента установки, пользователю необходимо вручную выполнить синхронизацию с Kaspersky Security Center.

Если в вашей организации не развернут Kaspersky Security Center, вы можете активировать Kaspersky Endpoint Security для Android с помощью специальной утилиты licutil.

Активация приложений в Kaspersky Security Center

Чтобы активировать приложение Kaspersky Endpoint Security для Android, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В окне **Свойства: <Название политики>** выберите раздел **Лицензирование**.
5. В блоке **Лицензия** в раскрывающемся списке **Ключ** выберите ключ для активации приложения, размещенный в хранилище ключей Сервера администрирования Kaspersky Security Center.

   В поле ниже отобразится информация о приложении, для которого приобретена лицензия, срок окончания действия лицензии, ее тип.
6. Установите флажок **Активировать ключом из хранилища Kaspersky Security Center**.

   Если приложение активировано без помощи ключа, размещенного в хранилище Kaspersky Security Center, Kaspersky Security для мобильных устройств заменит этот ключ на ключ активации выбранный в раскрывающемся списке **Ключ**.

7. Чтобы активировать приложение на мобильном устройстве пользователя, заблокируйте изменение параметров.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Активация Kaspersky Endpoint Security для Android без Kaspersky Security Center

Рекомендуется активировать Kaspersky Endpoint Security для Android без Kaspersky Security Center только если в вашей организации не развернут Kaspersky Security Center.

Активировать приложение можно следующими способами:

- Добавить код активации в дистрибутив приложения перед распространением дистрибутива среди пользователей.
- Добавить код активации в ссылку на Google Play для самостоятельной загрузки приложения перед отправкой ссылки пользователям.

После установки приложения на мобильном устройстве пользователя активация приложения выполняется автоматически.

Для добавления кода активации в дистрибутив приложения или в ссылку на Google Play используется утилита licutil. Утилита licutil входит в комплект поставки Kaspersky Security для мобильных устройств.

Если в вашей организации развернута система удаленного администрирования Kaspersky Security Center, вы можете подключить мобильные устройства с установленным Kaspersky Endpoint Security для Android к Kaspersky Security Center и дистанционно управлять мобильными устройствами с помощью Консоли администрирования. Для этого требуется активировать приложение ключом из хранилища Kaspersky Security Center. Если вы активировали приложение с помощью рассылки дистрибутива или ссылки на Google Play с добавленным кодом активации, замените активный ключ на ключ из хранилища Kaspersky Security Center. После замены ключа вы можете использовать освободившийся ключ на другом устройстве. Срок использования этого ключа ограничен сроком действия соответствующей ему лицензии.

Чтобы добавить код активации в ссылку для загрузки приложения из Google Play с помощью утилиты licutil,

в командной строке выполните команду `<путь к комплекту поставки>/licutil.exe -c <код активации>`.

Запустится утилита licutil. В командной строке отобразится ссылка на загрузку приложения из Google Play с добавленным кодом активации.

Пример:
```
C:\Users\Admin\Distrib\KSM\licutil.exe -c A1234-B5678-C9012-D3456
```

Вы можете отправить ссылку на загрузку приложения из Google Play пользователю мобильного приложения любым доступным способом (например, по электронной почте или в SMS-сообщении). В сопроводительном тексте рекомендуется указать, что в мастере первоначальной настройки приложения нужно пропустить шаг настройки параметров подключения устройства к Серверу администрирования. После того, как пользователь загрузит приложение из Google Play и установит его на своем мобильном устройстве, активация приложения будет выполнена автоматически.

Код активации является конфиденциальной информацией. Для предотвращения несанкционированного доступа к коду активации или возможной утечки кода активации вам необходимо самостоятельно обеспечить защиту сообщения со ссылкой на Google Play с добавленным кодом активации во время доставки сообщения пользователям.

Для установки приложения из Google Play должны быть выполнены следующие условия:

- У пользователя мобильного устройства должна быть учетная запись Google.
- Мобильное устройство должно быть привязано к учетной записи Google.
- На мобильном устройстве должно быть установлено соединение с интернетом.

Подробная информация о создании учетной записи Google, привязке устройства к учетной записи и работе с Google Play приведена на сайте технической поддержки Google.

Чтобы добавить код активации в дистрибутив приложения с помощью утилиты licutil,

в командной строке выполните команду `<путь к комплекту поставки>/licutil.exe –s <путь к дистрибутиву Kaspersky Endpoint Security для Android из комплекта поставки> -t <путь, по которому будет доступен дистрибутив с добавленным ключом> -c <код активации>.`

Запустится утилита licutil. В заданной папке будет создан дистрибутив приложения с добавленным кодом активации.

Пример:

```
cd C:\Users\Admin\Distrib\KSM\
licutil.exe –s KES10.apk -t KES10key.apk -c A1234-B5678-C9012-D3456
```

Вы можете доставить дистрибутив на мобильное устройство пользователя любым доступным способом (например, скопировав дистрибутив на рабочую станцию пользователя для последующего переноса на мобильное устройство). В сопроводительном сообщении рекомендуется указать, что в мастере первоначальной настройки приложения нужно пропустить шаг настройки параметров подключения устройства к Серверу администрирования. После того как пользователь получит дистрибутив приложения и установит приложение на своем мобильном устройстве, активация приложения будет выполнена автоматически.

Код активации является конфиденциальной информацией. Для предотвращения несанкционированного доступа к коду активации или возможной утечки кода активации вам необходимо самостоятельно обеспечить защиту дистрибутива с добавленным кодом активации во время его доставки пользователям.

Для установки приложения из дистрибутива на мобильном устройстве пользователя должна быть разрешена установка приложений, полученных не из Google Play.

Установка iOS MDM-профиля

В этом разделе описаны способы развертывания iOS MDM-профилей в сети организации.

Перед развертыванием iOS MDM-профиля администратор должен выполнить следующие действия:

1. Установить Сервер iOS MDM.
2. Получить сертификат Apple Push Notification Service (APNs-сертификат).
3. Установить APNs-сертификат на Сервер iOS MDM.

Подробная информация об установке Сервера iOS MDM и работе с APNs-сертификатом приведена в *справке Kaspersky Security Center*.

Подробная информация о развертывании iOS MDM-профиля в Kaspersky Endpoint Security Cloud приведена в *справке Kaspersky Endpoint Security Cloud*.

О режимах управления iOS-устройствами

Развертывание системы управления iOS-устройствами может быть выполнено несколькими способами. Режим управления зависит от того, кому принадлежит мобильное устройство (личное или корпоративное) и требований корпоративной безопасности. Вы можете выбрать наиболее подходящий для компании режим управления, а также использовать несколько режимов одновременно.

Неконтролируемые устройства

Неконтролируемые iOS-устройства – личные устройства сотрудников, подключенные к Kaspersky Security Center. В этом режиме пользователю разрешено использовать персональный Apple ID, работать с любыми приложениями и хранить персональные данные на устройстве. Доступ к корпоративным ресурсам, параметры безопасности и другие параметры вы можете настроить с помощью групповой политики Kaspersky Device Management для iOS. По умолчанию все iOS-устройства неконтролируемые.

Контролируемые устройства

Контролируемые iOS-устройства – корпоративные устройства, подключенные к Kaspersky Security Center. Первоначальная настройка мобильного устройства выполняется в Apple Configurator. *Apple Configurator* – программа для подготовки и настройки iOS-устройств. Apple Configurator устанавливается на компьютер под управлением OS X. Подробная информация о работе с Apple Configurator приведена на сайте технической поддержки Apple. Дальнейшее изменение параметров доступно с помощью групповой политики Kaspersky Device Management для iOS. На контролируемых устройствах доступен расширенный набор параметров: Глобальный HTTP-прокси, дополнительные ограничения (например, запрет на использование iMessage, Game Center) или запрет на изменение учетной записи пользователя.

Для работы с контролируемыми и неконтролируемыми iOS-устройствами на Сервер iOS MDM должен быть установлен APNs-сертификат, а на мобильных устройствах пользователей – iOS MDM-профиль.

Установка через Kaspersky Security Center

Установка iOS MDM-профиля выполняется на мобильные устройства пользователей, учетные записи которых добавлены в Kaspersky Security Center. Подробная информация о работе с учетными записями пользователей в Kaspersky Security Center приведена в справке *Kaspersky Security Center*.

Чтобы установить iOS MDM-профиль, выполните следующие действия:

1. В дереве консоли выберите папку **Управление мобильными устройствами → Мобильные устройства**.
2. В рабочей области папки **Мобильные устройства** нажмите на кнопку **Добавить мобильное устройство**.

   Запустится мастер подключения нового мобильного устройства. Следуйте его указаниям.
3. В окне мастера **Операционная система** выберите **iOS**.
4. В окне мастера **Способ защиты iOS MDM-устройства** выберите **Использовать iOS MDM-профиль Сервера iOS MDM** и укажите iOS MDM-профиль из списка.
5. В окне мастера **Выбор пользователей** выберите одного или несколько пользователей для установки iOS MDM-профиля на их мобильные устройства.

   Если пользователя нет в списке, вы можете добавить новую учетную запись не выходя из мастера подключения нового мобильного устройства.
6. В окне мастера **Источник сертификата** выберите источник сертификата для защиты обмена данными между мобильным устройством и Kaspersky Security Center:

   - **Выписать сертификат средствами Сервера администрирования**. В этом случае сертификат будет создан автоматически.
   - **Указать файл сертификата**. В этом случае требуется предварительно подготовить собственный сертификат и выбрать его в окне мастера. Этот вариант невозможно использовать, если вы хотите установить iOS MDM-профиль на несколько мобильных устройств. Для каждого пользователя должен быть создан отдельный сертификат.
7. В окне мастера **Способ уведомления пользователей** выберите канал передачи ссылки для установки приложения:

   - Для передачи ссылки по электронной почте выберите **Отправить ссылку на iOS MDM-профиль** и настройте параметры в блоке **По электронной почте**. Убедитесь, что в параметрах учетных записей пользователей указан адрес электронной почты.
   - Для передачи ссылки с помощью SMS-сообщения выберите **Отправить ссылку на iOS MDM-профиль** и настройте параметры в блоке **С помощью SMS**. Убедитесь, что в параметрах учетных записей пользователей указан номер телефона.
   - Для установки iOS MDM-профиля с помощью QR-кода выберите **Показать ссылку на инсталляционный пакет** и выполните сканирование QR-кода с помощью камеры мобильного устройства.
   - Если вам не подошел ни один из перечисленных способов, выберите **Показать ссылку на инсталляционный пакет → Скопировать**, чтобы сохранить ссылку для установки iOS MDM-профиля в буфер обмена. Передайте ссылку для установки приложения любым доступным способом.
8. Завершите работу мастера подключения нового мобильного устройства.

После установки iOS MDM-профиля на мобильные устройства пользователей вы сможете настроить параметры приложения с помощью групповых политик. Вы также сможете отправлять на мобильные устройства команды для защиты данных в случае потери или кражи устройств.

На мобильных устройствах под управлением iOS 12.1 и выше необходимо вручную подтвердить установку iOS MDM-профиля на мобильном устройстве. Также необходимо предоставить разрешение на удаленное управление устройством.

Установка плагинов управления

Для управления мобильными устройствами на рабочее место администратора необходимо установить следующие плагины управления:

- Плагин управления Kaspersky Endpoint Security для Android обеспечивает интерфейс управления мобильными устройствами и установленными на них мобильными приложениями через Консоль администрирования Kaspersky Security Center.
- Плагин управления Kaspersky Device Management для iOS обеспечивает интерфейс управления мобильными устройствами, подключенными по протоколам iOS MDM и Exchange ActiveSync, через Консоль администрирования Kaspersky Security Center.

Плагины управления можно установить следующими способами:

- Установить плагин управления с помощью мастера первоначальной настройки Kaspersky Security Center.

  Программа автоматически предложит запустить мастер первоначальной настройки после установки Сервера администрирования при первом подключении к нему. Мастер первоначальной настройки можно также запустить вручную в любое время.

  Мастер первоначальной настройки позволяет принимать условия и положения Лицензионного соглашения для приложения Kaspersky Endpoint Security для Android в Консоли администрирования. Если администратор принял условия Лицензионного соглашения в Консоли администрирования, во время установки приложения Kaspersky Endpoint Security для Android шаг принятия Лицензионного соглашения будет пропущен. Более подробная информация о мастере первоначальной настройки Kaspersky Security Center приведена в *справке Kaspersky Security Center*.

- Установить плагин управления с помощью списка доступных дистрибутивов в Консоли администрирования Kaspersky Security Center.

  Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "Лаборатории Касперского".

- Загрузить дистрибутив из внешнего источника и установить плагин управления, используя файл EXE.

  Например, дистрибутив плагина управления можно загрузить с сайта "Лаборатории Касперского".

Установка плагинов управления из списка в Консоли администрирования

Чтобы установить плагины управления, выполните следующие действия:

1. В дереве консоли выберите папку **Дополнительно → Удаленная установка → Инсталляционные пакеты**.
2. В рабочей области выберите **Дополнительные действия → Просмотр текущих версий программ "Лаборатории Касперского"**.

   Откроется список актуальных версий программ "Лаборатории Касперского".

3. В разделе **Мобильные устройства** выберите плагин **Kaspersky Endpoint Security для Android** или **Kaspersky Device Management для iOS**.

4. Нажмите на кнопку **Загрузить дистрибутивы**.

   Дистрибутив плагина будет загружен в память компьютера (файл EXE).

5. Запустите файл EXE и следуйте инструкциям мастера установки.

Установка плагинов управления из дистрибутива

Чтобы установить плагин управления Kaspersky Endpoint Security для Android,

скопируйте из дистрибутива комплексного решения установочный файл плагина `klcfinst.exe` и запустите его на рабочем месте администратора.

Установка выполняется с помощью мастера и не требует настройки параметров.

Чтобы установить плагин управления Kaspersky Device Management для iOS,

скопируйте из дистрибутива комплексного решения установочный файл плагина `klmdminst.exe` и запустите его на рабочем месте администратора.

Установка выполняется с помощью мастера и не требует настройки параметров.

Вы можете убедиться, что плагины управления установлены, просмотрев список установленных плагинов управления приложениями в окне свойств Сервера администрирования в разделе **Дополнительно** → **Информация об установленных плагинах управления программами**.

Обновление предыдущей версии программы

Обновление программы должно выполняться с учетом следующих требований:

- Соблюдайте версионность плагина управления Kaspersky Endpoint Security и мобильного приложения Kaspersky Endpoint Security для Android.

  Номера сборок версий плагина управления и мобильного приложения вы можете посмотреть в Release Notes к Kaspersky Security для мобильных устройств.

- Убедитесь, что Kaspersky Security Center удовлетворяет программным требованиям Kaspersky Security для мобильных устройств.

- Плагины управления Kaspersky Endpoint Security 10.0 Service Pack 2 (сборка 10.6.0.1801) и Kaspersky Device Management для iOS 10.0 Service Pack 2 (сборка 10.6.0.1767) и более поздние версии можно обновить до текущей версии автоматически. Обновление плагинов управления более ранних версий не поддерживается.

  Для обновления плагинов управления более ранних версий необходимо удалить установленные плагины управления и групповые политики, которые были созданы с их помощью. После этого установите новые версии плагинов управления. Подробная информация об удалении плагинов управления приведена на веб-сайте *Службы технической поддержки "Лаборатории Касперского"*.

- Используйте одну версию Kaspersky Endpoint Security для Android на всех мобильных устройствах организации.

Условия и положения предоставления технической поддержки для различных версий Kaspersky Security для мобильных устройств приведены на веб-сайте *Службы технической поддержки "Лаборатория Касперского"*.

Чтобы посмотреть версию и номер сборки плагинов управления, выполните следующие действия:

1. В дереве консоли в контекстном меню Сервера администрирования выберите пункт **Свойства**.
2. В окне свойств Сервера администрирования выберите **Дополнительно** → Информация об установленных плагинах управления программами.

   В рабочей области отобразится информация об установленных плагинах управления в формате `<Название плагина> <Версия> <Сборка>`.

Вы можете посмотреть версию и номер сборки приложения Kaspersky Endpoint Security для Android следующими способами:

- Если Kaspersky Endpoint Security для Android установлен с помощью автономного пакета установки, вы можете посмотреть версию и номер сборки приложения в свойствах пакета.
- Если Kaspersky Endpoint Security для Android установлен через Google Play, вы можете посмотреть номер сборки в настройках приложения (→ **О приложении**).

Обновление предыдущей версии Kaspersky Endpoint Security для Android

Kaspersky Endpoint Security для Android можно обновить следующими способами:

- С помощью Google Play. Пользователь мобильного устройства загружает с Google Play новую версию приложения и устанавливает ее на свое устройство.
- С помощью Kaspersky Security Center. Вы дистанционно обновляете версию приложения на устройстве с помощью системы удаленного администрирования Kaspersky Security Center.

Вы можете выбрать наиболее подходящий для вашей организации способ обновления приложения. Вы можете использовать только один способ обновления.

Обновление с помощью Google Play

Обновление с помощью Google Play выполняется обычным способом, принятым для платформы Android. Для обновления приложения должны быть выполнены следующие условия:

- у пользователя устройства должна быть учетная запись Google;
- Устройство должно быть привязано к учетной записи Google;
- На устройстве должно быть установлено соединение с интернетом.

После загрузки приложения из Google Play, Kaspersky Endpoint Security для Android проверяет условия и положения Лицензионного соглашения. Если условия Лицензионного соглашения обновились, приложение отправляет запрос в Kaspersky Security Center. Если администратор принял Лицензионное соглашение в Консоли администрирования, во время установки приложения Kaspersky Endpoint Security для Android шаг принятия Лицензионного соглашения будет пропущен. Если администратор использует устаревшую версию плагина управления, Kaspersky Security Center предложит обновить плагин управления. При обновлении плагина управления администратор может принять условия Лицензионного соглашения в Консоли администрирования Kaspersky Endpoint Security для Android.

Обновление с помощью Google Play доступно, если приложение Kaspersky Endpoint Security для Android было установлено из Google Play. Если приложение установлено другим способом, обновление приложения с помощью Google Play невозможно.

Обновление приложения с помощью Kaspersky Security Center

Обновление Kaspersky Endpoint Security для Android с помощью Kaspersky Security Center выполняется в результате применения групповой политики. В параметрах групповой политики вы можете выбрать автономный пакет установки Kaspersky Endpoint Security для Android, версия которого удовлетворяет требованиям корпоративной безопасности.

Можно выполнить обновление с помощью Kaspersky Security Center, если приложение Kaspersky Endpoint Security для Android было установлено с помощью Kaspersky Security Center. Если приложение установлено из Google Play, обновление с помощью Kaspersky Security Center невозможно.

Для обновления Kaspersky Endpoint Security для Android с помощью автономного пакета установки на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников. Подробная информация об установке приложений без использования Google Play приведена в *справке Android*.

Чтобы обновить версию приложения, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
5. В блоке **Обновление Kaspersky Endpoint Security для Android** нажмите на кнопку **Выбрать**.

   Откроется окно **Обновление Kaspersky Endpoint Security для Android**.
6. В списке автономных пакетов установки Kaspersky Endpoint Security выберите пакет, версия которого удовлетворяет требованиям корпоративной безопасности.

   Вы можете обновить Kaspersky Endpoint Security только до более новой версии приложения. Обновить Kaspersky Endpoint Security до более старой версии невозможно.
7. Нажмите кнопку **Выбрать**.

В блоке **Обновление Kaspersky Endpoint Security для Android** отобразится описание выбранного автономного пакета установки.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Пользователю мобильного устройства будет предложено установить новую версию приложения. После получения согласия новая версия приложения будет установлена на мобильное устройство.

Установка более ранней версии Kaspersky Endpoint Security для Android

Если вы хотите избежать автоматического обновления приложения и использовать определенную версию Kaspersky Endpoint Security для Android, выключите автообновление приложения в настройках Google Play. Более подробная информация приведена на сайте Службы технической поддержки Google.

Автоматическое обновление Kaspersky Endpoint Security для Android доступно только при установке приложения из Google Play или через Kaspersky Security Center по ссылке на Google Play. Если приложение установлено с помощью Kaspersky Security Center по ссылке на собственный веб-сервер (с использованием автономного пакета установки), автоматическое обновление недоступно. В этом случае обновите Kaspersky Endpoint Security для Android вручную с помощью групповой политики.

Для установки более ранней версии Kaspersky Endpoint Security для Android требуется выполнить следующие действия:

1. Удалите Kaspersky Endpoint Security для Android с мобильных устройств пользователей.

2. Установите Kaspersky Endpoint Security для Android через Kaspersky Security Center по ссылке на собственный Веб-сервер. Для этого вам понадобится инсталляционный пакет определенной версии. Вы можете загрузить дистрибутив Kaspersky Endpoint Security для Android более ранних версий на сайте Службы технической поддержки "Лаборатории Касперского".

Подробная информация о более ранних версиях Kaspersky Endpoint Security для Android приведена в *справке для соответствующей версии Kaspersky Security для мобильных устройств*.

Обновление предыдущих версий плагинов управления

Плагины управления можно обновить следующими способами:

- Установить новую версию плагина управления из списка доступных дистрибутивов в Консоли администрирования Kaspersky Security Center.

  Список доступных дистрибутивов обновляется автоматически после выпуска новых версий программ "Лаборатории Касперского".

- Загрузить дистрибутив из внешнего источника и установить новую версию плагина управления, используя файл EXE.

  Для обновления плагинов управления Kaspersky Endpoint Security для Android и Kaspersky Device Management для iOS требуется загрузить последнюю версию программы со страницы Kaspersky Security для мобильных устройств и запустить мастер установки каждого из плагинов. Предыдущие версии плагинов будут автоматически удалены во время работы мастера установки.

Рекомендуется использовать одинаковую версию приложения и плагинов управления. Если пользователь обновляет приложение из Google Play, в Kaspersky Security Center отображается уведомление с предложением обновить плагин управления.

При обновлении плагинов управления сохраняются уже существующие группы администрирования в папке **Управляемые устройства** и правила автоматического перемещения устройств из папки **Нераспределенные устройства** в эти группы. Существующие групповые политики для мобильных устройств тоже сохраняются. Новые параметры политик, реализующие новые функции комплексного решения Kaspersky Security для мобильных устройств, появятся в существующих политиках и будут иметь значения по умолчанию.

Если в новой версии плагина управления добавлены новые параметры или изменены значения по умолчанию, изменения будут применены только после открытия групповой политики. Пока администратор не откроет групповую политику, на мобильных устройствах будут применены параметры предыдущей версии плагина, даже если версия плагина была обновлена.

Обновление из списка в Консоли администрирования

Чтобы обновить плагины управления, выполните следующие действия:

1. В дереве консоли выберите папку **Дополнительно → Удаленная установка → Инсталляционные пакеты**.
2. В рабочей области выберите **Дополнительные действия → Просмотр текущих версий программ "Лаборатории Касперского"**.

   Откроется список актуальных версий программ "Лаборатории Касперского".
3. В разделе **Мобильные устройства** выберите плагин **Kaspersky Endpoint Security для Android** или **Kaspersky Device Management для iOS**.
4. Нажмите на кнопку **Загрузить дистрибутивы**.

   Дистрибутив плагина будет загружен в память компьютера (файл EXE). Запустите файл EXE. Следуйте инструкциям мастера установки.

Обновление из дистрибутива

Чтобы обновить плагин управления Kaspersky Endpoint Security для Android,

скопируйте из дистрибутива комплексного решения установочный файл плагина `klcfinst.exe` и запустите его на рабочем месте администратора.

Установка выполняется с помощью мастера и не требует настройки параметров.

Чтобы обновить плагин управления Kaspersky Device Management для iOS,

скопируйте из дистрибутива комплексного решения установочный файл плагина `klmdminst.exe` и запустите его на рабочем месте администратора.

Установка плагина выполняется с помощью мастера и не требует настройки параметров.

Вы можете убедиться, что плагины управления обновлены, просмотрев список установленных плагинов управления приложениями в окне свойств Сервера администрирования в разделе **Дополнительно** → **Информация об установленных плагинах управления программами**.

Удаление Kaspersky Endpoint Security для Android

Удаление Kaspersky Endpoint Security для Android может быть выполнено следующими способами:

1. Удаление приложения пользователем

   Пользователь самостоятельно удаляет Kaspersky Endpoint Security для Android, используя интерфейс приложения. Чтобы пользователи могли удалить приложение, в групповой политике, которая применена к устройству, должно быть разрешено удаление приложения.

2. Удаление приложения администратором.

   Администратор дистанционно удаляет приложение, используя Консоль администрирования Kaspersky Security Center. Можно удалить приложение с отдельного устройства или с нескольких устройств одновременно.

Дистанционное удаление приложения

Вы можете дистанционно удалить Kaspersky Endpoint Security для Android с мобильных устройств пользователя следующими способами:

- С помощью групповой политики. Этот способ удобен, если вы хотите удалить приложение с нескольких устройств одновременно.
- С помощью настройки локальных параметров приложения. Этот способ удобен, если вы хотите удалить приложение с отдельного устройства.

Чтобы удалить приложение с помощью применения групповой политики, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
5. В разделе **Удаление приложение Kaspersky Endpoint Security для Android** установите флажок **Удалить Kaspersky Endpoint Security для Android с устройства**.
6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

   В результате после синхронизации с Сервером администрирования приложение Kaspersky Endpoint Security для Android будет удалено с мобильных устройств. Пользователи мобильных устройств получат уведомление об удалении приложения.

Чтобы удалить приложение с помощью настройки локальных параметров, выполните следующие действия:

1. В дереве консоли выберите **Управление мобильными устройствами → Мобильные устройства**.
2. В списке устройств выберите устройство, на котором вы хотите удалить приложение.
3. Откройте окно свойств устройства двойным щелчком мыши.
4. Выберите раздел **Приложения → Kaspersky Endpoint Security для Android.**
5. Откройте окно свойств приложения Kaspersky Endpoint Security двойным щелчком мыши.
6. Выберите раздел **Дополнительно**.
7. В разделе **Удаление Kaspersky Endpoint Security для Android** установите флажок **Удалить Kaspersky Endpoint Security для Android с устройства**.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате после синхронизации с Сервером администрирования приложение Kaspersky Endpoint Security для Android будет удалено с мобильного устройства. Пользователь устройства получит уведомление об удалении приложения.

Разрешение пользователям удалять приложение

На устройствах под управлением операционной системы Android версии 7.0 и выше для защиты приложения от удаления Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android предлагает пользователю предоставить приложению необходимые права. Пользователь может пропустить эти шаги или выключить права в параметрах устройства позднее. В этом случае защита приложения от удаления не работает.

Вы можете разрешить пользователям удалять Kaspersky Endpoint Security для Android со своих мобильных устройств следующими способами:

- С помощью групповой политики. Этот способ удобен, если вы хотите разрешить удаление приложения пользователям нескольких устройств одновременно.
- С помощью локальных параметров приложения. Этот способ удобен, если вы хотите разрешить удаление приложения пользователю отдельного устройства.

Чтобы разрешить удаление приложения в групповой политике, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
5. В блоке **Удаление приложения Kaspersky Endpoint Security для Android** установите флажок **Разрешить удаление приложения Kaspersky Endpoint Security для Android**.
6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильных устройствах после синхронизации с Сервером администрирования будут разрешено удаление приложения пользователем. В настройках Kaspersky Endpoint Security для Android будет доступна кнопка удаления приложения.

Чтобы разрешить удаление приложения в локальных параметрах программы, выполните следующие действия:

1. В дереве консоли выберите **Дополнительно → Управление мобильными устройствами → Мобильные устройства**.
2. В списке устройств выберите устройство, для которого вы хотите разрешить удаление приложения пользователем.
3. Откройте окно свойств устройства двойным щелчком мыши.
4. Выберите **Программы → Kaspersky Endpoint Security для мобильных устройств**.
5. Откройте окно свойств приложения Kaspersky Endpoint Security двойным щелчком мыши.
6. Выберите раздел **Дополнительно**.
7. В блоке **Удаление приложения Kaspersky Endpoint Security для Android** установите флажок **Разрешить удаление приложения Kaspersky Endpoint Security для Android**.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве после синхронизации с Сервером администрирования будут разрешено удаление приложения пользователем. В настройках Kaspersky Endpoint Security для Android будет доступна кнопка удаления приложения.

Удаление приложения пользователем

Чтобы самостоятельно удалить Kaspersky Endpoint Security для Android со своего мобильного устройства, пользователь должен выполнить следующие действия:

1. В главном окне Kaspersky Endpoint Security для Android нажмите  → **Удалить приложение**.

   На экране появится запрос подтверждения.

   Если кнопка **Удалить приложение** отсутствует, значит администратор включил защиту Kaspersky Endpoint Security для Android от удаления.
2. Подтвердить удаление Kaspersky Endpoint Security для Android.

Приложение Kaspersky Endpoint Security для Android будет удалено с мобильного устройства пользователя.

Настройка и управление

Этот раздел справки адресован специалистам, которые осуществляют администрирование Kaspersky Security для мобильных устройств, и специалистам, которые осуществляют техническую поддержку организаций, использующих Kaspersky Security для мобильных устройств.

Начало работы

В этом разделе описаны действия, которые рекомендуется выполнить в начале работы с Kaspersky Security для мобильных устройств.

Запуск и остановка программы

Kaspersky Security Center автоматически запускает и останавливает плагины управления Kaspersky Endpoint Security и Kaspersky Device Management для iOS.

Kaspersky Endpoint Security для Android запускается при старте операционной системы и защищает мобильное устройство пользователя в течение всего сеанса работы. Пользователь может остановить приложение, выключив все компоненты Kaspersky Endpoint Security для Android. Вы можете настроить доступ пользователя к управлению компонентами приложения с помощью групповых политик.

На некоторых устройствах (например, Huawei, Meizu, Xiaomi) требуется вручную добавить Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы (**Безопасность** → **Разрешения** → **Автозапуск**). Если приложение не добавлено в список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства.

Также требуется выключить режим энергосбережения для Kaspersky Endpoint Security для Android. Это необходимо для работы приложения в фоновом режиме, например, запуска антивирусной проверки по расписанию или синхронизации устройства с Kaspersky Security Center. Проблема связана с особенностями встроенного программного обеспечения этих устройств.

Создание группы администрирования

Централизованная настройка параметров приложения Kaspersky Endpoint Security для Android, установленного на мобильных устройствах пользователей, выполняется посредством применения к этим устройствам групповых политик.

Для того чтобы применить политику к группе устройств, перед установкой мобильных приложений на устройства пользователей рекомендуется создать для этих устройств отдельную группу администрирования в папке **Управляемые устройства**.

После создания группы администрирования рекомендуется настроить автоматическое перемещение в эту группу устройств, на которые вы хотите установить приложения. Затем необходимо задать общие для всех устройств параметры с помощью групповой политики.

Чтобы создать группу администрирования, выполните следующие действия:

1. В дереве консоли выберите папку **Управляемые устройства**.
2. В рабочей области папки **Управляемые устройства** или вложенной папки выберите закладку **Устройства**.
3. Нажмите на кнопку **Создать группу**.

   Откроется окно создания новой группы.
4. В открывшемся окне **Имя группы** введите имя группы и нажмите на кнопку **OK**.

В результате в дереве консоли появится новая папка группы администрирования с заданным именем. Подробная информация о работе с группами администрирования приведена в *справке Kaspersky Security Center*.

Групповые политики для управления мобильными устройствами

Групповая политика – это единый набор параметров для управления мобильными устройствами, входящими в группу администрирования, а также установленными на устройствах мобильными приложениями. Вы можете создать групповую политику с помощью мастера создания политики.

С помощью политики вы можете настраивать параметры как отдельных устройств, так и группы. Для группы устройств параметры управления можно настроить в окне свойств групповой политики. Для отдельно устройства их можно настроить в окне локальных параметров программы. Параметры управления, заданные индивидуально для одного устройства, могут отличаться от значений параметров, установленных в политике для группы, в которую входит это устройство.

Каждый параметр, представленный в политике, имеет атрибут "замок", который показывает, разрешено ли изменение параметра в политиках вложенного уровня иерархии (для вложенных групп и подчиненных Серверов администрирования) и в локальных параметрах программы.

Значения параметров, заданные в политике и в локальных параметрах программы, сохраняются на Сервере администрирования, распространяются на мобильные устройства в ходе синхронизации и сохраняются на устройствах в качестве действующих параметров. Если пользователь установит на своем устройстве другие значения параметров, которые не были зафиксированы "замком", то при очередной синхронизации устройства с Сервером администрирования новые значения параметров будут переданы на Сервер администрирования и сохранены в локальных параметрах программы вместо значений, которые были установлены ранее администратором.

Чтобы поддерживать корпоративную безопасность мобильных устройств в актуальном состоянии, вы можете контролировать устройства пользователей на соответствие групповой политике управления.

В верхней части окна групповой политики отображается индикатор уровня защиты. Индикатор уровня защиты поможет вам настроить политику таким образом, чтобы обеспечить высокий уровень защиты устройств. Индикатор уровня защиты меняет состояние в зависимости от настройки политики:

- **Высокий уровень защиты** – защита устройств обеспечена на должном уровне. Все компоненты защиты работают в соответствии с параметрами, рекомендуемыми специалистами "Лаборатории Касперского".
- **Средний уровень защиты** – уровень защиты снижен. Некоторые важные компоненты защиты выключены (например, Веб-Фильтр). Важные проблемы отмечены знаком .
- **Низкий уровень защиты** – существуют проблемы, которые могут привести к заражению устройства и потере данных. Некоторые критические компоненты защиты выключены (например, выключена постоянная защита устройств). Критические проблемы отмечены знаком .

Подробная информация о работе с политиками и группами администрирования в Консоли администрирования Kaspersky Security Center приведена в *справке Kaspersky Security Center*.

Создание групповой политики

В этом разделе описано создание групповых политик для устройств, на которых установлено мобильное приложение Kaspersky Endpoint Security для Android, а также политики для EAS-устройств и iOS MDM-устройств.

Политики, сформированные для группы администрирования, отображаются в рабочей области группы в Консоли администрирования Kaspersky Security Center на закладке **Политики**. Перед именем каждой политики отображается значок, характеризующий ее статус (активна / неактивна). В одной группе можно создать несколько политик для разных приложений. Активной может быть только одна политика для каждого приложения. При создании новой активной политики предыдущая активная политика становится неактивной.

Вы можете изменять политику после ее создания.

Чтобы создать политику для управления мобильными устройствами, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для которой нужно создать политику.
2. В рабочей области группы выберите закладку **Политики**.
3. По ссылке **Создать политику** запустите мастер создания политики.

В результате запустится мастер создания политики.

Шаг 1. Выбор программы для создания групповой политики

На этом шаге в списке программ выберите программу для создания групповой политики:

- **Kaspersky Endpoint Security для Android** – для устройств, использующих мобильное приложение Kaspersky Endpoint Security для Android.

Рекомендуется создать отдельную политику для устройств Huawei и Honor, не имеющих сервисов Google play. Таким образом вы сможете отправлять ссылки на Huawei AppGallery пользователям этих устройств.

- **Kaspersky Device Management для iOS** – для EAS-устройств и iOS MDM-устройств.

Создание политики для мобильных устройств возможно, если на рабочем месте администратора установлены плагин управления Kaspersky Endpoint Security для Android и плагин управления Kaspersky Device Management для iOS. Если плагины не установлены, название соответствующей программы будет отсутствовать в списке программ.

Перейдите к следующему шагу мастера создания политики.

Шаг 2. Ввод названия групповой политики

На этом шаге в поле **Имя** укажите имя новой политики. Если вы укажете имя уже существующей политики, к нему автоматически будет добавлено окончание (1).

Перейдите к следующему шагу мастера создания политики.

Шаг 3. Создание групповой политики для программы

На этом шаге мастер предлагает выбрать состояние политики:

- **Активная политика**. Мастер сохраняет созданную политику на Сервере администрирования. При следующей синхронизации мобильного устройства с Сервером администрирования политика будет использоваться на устройстве в качестве действующей.
- **Неактивная политика.** Мастер сохраняет созданную политику на Сервере администрирования как резервную. В дальнейшем политика может быть активирована по событию. При необходимости неактивную политику можно сделать активной.

  Для одной программы в группе можно создать несколько политик, но активной может быть только одна из них. При создании новой активной политики предыдущая активная политика автоматически становится неактивной.

Завершите работу мастера.

Настройка параметров синхронизации

Для управления мобильными устройствами и получения отчетов или статистик от мобильных устройств пользователей требуется настроить параметры синхронизации. Синхронизация мобильного устройства с Kaspersky Security Center может быть выполнена следующими способами:

- **По расписанию**. Синхронизация по расписанию выполняется с помощью протокола HTTP. Вы можете настроить расписание синхронизации в параметрах групповой политики. Изменения параметров групповой политики, команды и задачи будут выполнены во время синхронизации устройства с Kaspersky Security Center по расписанию, т. е. с задержкой. По умолчанию мобильные устройства автоматически синхронизируются с Kaspersky Security Center каждые шесть часов.
- **Принудительно**. Принудительная синхронизация выполняется с помощью push-уведомлений сервиса FCM (Firebase Cloud Messaging). Принудительная синхронизация, в первую очередь, предназначена для своевременной доставки команд на мобильное устройство. Если вы хотите использовать принудительную синхронизацию, убедитесь что в Kaspersky Security Center настроены параметры GSM. Дополнительная информация приведена в справке Kaspersky Security Center.

Чтобы настроить параметры синхронизации мобильных устройств с Kaspersky Security Center, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Синхронизация**.

5. Выберите периодичность запуска синхронизации в раскрывающемся списке **Запускать синхронизацию**.

6. Чтобы запретить синхронизацию устройства с Kaspersky Security Center в роуминге, установите флажок **Выключить синхронизацию в роуминге**.

   Пользователь устройства может выполнять синхронизацию вручную в настройках приложения (→ **Настройки** → **Синхронизация** → **Синхронизировать**).

7. Чтобы скрыть от пользователя параметры синхронизации (адрес сервера, порт и группа администрирования) в настройках приложения, снимите флажок **Показывать параметры синхронизации на устройстве**. Изменить скрытые параметры невозможно.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Вы можете принудительно синхронизировать мобильное устройство с помощью специальной команды. Подробная информация о работе с командами для мобильных устройств приведена в справке *Kaspersky Security Center*.

Работа с ревизиями групповых политик

Kaspersky Security Center позволяет отслеживать изменения групповых политик. Каждый раз, когда вы сохраняете изменения групповой политики, создается *ревизия*. Каждая ревизия имеет номер.

Работа с ревизиями доступна только для политик Kaspersky Endpoint Security для Android. Для политики Kaspersky Device Management для iOS ревизии недоступны.

Вы можете выполнять с ревизиями групповых политик следующие действия:

- сравнивать выбранную ревизию с текущей ревизией;
- сравнивать выбранные ревизии;
- сравнивать политику с выбранной ревизией другой политики;
- просматривать выбранную ревизию;
- откатывать изменения политики к выбранной ревизии;
- сохранять ревизии в файле формата TXT.

Подробная информация о работе с ревизиями групповых политик и других объектов (например, учетных записей пользователей) приведена в *справке Kaspersky Security Center*.

Чтобы просмотреть историю ревизий групповой политики, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **История ревизий**.

Отобразится список ревизий политики со следующей информацией:

- номер ревизии политики;
- дата и время изменения политики;
- имя пользователя, изменившего политику;
- выполненное действие с политикой;
- описание ревизии изменения параметров политики.

Удаление групповой политики

Чтобы удалить групповую политику, выполните следующие действия:

1. В дереве консоли выберите группу администрирования, для которой нужно удалить политику.
2. В рабочей области группы администрирования на закладке **Политики** выберите политику, которую вы хотите удалить.
3. В контекстном меню политики выберите пункт **Удалить**.

В результате групповая политика будет удалена. До применения новой групповой политики мобильные устройства, входящие в группу администрирования, продолжат работу с параметрами, заданными в удаленной политике.

Ограничение прав на настройку групповых политик

Администраторы Kaspersky Security Center могут настраивать права доступа пользователей Консоли администрирования к различным функциям комплексного решения Kaspersky Security для мобильных устройств в зависимости от служебных обязанностей пользователей.

В интерфейсе Консоли администрирования настройка прав доступа выполняется в окне свойств Сервера администрирования на закладках **Безопасность** и **Роли пользователей**. На закладке **Роли пользователей** можно добавлять типовые роли пользователей с настроенным набором прав. В разделе **Безопасность** можно настраивать права для одного пользователя или для группы пользователей, а также назначать роли одному пользователю или группе пользователей. Права пользователей для каждой программы настраиваются по *функциональным областям*.

Вы также можете настраивать права пользователей по функциональным областям. Информация о соответствии функциональных областей закладкам политик приведена в Приложении.

Для каждой функциональной области администратор может назначать следующие права доступа:

- **Разрешить изменение**. Пользователю Консоли администрирования разрешено изменять параметры политики в окне ее свойств.
- **Запретить изменение**. Пользователю Консоли администрирования запрещено изменять параметры политики в окне ее свойств. Закладки политики, входящие в функциональную область, для которой назначено это право, не отображаются в интерфейсе.

Подробные сведения о работе с правами и ролями пользователей в Консоли администрирования Kaspersky Security Center приведены в *справке Kaspersky Security Center*.

Защита

Этот раздел содержит информацию о том, как удаленно управлять защитой мобильных устройств в Консоли администрирования Kaspersky Security Center.

Настройка антивирусной защиты Android-устройств

Для своевременного обнаружения угроз, поиска вирусов, а также других вредоносных приложений следует настроить параметры постоянной защиты и автоматический запуск антивирусной проверки.

Kaspersky Endpoint Security для Android обнаруживает следующие типы объектов:

- вирусы, черви, троянские приложения, вредоносные утилиты;
- рекламные приложения;
- приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя.

Антивирус имеет ряд ограничений:

- При работе Антивируса в рабочем профиле (Приложения с «портфелем», Настройка рабочего профиля Android) невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в рабочем профиле нет доступа к внешней памяти. Информация об обнаруженных объектах отображается в разделе **Статус** приложения. Для устранения обнаруженных во внешней памяти объектов необходимо удалить файл вручную и запустить проверку устройства повторно.
- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

Чтобы настроить параметры постоянной защиты мобильного устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В окне **Свойства: <Название политики>** выберите раздел **Защита**.
5. В блоке **Защита** настройте параметры защиты файловой системы мобильного устройства:
   - Чтобы включить постоянную защиту мобильного устройства пользователя от угроз, установите флажок **Включить защиту**.

     Kaspersky Endpoint Security для Android будет проверять только новые приложения и файлы из папки Загрузки.

- Чтобы включить расширенный режим защиты мобильного устройства пользователя от угроз, установите флажок **Расширенный режим защиты**.

  Kaspersky Endpoint Security для Android будет проверять все файлы, которые пользователь открывает, изменяет, перемещает, копирует, устанавливает и сохраняет на устройстве, а также мобильные приложения сразу после их установки.

  На устройствах под управлением операционной системы Android 8.0 и выше Kaspersky Endpoint Security для Android проверяет файлы, которые пользователь изменяет, перемещает, устанавливает, сохраняет, а также копии файлов. Kaspersky Endpoint Security для Android не проверяет файлы при их открытии, а также исходные файлы при копировании.

- Чтобы включить дополнительную проверку новых приложений до их первого запуска на устройстве пользователя при помощи облачной службы Kaspersky Security Network, установите флажок **Облачная защита (KSN)**.

- Чтобы блокировать рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламные приложения, приложения автодозвона и другие**.

6. В списке **Действие при обнаружении угрозы** выберите один из следующих вариантов:

   - **Удалить**

     Обнаруженные объекты будут удалены автоматически. От пользователя не требуется никаких дополнительных действий. Перед удалением Kaspersky Endpoint Security для Android отобразит временное уведомление об обнаружении объекта.

   - **Пропустить**

     Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. Информация о пропущенных объектах отображается в разделе **Статус** приложения. Для каждой пропущенной угрозы приведены действия, которые может выполнить пользователь для ее устранения. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

   - **Карантин**

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Чтобы настроить автоматический запуск антивирусной проверки мобильного устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В окне **Свойства: <Название политики>** выберите раздел **Проверка**.

5. Чтобы блокировать рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламные приложения, приложения автодозвона и другие**.

6. В списке **Действие при обнаружении угрозы** выберите один из следующих вариантов:

   - **Удалить**

     Обнаруженные объекты будут удалены автоматически. От пользователя не требуется никаких дополнительных действий. Перед удалением Kaspersky Endpoint Security для Android отобразит временное уведомление об обнаружении объекта.

   - **Пропустить**

     Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. Информация о пропущенных объектах отображается в разделе **Статус** приложения. Для каждой пропущенной угрозы приведены действия, которые может выполнить пользователь для ее устранения. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

   - **Карантин**

   - **Запросить действие**

     Приложение Kaspersky Endpoint Security для Android выводит уведомление, в котором пользователю предлагается выбрать действие над обнаруженным объектом: **Пропустить** или **Удалить**.

     Вариант **Запросить действие** позволяет пользователю устройства при обнаружении нескольких объектов применить выбранное действие к каждому файлу с помощью флажка **Применить ко всем угрозам**.

     Для отображения уведомления на мобильных устройствах под управлением операционной системы Android версии 10.0 и выше Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Kaspersky Endpoint Security для Android предлагает пользователю установить приложение в качестве службы Специальных возможностей во время работы мастера первоначальной настройки. Пользователь может пропустить этот шаг или выключить службу в параметрах устройства позднее. В этом случае Kaspersky Endpoint Security для Android выводит системное окно Android, в котором пользователю предлагается выбрать действие над обнаруженным объектом: Пропустить или Удалить. Чтобы применить действие к нескольким объектам нужно откройте Kaspersky Endpoint Security.

7. В блоке **Проверка по расписанию** настройте параметры автоматического запуска полной проверки файловой системы устройства. Для этого нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** задайте периодичность и время запуска полной проверки.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Kaspersky Endpoint Security для Android проверяет все файлы, в том числе содержимое архивов.

Для поддержания защиты мобильного устройства в актуальном состоянии следует настроить параметры обновления антивирусных баз.

По умолчанию обновление антивирусных баз приложения в зоне роуминга выключено. Обновление антивирусных баз приложения по расписанию не выполняется.

Чтобы настроить параметры обновления антивирусных баз приложения, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В окне **Свойства: <Название политики>** выберите раздел **Обновление баз**.

5. Чтобы Kaspersky Endpoint Security для Android загружал обновления баз по сформированному расписанию, когда устройство находится в зоне роуминга, в блоке **Обновление баз в роуминге** установите флажок **Разрешать обновление баз в роуминге**.

   Даже если флажок снят, пользователь может запустить обновление антивирусных баз в роуминге вручную.

6. В блоке **Источник обновлений баз** укажите источник обновлений, из которого Kaspersky Endpoint Security для Android будет получать и устанавливать обновления антивирусных баз приложения:

   - **Серверы «Лаборатории Касперского»**

     Использование сервера обновлений «Лаборатории Касперского» в качестве источника обновлений для загрузки баз Kaspersky Endpoint Security для Android на мобильные устройства пользователей. Для обновления баз с серверов «Лаборатории Касперского» Kaspersky Endpoint Security для Android передает в «Лабораторию Касперского» данные (например, идентификатор запуска задачи обновления). Список передаваемых данных при обновлении баз вы можете просмотреть в Лицензионном соглашении.

   - **Сервер администрирования**

     Использование хранилища Сервера администрирования Kaspersky Security Center в качестве источника обновлений для загрузки баз приложения Kaspersky Endpoint Security для Android на мобильные устройства пользователей.

   - **Другой источник**

     Использование стороннего сервера в качестве источника обновлений для загрузки баз приложения Kaspersky Endpoint Security для Android на мобильные устройства пользователей. Для обновления требуется задать адрес HTTP-сервера в поле ниже (например, http://domain.com/).

7. В блоке **Обновление баз по расписанию** настройте параметры автоматического запуска обновлений антивирусных баз на устройстве пользователя. Для этого нажмите на кнопку **Расписание** и в открывшемся окне **Расписание** задайте периодичность и время запуска обновления.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Защита Android-устройств в интернете

Для защиты персональных данных пользователя мобильного устройства в интернете включите Веб-Фильтр. Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также фишинговые веб-сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам. Веб-Фильтр проверяет веб-сайты до открытия, используя облачную службу Kaspersky Security Network. Веб-Фильтр также позволяет настроить доступ пользователя к веб-сайтам на основе сформированных списков разрешенных и запрещенных веб-сайтов.

Приложение Kaspersky Endpoint Security для Android должно быть установлено в качестве службы Специальных возможностей. Kaspersky Endpoint Security для Android предлагает пользователю установить приложение в качестве службы Специальных возможностей во время работы мастера первоначальной настройки. Пользователь может пропустить этот шаг или выключить службу в параметрах устройства позднее.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome, Huawei Browser и Samsung Internet Browser. В браузере Samsung Internet Browser Веб-Фильтр не блокирует сайты на мобильных устройствах, если используется рабочий профиль и Веб-Фильтр включен только для рабочего профиля.

Чтобы включить Веб-Фильтр в Google Chrome, Huawei Browser и Samsung Internet Browser, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Веб-Фильтр**.
5. Для использования Веб-Фильтра вам или пользователю устройства необходимо прочитать и принять Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре).
   a. Перейдите по ссылке **Положение о Веб-Фильтре**.

      Откроется окно **Положение об обработке данных в целях использования Веб-Фильтра**. Чтобы принять Положение о Веб-Фильтре, необходимо прочитать и принять Политику конфиденциальности.

   b. Перейдите по ссылке Политика конфиденциальности. Прочитайте и примите Политику конфиденциальности.

      Если вы не принимаете Политику конфиденциальности, пользователь мобильного устройства может принять Политику конфиденциальности в мастере первоначальной настройки или в приложении (→ **О приложении** → **Правовая информация** → **Политика конфиденциальности**).

   c. Укажите, принимаете ли вы Положение о Веб-Фильтре:

      - **Я прочитал и принимаю Положение о Веб-Фильтре**
      - **Запросить принятие Положения о Веб-Фильтре у пользователя устройства**
      - **Я не принимаю Положение о Веб-Фильтре**
6. Если вы выбрали вариант **Я не принимаю Положение о Веб-Фильтре**, Веб-Фильтр не будет блокировать сайты на мобильном устройстве. Пользователь мобильного устройства не сможет включить Веб-Фильтр

в Kaspersky Endpoint Security.

7. Установите флажок **Включить Веб-Фильтр**.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Защита данных при потере или краже устройств

Этот раздел содержит информацию о настройке параметров защиты мобильного устройства от несанкционированного доступа в случае потери или кражи.

Отправка команд на мобильное устройство

Для защиты данных на мобильном устройстве в случае его потери или кражи вы можете отправить специальные команды (см. таблицу ниже).

Команды для защиты данных при потере или краже устройства

Способ подключения к Kaspersky Security Center	Команда	Результат выполнения команды
Kaspersky Endpoint Security для Android	Замок	Мобильное устройство заблокировано.
	Разблокировать	На устройствах под управлением операционной системы Android версии 4.1 – 6.X после разблокировки мобильного устройства пароль разблокировки экрана (PIN-код) будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.
	Определить местоположение устройства	Местоположение устройства определено и показано на Google Картах. Оператор мобильной связи взимает оплату за передачу SMS и доступ в интернет.
	Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства при попытке разблокировать устройство. Оператор мобильной связи взимает оплату за передачу SMS и доступ в интернет. При попытке разблокировки устройства пользователь автоматически соглашается на фотографирование.
	Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал. Звуковой сигнал воспроизводится 5 мин (при низком уровне заряда батареи – 1 мин).
	Удалить корпоративные	Удалены данные в контейнерах, учетная запись корпоративной электронной почты, параметры подключения к корпоративной

	данные	сети Wi-Fi, VPN-сети, точке доступа (APN), рабочий профиль Android, KNOX-контейнер, а также ключ KNOX License Manager.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских. После выполнения этой команды устройство не сможет получать и выполнять последующие команды.
iOS MDM-профиль	Замок	Мобильное устройство заблокировано.
	Разблокировать	Выключена блокировка мобильного устройства PIN-кодом. Установленный ранее PIN-код сброшен.
	Удалить корпоративные данные	Удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских. После выполнения этой команды устройство не сможет получать и выполнять последующие команды.
Почтовый ящик Exchange	Сбросить настройки до заводских	Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских. После выполнения этой команды устройство не сможет получать и выполнять последующие команды.

Для выполнения команд Kaspersky Endpoint Security для Android требуются специальные права и разрешения. Во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android предлагает пользователю предоставить приложению необходимые права и разрешения. Пользователь может пропустить эти шаги или выключить права в параметрах устройства позднее. В этом случае выполнение команд невозможно.

На устройствах с операционной системой Android 10.0 и выше необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства. На устройствах с операционной системой Android 11.0 и выше необходимо также предоставить разрешение "При использовании приложения" для доступа к камере. В противном случае команды Антивора работать не будут. Пользователю будет выведено уведомление об этом ограничении и будет предложено повторно предоставить требуемые разрешения. Если пользователь выбрал вариант "Только сейчас" для разрешения камеры, считается, что доступ предоставлен приложением. Рекомендуется связаться с пользователем напрямую при повторном запросе разрешения для камеры.

Подробная информация об отправке команд из списка мобильных устройств в Консоли администрирования приведена в *справке Kaspersky Security Center*.

Разблокировка мобильного устройства

Вы можете разблокировать мобильное устройство следующими способами:

- отправить команду разблокировки мобильного устройства;
- ввести на мобильном устройстве одноразовый код разблокировки (только для Android-устройств).

На некоторых устройствах (например, Huawei, Meizu, Xiaomi) требуется вручную добавить Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы. Если приложение не добавлено в список, вы можете разблокировать устройство только с помощью одноразового кода разблокировки. Разблокировать устройство с помощью команд невозможно.

Подробная информация об отправке команд из списка мобильных устройств в Консоли администрирования приведена в *справке Kaspersky Security Center*.

Одноразовый код разблокировки – секретный код программы для разблокировки мобильного устройства. Одноразовый код создается программой и является уникальным для каждого мобильного устройства. Вы можете изменить длину одноразового кода (4, 8 или 16 цифр) в параметрах групповой политики в разделе **Анти-Вор**.

Чтобы разблокировать мобильное устройство с помощью одноразового кода, выполните следующие действия:

1. В дереве консоли выберите **Управление мобильными устройствами → Мобильные устройства**.
2. Выберите мобильное устройство, для которого вы хотите получить одноразовый код для разблокировки.
3. Откройте окно свойств мобильного устройства двойным щелчком мыши.
4. Выберите раздел **Приложения → Kaspersky Endpoint Security для Android**.
5. Откройте окно свойств приложения Kaspersky Endpoint Security двойным щелчком мыши.
6. Выберите раздел **Анти-Вор**.
7. В блоке **Одноразовый код разблокировки устройства** в поле **Одноразовый код** будет указан уникальный для выбранного устройства код.
8. Сообщите пользователю заблокированного мобильного устройства одноразовый код любым доступным способом (например, в сообщении электронной почты).
9. Пользователь вводит одноразовый код на экране устройства, заблокированном Kaspersky Endpoint Security для Android.

Мобильное устройство будет разблокировано. На устройствах под управлением операционной системы Android версии 4.1 – 6.X после разблокировки мобильного устройства пароль разблокировки экрана (PIN-код) будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.

Шифрование данных

Для защиты данных от несанкционированного доступа требуется включить шифрование всех данных на устройстве (например, учетных данных, внешних устройств и приложений, а также сообщений электронной почты, SMS-сообщений, контактов, фотографий и других файлов). Для доступа к зашифрованным данным требуется задать специальный ключ – пароль для разблокировки устройства. Таким образом, если данные зашифрованы, доступ к ним можно получить, только когда устройство разблокировано.

На iOS-устройствах шифрование данных включено по умолчанию, если установлен пароль для разблокировки устройства (**Настройки → Touch ID и пароль / Face ID и пароль → Включить пароль)**.

Чтобы зашифровать все данные на Android-устройстве, выполните следующие действия:

1. Включите блокирование экрана на Android-устройстве (**Настройки** → **Безопасность** → **Блокирование экрана**).

2. Установите пароль разблокировки устройства, соответствующий требованиям корпоративной безопасности.

   Не рекомендуется использовать графический пароль для разблокировки устройства. На некоторых Android-устройствах под управлением Android 6.0 и выше после шифрования данных и перезагрузки устройства Android требует ввести цифровой пароль для разблокировки устройства вместо графического. Проблема связана с особенностями работы службы Специальных возможностей. Для разблокировки экрана устройства в этом случае переведите графический пароль в цифровой. Подробнее о переводе графического пароля в цифровой см. на сайте Службы технической поддержки компании-производителя мобильного устройства.

3. Включите шифрование всех данных устройства (**Настройки** → **Безопасность** → **Зашифровать данные**).

Настройка надежности пароля разблокировки устройства

Для защиты доступа к мобильному устройству пользователя следует настроить пароль разблокировки устройства.

Этот раздел содержит информацию о настройке защиты паролем Android-устройств и iOS-устройств.

Настройка надежности пароля разблокировки Android-устройства

Для обеспечения безопасности Android-устройства нужно настроить использование пароля, который запрашивается при выходе устройства из спящего режима.

Вы можете установить ограничения при работе пользователя с устройством, если пароль разблокировки недостаточно сложный (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого в параметрах правила проверки требуется выбрать критерий **Пароль разблокировки не соответствует требованиям безопасности**.

На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия: включена защита Kaspersky Endpoint Security для Android от удаления и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

Чтобы настроить использование пароля разблокировки, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В окне **Свойства: <Название политики>** выберите раздел **Управление устройством**.

5. Если вы хотите, чтобы приложение проверяло наличие пароля разблокировки, в блоке **Блокирование экрана** установите флажок **Требовать установить пароль для разблокировки экрана**.

   Если приложение обнаружит, что пароль на устройстве не задан, пользователю потребуется указать его. Пароль указывается с учетом параметров, заданных администратором.

6. Укажите минимальное количество символов в пароле.

   Минимальное количество символов в пароле пользователя. Возможные значения: от 4 до 16 символов.

   По умолчанию пароль пользователя содержит 4 символа.

   На устройствах под управлением Android 10.0 и выше Kaspersky Endpoint Security приводит требования надежности пароля к одному из системных значений: средний или высокий.

   Значения для устройств под управлением Android 10.0 и выше определяются по следующим правилам:

   - Если требуемая длина пароля составляет от 1 до 4 символов, приложение предлагает пользователю установить пароль средней надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей (например, 1234), либо буквенным / буквенно-цифровым. PIN-код или пароль должны состоять не менее чем из 4 символов.

   - Если требуемая длина пароля составляет не менее 5 символов, приложение предлагает пользователю установить пароль высокой надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей, либо буквенным / буквенно-цифровым (пароль). PIN-код должен состоять не менее чем из 8 цифр; пароль должен состоять не менее чем из 6 символов.

7. Если вы хотите, чтобы у пользователя была возможность использовать отпечатки пальцев для разблокировки экрана, установите флажок **Разрешить использование отпечатков пальцев**. Если пароль разблокировки не соответствует требованиям корпоративной безопасности, использовать сканер отпечатков пальцев для разблокировки экрана невозможно.

   На устройствах под управлением Android 10.0 и выше управлять использованием отпечатка пальца для разблокировки экрана можно только в рабочем профиле.

   Kaspersky Endpoint Security для Android не ограничивает использование сканера отпечатков пальцев для входа в приложения или подтверждения покупок.

   На некоторых Samsung-устройствах невозможно запретить использование отпечатков пальцев для разблокировки экрана. Также на некоторых Samsung-устройствах при несоответствии пароля разблокировки требованиям корпоративной безопасности Kaspersky Endpoint Security для Android не запрещает использование отпечатков пальцев для разблокировки экрана.

   После добавления отпечатка пальца в настройках устройства пользователь может разблокировать экран следующими способами:

   - приложить палец к сканеру отпечатков – основной способ;

   - ввести пароль разблокировки – резервный способ.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка надежности пароля разблокировки iOS MDM-устройств

Для защиты данных iOS MDM-устройства следует настроить требования к надежности пароля разблокировки.

По умолчанию пользователь может использовать простой пароль. *Простой пароль* – это пароль, который может содержать последовательность символов или повторяющиеся символы, например, "abcd" или "2222". Вводить алфавитно-цифровой пароль с использованием специальных символов не обязательно. Срок действия пароля и количество попыток ввода пароля по умолчанию не ограничены.

Чтобы настроить параметры надежности пароля разблокировки iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Пароль**.

5. В блоке **Параметры пароля** установите флажок **Применить параметры на устройстве**.

6. Настройте параметры надежности пароля разблокировки:

   - Чтобы разрешить пользователю использовать простой пароль, установите флажок **Разрешить простой пароль**.

   - Чтобы требовать использование алфавитно-цифрового пароля, установите флажок **Требовать ввод алфавитно-цифрового значения**.

   - В списке **Минимальное количество символов** выберите минимальную длину пароля в символах.

   - В списке **Минимальное количество специальных символов** выберите минимальное количество специальных символов в пароле (например, "$", "&", "!").

   - В поле **Максимальный срок использования** укажите период времени в днях, в течение которого будет действовать пароль. По истечении установленного срока Kaspersky Device Management для iOS запрашивает у пользователя смену пароля.

   - В списке **Включать автоблокировку через** выберите время включения автоблокировки iOS MDM-устройства.

   - В поле **История паролей** укажите количество использованных паролей (включая текущий), которые Kaspersky Device Management для iOS при смене пароля сравнивает с новым паролем. Если пароли совпадут, новый пароль не будет принят.

   - В списке **Максимальное время для разблокировки без пароля** выберите время, в течение которого пользователь может разблокировать iOS MDM-устройство без ввода пароля.

- В списке **Максимальное количество попыток ввода** выберите число доступных пользователю попыток ввести пароль для разблокировки iOS MDM-устройства.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики Kaspersky Device Management для iOS проверит надежность пароля. Если надежность пароля разблокировки на устройстве не соответствует политике, пользователю будет предложено его изменить.

Настройка надежности пароля разблокировки EAS-устройств

Для защиты данных EAS-устройства следует установить надежный пароль разблокировки.

По умолчанию при включении мобильного устройства Kaspersky Device Management для iOS не требует ввести или задать пароль разблокировки.

Чтобы настроить параметры надежности пароля разблокировки EAS-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят EAS-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне Свойства выберите раздел **Пароль**.

5. В блоке **Параметры пароля** установите флажок **Требовать пароль**.

6. Настройте параметры надежности пароля разблокировки:

   - Чтобы обязательно использовать в пароле буквенные и цифровые символы, установите флажок **Требовать ввод алфавитно-цифрового значения**. В поле **Минимальное число наборов символов** задайте уровень сложности алфавитно-цифрового пароля. Возможные значения: от 1 до 4. Значение 1 соответствует минимальному уровню сложности.

   - Чтобы разрешить пользователю использовать функцию восстановления пароля, установите флажок **Включить восстановление пароля**.

   - Чтобы выполнять шифрование файлов в памяти устройства, установите флажок **Требовать шифрования на устройстве**.

   - Чтобы выполнять шифрование файлов на карте памяти, установите флажок **Требовать шифрования на карте памяти**.

   - Чтобы разрешить пользователю использовать простой пароль, состоящий только из цифр, установите флажок **Разрешить простой пароль**.

   - Чтобы ограничить число попыток ввода пароля для доступа к устройству, установите флажок **Максимальное количество попыток ввода**. В поле справа от флажка укажите число доступных пользователю попыток ввести пароль для разблокировки устройства. Если пользователь не смог правильно ввести пароль указанное количество раз подряд, Kaspersky Device Management для iOS удаляет с устройства все данные.

- Чтобы настроить минимальное количество символов в пароле пользователя, установите флажок **Минимальное количество символов**. В поле справа от флажка укажите минимальное количество символов в пароле. Возможные значения: от 4 до 16 символов.

- Чтобы требовать ввод пароля после периода бездействия пользователя (пользователь не выполнял действия с устройством), установите флажок **Время бездействия до повторного ввода пароля (мин)**. В поле справа от флажка укажите время бездействия пользователя в минутах. По истечении этого времени программа предлагает пользователю ввести пароль.

- Чтобы ограничить срок действия пароля, установите флажок **Срок действия пароля (дни)**. В поле справа от флажка укажите срок действия пароля. По истечении этого срока программа предлагает пользователю сменить пароль.

- В поле **История паролей** укажите количество предыдущих паролей, запрещенных к использованию.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. После применения политики Kaspersky Device Management для iOS проверит наличие пароля на мобильном устройстве пользователя. Если пароль разблокировки на устройстве не задан, пользователю будет предложено его указать. Пароль указывается с учетом параметров, заданных в политике. Если пароль разблокировки на устройстве задан, но не соответствует требованиям политики, пользователю будет предложено его изменить.

Настройка виртуальной частной сети (VPN)

Этот раздел содержит информацию о настройке параметров виртуальной частной сети (VPN) для безопасного подключения к сетям Wi-Fi.

Настройка VPN на Android-устройствах (только Samsung)

Для безопасного подключения Android-устройства к сетям Wi-Fi и защиты передачи данных следует настроить параметры VPN (Virtual Private Network).

Настройка VPN возможна только для Samsung-устройств под управлением операционной системы Android версии 5.0 и выше.

При использовании виртуальной частной сети следует учитывать следующие требования:

- Приложение, использующее VPN-соединение, должно быть разрешено в параметрах Сетевого экрана.

- Параметры виртуальной частной сети, настроенные в политике, не могут быть применены для системных приложений. Для системных приложений VPN-соединение нужно настраивать вручную.

- Для некоторых приложений, использующих VPN-соединение, при первом запуске требуется дополнительная настройка. Чтобы выполнить настройку, нужно разрешить VPN-соединение в параметрах приложения.

Чтобы настроить VPN на мобильном устройстве пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → Управление Samsung-устройствами**.
5. В блоке **VPN** нажмите на кнопку **Настроить**.

   Откроется окно **Сеть VPN**.
6. В раскрывающемся списке **Тип соединения** выберите тип VPN-соединения.
7. В поле **Имя сети** введите название VPN-туннеля.
8. В поле **Адрес сервера** введите сетевое имя или IP-адрес VPN-сервера.
9. В поле **Домен(ы) поиска DNS** введите домен поиска DNS, который автоматически добавляется к имени DNS-сервера.

   Вы можете ввести несколько доменов поиска DNS через пробел.
10. В поле **DNS-сервер(ы)** введите полное доменное имя или IP-адрес DNS-сервера.

    Вы можете ввести несколько DNS-серверов через пробел.
11. В поле **Перенаправление маршрутов** введите диапазон IP-адресов сети, обмен данными с которыми осуществляется через VPN-соединение.

    > Если в поле **Перенаправление маршрутов** не указан диапазон IP-адресов, весь интернет-трафик будет проходить через VPN-соединение.
12. Для типов сети **IPSec Xauth PSK** и **L2TP IPSec PSK** дополнительно настройте следующие параметры:
    a. В поле **Общий ключ IPSec** введите пароль от предварительно установленного ключа безопасности IPSec.
    b. В поле **Идентификатор IPSec** введите имя пользователя мобильного устройства.
13. Для типа сети **L2TP IPSec PSK** дополнительно укажите пароль для ключа L2TP в поле **Ключ L2TP**.
14. Для типа сети **PPTP** установите флажок **Использовать SSL-соединение**, чтобы приложение использовало метод шифрования данных MPPE (Microsoft Point-to-Point Encryption) для обеспечения безопасности передачи данных при подключении мобильного устройства к VPN-серверу.
15. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка VPN на iOS MDM-устройствах

Для подключения iOS MDM-устройства к виртуальной частной сети (VPN) и обеспечения безопасности данных при подключении к сети VPN следует настроить параметры подключения к сети VPN.

Чтобы настроить VPN-соединение на iOS MDM-устройстве пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **VPN**.

5. В блоке **Сети VPN** нажмите на кнопку **Добавить**.

   Откроется окно **Сеть VPN**.

6. В поле **Имя сети** введите название VPN-туннеля.

7. В раскрывающемся списке **Тип соединения** выберите тип VPN-соединения:

   - **L2TP** (Layer 2 Tunneling Protocol). Соединение поддерживает аутентификацию пользователя мобильного устройства iOS MDM с помощью паролей MS-CHAP v2, двухфакторную аутентификацию и автоматическую аутентификацию с помощью общего ключа.

   - **PPTP** (Point-to-Point Tunneling Protocol). Соединение поддерживает аутентификацию пользователя мобильного устройства iOS MDM с помощью паролей MS-CHAP v2 и двухфакторную аутентификацию.

   - **IPSec (Cisco)**. Соединение поддерживает аутентификацию пользователей с помощью паролей, двухфакторную аутентификацию и автоматическую аутентификацию с помощью общего ключа и сертификатов.

   - **Cisco AnyConnect**. Соединение поддерживает межсетевой экран Cisco Adaptive Security Appliance (ASA) версии 8.0(3).1 и выше. Для настройки VPN-соединения требуется установить на мобильное устройство iOS MDM приложение Cisco AnyConnect из App Store.

   - **Juniper SSL**. Соединение поддерживает шлюз Juniper Networks SSL VPN серии SA версии 6.4 и выше с пакетом Juniper Networks IVE версии 7.0 и выше. Для настройки VPN-соединения требуется установить на мобильное приложение iOS MDM приложение JUNOS из App Store.

   - **F5 SSL**. Соединение поддерживает решения F5 BIG-IP Edge Gateway, Access Policy Manager и Fire SSL VPN. Для настройки VPN-соединения требуется установить на мобильное устройство iOS MDM приложение F5 BIG-IP Edge Client из App Store.

   - **SonicWALL Mobile Connect**. Соединение поддерживает устройства SonicWALL Aventail E-Class Secure Remote Access версии 10.5.4 и выше, устройства SonicWALL SRA версии 5.5 и выше, а также устройства SonicWALL Next-Generation Firewall, включая TZ, NSA, E-Class NSA с SonicOS версии 5.8.1.0 и выше. Для настройки VPN-соединения требуется установить на мобильное устройство iOS MDM приложение SonicWALL Mobile Connect из App Store.

   - **Aruba VIA**. Соединение поддерживает контроллеры мобильного доступа Aruba Networks. Для их настройки требуется установить на мобильное устройство iOS MDM приложение Aruba Networks VIA из App Store.

   - **Custom SSL**. Соединение поддерживает аутентификацию пользователя мобильного устройства iOS MDM с помощью паролей и сертификатов, а также двухфакторную аутентификацию.

8. В поле **Адрес сервера** введите сетевое имя или IP-адрес VPN-сервера.

9. В поле **Имя учетной записи** введите имя учетной записи пользователя для авторизации на сервере VPN. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

10. Настройте параметры безопасности для VPN-соединения в соответствии с выбранным типом виртуальной частной сети.

11. Настройте (если требуется) параметры подключения к сети VPN через прокси-сервер:

    a. Выберите закладку **Параметры прокси-сервера**.

    b. Выберите режим настройки прокси-сервера и укажите параметры подключения.

    c. Нажмите кнопку **ОК**.

    В результате на iOS MDM-устройстве будут настроены параметры подключения устройства к VPN-сети через прокси-сервер

12. Нажмите кнопку **ОК**.

    Новая сеть VPN отобразится в списке.

13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на iOS MDM-устройстве пользователя после применения политики будет настроено подключение к VPN-сети.

Настройка Сетевого экрана на Android-устройствах (только Samsung)

Для контроля сетевых соединений на мобильном устройстве пользователя следует настроить параметры Сетевого экрана.

Чтобы настроить Сетевой экран на мобильном устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX** → **Управление Samsung-устройствами**.

5. В блоке **Сетевой экран** нажмите на кнопку **Настроить**.

   Откроется окно **Сетевой экран**.

6. Выберите режим работы Сетевого экрана:

   - Чтобы разрешить все входящие и исходящие соединения, переместите ползунок в положение **Разрешать все**.

   - Чтобы блокировать любую сетевую активность, кроме приложений из списка исключений, переместите ползунок в положение **Блокировать все, кроме исключений**.

7. Если вы выбрали режим работы Сетевого экрана **Блокировать все, кроме исключений**, сформируйте список исключений:

   a. Нажмите на кнопку **Добавить**.

      Откроется окно **Исключение для Сетевого экрана**.

   b. В поле **Название приложения** введите название мобильного приложения.

   c. В поле **Имя пакета** введите системное имя пакета мобильного приложения (например, `com.mobileapp.example`).

   d. Нажмите кнопку **ОК**.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Защита Kaspersky Endpoint Security для Android от удаления

Для защиты мобильного устройства и выполнения требований корпоративной безопасности вы можете включить защиту Kaspersky Endpoint Security для Android от удаления. В этом случае пользователю недоступно удаление приложения с помощью интерфейса Kaspersky Endpoint Security для Android. При удалении приложения с помощью инструментов операционной системы Android появится запрос на выключение прав администратора для Kaspersky Endpoint Security для Android. После выключения прав мобильное устройство будет заблокировано.

На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия: включена защита Kaspersky Endpoint Security для Android от удаления и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

Чтобы включить защиту Kaspersky Endpoint Security для Android от удаления, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Дополнительно**.

5. В блоке **Удаление приложения Kaspersky Endpoint Security для Android** снимите флажок **Разрешить удаление приложения Kaspersky Endpoint Security для Android**.

На устройствах под управлением операционной системы Android версии 7.0 и выше для защиты приложения от удаления Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android предлагает пользователю предоставить приложению необходимые права. Пользователь может пропустить эти шаги или выключить права в параметрах устройства позднее. В этом случае защита приложения от удаления не работает.

6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. При попытке удаления приложения мобильное устройство будет заблокировано.

Обнаружение взлома устройства (получение root-прав)

Kaspersky Security для мобильных устройств позволяет обнаруживать взлом устройства (получение root-прав). На взломанном устройстве системные файлы не защищены и доступны для изменения. Также на взломанном устройстве доступна установка сторонних приложений из неизвестных источников. После обнаружения взлома рекомендуется восстановить нормальную работу устройства.

Для обнаружения получения root-прав пользователем Kaspersky Endpoint Security для Android использует следующие сервисы:

- *встроенный сервис Kaspersky Endpoint Security для Android* – сервис "Лаборатории Касперского", который проверяет получение root-прав пользователем мобильного устройства (Kaspersky Mobile Security SDK).

- *SafetyNet Attestation* – сервис Google, который проверяет целостность операционной системы, анализирует программно-аппаратное обеспечение устройства, а также определяет другие проблемы безопасности. Подробная информация о работе SafetyNet Attestation приведена на веб-сайте Службы технической поддержки Android.

При взломе устройства вы получите уведомление. Вы можете просмотреть уведомления о взломе в рабочей области Сервера администрирования на закладке **Мониторинг**. Вы также можете выключить уведомление о взломе в параметрах уведомлений о событиях.

На устройствах под управлением операционной системы Android вы можете установить ограничения при работе пользователя с устройством в случае взлома (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия (см. рис. ниже). Для этого в параметрах правила проверки требуется выбрать критерий **На устройстве получены root-права**.

Настройка глобального HTTP-прокси на iOS MDM-устройствах

Для защиты интернет-трафика пользователя нужно настроить подключение iOS MDM-устройства к интернету через прокси-сервер.

Автоматическое подключение к интернету через прокси-сервер доступно только для контролируемых устройств.

Чтобы настроить глобальный HTTP-прокси на iOS MDM-устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Глобальный HTTP-прокси**.

5. В блоке **Параметры глобального HTTP-прокси** установите флажок **Применить параметры на устройстве**.

6. Выберите тип настройки глобального HTTP-прокси.

   По умолчанию выбран ручной тип настройки глобального HTTP-прокси и пользователю запрещено подключаться к подписным сетям без подключения к прокси-серверу. *Подписные сети* – беспроводные сети, требующие предварительной аутентификации на мобильном устройстве без подключения к прокси-серверу.

   - Если вы хотите вручную ввести параметры подключения к прокси-серверу, выполните следующие действия:

     a. В раскрывающемся списке **Тип настройки** выберите **Вручную**.

     b. В поле **Адрес прокси-сервера и порт** введите имя хоста, домена или IP-адрес прокси-сервера и номер порта прокси-сервера.

     c. В поле **Имя пользователя** задайте имя учетной записи пользователя для авторизации на прокси-сервере. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

     d. В поле **Пароль** задайте пароль учетной записи пользователя для авторизации на прокси-сервере.

     e. Чтобы разрешить пользователю доступ к подписным сетям, установите флажок **Разрешить доступ к подписным сетям без подключения к прокси-серверу**.

   - Чтобы настроить параметры подключения к прокси-серверу с помощью подготовленного файла PAC (Proxy Auto Configuration), выполните следующие действия:

     a. В раскрывающемся списке **Тип настройки** выберите **Автоматически**.

     b. В поле **Веб-адрес PAC-файла** введите веб-адрес PAC-файла (например, http://www.example.com/filename.pac).

     c. Чтобы разрешить пользователю подключение мобильного устройства к беспроводной сети без использования прокси-сервера в случае, если PAC-файл недоступен, установите флажок **Разрешить прямое соединение, если PAC-файл недоступен**.

     d. Чтобы разрешить пользователю доступ к подписным сетям, установите флажок **Разрешить доступ к подписным сетям без подключения к прокси-серверу**.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате пользователь мобильного устройства пользователя после применения политики будет подключаться к интернету через прокси-сервер.

Добавление сертификатов безопасности на iOS MDM-устройства

Для упрощения аутентификации пользователя и обеспечения безопасности данных следует добавить на iOS MDM-устройство пользователя сертификаты. Подписание данных с помощью сертификата защищает данные от изменения во время сетевого обмена. Шифрование данных с помощью сертификата обеспечивает дополнительную защиту информации. Сертификат также может использоваться для удостоверения личности пользователя.

Kaspersky Device Management для iOS поддерживает следующие стандарты сертификатов:

- **PKCS#1** – шифрование с открытым ключом на основе алгоритмов RSA.
- **PKCS#12** – хранение и передача сертификата и закрытого ключа.

Чтобы добавить сертификат безопасности на iOS MDM-устройство пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **Сертификаты**.
5. В блоке **Сертификаты** нажмите на кнопку **Добавить**.

   Откроется окно **Сертификат**.
6. В поле **Имя файла** укажите путь к сертификату:

   Файлы сертификатов PKCS#1 имеют расширения cer, crt или der. Файлы сертификатов PKCS#12 имеют расширения p12 или pfx.
7. Нажмите на кнопку **Открыть**.

   Если сертификат защищен паролем, требуется указать пароль. После этого новый сертификат отобразится в списке.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве после применения политики пользователю будет предложено установить сертификаты из сформированного списка.

Добавление профиля SCEP на iOS MDM-устройства

Чтобы пользователь iOS MDM-устройства мог автоматически получать сертификаты из Центра сертификации через интернет, следует добавить профиль SCEP. Профиль SCEP позволяет поддерживать протокол простой регистрации сертификатов.

По умолчанию добавляется профиль SCEP со следующими параметрами:

- Для регистрации сертификатов не используется альтернативное имя субъекта.
- Предпринимаются три попытки опроса SCEP-сервера с интервалом 10 секунд между попытками. Если все попытки подписать сертификат были неудачными, следует сформировать новый запрос на подписание сертификата.
- Полученный сертификат запрещено использовать для подписи или шифрования данных.

Вы можете изменить указанные параметры при добавлении профиля SCEP.

Чтобы добавить профиль SCEP, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **SCEP**.
5. В блоке **Профили SCEP** нажмите на кнопку **Добавить**.

   Откроется окно **Профиль SCEP**.
6. В поле **Веб-адрес сервера** введите веб-адрес SCEP-сервера, на котором развернут Центр сертификации.

   Веб-адрес может содержать IP-адрес или полное доменное имя (FQDN). Например, http://10.10.10.10/certserver/companyscep.
7. В поле **Название** введите название Центра сертификации, развернутого на SCEP-сервере.
8. В поле **Субъект** введите строку с атрибутами пользователя iOS MDM-устройства, которые содержатся в сертификате X.500.

   Атрибуты могут содержать сведения о стране (C), организации (O) и общем имени пользователя (CN). Например, /C=RU/O=MyCompany/CN=User/. Вы можете использовать и другие атрибуты, которые приведены в RFC 5280.
9. В раскрывающемся списке **Тип альтернативного имени субъекта** выберите тип альтернативного имени субъекта SCEP-сервера:

   - **Нет** – идентификация по альтернативному имени не используется.
   - **RFC 822 имя** – идентификация по адресу электронной почты. Адрес электронной почты должен быть представлен в соответствии с RFC 822.
   - **DNS-имя** – идентификация по доменному имени.
   - **URI** – идентификация по IP-адресу или адресу в формате FQDN.

   Вы можете использовать альтернативное имя субъекта для идентификации пользователя мобильного устройства iOS MDM.
10. В поле **Альтернативное имя субъекта** введите альтернативное имя субъекта сертификата X.500. Значение альтернативного имени субъекта зависит от типа субъекта: адрес электронной почты пользователя, домен или веб-адрес.

11. В поле **Имя субъекта NT** введите DNS-имя пользователя мобильного устройства iOS MDM в сети Windows NT.

    Имя субъекта NT содержится в запросе на сертификат в SCEP-сервер.

12. В поле **Количество попыток опроса SCEP-сервера** укажите максимальное количество попыток опроса SCEP-сервера для подписания сертификата.

13. В поле **Интервал между попытками (сек)** укажите период времени в секундах между попытками опроса SCEP-сервера для подписания сертификата.

14. В поле **Запрос регистрации** введите предварительно опубликованный ключ регистрации.

    Перед подписанием сертификата SCEP-сервер запрашивает у пользователя мобильного устройства ключ. Если оставить поле пустым, SCEP-сервер не будет запрашивать ключ.

15. В раскрывающемся списке **Размер ключа** выберите размер ключа регистрации в битах: 1024 или 2048.

16. Если вы хотите разрешить пользователю использовать сертификат, полученный от SCEP-сервера, в качестве сертификата подписи, установите флажок **Использовать для подписи**.

17. Если вы хотите разрешить пользователю использовать сертификат, полученный от SCEP-сервера, для шифрования данных, установите флажок **Использовать для шифрования**.

    Запрещено использовать сертификат SCEP-сервера в качестве сертификата подписи данных и сертификата шифрования данных одновременно.

18. В поле **Отпечаток сертификата** введите уникальный отпечаток сертификата для проверки подлинности ответа от Центра сертификации. Вы можете использовать отпечатки сертификатов с алгоритмом хеширования SHA-1 или MD5. Вы можете скопировать отпечаток сертификата вручную или выбрать сертификат с помощью кнопки **Создать из сертификата**. При создании отпечатка с помощью кнопки **Создать из сертификата** отпечаток будет добавлен в поле автоматически.

    Отпечаток сертификата требуется указать, если обмен данными между мобильным устройством и Центром сертификации осуществляется по протоколу HTTP.

19. Нажмите кнопку **ОК**.

    Новый профиль SCEP отобразится в списке.

20. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будет настроено автоматическое получение сертификата из Центра сертификации через интернет.

Контроль

Этот раздел содержит информацию о том, как удаленно контролировать мобильные устройства в Консоли администрирования Kaspersky Security Center.

Настройка ограничений

В этом разделе содержатся инструкции по настройке доступа пользователей к функциям мобильных устройств.

Особые рекомендации для устройств под управлением Android 10 и выше

В Android 10 реализованы многочисленные изменения и ограничения, ориентированные на API 29 или выше. Некоторые из этих изменений влияют на доступность и работу отдельных функций приложения. Эти рекомендации применимы только для устройств под управлением Android 10 и выше.

Включение, выключение и настройка Wi-Fi

- Сети Wi-Fi можно добавлять, удалять и настраивать в Консоли администрирования Kaspersky Security Center. Когда в политику добавляется сеть Wi-Fi, Kaspersky Endpoint Security получает конфигурацию этой сети при первом подключении к Kaspersky Security Center.

- Когда устройство обнаруживает сеть, настроенную с помощью Kaspersky Security Center, Kaspersky Endpoint Security предлагает пользователю подключиться к этой сети. Если пользователь выбирает подключение к сети, все параметры, настроенные в Kaspersky Security Center, применяются автоматически. Затем устройство автоматически подключается к этой сети, когда находится в пределах досягаемости. Никакие дополнительные уведомления для пользователя не отображаются.

- Если устройство пользователя уже подключено к другой сети Wi-Fi, иногда приложение может не предложить пользователю одобрить добавление сети. В таких случаях пользователю необходимо отключить и снова включить Wi-Fi, чтобы получить предложение.

- Когда Kaspersky Endpoint Security предлагает пользователю подключиться к сети Wi-Fi, а пользователь отказывается это сделать, разрешение приложения на изменение состояния Wi-Fi аннулируется. После этого Kaspersky Endpoint Security не сможет предложить подключиться к сетям Wi-Fi, пока пользователь не предоставит разрешение повторно, перейдя в **Настройки** → **Приложения и уведомления** → **Разрешения приложений** → **Контроль Wi-Fi** → **Kaspersky Endpoint Security**.

- Поддерживаются только открытые сети и сети, зашифрованные с помощью WPA2-PSK. Шифрование WEP и WPA не поддерживается.

- Если пароль для сети, ранее предложенный приложением, был изменен, пользователю необходимо вручную удалить эту сеть из списка известных сетей. После этого устройство сможет получить предложение сети от Kaspersky Endpoint Security и подключиться к этой сети.

- При обновлении операционной системы устройства с Android 9 и ниже до Android 10 и выше, или при обновлении приложения Kaspersky Endpoint Security, установленного на устройстве под управлением Android 10 и выше, нельзя изменить или удалить сети, которые были ранее добавлены в Kaspersky Security Center, с помощью политик Kaspersky Security Center. Однако пользователь может изменить или удалить такие сети вручную в настройках устройства.

- На устройствах под управлением Android 10 у пользователя запрашивается пароль при попытке вручную подключиться к предлагаемой защищенной сети. При автоматическом подключении ввод пароля не требуется. Если устройство пользователя подключено к какой-либо другой сети Wi-Fi, пользователю сначала необходимо отключиться от этой сети, чтобы автоматически подключиться к одной из предложенных сетей.

- На устройствах под управлением Android 11 пользователь может вручную подключиться к защищенной сети, предложенной приложением, без ввода пароля.

- При удалении Kaspersky Endpoint Security с устройства, сети, ранее предлагаемые приложением, игнорируются.
- Не поддерживается запрет на использование сетей Wi-Fi.

Доступ к камере

- На устройствах под управлением Android 10 использование камеры нельзя запретить полностью. Запрет на использование камеры для рабочего профиля по-прежнему доступен.
- Если стороннее приложение пытается получить доступ к камере устройства, это приложение будет заблокировано, а пользователь получит уведомление о проблеме. Однако приложения, использующие камеру во время работы в фоновом режиме, не могут быть заблокированы.
- Когда внешняя камера отключена от устройства, в некоторых случаях может отображаться уведомление о недоступности камеры.

Управление методами разблокировки экрана

- Kaspersky Endpoint Security приводит требования надежности пароля к одному из системных значений: средний или высокий.
  - Если требуемая длина пароля составляет от 1 до 4 символов, приложение предлагает пользователю установить пароль средней надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей (например, 1234), либо буквенно-цифровым. PIN-код или пароль должны состоять не менее чем из 4 символов.
  - Если требуемая длина пароля составляет не менее 5 символов, приложение предлагает пользователю установить пароль высокой надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей, либо буквенно-цифровым (пароль). PIN-код должен состоять не менее чем из 8 цифр; пароль должен состоять не менее чем из 6 символов.
- Управлять использованием отпечатка пальца для разблокировки экрана можно только в рабочем профиле.

Настройка ограничений для Android-устройств

Для обеспечения безопасности Android-устройства нужно настроить параметры использования на устройстве Wi-Fi, камеры и Bluetooth.

По умолчанию пользователь может использовать на устройстве Wi-Fi, камеру, Bluetooth без ограничений.

Чтобы настроить ограничения использования на устройстве Wi-Fi, камеры и Bluetooth, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В окне **Свойства: <Название политики>** выберите раздел **Управление устройством**.

5. В блоке **Ограничения** настройте использование модуля Wi-Fi, камеры, Bluetooth:

   - Чтобы выключить модуль Wi-Fi на мобильном устройстве пользователя, установите флажок **Запретить использование Wi-Fi**.

   - Чтобы выключить камеру на мобильном устройстве пользователя, установите флажок **Запретить использование камеры**. Чтобы выключить Bluetooth на мобильном устройстве пользователя, установите флажок **Запретить использование Bluetooth**.

6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка ограничений для iOS MDM-устройств

Для выполнения требований корпоративной безопасности следует настроить ограничения в работе iOS MDM-устройства.

Чтобы настроить ограничения iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Ограничения функций**.

5. В блоке **Параметры ограничений функций** установите флажок **Применить параметры на устройстве**.

6. Настройте ограничения функций iOS MDM-устройства.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

8. Выберите раздел **Ограничения приложений**.

9. В блоке **Параметры ограничений приложений** установите флажок **Применить параметры на устройстве**.

10. Настройте ограничения для приложений на iOS MDM-устройстве.

11. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

12. Выберите раздел **Ограничения медиаконтента**.

13. В блоке **Параметры ограничения медиаконтента** установите флажок **Применить параметры на устройстве**.

14. Настройте ограничения для медиаконтента на iOS MDM-устройстве.

15. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будет настроены ограничения функций, приложений и медиаконтента.

Настройка ограничений функций для EAS-устройств

Для обеспечения безопасности EAS-устройства следует настроить ограничения функций устройства.

По умолчанию пользователь может использовать функции EAS-устройства без ограничений.

Чтобы настроить ограничения функций на EAS-устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят EAS-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне Свойства выберите раздел **Ограничения функций**.
5. В блоке **Параметры ограничения функций** разрешите или запретите использование функций EAS-устройства:
   - Чтобы разрешить подключение к устройству карты памяти и других съемных дисков, установите флажок **Разрешить съемные диски**.
   - Чтобы разрешить камеру, установите флажок **Разрешить использование камеры**.
   - Чтобы разрешить Wi-Fi-соединения, установите флажок **Разрешить использование Wi-Fi**.
   - Чтобы разрешить использование порта инфракрасной связи, установите флажок **Разрешить инфракрасное соединение**.
   - Чтобы разрешить использование устройства как точки доступа Wi-Fi для создания беспроводной сети, установите флажок **Разрешить использовать устройство как точку доступа Wi-Fi**.
   - Чтобы разрешить подключение с устройства к удаленному рабочему столу, установите флажок **Разрешить подключение к удаленному рабочему столу**.
   - Чтобы использовать на устройстве клиент Desktop ActiveSync, установите флажок **Разрешить синхронизацию рабочего стола**.
   - В раскрывающемся списке **Использование Bluetooth** разрешите или запретите использование Bluetooth на EAS-устройстве:
     - **Разрешить**. Использование Bluetooth на мобильном устройстве разрешено.
     - **Во время беспроводной связи**. Использование Bluetooth разрешено, когда к мобильному устройству подключена гарнитура беспроводной связи.
     - **Запретить**. Использование Bluetooth на мобильном устройстве запрещено.
6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка доступа пользователей к веб-сайтам

В этом разделе содержатся инструкции по настройке доступа к веб-сайтам на Android- и iOS-устройствах.

Настройка доступа к веб-сайтам на Android-устройствах

Вы можете настраивать доступ пользователей Android-устройств к веб-сайтам с помощью Веб-Фильтра. Веб-Фильтр поддерживает фильтрацию веб-сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Фильтрация позволяет вам ограничить доступ пользователей к отдельным веб-сайтам или категориям веб-сайтов (например, к веб-сайтам из категории "Азартные игры, лотереи, тотализаторы" или "Общение в сети"). Веб-Фильтр также защищает персональные данные пользователей в интернете.

Приложение Kaspersky Endpoint Security для Android должно быть установлено в качестве службы Специальных возможностей. Kaspersky Endpoint Security для Android предлагает пользователю установить приложение в качестве службы Специальных возможностей во время работы мастера первоначальной настройки. Пользователь может пропустить этот шаг или выключить службу в параметрах устройства позднее. В этом случае Веб-Фильтр не работает.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome, Huawei Browser и Samsung Internet Browser. В браузере Samsung Internet Browser Веб-Фильтр не блокирует сайты на мобильных устройствах, если используется рабочий профиль и Веб-Фильтр включен только для рабочего профиля.

По умолчанию Веб-Фильтр включен: ограничен доступ пользователя к веб-сайтам категорий **Фишинг** и **Вредоносное программное обеспечение**.

Чтобы настроить доступ пользователя устройства к веб-сайтам, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Веб-Фильтр**.
5. Установите флажок **Включить Веб-Фильтр**.
6. Для использования Веб-Фильтра вам или пользователю устройства необходимо прочитать и принять Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре).

    a. Перейдите по ссылке **Положение о Веб-Фильтре**.

    Откроется окно **Положение об обработке данных в целях использования Веб-Фильтра**. Чтобы принять Положение о Веб-Фильтре, необходимо прочитать и принять Политику конфиденциальности.

b. Перейдите по ссылке Политика конфиденциальности. Прочитайте и примите Политику конфиденциальности.

Если вы не принимаете Политику конфиденциальности, пользователь мобильного устройства может принять Политику конфиденциальности в мастере первоначальной настройки или в приложении (→ **О приложении** → **Правовая информация** → **Политика конфиденциальности**).

c. Укажите, принимаете ли вы Положение о Веб-Фильтре:

- **Я прочитал и принимаю Положение о Веб-Фильтре**
- **Запросить принятие Положения о Веб-Фильтре у пользователя устройства**
- **Я не принимаю Положение о Веб-Фильтре**

Если вы выбрали вариант **Я не принимаю Положение о Веб-Фильтре**, Веб-Фильтр не будет блокировать сайты на мобильном устройстве. Пользователь мобильного устройства не сможет включить Веб-Фильтр в Kaspersky Endpoint Security.

7. Если вы хотите, чтобы приложение ограничивало доступ пользователя к веб-сайтам в зависимости от их содержания, выполните следующие действия:

a. В разделе **Веб-Фильтр** в раскрывающемся списке выберите пункт **Запрещены веб-сайты выбранных категорий**.

b. Сформируйте список запрещенных категорий, установив флажки для категорий веб-сайтов, доступ к которым приложение будет блокировать.

8. Если вы хотите, чтобы приложение разрешало доступ пользователя только к веб-сайтам, указанным администратором, выполните следующие действия:

a. В разделе **Веб-Фильтр** в раскрывающемся списке выберите пункт **Разрешены только перечисленные веб-сайты**.

b. Сформируйте список веб-сайтов, добавив адреса веб-сайтов, к которым приложение не будет блокировать доступ. Kaspersky Endpoint Security для Android поддерживает только регулярные выражения. При вводе адреса разрешенного веб-сайта используйте следующие шаблоны:

- `http:\/\/www\.example\.com.*` – разрешены все страницы веб-сайта (например, `http://www.example.com/about`).
- `https:\/\/.*example\.com` – разрешены все поддоменные страницы веб-сайта (например, `https://pictures.example.com`).

Вы также можете использовать выражение `https?`, чтобы выбрать проколы HTTP и HTTPS. Подробнее о регулярных выражениях см. на сайте Службы технической поддержки Oracle.

9. Если вы хотите, чтобы приложение ограничивало доступ пользователя к любым веб-сайтам, в разделе **Веб-Фильтр** в раскрывающемся списке выберите элемент **Запрещены все веб-сайты**.

10. Если вы хотите снять ограничение на доступ пользователя устройства к веб-сайтам в зависимости от их содержимого, снимите флажок **Включить Веб-Фильтр**.

11. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка доступа к веб-сайтам на iOS MDM-устройствах

Настройка параметров Веб-Фильтра позволяет контролировать доступ пользователей iOS MDM-устройств к веб-сайтам. Веб-Фильтр контролирует доступ пользователей к веб-сайтам на основе списков разрешенных и запрещенных веб-сайтов. Также Веб-Фильтр позволяет добавлять закладки веб-сайтов на панель закладок Safari.

По умолчанию доступ к веб-сайтам не ограничен.

Настройка Веб-Фильтра доступна только для контролируемых устройств.

Чтобы настроить доступ к веб-сайтам на iOS MDM-устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **Веб-Фильтр**.
5. В блоке **Параметры Веб-Фильтра** установите флажок **Применить параметры на устройстве**.
6. Чтобы блокировать доступ к запрещенным веб-сайтам и разрешить доступ к разрешенным веб-сайтам, выполните следующие действия:
   a. В раскрывающемся списке **Режим фильтрации веб-сайтов** выберите режим **Ограничить содержание "для взрослых"**.
   b. В блоке **Разрешенные веб-сайты** сформируйте список разрешенных веб-сайтов.

      Адрес веб-сайта должен начинаться с `"http://" или "https://"`. Kaspersky Device Management для iOS предоставляет доступ ко всем веб-сайтам домена. Например, если вы добавили в список разрешенных веб-сайтов http://www.example.com, доступ разрешен к http://pictures.example.com и http://example.com/movies. Если список разрешенных веб-сайтов пуст, приложение разрешает доступ ко всем веб-сайтам, кроме указанных в списке запрещенных.
   c. В блоке **Запрещенные веб-сайты** сформируйте список запрещенных веб-сайтов.

      Адрес веб-сайта должен начинаться с `"http://" или "https://"`. Kaspersky Device Management для iOS запрещает доступ ко всем веб-сайтам домена.
7. Чтобы блокировать доступ ко всем веб-сайтам, кроме разрешенных веб-сайтов из списка закладок, выполните следующие действия:
   a. В раскрывающемся списке **Режим фильтрации веб-сайтов** выберите режим **Разрешить веб-сайты только из списка закладок**.
   b. В блоке **Закладки** сформируйте список закладок разрешенных веб-сайтов.

      Адрес веб-сайта должен начинаться с `"http://" или "https://"`. Kaspersky Device Management для iOS предоставляет доступ ко всем веб-сайтам домена. Если список закладок пуст, приложение разрешает доступ ко всем веб-сайтам. Kaspersky Device Management для iOS добавляет веб-сайты из списка закладок на панель закладок Safari на мобильном устройстве пользователя.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будет настроена фильтрация веб-сайтов в соответствии с выбранным режимом и сформированными списками.

Контроль соответствия Android-устройств требованиям корпоративной безопасности

Вы можете контролировать Android-устройства на соответствие требованиям корпоративной безопасности. Требования корпоративной безопасности регламентируют работу пользователя с устройством. Например, на устройстве должна быть включена постоянная защита, антивирусные базы должны быть актуальны, пароль устройства должен быть достаточно сложным. Контроль соответствия работает на основе списка правил. Правило соответствия состоит из следующих компонентов:

- критерий проверки устройства (например, отсутствие на устройстве запрещенных приложений);
- время, выделенное пользователю устройства для устранения несоответствия (например, 24 часа);
- действие, которое будет выполнено с устройством, если пользователь не устранит несоответствие в течение указанного времени (например, блокирование устройства).

Доступны следующие действия, если пользователь не устранит несоответствие в течение указанного времени:

- **Блокирование всех приложений, кроме системных**. Запуск всех приложений, кроме системных, на мобильном устройстве пользователя заблокирован.
- **Блокирование устройства**. Мобильное устройство заблокировано. Для получения доступа к данным необходимо разблокировать устройство. Если после разблокирования устройства причина блокировки не устранена, устройство будет заблокировано снова через указанный период.
- **Удаление корпоративных данных**. Удалены данные в контейнерах, учетная запись корпоративной электронной почты, параметры подключения к корпоративной сети Wi-Fi, VPN-сети, точке доступа (APN), рабочий профиль Android, KNOX-контейнер, а также ключ KNOX License Manager.
- **Сброс настроек до заводских**. Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских. После выполнения этого действия устройство перестает быть управляемым. Для подключения устройства к Kaspersky Security Center требуется повторно установить Kaspersky Endpoint Security для Android.

Чтобы сформировать правило проверки устройств на соответствие групповой политике, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Контроль соответствия**.
5. Чтобы получать уведомления об устройствах, не соответствующих политике, в блоке **Уведомления о несоответствии** установите флажок **Уведомлять администратора**.

Если устройство не соответствует политике, при синхронизации устройства с Сервером администрирования Kaspersky Endpoint Security для Android сформирует запись в журнале событий **Обнаружено несоответствие: <название критерия для проверки>**. Журнал событий можно просмотреть на закладке **События** в свойствах Сервера администрирования или в локальных свойствах программы.

6. Чтобы уведомлять пользователя устройства о том, что его устройство не соответствует политике, в блоке **Уведомления о несоответствии** установите флажок **Уведомлять пользователя**.

   Если устройство не соответствует политике, при синхронизации устройства с Сервером администрирования Kaspersky Endpoint Security для Android уведомляет об этом пользователя в разделе **Статус**.

7. В блоке **Правила соответствия** сформируйте список правил проверки на соответствие устройства политике. Для этого выполните следующие действия:

   a. Нажмите на кнопку **Добавить**.

      Запустится мастер создания правила проверки.

   b. Следуйте указаниям мастера создания правила проверки.

      После завершения работы мастера новое правило отобразится в блоке **Правила соответствия** в списке правил проверки.

8. Чтобы временно выключить сформированное правило проверки, используйте переключатель напротив выбранного правила.

9. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Если устройство пользователя не соответствует правилам, к устройству применяются ограничения, которые вы указали в списке правил проверки.

Контроль запуска приложений

В этом разделе содержатся инструкции по настройке доступа пользователей к приложениям на мобильном устройстве.

Контроль запуска приложений на Android-устройствах

Для обеспечения безопасности мобильного устройства пользователя необходимо настроить параметры запуска приложений на устройстве.

Вы можете установить ограничения при работе пользователя с устройством, на котором установлены запрещенные приложения или не установлены обязательные приложения (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого в параметрах правила проверки требуется выбрать критерий **Установлены запрещенные приложения**, **Установлены приложения запрещенных категорий** или **Не установлены все обязательные приложения**.

Для работы Контроля приложений на мобильных устройствах под управлением операционной системы Android версии 5.0 и выше Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Kaspersky Endpoint Security для Android предлагает пользователю установить приложение в качестве службы Специальных возможностей во время работы мастера первоначальной настройки. Пользователь может пропустить этот шаг или выключить службу в параметрах устройства позднее. В этом случае Контроль приложений не работает.

Чтобы настроить параметры запуска приложений на мобильном устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В окне **Свойства: <Название политики>** выберите раздел **Контроль приложений**.
5. В блоке **Режим работы** выберите режим запуска приложений на мобильном устройстве пользователя:
   - Чтобы разрешить пользователю запускать все приложения, кроме указанных в списке категорий и приложений как запрещенные, выберите режим **Запрещенные приложения**.
   - Чтобы разрешить пользователю запускать только приложения, указанные в списке категорий и приложений как разрешенные, рекомендованные или обязательные, выберите режим **Разрешенные приложения**.
6. Чтобы Kaspersky Endpoint Security для Android отправлял данные о запрещенных приложениях в журнал событий не блокируя их, установите флажок **Не блокировать запрещенные приложения, только запись в журнал событий**.

   При следующей синхронизации мобильного устройства пользователя с Сервером администрирования Kaspersky Endpoint Security для Android сформирует в журнале событий запись **Установлено запрещенное приложение**. Журнал событий можно просмотреть на закладке **События** в свойствах Сервера администрирования или в локальных свойствах программы.
7. Чтобы Kaspersky Endpoint Security для Android блокировал запуск системных приложений на мобильном устройстве пользователя (например, Календарь, Камера, Настройки) в режиме **Разрешенные приложения**, установите флажок **Блокировать системные приложения**.

   Специалисты "Лаборатории Касперского" не рекомендуют блокировать системные приложения, так как это может привести к сбоям в работе устройства.
8. Сформируйте список категорий и приложений для настройки запуска приложений.

   Подробную информацию о категориях приложений см. в Приложении.

   Список приложений, которые входят в каждую категорию, приведен на сайте "Лаборатории Касперского".
9. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка ограничений приложений для EAS-устройств

Для обеспечения безопасности EAS-устройства следует настроить ограничения работы приложений (браузер, неподписанные приложения).

По умолчанию пользователь может работать с приложениями на EAS-устройстве без ограничений.

Чтобы настроить ограничения работы приложений на EAS-устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят EAS-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне Свойства выберите раздел **Ограничения приложений**.
5. В блоке **Параметры ограничения приложений** настройте ограничения работы приложений:
   - Чтобы разрешить пользователю использовать браузер, установите флажок **Разрешить использование браузера**.
   - Чтобы разрешить пользователю создавать личные учетные записи электронной почты (POP3 или IMAP4), установите флажок **Разрешить личную почту**.
   - Чтобы разрешить пользователю запускать приложения, не подписанные сертификатом подлинности, установите флажок **Разрешить неподписанные приложения**.
   - Чтобы разрешить пользователю устанавливать приложения, не подписанные сертификатом подлинности, установите флажок **Разрешить неподписанные инсталляционные пакеты**.
6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Инвентаризация программного обеспечения на Android-устройствах

Вы можете выполнять инвентаризацию приложений на Android-устройствах, подключенных к Kaspersky Security Center. Kaspersky Endpoint Security для Android получает информацию обо всех приложениях, установленных на мобильных устройствах. Информация, полученная в результате инвентаризации, отображается в свойствах устройства в разделе **События**. Вы можете просматривать подробную информацию о каждом установленном приложении, в том числе версию и производителя.

Чтобы включить инвентаризацию программного обеспечения, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В окне **Свойства: <Название политики>** выберите раздел **Контроль приложений**.

5. В разделе **Инвентаризация программного обеспечения** установите флажок **Отправлять данные об установленных приложениях**.

6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Kaspersky Endpoint Security для Android отправляет данные в журнал событий каждый раз после установки или удаления приложения с устройства.

Настройка отображения Android-устройств в Kaspersky Security Center

Для удобства работы со списком мобильных устройств следует настроить параметры отображения устройства в Kaspersky Security Center. По умолчанию список мобильных устройств отображается в дереве консоли **Дополнительно → Управление мобильными устройствами → Мобильные устройства**. Информация об устройстве обновляется автоматически. Вы также можете обновить список мобильных устройств вручную по кнопке **Обновить** в правом верхнем углу.

После подключения устройства к Kaspersky Security Center оно автоматически добавляется в список мобильных устройств. В списке мобильных устройств может содержаться подробная информация об устройстве: модель, операционная система, IP-адрес и другие данные.

Вы можете настроить формат имени устройства, а также выбрать статус устройства. Статус устройства информирует вас о работе компонентов Kaspersky Endpoint Security для Android на мобильном устройстве пользователя.

Компоненты Kaspersky Endpoint Security для Android могут не работать по следующим причинам:

- Пользователь выключил компонент в настройках устройства.
- Пользователь не предоставил приложению необходимые права для работы компонента (например, отсутствует разрешение на определение местоположения устройства для выполнения соответствующей команды Анти-Вора).

Для отображения статуса устройства необходимо включить условие **Определяемый программой** в свойствах группы администрирования (**Свойства → Статус устройства → Условия для статуса устройства "Критический"** и **Условия для статуса устройства "Предупреждение"**). В свойствах группы администрирования вы также можете выбрать другие критерии для формирования статуса мобильного устройства.

Чтобы настроить отображение Android-устройств в Kaspersky Security Center, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В окне **Свойства: <Название политики>** выберите раздел **Информация об устройстве**.

5. В разделе **Имя устройства в Kaspersky Security Center** выберите формат имени устройства для отображения в Консоли администрирования:

   - `Модель устройства [Электронная почта, идентификатор устройства];`
   - `Модель устройства [Электронная почта (если есть) или идентификатор устройства].`

   Идентификатор устройства – уникальный идентификатор, который Kaspersky Endpoint Security для Android генерирует из данных, полученных от устройства. Для мобильных устройств под управлением Android 10 и выше Kaspersky Endpoint Security для Android использует SSAID (идентификатор Android) или хеш-сумму других данных, полученных от устройства. Для предыдущих версий Android приложение использует IMEI.

6. Установите атрибут "замок" в закрытое положение ( ).

7. В блоке **Статус устройства в Kaspersky Security Center** выберите статус устройства, если не работает компонент Kaspersky Endpoint Security для Android: (**Критический**), (**Предупреждение**) или (**ОК**).

   В списке мобильных устройств статус устройства будет изменен в соответствии с выбранным статусом.

8. Установите атрибут "замок" в закрытое положение.

9. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Управление

Этот раздел содержит информацию о том, как удаленно управлять параметрами мобильных устройств в Консоли администрирования Kaspersky Security Center.

Настройка подключения к сети Wi-Fi

В этом разделе содержатся инструкции по настройке автоматического подключения к корпоративной сети Wi-Fi на Android- и iOS MDM-устройствах.

Подключение Android-устройств к сети Wi-Fi

Чтобы подключить мобильное устройство к сети Wi-Fi, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Wi-Fi**.

5. В блоке **Сети Wi-Fi** нажмите **Добавить**.

   Откроется окно **Сеть Wi-Fi**.

6. В поле **Идентификатор сети SSID** укажите имя сети Wi-Fi, содержащей точку доступа (SSID).

7. В блоке **Защита сети** выберите тип безопасности сети Wi-Fi (открытая или защищенная по протоколу WEP или WPA/WPA2 PSK).

8. В поле **Пароль** задайте пароль для доступа к сети, если на предыдущем шаге вы выбрали защищенную сеть.

9. В поле **Адрес прокси-сервера и порт** укажите IP-адрес или DNS-имя прокси-сервера и номер порта (если требуется).

   · На устройствах под управлением операционной системы Android версии 8.0 или выше настроить параметры прокси-сервера для сети Wi-Fi с помощью политики невозможно. Вы можете настроить параметры прокси-сервера для сети Wi-Fi на мобильном устройстве вручную.

   Если вы используете прокси-сервер для подключения к сети Wi-Fi, вы можете настроить параметры подключения к сети с помощью политики. Параметры прокси-сервера на устройствах Android 8.0 и выше необходимо настроить вручную. Изменить параметры подключения к сети Wi-Fi с помощью политики на устройствах 8.0 и выше невозможно, кроме пароля для доступа к сети.

   Если вы не используете прокси-сервер для подключения к сети Wi-Fi, управление подключением к сети Wi-Fi с помощью политик не имеет ограничений.

10. Сформируйте список веб-адресов, для соединения с которыми не нужно использовать прокси-сервер, в поле **Не использовать прокси-сервер для адресов**.

    Вы можете, например, ввести адрес `example.com`. В этом случае прокси-сервер не будет использоваться для адресов `pictures.example.com`, `example.com/movies` и т. п. Протокол (например, `http://`) указывать необязательно.

    На устройствах под управлением операционной системы Android версии 8.0 или выше исключение прокси-сервера для веб-адресов не работает.

11. Нажмите кнопку **OK**.

    Добавленная сеть Wi-Fi отобразится в списке **Сети Wi-Fi**.

    Вы можете изменять или удалять сети Wi-Fi, входящие в список сетей, с помощью кнопок **Изменить** и **Удалить** в верхней части списка.

12. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. После применения политики на мобильном устройстве пользователь сможет подключаться к добавленной сети Wi-Fi, не указывая параметры сети.

На устройствах под управлением Android 10.0 и выше, если пользователь отказывается подключаться к предлагаемой сети Wi-Fi, разрешение приложения на изменение состояния Wi-Fi аннулируется. Пользователю необходимо предоставить это разрешение вручную.

Подключение iOS MDM-устройств к сети Wi-Fi

Для автоматического подключения iOS MDM-устройства к доступной сети Wi-Fi и обеспечения безопасности данных следует настроить параметры подключения.

Чтобы настроить подключение iOS MDM-устройства к сети Wi-Fi, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Wi-Fi**.

5. В блоке **Сети Wi-Fi** нажмите на кнопку **Добавить**.

   Откроется окно **Сеть Wi-Fi**.

6. В поле **Идентификатор сети SSID** укажите имя сети Wi-Fi, содержащей точку доступа (SSID).

7. Чтобы iOS MDM-устройство автоматически подключалось к сети Wi-Fi, установите флажок **Автоматическое подключение**.

8. Чтобы подключение iOS MDM-устройства к сети Wi-Fi, требующей предварительной аутентификации, (подписной сети) было невозможно, установите флажок **Запретить обнаружение сетей с аутентификацией**.

   Для использования подписной сети необходимо оформить подписку, принять соглашение или внести плату. Подписные сети развернуты, например, в кафе или гостиницах.

9. Чтобы сеть Wi-Fi не отображалась в списке доступных сетей на iOS MDM-устройстве, установите флажок **Скрытая сеть**.

   В этом случае для подключения к сети пользователю потребуется вручную ввести на мобильном устройстве идентификатор сети SSID, заданный в параметрах маршрутизатора Wi-Fi.

10. В раскрывающемся списке **Защита сети** выберите тип защиты подключения к сети Wi-Fi:

    - **Выключена**. Аутентификация пользователя не требуется.
    - **WEP**. Сеть защищена по протоколу шифрования WEP (Wireless Encryption Protocol).
    - **WPA/WPA2 (личная)**. Сеть защищена по протоколу шифрования WPA/WPA2 (Wi-Fi Protected Access).
    - **WPA2 (личная)**. Сеть защищена по протоколу шифрования WPA2 (Wi-Fi Protected Access 2.0). Тип защиты WPA2 доступен на устройствах под управлением iOS версии 8 и выше. WPA2 не доступен на устройствах Apple TV.
    - **Любая (личная)**. Сеть защищена по протоколу шифрования WEP, WPA или WPA2 в зависимости от типа маршрутизатора Wi-Fi. Для аутентификации используется индивидуальный для каждого пользователя ключ шифрования.
    - **WEP (динамическая)**. Сеть защищена по протоколу шифрования WEP с использованием динамического ключа.

- **WPA/WPA2 (корпоративная)**. Сеть защищена по протоколу шифрования WPA/WPA2 с использованием протокола 802.1X.

- **WPA2 (корпоративная)**. Сеть защищена по протоколу шифрования WPA2 с использованием одного ключа шифрования для всех пользователей (802.1X). Тип защиты WPA2 доступен на устройствах под управлением iOS версии 8 и выше. WPA2 не доступен на устройствах Apple TV.

- **Любая (корпоративная)**. Сеть защищена по протоколу шифрования WEP или WPA/WPA2 в зависимости от типа маршрутизатора Wi-Fi. Для аутентификации используется один ключ шифрования для всех пользователей.

Если в списке **Защита сети** вы выбрали **WEP (динамическая)**, **WPA/WPA2 (корпоративная)**, **WPA2 (корпоративная)** или **Любая (корпоративная)**, в блоке **Протоколы** вы можете выбрать типы протоколов EAP (Extensible Authentication Protocol) для идентификации пользователя в сети Wi-Fi.

В блоке **Доверенные сертификаты** вы также можете сформировать список доверенных сертификатов для аутентификации пользователя iOS MDM-устройства на доверенных серверах.

11. Настройте параметры учетной записи для аутентификации пользователя при подключении iOS MDM-устройства к сети Wi-Fi:

    a. В блоке **Аутентификация** нажмите кнопку **Настроить**.

    Откроется окно **Аутентификация**.

    b. В поле **Имя пользователя** введите имя учетной записи для аутентификации пользователя при подключении к сети Wi-Fi.

    c. Чтобы требовать у пользователя ввести пароль вручную при каждом подключении к сети Wi-Fi, установите флажок **Требовать пароль при каждом подключении**.

    d. В поле **Пароль** введите пароль учетной записи для аутентификации в сети Wi-Fi.

    e. В раскрывающемся списке **Сертификат для аутентификации** выберите сертификат для аутентификации пользователя в сети Wi-Fi. Если в списке отсутствуют сертификаты, вы можете их **добавить в разделе** Сертификаты.

    f. В поле **Идентификатор пользователя** введите идентификатор пользователя, который будет отображаться во время передачи данных при аутентификации вместо реального имени пользователя.

    Идентификатор пользователя предназначен для повышения уровня безопасности аутентификации, так как имя пользователя не представлено в открытом виде, а отображается в зашифрованном TLS-туннеле.

    g. Нажмите кнопку **ОК**.

В результате на iOS MDM-устройстве будут настроены параметры учетной записи для аутентификации пользователя при подключении к сети Wi-Fi.

12. Настройте (если требуется) параметры подключения к сети Wi-Fi через прокси-сервер:

    a. В блоке **Прокси-сервер** нажмите на кнопку **Настроить**.

    b. В открывшемся окне **Прокси-сервер** выберите режим настройки прокси-сервера и укажите параметры подключения.

    c. Нажмите кнопку **ОК**.

В результате на iOS MDM-устройстве будут настроены параметры подключения устройства к сети Wi-Fi через прокси-сервер.

13. Нажмите кнопку **ОК**.

    Новая сеть Wi-Fi отобразится в списке.

14. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на iOS MDM-устройстве пользователя после применения политики будет настроено подключение к сети Wi-Fi. Мобильное устройство пользователя будет автоматически подключаться к доступной сети Wi-Fi. Безопасность данных при подключении к сети Wi-Fi обеспечивается технологией аутентификации.

Настройка электронной почты

Этот раздел содержит информацию о настройке почтовых ящиков на мобильных устройствах.

Настройка почтового ящика на iOS MDM-устройствах

Чтобы пользователь iOS MDM-устройства мог работать с электронной почтой, следует добавить учетную запись электронной почты в список учетных записей на iOS MDM-устройстве.

По умолчанию добавляется учетная запись электронной почты со следующими параметрами:

- протокол электронной почты – IMAP;
- пользователь может перемещать сообщения электронной почты между своими учетными записями и синхронизировать адреса учетных записей;
- для работы с почтой пользователь может использовать любые почтовые клиенты (не только Mail);
- при передаче сообщений не используется SSL-соединение.

Вы можете изменить указанные параметры при добавлении учетной записи.

Чтобы добавить учетную запись электронной почты пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **Электронная почта**.
5. В блоке **Учетные записи электронной почты** нажмите на кнопку **Добавить**.

   Откроется окно **Учетная запись электронной почты**.

6. В поле **Описание** введите описание учетной записи электронной почты пользователя.

7. Выберите протокол электронной почты:

   - **POP**
   - **IMAP**

8. Если требуется, укажите префикс пути IMAP в поле **Префикс пути IMAP**.

   Префикс пути IMAP нужно указывать прописными буквами (например, GMAIL для Google Mail). Поле доступно, если выбран протокол учетной записи IMAP.

9. В поле **Имя пользователя для отображения в сообщениях** введите имя пользователя, которое будет отображаться в поле **От:** для всех исходящих сообщений.

10. В поле **Адрес электронной почты** введите адрес электронной почты пользователя iOS MDM-устройства.

11. Настройте дополнительные параметры учетной записи электронной почты:

    - Чтобы разрешить пользователю перемещать сообщения электронной почты между своими учетными записями, установите флажок **Разрешить перемещать сообщения между учетными записями**.
    - Чтобы разрешить синхронизацию используемых адресов электронной почты между учетными записями пользователя, установите флажок **Разрешить синхронизировать последние используемые адреса**.
    - Чтобы разрешить пользователю использовать сервис Mail Drop для передачи вложений большого размера, установите флажок **Разрешить Mail Drop**.
    - Чтобы разрешить пользователю использовать только стандартный почтовый клиент iOS, установите флажок **Разрешить использовать только приложение Mail**.

12. Настройте параметры использования протокола S/MIME в приложении Mail. *S/MIME* – это протокол для передачи зашифрованных сообщений с цифровой подписью.

    - Чтобы использовать протокол S/MIME для подписи исходящей почты, установите флажок **Подписывать сообщения** и выберите сертификат для подписи. Цифровая подпись подтверждает подлинность отправителя и указывает получателю, что содержимое сообщения не изменилось в процессе передачи. Подпись сообщений доступна на устройствах под управлением iOS версии 10.3 и выше.
    - Чтобы использовать протокол S/MIME для шифрования исходящей почты, установите флажок **Шифровать сообщения по умолчанию** и выберите сертификат для шифрования (открытый ключ). Шифрование сообщений доступно на устройствах под управлением iOS версии 10.3 и выше.
    - Чтобы предоставить пользователю возможность выполнять шифрование сообщений по отдельности, установите флажок **Показывать переключатель для шифрования сообщений**. Для отправки зашифрованных сообщений пользователю необходимо нажать на значок в приложении Mail в поле **Кому**.

13. В блоках **Сервер входящей почты** и **Сервер исходящей почты** по кнопке **Настройка** настройте параметры подключения к серверам:

    - **Адрес сервера и порт**: имена хостов или IP-адреса серверов входящей и исходящей почты и номера портов серверов.
    - **Имя учетной записи**: имя учетной записи пользователя для авторизации на сервере входящей и исходящей почты.

- **Тип аутентификации**: тип аутентификации учетной записи пользователя электронной почты на серверах входящей и исходящей почты.
- **Пароль**: пароль учетной записи для авторизации на сервере входящей и исходящей почты, защищенный выбранным методом аутентификации.
- **Использовать один пароль для серверов входящей и исходящей почты**: использование одного пароля для аутентификации пользователя на серверах входящей и исходящей почты.
- **Использовать SSL-соединение**: использование транспортного протокола передачи данных SSL (Secure Sockets Layer), который применяет шифрование и аутентификацию на базе сертификатов для защиты передачи данных.

14. Нажмите кнопку **ОК**.

    Новая учетная запись электронной почты отобразится в списке.

15. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильное устройство пользователя после применения политики будут добавлены учетные записи электронной почты из сформированного списка.

Настройка почтового ящика Exchange на iOS MDM-устройствах

Чтобы пользователь iOS MDM-устройства мог работать с корпоративной электронной почтой, календарем, контактами, заметками и задачами, на сервер Microsoft Exchange следует добавить учетную запись Exchange ActiveSync.

По умолчанию на сервер Microsoft Exchange добавляется учетная запись со следующими параметрами:

- почта синхронизируется один раз в неделю;
- пользователь может перемещать сообщения между своими учетными записями и синхронизировать адреса учетных записей;
- для работы с почтой пользователь может использовать любые почтовые клиенты (не только Mail);
- при передаче сообщений не используется SSL-соединение.

Вы можете изменить указанные параметры при добавлении учетной записи Exchange ActiveSync.

Чтобы добавить учетную запись Exchange ActiveSync пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **Exchange ActiveSync**.
5. В блоке **Учетные записи Exchange ActiveSync** нажмите на кнопку **Добавить**.

   Откроется окно **Учетная запись Exchange ActiveSync** на закладке **Общие**.

6. В поле **Имя учетной записи** введите имя учетной записи для авторизации на сервере Microsoft Exchange. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

7. В поле **Адрес сервера** введите сетевое имя или IP-адрес сервера Microsoft Exchange.

8. Если вы хотите использовать транспортный протокол передачи данных SSL для защиты передачи данных, установите флажок **Использовать SSL-соединение**.

9. В поле **Домен** введите имя домена пользователя iOS MDM-устройства. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

10. В поле **Пользователь учетной записи** введите имя пользователя iOS MDM-устройства.

    Если оставить это поле пустым, при применении политики на iOS MDM-устройстве Kaspersky Device Management для iOS запросит имя у пользователя. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

11. В поле **Адрес электронной почты** введите адрес электронной почты пользователя iOS MDM-устройства. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

12. В поле **Пароль** введите пароль учетной записи Exchange ActiveSync для авторизации на сервере Microsoft Exchange.

13. Выберите закладку **Дополнительно** и настройте на закладке дополнительные параметры учетной записи Exchange ActiveSync:

    - **Синхронизировать почту за период <период времени>**;
    - **Тип аутентификации**;
    - **Разрешить перемещать сообщения между учетными записями**;
    - **Разрешить синхронизировать последние используемые адреса**;
    - **Разрешить использовать только приложение Mail**.

14. Настройте параметры использования протокола S/MIME в приложении Mail. *S/MIME* – это протокол для передачи зашифрованных сообщений с цифровой подписью.

    - Чтобы использовать протокол S/MIME для подписи исходящей почты, установите флажок **Подписывать сообщения** и выберите сертификат для подписи. Цифровая подпись подтверждает подлинность отправителя и указывает получателю, что содержимое сообщения не изменилось в процессе передачи. Подпись сообщений доступна на устройствах под управлением iOS версии 10.3 и выше.
    - Чтобы использовать протокол S/MIME для шифрования исходящей почты, установите флажок **Шифровать сообщения по умолчанию** и выберите сертификат для шифрования (открытый ключ). Шифрование сообщений доступно на устройствах под управлением iOS версии 10.3 и выше.
    - Чтобы предоставить пользователю возможность выполнять шифрование сообщений по отдельности, установите флажок **Показывать переключатель для шифрования сообщений**. Для отправки зашифрованных сообщений пользователю необходимо нажать на значок в приложении Mail в поле **Кому**.

15. Нажмите кнопку **ОК**.

    Новая учетная запись Exchange ActiveSync отобразится в списке.

16. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильное устройство пользователя после применения политики будут добавлены учетные записи Exchange ActiveSync из сформированного списка.

Настройка почтового ящика Exchange на Android-устройствах (только Samsung)

Для работы с корпоративной почтой, контактами и календарем на мобильном устройстве следует настроить параметры почтового ящика Exchange.

Настройка почтового ящика Exchange возможна только для Samsung-устройств под управлением операционной системы Android версии 5.0 и выше.

Чтобы настроить почтовый ящик Exchange на мобильном устройстве, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → Управление Samsung-устройствами**.
5. В блоке **Exchange ActiveSync** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры почтового сервера Exchange**.
6. В поле **Адрес сервера** введите IP-адрес или DNS-имя сервера, на котором размещен почтовый сервер.
7. В поле **Домен** введите имя домена пользователя мобильного устройства в корпоративной сети.
8. В раскрывающемся списке **Периодичность синхронизации** выберите желаемый период синхронизации мобильного устройства с сервером Microsoft Exchange.
9. Чтобы использовать транспортный протокол передачи данных SSL, установите флажок **Использовать SSL-соединение**.
10. Чтобы использовать цифровые сертификаты для защиты передачи данных между мобильным устройством и сервером Microsoft Exchange, установите флажок **Проверять сертификат сервера**.
11. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

    Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Управление сторонними мобильными приложениями

Для контроля активности мобильных приложений, запускаемых на устройстве пользователя, вы можете использовать контейнеры. *Контейнер* – это специальная оболочка для мобильных приложений, которая позволяет контролировать действия содержащегося в ней приложения, тем самым защищая персональные и корпоративные данные пользователя на устройстве.

В Kaspersky Security для мобильных устройств Service Pack 3 Maintenance Release 2 поддержка создания контейнеров для мобильных приложений прекращена. Однако вы можете добавлять на Android-устройства контейнеры, созданные в более ранних версиях программы.

Для установки приложения в контейнере на устройство пользователя вы можете использовать один из следующих способов:

- отправить пользователю сообщение электронной почты, содержащее ссылку на дистрибутив приложения в контейнере.
- в свойствах политики в разделе **Контроль приложений** указать приложение в контейнере как обязательное или разрешенное к установке. После синхронизации мобильного устройства с Kaspersky Security Center дистрибутив приложения в контейнере будет автоматически скопирован на устройство пользователя.

Для установки приложений в контейнерах на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников. Для обеспечения безопасности устройства и защиты данных после установки приложений в контейнерах рекомендуется запретить установку приложений из неизвестных источников. Подробная информация об установке приложений без использования Google Play приведена в *справке Android*.

Настройка уведомлений Kaspersky Endpoint Security для Android

Если вы хотите, чтобы пользователь мобильного устройства не отвлекался на уведомления Kaspersky Endpoint Security для Android, вы можете выключить некоторые уведомления.

В Kaspersky Endpoint Security используются следующие средства для отображения статуса защиты устройства:

- **Уведомление о состоянии защиты**. Уведомление закреплено в панели уведомлений. Уведомление о состоянии защиты нельзя удалить. В уведомлении отображается статус защиты устройства (например,) и количество проблем, если они имеются. Чтобы посмотреть список проблем в приложении, выберите статус защиты устройства.
- **Уведомления приложения**. Уведомления информируют пользователя устройства о приложении (например, об обнаружении угрозы).
- **Всплывающие сообщения**. Всплывающие сообщения требуют внимания со стороны пользователя устройства (например, действия, предпринимаемые при обнаружении угрозы).

По умолчанию все уведомления Kaspersky Endpoint Security для Android включены.

Пользователь Android-устройства может выключить все уведомления от Kaspersky Endpoint Security для Android в настройках панели уведомлений. Если уведомления выключены, пользователь не контролирует работу приложения и может пропустить важную информацию (например, о сбоях при синхронизации устройства с Kaspersky Security Center). Чтобы пользователь узнал статус работы приложения, ему необходимо открыть Kaspersky Endpoint Security для Android.

Чтобы настроить отображение уведомлений о работе Kaspersky Endpoint Security для Android, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Дополнительно**.

5. В разделе **Уведомления приложения** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры уведомлений на устройстве**.

6. Выберите проблемы Kaspersky Endpoint Security для Android, которые вы хотите скрыть на мобильном устройстве пользователя и нажмите на кнопку **OK**.

   Уведомления о проблемах состояния защиты не будут отображаться в Kaspersky Endpoint Security для Android, а также в разделе **Статус** приложения. Уведомления о состоянии защиты и уведомления приложения продолжат отображаться в Kaspersky Endpoint Security для Android.

   Некоторые уведомления Kaspersky Endpoint Security для Android являются обязательными и их невозможно отключить (например, уведомления об истечении срока действия лицензии).

7. Чтобы скрыть все уведомления и всплывающие сообщения, выберите **Отключать уведомления и всплывающие сообщения, когда приложение работает в фоновом режиме**.

   Kaspersky Endpoint Security для Android будет показывать только уведомления о состоянии защиты. В уведомлении отображается статус защиты устройства (например,) и количество проблем. Также в приложении будут отображаться уведомления, когда пользователь работает с приложением (например, вручную обновляет антивирусные базы).

   Специалисты "Лаборатории Касперского" рекомендуют включить уведомления и всплывающие сообщения. Если уведомления и всплывающие сообщения отключены, когда приложение работает в фоновом режиме, приложение не уведомляет пользователей об угрозах в реальном времени. Пользователи мобильных устройств узнают о состоянии защиты устройства, только когда откроют приложение.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. На мобильном устройстве пользователя не будут отображаться уведомления Kaspersky Endpoint Security для Android, которые вы выключили.

Подключение iOS MDM-устройств к AirPlay

Для потоковой передачи музыки, фотографий и видео с iOS MDM-устройства на устройства AirPlay следует настроить автоматическое подключение к устройствам AirPlay. Для использования технологии AirPlay мобильное устройство и устройства AirPlay должны быть подключены к одной беспроводной сети. К устройствам AirPlay относятся устройства Apple TV (второго и третьего поколений), устройства AirPort Express, динамики или приемники с поддержкой AirPlay.

Автоматическое подключение к устройствам AirPlay доступно только для контролируемых устройств.

Чтобы настроить подключение iOS MDM-устройства к устройствам AirPlay, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **AirPlay**.
5. В блоке **Устройства AirPlay** установите флажок **Применить параметры на устройстве**.
6. В блоке **Пароли** нажмите на кнопку **Добавить**.

   В таблице паролей добавится пустая строка.
7. В графе **Имя устройства** введите имя устройства AirPlay в беспроводной сети.
8. В графе **Пароль** введите пароль от устройства AirPlay.
9. Чтобы ограничить подключение iOS MDM-устройства к устройствам AirPlay, сформируйте список разрешенных устройств в блоке **Разрешенные устройства**. Для этого добавьте в список разрешенных устройств MAC-адреса устройств AirPlay.

   К устройствам AirPlay, не входящим в список разрешенных устройств, доступ запрещен. Если оставить список разрешенных устройств пустым, Kaspersky Device Management для iOS разрешит доступ ко всем устройствам AirPlay.
10. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате мобильное устройство пользователя после применения политики будет автоматически подключаться к устройствам AirPlay для передачи медиа-контента.

Подключение iOS MDM-устройств к AirPrint

Для печати документов с iOS MDM-устройства беспроводным способом с помощью технологии AirPrint следует настроить автоматическое подключение к принтерам AirPrint. Мобильное устройство и принтер должны быть подключены к одной беспроводной сети. На принтере AirPrint требуется настроить общий доступ для всех пользователей.

Чтобы настроить подключение iOS MDM-устройства к принтеру AirPrint, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **AirPrint**.
5. В блоке **Принтеры AirPrint** нажмите на кнопку **Добавить**.

   Откроется окно **Принтер**.
6. В поле **IP-адрес** введите IP-адрес принтера AirPrint.
7. В поле **Путь к ресурсу** введите путь к принтеру AirPrint.

Путь к принтеру соответствует ключу rp (resourse path) протокола Bonjour. Например:

- printers/Canon_MG5300_series;
- ipp/print;
- Epson_IPP_Printer.

8. Нажмите кнопку **OK**.

   Добавленный принтер AirPrint отобразится в списке.

9. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате пользователь мобильного устройства после применения политики сможет печатать документы на принтере AirPrint по беспроводной связи.

Настройка точки доступа (APN)

Для подключения мобильного устройства к услугам передачи данных в мобильной сети следует настроить параметры APN (Access Point Name).

Настройка APN на Android-устройствах (только Samsung)

Настройка APN возможна только для Samsung-устройств под управлением операционной системы Android версии 5.0 и выше.

Для использования точки доступа на мобильном устройстве пользователя должна быть установлена SIM-карта. Параметры точки доступа предоставляются оператором мобильной связи. Неправильная настройка точки доступа может привести к дополнительным расходам на мобильную связь.

Чтобы настроить параметры точки доступа (APN), выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → APN**.
5. В блоке **APN** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры APN**.

6. На закладке **Общие** укажите следующие параметры точки доступа:

   a. В раскрывающемся списке **Тип точки доступа** выберите тип точки доступа.

b. В поле **Имя точки доступа** укажите название точки доступа.

c. В поле **MCC** укажите мобильный код страны (MCC).

d. В поле **MNC** укажите мобильный код сети (MNC).

e. Если в качестве типа точки доступа вы выбрали **MMS** или **Интернет и MMS**, укажите дополнительные параметры для MMS:

- В поле **Сервер для MMS** укажите полное доменное имя сервера мобильного оператора для обмена MMS.
- В поле **Прокси-сервер для MMS** укажите сетевое имя или IP-адрес прокси-сервера и номер порта прокси-сервера мобильного оператора для обмена MMS.

7. На закладке **Дополнительно** настройте дополнительные параметры точки доступа (APN):

a. В раскрывающемся списке **Тип аутентификации** выберите тип авторизации пользователя мобильного устройства на сервере мобильного оператора для доступа к сети.

b. В поле **Адрес сервера** укажите сетевое имя сервера оператора мобильной связи, через который осуществляется доступ к услугам передачи данных.

c. В поле **Адрес прокси-сервера** укажите сетевое имя или IP-адрес и номер порта прокси-сервера мобильного оператора для доступа к сети.

d. В поле **Имя пользователя** укажите имя пользователя для авторизации в мобильной сети.

e. В поле **Пароль** укажите пароль для авторизации пользователя в мобильной сети.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка APN на iOS MDM-устройствах

Для подключения пользователя iOS MDM-устройства к услугам передачи данных в мобильной сети следует настроить точку доступа (APN).

Раздел **APN** устарел. Рекомендуется настраивать параметры APN в разделе **Сотовая связь**. Перед настройкой параметров сотовой связи убедитесь, что параметры раздела **APN** не применены на устройстве (снят флажок **Применить параметры на устройстве**). Совместное использование параметров разделов **APN** и **Сотовая связь** невозможно.

Чтобы настроить точку доступа на iOS MDM-устройстве пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Сотовая связь**.

5. В блоке **Параметры сотовой связи** установите флажок **Применить параметры на устройстве**.

6. В списке **Тип APN** выберите тип точки доступа для передачи данных в мобильной сети GPRS/3G/4G:

   - **Встроенная APN** – конфигурация параметров сотовой связи для передачи данных через оператора мобильной сети, который поддерживает работу со встроенной Apple SIM. Подробная информация об устройствах со встроенной Apple SIM приведена на веб-сайте Службы технической поддержки Apple.
   - **APN** – настройка параметров сотовой связи для передачи данных через оператора мобильной сети вставленной SIM-карты.
   - **Встроенная APN и APN** – конфигурация параметров сотовой связи для передачи данных через операторов мобильных сетей вставленной SIM-карты и встроенной Apple SIM. Подробная информация об устройствах со встроенной Apple SIM и слотом для SIM-карты приведена на веб-сайте Службы технической поддержки Apple.

7. В поле **Имя точки доступа** укажите название точки доступа.

8. Выберите тип аутентификации пользователя устройства на сервере мобильного оператора для доступа к сети (интернет и MMS) в раскрывающемся списке **Тип аутентификации**.

9. В поле **Имя пользователя** укажите имя пользователя для авторизации в мобильной сети.

10. В поле **Пароль** укажите пароль для авторизации пользователя в мобильной сети.

11. В поле **Адрес прокси-сервера и порт** введите имя хоста, домена или IP-адрес прокси-сервера и номер порта прокси-сервера.

12. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будет настроена точка доступа (APN).

Настройка рабочего профиля Android

Этот раздел содержит информацию о работе с рабочим профилем Android.

Использование рабочих профилей Android доступно только на устройствах под управлением операционной системы Android версии 5.0 или выше.

О рабочем профиле Android

Android Enterprise – платформа для управления мобильной инфраструктурой компании, предоставляющая сотрудникам компании рабочую среду для работы на мобильных устройствах. Подробная информация о работе с Android Enterprise приведена на сайте технической поддержки Google.

Вы можете создать на мобильном устройстве пользователя рабочий профиль Android (далее также "рабочий профиль"). *Рабочий профиль Android* – безопасная среда на устройстве пользователя, в которой администратор может управлять приложениями и учетными записями пользователя, не ограничивая возможности при работе с его собственными данными. При создании на мобильном устройстве пользователя рабочего профиля в него автоматически устанавливаются следующие корпоративные приложения: Google Play Маркет, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие. Корпоративные приложения, размещенные в рабочем профиле, а также уведомления этих приложений, отмечены значком  . Для приложения Google Play Маркет требуется создать отдельную корпоративную учетную запись Google. Приложения, размещенные в рабочем профиле, отображаются в общем списке приложений.

Использование рабочих профилей Android доступно только на устройствах под управлением операционной системы Android версии 5.0 или выше.

Настройка рабочего профиля

Чтобы настроить параметры рабочего профиля Android, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Рабочий профиль Android**.
5. В рабочей области **Рабочий профиль Android** установите флажок **Создать рабочий профиль**.
6. Укажите параметры рабочего профиля:

   - Чтобы включить Контроль приложений в рабочем профиле Android и выключить в личном профиле, установите флажок **Включить Контроль приложений только в рабочем профиле**.

     В разделе **Пользователи** можно выбрать Контроль приложений и в рабочей области создать списки разрешенных, запрещенных, рекомендуемых и необходимых приложений, а также разрешенных и запрещенных категорий приложений.

   - Чтобы в Google Chrome включить Веб-Фильтр в рабочем профиле и отключить в личном профиле, в рабочей области раздела **Рабочий профиль Android** установите флажок **Включить Веб-Фильтр только в рабочем профиле**.

     Веб-Фильтр для браузера Samsung Internet Browser блокирует веб-сайты в рабочем и личном профилях. Нельзя включить Веб-Фильтр для браузера Samsung Internet Browser только в рабочем профиле. Чтобы использовать Веб-Фильтр в рабочем профиле в браузере Samsung Internet Browser отключите параметр **Включить Веб-Фильтр только в рабочем профиле**. Если включен этот параметр, Веб-Фильтр для браузера Samsung Internet Browser не будет работать. По умолчанию, Веб-Фильтр выключен в рабочем профиле.

     Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome и Samsung Internet Browser.

Вы можете указать параметры доступа к веб-сайтам (создать список запрещенных категорий веб-сайтов или список разрешенных веб-сайтов) в разделе **Веб-Фильтр**.

- Чтобы запретить пользователю копировать данные с помощью буфера обмена из приложений рабочего профиля в личные приложения, установите флажок **Запретить перенос данных из рабочего профиля в личный**.

- Чтобы запретить пользователю использовать режим отладки по USB на мобильном устройстве в рабочем профиле, установите флажок **Запретить включать режим отладки по USB**.

  В режиме отладки по USB пользователь может, например, загрузить приложение через рабочую станцию.

- Чтобы запретить пользователю устанавливать приложения в рабочий профиль Android из всех источников, кроме Google Play, установите флажок **Запретить установку приложений в рабочий профиль из неизвестных источников**.

- Чтобы запретить пользователю удалять приложения из рабочего профиля Android, установите флажок **Запретить удаление приложений из рабочего профиля**.

7. Чтобы настроить параметры рабочего профиля на мобильном устройстве пользователя, заблокируйте изменение параметров.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Пространство мобильного устройства пользователя будет разделено на рабочий и личный профили.

Добавление учетной записи LDAP

Чтобы пользователь iOS MDM-устройства мог получить доступ к корпоративным контактам на сервере LDAP, следует добавить учетную запись LDAP.

Чтобы добавить учетную запись LDAP пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **LDAP**.

5. В блоке **Учетные записи LDAP** нажмите на кнопку **Добавить**.

   Откроется окно **Учетная запись LDAP**.

6. В поле **Описание** введите описание учетной записи LDAP пользователя. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

7. В поле **Имя учетной записи** введите имя учетной записи для авторизации на сервере LDAP. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

8. В поле **Пароль** введите пароль учетной записи LDAP для авторизации на сервере LDAP.

9. В поле **Адрес сервера** введите имя домена сервера LDAP. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

10. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи сообщений, установите флажок **Использовать SSL-соединение**.

11. Сформируйте список поисковых запросов для доступа пользователя iOS MDM-устройства к папкам с корпоративными данными на сервере LDAP:

    a. В блоке **Параметры поиска** нажмите на кнопку **Добавить**.

    В таблице поисковых запросов отобразится пустая строка.

    b. В графе **Название** введите название поискового запроса.

    c. В графе **Глубина поиска** выберите уровень вложенности папки для поиска корпоративных данных на сервере LDAP:

    - **Корень дерева** – поиск в базовой папке сервера LDAP.
    - **Один уровень** – поиск в папках на первом уровне вложенности от базовой папки.
    - **Поддерево** – поиск в папках на всех уровнях вложенности от базовой папки.

    d. В графе **База поиска** укажите путь к папке на сервере LDAP, с которой начинается поиск (например, "ou=people", "o=example corp").

    e. Повторите пункты a-d для всех поисковых запросов, которые вы хотите добавить на iOS MDM-устройство.

12. Нажмите кнопку **ОК**.

    Новая учетная запись LDAP отобразится в списке.

13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будут добавлены учетные записи LDAP из сформированного списка. Пользователь может получить доступ к корпоративным контактам в стандартных приложениях iOS Контакты, Сообщения и Mail.

Добавление учетной записи календаря

Чтобы пользователь iOS MDM-устройства мог работать со своими событиями календаря на сервере CalDAV, следует добавить учетную запись на CalDAV. Синхронизация с сервером CalDAV позволит пользователю создавать и принимать приглашения, получать обновления событий и синхронизировать задачи с приложением Напоминания.

Чтобы добавить учетную запись CalDAV пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Календарь**.

5. В блоке **Учетные записи CalDAV** нажмите на кнопку **Добавить**.

   Откроется окно **Учетная запись CalDAV**.

6. В поле **Описание** введите описание учетной записи CalDAV пользователя.

7. В поле **Адрес сервера и порт** введите имя хоста или IP-адрес сервера CalDAV и номер порта сервера CalDAV.

8. В поле **Основной веб-адрес** задайте веб-адрес учетной записи CalDAV пользователя iOS MDM-устройства на сервере CalDAV (например, http://example.com/caldav/users/mycompany/user).

   Веб-адрес должен начинаться `с "http://" или "https://"`.

9. В поле **Имя учетной записи** задайте имя учетной записи пользователя для авторизации на сервере CalDAV.

10. В поле **Пароль** задайте пароль учетной записи CalDAV для авторизации на сервере CalDAV.

11. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи данных о событиях между сервером CalDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.

12. Нажмите кнопку **ОК**.

    Новая учетная запись CalDAV отобразится в списке.

13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будут добавлены учетные записи CalDAV из сформированного списка.

Добавление учетной записи контактов

Чтобы пользователь iOS MDM-устройства мог синхронизировать свои контакты с сервером CardDAV, следует добавить учетную запись CardDAV. Синхронизация с сервером CardDAV позволит пользователю получить доступ к данным контактов с любого устройства.

Чтобы добавить учетную запись CardDAV пользователя iOS MDM-устройства, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Контакты**.

5. В блоке **Учетные записи CardDAV** нажмите на кнопку **Добавить**.

   Откроется окно **Учетная запись CardDAV**.

6. В поле **Описание** введите описание учетной записи CardDAV пользователя. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

7. В поле **Адрес сервера и порт** введите имя хоста или IP-адрес сервера CardDAV и номер порта сервера CardDAV.

8. В поле **Основной веб-адрес** задайте веб-адрес учетной записи CardDAV пользователя iOS MDM-устройства на сервере CardDAV (например, http://example.com/carddav/users/mycompany/user).

   Веб-адрес должен начинаться `с "http://" или "https://"`.

9. В поле **Имя учетной записи** задайте имя учетной записи пользователя для авторизации на сервере CardDAV. Вы можете использовать макросы из раскрывающегося списка **Добавить макрос**.

10. В поле **Пароль** задайте пароль учетной записи CardDAV для авторизации на сервере CardDAV.

11. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи контактов между сервером CardDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.

12. Нажмите кнопку **ОК**.

    Новая учетная запись CardDAV отобразится в списке.

13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве пользователя после применения политики будут добавлены учетные записи CardDAV из сформированного списка.

Настройка подписки на календарь

Чтобы пользователь iOS MDM-устройства мог добавить в свой календарь события сторонних календарей (например, корпоративного календаря), нужно добавить на календарь подписку. *Сторонние календари* – календари других пользователей, у которых есть учетная запись CalDAV, календари iCal, а также другие открыто опубликованные календари.

Чтобы добавить подписку на календарь, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Подписка на календарь**.

5. В блоке **Подписки на календари** нажмите на кнопку **Добавить**.

   Откроется окно **Подписка на календарь**.

6. В поле **Описание** введите описание подписки на календарь.

7. В поле **Веб-адрес сервера** укажите веб-адрес стороннего календаря.

   Вы можете указать в поле основной веб-адрес учетной записи CalDAV пользователя, на календарь которого оформляется подписка. Также вы можете указать веб-адрес календаря iCal или другого открыто публикуемого календаря.

8. В поле **Имя пользователя** введите имя учетной записи пользователя для аутентификации на сервере стороннего календаря.

9. В поле **Пароль** введите пароль от подписки на календарь для аутентификации на сервере стороннего календаря.

10. Чтобы использовать транспортный протокол передачи данных SSL для защиты передачи данных о событиях между сервером CalDAV и мобильным устройством, установите флажок **Использовать SSL-соединение**.

11. Нажмите кнопку **OK**.

12. Новая подписка на календарь отобразится в списке.

13. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате в календарь мобильного устройства пользователя после применения политики будут добавлены события сторонних календарей из сформированного списка.

Добавление веб-клипов

Веб-клип – приложение, которое открывает веб-сайт с главного экрана мобильного устройства. Нажимая на значки веб-клипов на главном экране устройства, пользователь может быстро открывать веб-сайты (например, корпоративный веб-сайт). Вы можете добавлять веб-клипы на устройства пользователей и настраивать вид значка веб-клипа, который отображается на экране.

По умолчанию применяются следующие ограничения на использование веб-клипов:

- Пользователь не может самостоятельно удалять веб-клипы с мобильного устройства.
- Веб-сайты, которые отображаются при нажатии на значок веб-клипа, открываются не на весь экран устройства.
- К значку веб-клипа на экране применяются визуальные эффекты сглаживания углов, тени и глянца.

Чтобы добавить веб-клип на iOS MDM-устройство пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши.

4. В политике, в окне **Свойства** выберите раздел **Веб-клипы**.

5. В блоке **Веб-клипы** нажмите на кнопку **Добавить**.

   Откроется окно **Веб-клипы**.

6. В поле **Название** введите название веб-клипа, которое будет отображаться на главном экране iOS MDM-устройства.

7. В поле **Веб-адрес** введите адрес веб-сайта, который будет открываться при нажатии на значок веб-клипа. Адрес должен начинаться с `"http://" или "https://".`

8. Чтобы разрешить пользователю удалить веб-клип с iOS MDM-устройства, установите флажок **Разрешить удаление**.

9. Нажмите на кнопку **Выбрать** и укажите файл с изображением для значка веб-клипа.

   Значок отображается на главном экране iOS MDM-устройства. Изображение должно удовлетворять следующим требованиям:

   - размер изображения не более 400 x 400 пикселей;
   - формат файла GIF, JPEG или PNG;
   - размер файла не более 1 МБ.

   Значок веб-клипа доступен для предварительного просмотра в поле **Значок**. Если вы не выберете изображение для веб-клипа, в качестве значка будет отображаться пустой квадрат.

   Если вы хотите, чтобы значок веб-клипа отображался без специальных визуальных эффектов (скругление углов значка и эффект глянца), установите флажок **Веб-клип без визуальных эффектов**.

10. Если вы хотите, чтобы при нажатии на значок веб-сайт открывался на весь экран iOS MDM-устройства, установите флажок **Полноэкранный веб-клип**.

11. Нажмите кнопку **ОК**.

    Новый веб-клип отобразится в списке.

12. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на главный экран мобильного устройства пользователя после применения политики будут добавлены значки веб-клипов из сформированного списка.

Добавление шрифтов

Чтобы добавить шрифт на iOS MDM-устройство пользователя, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят iOS MDM-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши.
4. В политике, в окне **Свойства** выберите раздел **Шрифты**.
5. В блоке **Шрифты** нажмите на кнопку **Добавить**.

   Откроется окно **Шрифт**.

6. В поле **Имя файла** укажите путь к файлу шрифта (файл с расширением ttf или otf).

   Шрифты с расширением ttc или otc не поддерживаются.

   Шрифты идентифицируются по имени PostScript. Не устанавливайте шрифты с одинаковым именем PostScript, даже если их содержание отличается. Установка шрифтов с одинаковым именем PostScript приведет к неопределенной ошибке.

7. Нажмите кнопку **Открыть**.

   Новый шрифт отобразится в списке.

8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

В результате на мобильном устройстве после применения политики пользователю будет предложено установить шрифты из сформированного списка.

Управление приложением с помощью сторонних EMM-систем (только Android)

Приложение Kaspersky Endpoint Security для Android можно использовать без систем администрирования "Лаборатории Касперского". Для развертывания и управления приложением Kaspersky Endpoint Security для Android можно использовать EMM-решения (Enterprise Mobility Management) сторонних поставщиков. Для работы приложения со сторонними EMM-решениями "Лаборатория Касперского" участвует в AppConfig Community.

Управление приложением Kaspersky Endpoint Security для Android через сторонние EMM-решения доступно только на устройствах под управлением Android версии 5.0 и выше.

Сторонние EMM-решения можно использовать только для развертывания приложения Kaspersky Endpoint Security для Android. Подключите устройство к Kaspersky Security Center и управляйте приложением с помощью Консоли управления. В этом случае управление приложением Kaspersky Endpoint Security для Android с помощью EMM-консоли будет недоступно.

Если вы развернули приложение Kaspersky Endpoint Security для Android с помощью сторонней EMM-системы, управлять приложением с помощью Kaspersky Endpoint Security Cloud будет невозможно. Вы можете управлять приложением Kaspersky Endpoint Security для Android с помощью EMM-консоли.

Следующие EMM-решения поддерживают использование приложения Kaspersky Endpoint Security для Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

В EMM-Консоли вы можете выполнять следующие действия:

- Разворачивать приложение в рабочий профиль Android на устройствах пользователей.
- Активировать приложение.
- Настраивать параметры приложения:
  - включать защиту от вредоносных и фишинговых веб-сайтов в интернете;
  - настраивать параметры подключения устройства к Kaspersky Security Center;
  - настраивать параметры Антивируса;
  - настраивать расписание запуска антивирусной проверки устройства;
  - включать обнаружение рекламных приложений и приложений, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя;

- настраивать расписание обновления баз приложения.

Начало работы

Для развертывания приложения на мобильных устройствах пользователей необходимо добавить Kaspersky Endpoint Security для Android в магазин приложений EMM. Вы можете добавить Kaspersky Endpoint Security для Android в магазин приложений EMM с помощью ссылки Google Play. Подробнее о работе с приложениями в EMM-Консоли см. на *сайте Службы технической поддержки поставщика услуг EMM*.

Приложение Kaspersky Endpoint Security для Android разворачивается в рабочем профиле Android. Приложение изолировано от персональных данных пользователя и защищает только корпоративные данные в рабочем профиле. Рекомендуется обеспечить защиту Kaspersky Endpoint Security для Android от удаления средствами EMM-Консоли.

Как установить приложение

В зависимости от EMM-Консоли выберите способ установки приложения на устройства: тихая установка, отправка сообщения электронной почты с ссылкой на приложение в Google Play или другой доступный способ.

Для работы приложения требуются следующие разрешения:

- Разрешение "Память" для доступа к файлам при работе Антивируса (только для Android 6.0 и выше).
- Разрешение "Телефон" для идентификации устройства, например, при активации приложения.
- Запрос на добавление Kaspersky Endpoint Security для Android в список приложений, запускаемых при загрузке операционной системы (на некоторых устройствах, например, Huawei, Meizu, Xiaomi). Если запрос на добавление не отображается, добавьте Kaspersky Endpoint Security для Android в список приложений автозапуска вручную. Запрос может не отображается, если в рабочем профиле не установлено приложение Безопасность.

Требуемые разрешения можно предоставить в EMM-консоли перед развертыванием приложения Kaspersky Endpoint Security для Android. Более подробную информацию о предоставлении разрешений в EMM-консоли см. на *сайте Службы технической поддержки поставщика услуг EMM*. Разрешения можно также предоставить при выполнении первоначальной настройки Kaspersky Endpoint Security для Android на устройстве с помощью мастера.

Приложение Kaspersky Endpoint Security для Android будет установлено в рабочий профиль Android.

Для работы Веб-Фильтра в параметрах Google Chrome дополнительно требуется настроить прокси-сервер:

- Режим настройка прокси-сервера: вручную.
- Адрес и порт прокси-сервера: 127.0.0.1:3128.
- Поддержка протокола SPDY: выключено.
- Сжатие данных через прокси-сервер: выключено.

Как активировать приложение

Информация о лицензии передается на мобильное устройство вместе с остальными параметрами в файле конфигурации.

Если активация приложения не произошла в течение 30 дней с момента установки на мобильное устройство, то срок действия пробной лицензии истекает. По истечении срока действия пробной лицензии мобильное приложение Kaspersky Endpoint Security для Android прекращает выполнять все свои функции.

По истечении срока действия коммерческой лицензии мобильное приложение продолжает работу, но с ограниченной функциональностью (например, недоступно обновление баз Kaspersky Endpoint Security для Android). Чтобы продолжить использование приложения в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии.

Чтобы активировать приложение Kaspersky Endpoint Security для Android, выполните следующие действия:

1. В EMM-Консоли откройте настройки приложения Kaspersky Endpoint Security для Android.
2. В поле параметра `LicenseActivationCode` введите код активации приложения.

   Для активации приложения на устройстве требуется доступ к серверам активации "Лаборатории Касперского".

Как подключить устройство к Kaspersky Security Center

После установки приложения Kaspersky Endpoint Security для Android на мобильное устройство вы можете подключить устройство к Kaspersky Security Center. Данные для подключения устройства к Kaspersky Security Center передаются на мобильное устройство вместе с остальными параметрами, перечисленными в файле конфигурации. После подключения устройства к Kaspersky Security Center вы можете централизовано настраивать параметры приложения с помощью групповых политик. Также вы можете получать отчеты и статистику о работе приложения Kaspersky Endpoint Security для Android.

Перед подключением устройств к Kaspersky Security Center убедитесь, что выполнены следующие условия:

- На рабочем месте администратора установлен плагин управления Kaspersky Endpoint Security для Android.
- В свойствах Сервера администрирования открыт порт для подключения мобильных устройств.
- В Консоли администрирования включено отображение папки **Управление мобильными устройствами**.
- В хранилище сертификатов Kaspersky Security Center создан общий сертификат для идентификации пользователя мобильного устройства.

Перед подключением устройств к Kaspersky Security Center рекомендуется выполнить следующие действия:

- Если вы хотите создавать задачи и политики для мобильных устройств, создайте отдельную группу администрирования для мобильных устройств.
- Если вы хотите автоматически перемещать мобильные устройства в отдельную группу администрирования, создайте правило автоматического перемещения устройств из папки **Нераспределенные устройства**.

- Если вы хотите централизованно настраивать параметры приложения Kaspersky Endpoint Security для Android, создайте групповую политику.

Чтобы подключить устройство к Kaspersky Security Center, выполните следующие действия:

1. В EMM-Консоли откройте настройки приложения Kaspersky Endpoint Security для Android.
2. В поле параметра KscServer введите DNS-имя или IP-адрес сервера администрирования Kaspersky Security Center. Порт по умолчанию 13292.
3. Если вы хотите, чтобы пользователь не отвлекался на уведомления Kaspersky Endpoint Security для Android, выключите уведомления приложения. Для этого установите параметр DisableNotification = True.

   После подключения приложение показывает все уведомления. Вы можете выключить некоторые уведомления приложения в параметрах политики.

   Не выключайте уведомления о работе приложения, если вы не используете Kaspersky Security Center. Например, пользователь может не получить уведомление об истечении срока действия лицензии. В результате приложение прекратит выполнять все свой функции.

После настройки параметров подключения приложение Kaspersky Endpoint Security для Android отобразит уведомление с запросом следующих дополнительных разрешений и прав:

- Разрешение "Камера" для работы Анти-Вора (команда **Сфотографировать**).
- Разрешение "Местоположение" для работы Анти-Вора (команда **Определить местоположение устройства**).
- Права администратора устройства (владельца рабочего профиля Android) для работы следующих функций приложения:
  - установка сертификатов безопасности;
  - настройка Wi-Fi;
  - настройка Exchange ActiveSync;
  - ограничение использования камеры, Bluetooth, Wi-Fi.

Из-за особенностей работы рабочего профиля Android (отсутствие службы Специальных возможностей) в приложении недоступны Контроль приложений и Анти-Вор.

Когда пользователь предоставит необходимые разрешения и права, устройство будет подключено к Kaspersky Security Center. Если не создано правило автоматического перемещения устройств в группу администрирования, устройство будет автоматически добавлено в папку **Нераспределенные устройства**. Если создано правило автоматического переноса устройств в группу администрирования, то устройство будет автоматически добавлено в заданную группу.

Kaspersky Endpoint Security позволяет использовать следующий формат названий устройств:

- Модель устройства [Электронная почта, идентификатор устройства];
- Модель устройства [Электронная почта (если есть) или идентификатор устройства].

Идентификатор устройства – уникальный идентификатор, который Kaspersky Endpoint Security для Android формирует из данных, полученных от устройства. Для мобильных устройств под управлением Android 10 и выше Kaspersky Endpoint Security для Android использует SSAID (идентификатор Android) или хеш-сумму других данных, полученных от устройства. Для предыдущих версий Android приложение использует IMEI. Можно настроить формат названия устройства в групповой политике. Можно также добавить тег к названию устройства. Это упрощает поиск и сортировку устройств в Kaspersky Security Center. Использование тега доступно только для VMware AirWatch.

Чтобы добавить тег к названию устройства:

1. В EMM-Консоли откройте настройки приложения Kaspersky Endpoint Security для Android.
2. В поле KscDeviceNameTag выберите значения:
   - {DeviceSerialNumber} – серийный номер устройства.
   - {DeviceUid} – уникальный идентификатор устройства (UDID).
   - {DeviceAssetNumber} – инвентарный номер устройства. Это внутренний номер, создаваемый в организации.

Рекомендуется использовать только эти значения. VMware AirWatch также поддерживает другие значения, но Kaspersky Endpoint Security не гарантирует корректность использования этих значений.

Можно добавить несколько значений (например, {DeviceSerialNumber} {DeviceUid}). Тег будет добавлен к названию устройства в Kaspersky Security Center. Тег и название устройства разделены пробелом. Например, если название устройства – Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E, то его UDID-тег будет 22:7D:78:9E:C5:1E. При совместном использовании Kaspersky Security Center и VMwareAirWatch, тег позволяет идентифицировать устройства в обеих консолях. Чтобы сопоставить устройства, выберите одинаковые значения названия устройства (например, серийный номер устройства).

После подключения устройства к Kaspersky Security Center параметры приложения будут изменены в соответствии с групповой политикой. Приложение Kaspersky Endpoint Security для Android игнорирует параметры приложения из файла конфигурации, настроенные в EMM-консоли. Для настройки доступны все разделы политики за исключением следующих разделов:

- **Анти-Вор** (блокирование устройства);
- **Контейнеры;**
- **Управление устройством** (Блокирование экрана);
- **Контроль приложений** (Блокирование запрещенных приложений);
- **Рабочий профиль Android;**
- **Управление Samsung KNOX.**

Из-за способа развертывания рабочего профиля невозможно применить параметры групповой политики из раздела **Рабочий профиль Android**. Эти параметры можно применить, только если рабочий профиль создан с помощью Kaspersky Security Center.

Файл AppConfig

Конфигурационный файл создается для настройки приложения в EMM-консоли. Параметры приложения в конфигурационном файле приведены в следующей таблице.

Параметры конфигурационного файла

Ключ конфигурации	Описание	Тип	Значение
`LicenseActivationCode`	Код активации приложения	String	Код активации приложения из 20 латинских букв и цифр. Чтобы активировать приложение с помощ кода активации, требуется доступ интернет для подключения к серве активации "Лаборатории Касперск Если оставить поле пустым, приложение будет активировано п пробной лицензии. Пробная лицен имеет срок 30 дней. По истечении срока действия пробной лицензии мобильное приложение Kaspersky Endpoint Security для Android прекращает выполнять все свои функции. Чтобы продолжить использование приложения, вам ну приобрести коммерческую лицензи
`EulaAcceptanceConfirmationV1`	<Ссылка на Лицензионное соглашение>	Choice	Этот параметр доступен только для VMware AirWatch. `Принять` – я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения `Отказаться` – я не принимаю усло и положения настоящего Лицензионного соглашения. Чтобы принять условия и положени Лицензионного соглашения для вс мобильных устройств, необходим доступ в интернет для подключени серверам "Лаборатории Касперск Если вы выберете вариант `Отказаться`, приложение предлож пользователю принять условия и положения Лицензионного соглашения. Пользователи мобиль устройств могут принять эти усло мастере первоначальной настройк
`EulaAcceptanceCodeV1`	Код Лицензионного соглашения	String	

			Этот параметр доступен только для VMware AirWatch. Код Лицензионного соглашения содержится в Лицензионном соглашении. *Чтобы просмотреть код Лицензионного соглашения, выполните следующие действия:* 1. Скопируйте ссылку на Лицензионное соглашение (`EulaAcceptanceConfirmatio` из EMM-консоли. 2. Вставьте ссылку в браузер. Откроется Лицензионное соглашение. 3. Ознакомьтесь с условиями и положениями Лицензионного соглашения и определите код Лицензионного соглашения. Чтобы принять условия и положения Лицензионного соглашения для всех мобильны устройств, необходим доступ в интернет для подключения к серверам "Лаборатории Касперского". Если вы не заполните это поле, приложение предложит пользоват принять условия и положения Лицензионного соглашения. Пользователь мобильного устройс может принять эти условия в маст первоначальной настройки.
`KscServer`	Адрес и порт Сервера администрирования Kaspersky Security Center	String	DNS-имя или IP-адрес Сервера администрирования Kaspersky Sec Center и номер порта. Введите адр следующим образом: `<адрес сервера>:<порт>`. Если вы ввели адрес сервера без указания порта приложение использует порт по умолчанию 13292.
`DisableNotification`	Выключить уведомления приложения до подключения к Kaspersky Security Center	Boolean	`True` – Kaspersky Endpoint Securit Android скрывает все уведомления работе приложения. Приложение Kaspersky Endpoint Security для Android скрывает уведомления до подключения устройства к Kaspers Security Center. После подключени приложение показывает все уведомления. Вы можете выключит

			некоторые уведомления приложен параметрах политики. Не выключайте уведомления о работе приложения, если вы не используете Kaspersky Security Center. Иначе пользователь мож не получить уведомление об истечении срока действия лицензии. В этом случае приложение перестанет функционировать. `False` – Kaspersky Endpoint Securi для Android показывает все уведомления о работе приложени
`ScanScheduleType`	Режим запуска проверки	Choice	`AfterUpdate` – запуск антивирусн проверки после обновления баз. Приложение обновляет антивирус базы по сформированному расписанию (`UpdateScheduleTyp` `Daily` – запуск антивирусной проверки раз в день. Настройте вр запуска проверки (`ScanScheduleTime`). `Weekly` – запуск антивирусной проверки раз в неделю. Выберите недели запуска антивирусной проверки (`ScanScheduleDay`) и настройте время (`ScanScheduleTime`). `Off` – автоматический запуск антивирусной проверки выключен При любом значении параметра пользователь устройства может запустить антивирусную проверку вручную.
`ScanScheduleDay`	День запуска проверки	Choice	`Monday / Tuesday / Wednesday Thursday / Friday / Saturday Sunday` Вы можете выбрать только одно значение параметра.
`ScanScheduleTime`	Время запуска проверки	String	Время в 24-часовом формате (например, 13:00) или 12-часовом (например, 10.30 pm).
`ScanScheduleLock`	Запретить настраивать режим запуска проверки	Boolean	`True` – параметры режима запуска антивирусной проверки недоступн для пользователя в настройках приложения.

			`False` – пользователь может настроить режим запуска антивирусной проверки и, наприме выключить автоматический запуск антивирусной проверки.
`ScanOnlyExecutableFiles`	Типы файлов для проверки (Антивирусная проверка)	Choice	`AllFiles` – проверка всех файлов `OnlyExecutables` – проверка тол исполняемых файлов. К исполняем файлам относятся файлы с расширением .apk (.zip), .dex, .so. В Kaspersky Endpoint Security для Android Service Pack 4 Maintenance Release 1 невозможно включить проверку только исполняемых фай
`ScanArchives`	Проверять архивы с распаковкой	Boolean	`True` – приложение распаковывае архивы и проверяет их содержимо `False` – приложение проверяет только файлы архивов. Приложение проверяет только арх с расширением .zip (.apk). В Kaspersky Endpoint Security для Android Service Pack 4 Maintenance Release 1 невозможно выключить проверку содержимого архивов.
`ScanActionOnThreatFound`	Действие при обнаружении угрозы (Антивирусная проверка)	Choice	`Quarantine` – приложение помеш обнаруженные объекты на каранти Карантин хранит файлы в упакован виде, в котором они не могут нане вред устройству. Карантин предоставляет возможность удали или восстановить файлы, помещен в изолированное хранилище. `Delete` – приложение удаляет обнаруженные объекты. `Skip` – приложение оставляет обнаруженные объекты без изменений. Если обнаруженные объекты были пропущены, Kaspers Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. П попытке обращения к объекту на устройстве (например, попытке скопировать или открыть) приложе блокирует доступ к нему. `AskUser` – приложение предлагае пользователю выбрать действие д каждого обнаруженного объекта: пропустить, поместить на каранти или удалить. При обнаружении нескольких объектов пользовател может применить выбранное дейс ко всем объектам.

			Приложение записывает информа об обнаруженных угрозах и выполненных действиях в отчеты приложения.
`ScanLock`	Запретить настраивать параметры проверки	Boolean	`True` – следующие параметры проверки недоступны для пользователя в настройках приложения: тип файлов для прове проверка архивов, действие при обнаружении угрозы. `False` – пользователь может настроить параметры проверки и, например, выбрать действие `Skip` обнаружении угрозы.
`ScanAndProtectionAdwareRiskware`	Блокировать рекламные приложения, приложения автодозвона и другие	Boolean	`True` – приложение обнаруживает рекламные приложения и приложе которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя. `False` – приложение пропускает рекламные приложения и приложе которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя.
`ProtectionMode`	Режим постоянной защиты	Choice	`Recommended` – приложение тольк однократно проверяет новые приложения (сразу после установ файлы из папки Загрузки. `Extended` – приложение проверяе все файлы, которые пользователь открывает, изменяет, копирует, запускает и сохраняет на устройст Также приложение проверяет новы приложения и файлы из папки Загрузки. `Disabled` – постоянная защита выключена.
`UseKsnMode`	Режим Kaspersky Security Network	Choice	`Recommended` – приложение обменивается данными с Kaspersk Security Network (KSN). Kaspersky Endpoint Security для Android использует KSN для постоянной защиты устройства от угроз (Облачная защита) и работы Веб-Фильтра в интернете.

			`Extended` – приложение обменивается данными с Kaspersk Security Network и дополнительно отправляет в Вирусную лаборатор определенную статистику о работ Kaspersky Endpoint Security для Android. Эта информация позволяе отслеживать угрозы в режиме реального времени. Сбор, обрабо хранение персональных данных пользователя службами KSN не производится. `Disabled` – приложение не использует данные от Kaspersky Security Network. Включить Веб-Фильтр (`EnableWebFilter`) невозможно. Для Антивируса недоступен компонент Облачная защита.
`ProtectScanOnlyExecutableFiles`	Типы файлов для проверки (Постоянная защита)	Boolean	`AllFiles` – проверка всех файлов `OnlyExecutables` – проверка тол исполняемых файлов. К исполняем файлам относятся файлы с расширением .apk (.zip), .dex, .so. В Kaspersky Endpoint Security для Android Service Pack 4 Maintenance Release 1 невозможно включить проверку только исполняемых фай
`ProtectionActionOnThreatFound`	Действие при обнаружении угрозы (Постоянная защита)	Choice	`Quarantine` – приложение помеш обнаруженные объекты на каранти Карантин хранит файлы в упакован виде, в котором они не могут нане вред устройству. Карантин предоставляет возможность удали или восстановить файлы, помещен в изолированное хранилище. `Delete` – приложение удаляет обнаруженные объекты. `Skip` – приложение оставляет обнаруженные объекты без изменений. Если обнаруженные объекты были пропущены, Kaspers Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. П попытке обращения к объекту на устройстве (например, попытке скопировать или открыть объект) приложение блокирует доступ к не Приложение записывает информа об обнаруженных угрозах и выполненных действиях в отчеты приложения.
`ProtectionLock`	Запретить	Boolean	`True` – следующие параметры

	настраивать параметры постоянной защиты		постоянной защиты недоступны дл пользователя в настройках приложения: режим постоянной защиты, тип файлов для проверки действие при обнаружении угрозы `False` – пользователь может настроить параметры постоянной защиты и, например, выбрать дейс `Skip` при обнаружении угрозы.
`UpdateScheduleType`	Режим запуска обновления баз	Choice	`Daily` – проверка наличия новых антивирусных баз и загрузка их на устройства раз в день. Настройте время запуска обновления баз (`UpdateScheduleTime`). `Weekly` – проверка наличия антивирусных баз и загрузка их на устройства раз в неделю. Выберит день недели запуска обновления б (`UpdateScheduleDay`) и настройте время (`UpdateScheduleTime`). `Off` – автоматическое обновление антивирусных баз выключено. При любом значении параметра пользователь устройства может запустить обновление антивирусн баз вручную.
`UpdateScheduleDay`	День запуска обновления баз	Choice	`Monday / Tuesday / Wednesday Thursday / Friday / Saturday Sunday` Вы можете выбрать только одно значение параметра.
`UpdateScheduleTime`	Время запуска обновления баз	String	Время в 24-часовом формате (например, 13:00) или 12-часовом (например, 10.30 pm).
`UpdateScheduleLock`	Запретить настраивать режим запуска обновления баз	Boolean	`True` – параметры режима запуска обновления баз недоступны для пользователя в настройках приложения. `False` – пользователь может настроить режим запуска обновле баз и, например, выключить автоматический запуск обновлени антивирусных баз.
`AllowUpdateInRoaming`	Обновлять базы в роуминге	Boolean	`True` – приложение загружает антивирусные базы, если устройст находится в зоне роуминга. Приложение загружает антивирус базы по сформированному расписанию (`UpdateScheduleTyp` `False` – приложение загружает антивирусные базы, только если устройство находится в домашней сети.

`EnableWebFilter`	Веб-Фильтр	Boolean	`True` – приложение блокирует вредоносные и фишинговые веб-с в интернете с помощью компонент Веб-Фильтр. Веб-Фильтр работае только в Google Chrome. Вредоносные и фишинговые веб сайты, использующие протокол HTTPS, разрешается не блокировать, если домен являет доверенным. Если домен не является доверенным, Веб-Фильтр блокирует вредоносные фишинговые веб-сайты. `False` – защита от вредоносных и фишинговых веб-сайтов выключен Для работы Веб-Фильтра должны выполнены следующие условия: • Пользователи устройств приня Политику конфиденциальности Положение о Веб-Фильтре в мастере первоначальной настройки или параметрах приложения. • В параметрах браузера настро прокси-сервер: `ProxyMode = "fixed_server` `ProxyServer = "127.0.0.1:3128"` `DisableSpdy = true` `DataCompressionProxyEnabl` `false` Конфигурации прокси-сервера могут различаться в зависимос от версии Google Chrome. Подробная информация настро Google Chrome приведена на ве сайте проекта Chromium. После удаления приложения Kaspersky Endpoint Security дл Android с мобильного устройст сбросьте настройки прокси-сервера. • В параметрах приложения включено использование KSN: `UseKsnMode = Recommended` и `UseKsnMode = Extended`. • В параметрах операционной системы рекомендуется выбра Google Chrome в качестве браузера по умолчанию.

`EnableWebFilterLock`	Запретить настраивать Веб-Фильтр	Boolean	`True` – параметры Веб-Фильтра недоступны для пользователя в настройках приложения. `False` – пользователь может настроить параметры Веб-Фильтр например, выключить защиту от вредоносных и фишинговых веб-сайтов в интернете.
`UpdateServer`	Адрес сервера источника обновлений баз	String	Адрес сервера источника обновле баз, например, `http://update.server.com`. Если оставить поле пустым, Kaspe Endpoint Security для Android использует серверы обновлений б "Лаборатории Касперского".
`AllowGoogleAnalytics`	Отправлять данные в Google Analytics для Firebase	Boolean	`True` – приложение автоматическ передает данные о работе Kasper Endpoint Security для Android в се Google Analytics для Firebase. Данн необходимы для повышения качес работы приложения и анализа удовлетворенности пользователе Передача данных в сервис Google Analytics для Firebase осуществля по защищенному каналу. Доступ к данным и защита данных регулиру соответствующими условиями использования сервиса Google Analytics для Firebase. `False` – передача данных в сервис Google Analytics для Firebase выключена.
`KscDeviceNameTag`	Тег названия устройства для Kaspersky Security Center	String	Этот параметр доступен только для VMware AirWatch. Тег будет добавлен к названию устройства в Kaspersky Security Center. Тег и название устройства разделены пробелом. Это упроща поиск и сортировку устройств в Kaspersky Security Center. • `{DeviceSerialNumber}` – серийный номер устройства. • `{DeviceUid}` – уникальный идентификатор устройства (UD • `{DeviceAssetNumber}` – инвентарный номер устройства Это внутренний номер, создаваемый в организации.

			Можно добавить несколько значений (например, `{DeviceSerialNumber}` `{DeviceUid}`). Рекомендуется использовать только эти значения. VMware AirWatch также поддерживает другие значения, но Kaspersky Endpoint Security не гарантирует корректность использования эти значений.
`KscGroup`	Название группы устройств	String	Группы устройств можно указывать EMM-консоли. При подключении устройства к Kaspersky Security Center, оно автоматически добавляется в подпапку папки "Нераспределенные устройства". И подпапки соответствует названию группы, указанному с помощью это параметра. Затем можно создать правила автоматического перемещения устройств из подпап папки "Нераспределенные устройс в группы администрирования папк "Управляемые устройства". Если это поле не заполнено, устройство автоматически добавляется в корень папки "Нераспределенные устройства".
`KscCorporateEmail`	Корпоративная электронная почта пользователя	String	В консоли EMM можно указать корпоративные адреса электронно почты пользователей. Эти адреса электронной почты будут отображаться в Kaspersky Security Center. Строка должна представлять собо действующий адрес электронной почты. Другие значения будут игнорироваться.

Для пользователей мобильных устройств

Часто задаваемые вопросы

Что нового

- Обновлен дизайн пользовательского интерфейса Kaspersky Endpoint Security для Android.
- Все разделы справки теперь доступны онлайн.

Почему специалисты IT-отдела установили Kaspersky Endpoint Security на мобильное устройство?

Добро пожаловать в Kaspersky Endpoint Security. Приложение обеспечивает защиту мобильных устройств от веб-угроз, вирусов и других программ, представляющих риски. Kaspersky Endpoint Security поддерживает взаимодействие с системой удаленного администрирования Kaspersky Security Center и другими системами Enterprise Mobility Management (EMM). Система удаленного администрирования позволяет администратору настраивать ваше устройство в соответствии с требованиями корпоративной безопасности. Администратор может выполнять следующие действия:

- устанавливать, обновлять и удалять Kaspersky Endpoint Security на вашем устройстве;
- настраивать параметры Kaspersky Endpoint Security;
- контролировать запуск приложений на вашем мобильном устройстве;
- настраивать и контролировать ваше мобильное устройство;
- проверять соответствие вашего мобильного устройства требованиям корпоративной безопасности;
- реагировать на нарушения требований корпоративной безопасности, накладывая ограничения на устройство (например, блокировка устройства);
- формировать отчеты о работе компонентов Kaspersky Endpoint Security.

Kaspersky Endpoint Security информирует о нарушениях требований корпоративной безопасности и предлагает варианты действий для их устранения в разделе **Статус**.

Как активировать приложение?

Приложение может активировать только администратор. Администратор добавляет лицензионный ключ в Консоль администрирования. Если приложение Kaspersky Endpoint Security не активировано, оно будет активировано с помощью пробной лицензии. Пробная лицензия имеет срок 30 дней. По истечении срока действия пробной лицензии все функции приложения Kaspersky Endpoint Security будут отключены.

Вы можете просмотреть информацию о лицензии в настройках приложения (**Настройки** → **Дополнительно** → **Лицензия**).

Почему нельзя изменить параметры приложения?

Система удаленного администрирования позволяет администратору настраивать ваше устройство в соответствии с требованиями корпоративной безопасности. Администратор заблокировал настройку параметров приложения, чтобы вы не меняли их вручную. Администратор выбрал оптимальный режим защиты и установил расписание проверки. Вы можете быть уверены, что ваше устройство защищено.

Почему уведомление Kaspersky Endpoint Security невозможно удалить из панели уведомлений?

Уведомление Kaspersky Endpoint Security Устройство защищено нельзя удалить с устройства. Приложение работает непрерывно и хранится в памяти устройства. Это необходимо для постоянной защиты устройства, проверки новых приложений и защиты ваших данных в Интернете.

Уведомление Устройство защищено всегда отображается на панели уведомлений. При возникновении проблемы на экране появляется дополнительное уведомление. Нажмите на уведомление о проблеме и следуйте инструкциям приложения Kaspersky Endpoint Security, чтобы решить проблему. Уведомление о проблеме исчезнет. На панели уведомлений останется только постоянное уведомление.

Что делать, если Kaspersky Endpoint Security отправляет уведомления?

Если Kaspersky Endpoint Security уведомляет вас о проблеме, нажмите на уведомление. Приложение предложит возможные способы решения проблемы. Если вы не решите проблему, администратор может наложить ограничения на ваше устройство (например, заблокировать устройство). Проблемы, угрожающие вашему устройству, угрожают безопасности данных всей организации.

Что делать, чтобы защитить мобильное устройство после установки?

Если вы самостоятельно установили приложение Kaspersky Endpoint Security, необходимо добавить мобильное устройство в корпоративную сеть. Для этого вы укажите адрес Сервера администрирования Kaspersky Security Center в настройках приложения. Вы можете узнать адрес сервера у администратора. После синхронизации администратор увидит ваше устройство в Консоли администрирования. В Консоли администрирования администратор может указать параметры Kaspersky Endpoint Security и устройства. Кроме того, администратор может запускать команды на вашем устройстве (например, чтобы узнать местоположение устройства).

Если вы установили Kaspersky Endpoint Security по ссылке, отправленной администратором по электронной почте, описанные выше действия не требуются.

Что нужно знать об удалении Kaspersky Endpoint Security?

Обычно администратор запрещает удалять приложение в соответствии с требованиями корпоративной безопасности. Если администратор запретил удаление Kaspersky Endpoint Security, его невозможно удалить. Однако, если вы случайно установили приложение, вы можете удалить его обычным способом.

Статьи в этом разделе содержат описание всех параметров, доступных и видимых на мобильных устройствах. Фактический внешний вид и работа приложения зависит от того, какая система удаленного администрирования используется и как администратор настроил ваше устройство в соответствии с требованиями корпоративной безопасности. Некоторые функции и параметры приложения, описанные в этом разделе, могут не соответствовать тем, что вы увидите при работе приложением. При возникновении вопросов о работе приложения на вашем конкретном устройстве, обратитесь к администратору.

Возможности приложения

Kaspersky Endpoint Security обладает следующими основными возможностями.

Защита от вирусов и других вредоносных приложений

Для защиты от вирусов и других вредоносных приложений используется компонент Антивирус.

Антивирус выполняет следующие функции:

- проверяет на наличие угроз все устройство, установленные приложения или выбранные папки;
- защищает устройство в режиме реального времени;
- проверяет новые установленные приложения до их первого запуска;
- обновляет антивирусные базы.

Если на мобильном устройстве установлено приложение, выполняющее сбор и отправку информации на обработку, Kaspersky Endpoint Security для Android может классифицировать такое приложение как вредоносное.

Контроль установленных приложений

В соответствии с требованиями корпоративной безопасности *администратор системы удаленного администрирования* (далее также "администратор") формирует списки рекомендованных, запрещенных и обязательных приложений. Для установки рекомендованных и обязательных приложений, их обновления, а также для удаления запрещенных приложений используется компонент Контроль приложений.

Контроль приложений позволяет вам устанавливать на ваше устройство рекомендованные и обязательные приложения с помощью прямой ссылки на дистрибутив или ссылки на Google Play. С помощью Контроля приложений вы можете удалять запрещенные приложения, которые не удовлетворяют требованиям корпоративной безопасности.

Для работы Контроля приложений на мобильных устройствах под управлением операционной системы Android версии 5.0 и выше Kaspersky Endpoint Security должен быть включен в качестве службы Специальных возможностей. Если вы не включили службу во время работы мастера первоначальной настройки приложения, включите Kaspersky Endpoint Security в качестве службы Специальных возможностей в разделе **Статус**, выбрав соответствующее уведомление, или в настройках устройства (**Настройки Android → Специальные возможности → Службы**).

Защита данных при потере или краже устройств

Для защиты информации от попадания в чужие руки, а также для поиска устройства при его потере или краже используется компонент Анти-Вор.

Анти-Вор позволяет дистанционно выполнить следующие действия:

- Заблокировать устройство.

  Чтобы злоумышленник не имел возможности разблокировать устройство, на мобильных устройствах под управлением операционной системы Android версии 7.0 и выше Kaspersky Endpoint Security должен быть включен в качестве службы Специальных возможностей.

- Включить на устройстве громкую сирену, даже если на устройстве выключен звук.
- Получить координаты местоположения устройства на карте.
- Удалить данные, хранящиеся на устройстве.
- Сбросить настройки до заводских.
- Незаметно сделать фотографии человека, который использует ваше устройство.

Для работы Анти-Вора Kaspersky Endpoint Security должен быть включен в качестве администратора устройства. Если вы не предоставили права администратора устройства во время первоначальной настройки приложений, предоставьте Kaspersky Endpoint Security права администратора в разделе **Статус**, выбрав соответствующее уведомление, или в настройках устройства (**Настройки Android** → **Безопасность** → **Администраторы устройства**).

Защита от интернет-угроз

Для защиты от интернет-угроз используется компонент Веб-Фильтр.

Веб-Фильтр блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также фишинговые веб-сайты, цель которых – украсть ваши конфиденциальные данные и получить доступ к вашим финансовым счетам. Веб-Фильтр проверяет веб-сайты до открытия, используя облачную службу Kaspersky Security Network.

Для работы Веб-Фильтра необходимо выполнение следующих условий:

- Приложение Kaspersky Endpoint Security включено в качестве службы Специальных возможностей.
- Принято Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре). Kaspersky Endpoint Security использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN.

  Администратор вашей сети может принять Положение о Веб-Фильтре в Kaspersky Security Center. В этом случае вам не потребуется выполнять никаких действий.

  Если администратор вашей сети не принял Положение о Веб-Фильтре и направил вам запрос на принятие Положения, прочитайте и примите Положение о Веб-Фильтре в настройках приложения.

  Если администратор вашей сети не принял Положение о Веб-Фильтре, Веб-Фильтр будет недоступен.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome, Huawei Browser и Samsung Internet Browser. В браузере Samsung Internet Browser Веб-Фильтр не блокирует сайты на мобильных устройствах, если используется рабочий профиль и Веб-Фильтр включен только для рабочего профиля.

Обзор главного окна

Вид главного окна для разных разрешений экрана незначительно отличается.

При появлении проблем, которые могут привести к снижению уровня защиты, заражению устройства или потере информации, вид главного экрана изменится.

В разделе **Статус** отображается следующая информация:

- проблемы в защите вашего устройства;
- информация о соответствии вашего устройства требованиям корпоративной безопасности;
- информация о состоянии защиты вашего устройства.

Вы можете открыть раздел **Статус**, нажав на верхнюю часть главного окна Kaspersky Endpoint Security.

Проблемы в защите устройства

Проблемы в защите сгруппированы по категориям, к которым они относятся. Для каждой проблемы приведены действия, которые вы можете выполнить, чтобы решить проблему.

> В разделе **Статус** также отображается список пропущенных объектов, обнаруженных приложением. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

Проблемы в защите бывают двух типов:

- *Уведомительные*. Выделены желтым цветом. Уведомительные проблемы информируют о событиях, важных для безопасности устройства (например, последняя проверка выполнялась более 14 дней назад или установлено новое непроверенное приложение). Уведомительную проблему можно скрыть. После этого информация о проблеме будет доступна в меню **Скрытые проблемы**.
- *Критические*. Выделены красным цветом. Критические проблемы информируют о событиях, имеющих первостепенную важность для безопасности устройства (например, антивирусные базы давно не обновлялись, или на вашем устройстве установлено запрещенное приложение). Критическую проблему скрыть нельзя.

Контроль соответствия

Приложение автоматически проверяет соответствие устройства требованиям корпоративной безопасности. В разделе **Статус** отображается следующая информация о соответствии вашего устройства требованиям корпоративной безопасности:

- содержание несоответствия устройства требованиям корпоративной безопасности (например, на устройстве обнаружены запрещенные приложения);
- время, за которое вы должны устранить несоответствие (например, 24 часа);

- действие, которое будет выполнено с устройством, если вы не устраните несоответствие в течение указанного времени (например, блокирование устройства);
- вариант действия для устранения несоответствия устройства требованиям корпоративной политики.

Значок в строке состояния

После завершения мастера первого запуска приложения значок Kaspersky Endpoint Security появляется в строке состояния.

Значок служит индикатором работы приложения и обеспечивает доступ к главному окну Kaspersky Endpoint Security.

Значок служит индикатором работы Kaspersky Endpoint Security и отражает состояние защиты вашего устройства:

– устройство защищено;

– есть проблемы в защите (например, антивирусные базы устарели или установлено новое непроверенное приложение).

Проверка устройства

Антивирус имеет ряд ограничений:

- При работе Антивируса в рабочем профиле (Приложения с «портфелем», Настройка рабочего профиля Android) невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в рабочем профиле нет доступа к внешней памяти. Информация об обнаруженных объектах отображается в разделе **Статус** приложения. Для устранения обнаруженных во внешней памяти объектов необходимо удалить файл вручную и запустить проверку устройства повторно.
- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

Чтобы запустить проверку устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security в панели быстрого запуска нажмите **Проверка**.
2. Выберите область проверки устройства:
   - **Проверить все устройство**. Приложение проверит всю файловую систему устройства.
   - **Проверить установленные приложения**. Приложение проверит только установленные приложения.
   - **Выборочная проверка**. Приложение проверит выбранную папку или отдельный файл. Вы можете выбрать отдельный объект (папку или файл) или один из следующих разделов памяти устройства:
     - **Память устройства**. Память всего устройства, доступная для чтения. В эту область также входит системный раздел памяти, на котором хранятся файлы операционной системы.
     - **Внутренняя память**. Раздел памяти устройства, предназначенная для установки приложений, хранения медиаконтента, документов и других файлов.

- **Внешняя память**. Память внешней SD-карты. Если внешняя SD-карта не установлена, вариант скрыт.

Доступ к настройкам антивирусной проверки может быть ограничен вашим администратором.

Чтобы настроить антивирусную проверку, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security в панели быстрого запуска нажмите → **Настройки** → **Антивирус** → **Проверка**.

2. Если вы хотите, чтобы во время проверки приложение обнаруживало рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или вашим данным, включите переключатель **Реклама, автодозвон и другое**.

3. Нажмите **Действие при обнаружении угрозы** и выберите действие приложения по умолчанию:

   - **Карантин**

     Карантин хранит файлы в упакованном виде, в котором они не могут нанести вред устройству. Карантин предоставляет возможность удалить или восстановить файлы, помещенные в изолированное хранилище.

   - **Запросить действие**

     Приложение предложит вам выбрать действие для каждого обнаруженного объекта: пропустить, поместить на карантин или удалить. При обнаружении нескольких объектов вы можете применить выбранное действие ко всем объектам.

   - **Удалить**

     Обнаруженные объекты будут удалены автоматически. Никаких дополнительных действий не требуется. Перед удалением Kaspersky Endpoint Security отобразит временное уведомление об обнаружении объекта.

   - **Пропустить**

     Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security предупреждает вас о проблемах в защите устройства. Информация о пропущенных объектах отображается в разделе **Статус** приложения. Для каждой пропущенной угрозы приведены действия, которые вы можете выполнить для ее устранения. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

Информация об обнаруженных угрозах и выполненных над ними действиях записывается в отчеты приложения (→ **Отчеты**). Вы можете выбрать отображение отчетов по работе Антивируса.

Проверка устройства по расписанию

Антивирус имеет ряд ограничений:

- При работе Антивируса в рабочем профиле (Приложения с «портфелем», Настройка рабочего профиля Android) невозможно автоматически устранить угрозу, обнаруженную во внешней памяти устройства (например, на SD-карте). У Kaspersky Endpoint Security для Android в рабочем профиле нет доступа к внешней памяти. Информация об обнаруженных объектах отображается в разделе **Статус** приложения. Для устранения обнаруженных во внешней памяти объектов необходимо удалить файл вручную и запустить проверку устройства повторно.

- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.

Чтобы настроить расписание полной проверки устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security в панели быстрого запуска нажмите → **Настройки** → **Антивирус** → **Проверка**.
2. Нажмите **Расписание** и выберите периодичность запуска полной проверки:
   - **Раз в неделю;**
   - **Раз в день;**
   - **Выключено;**
   - **После обновления баз.**
3. Нажмите **День запуска** и выберите день недели, в который нужно запускать полную проверку.
4. Нажмите **Время запуска** и укажите время запуска полной проверки.

Полная проверка устройства будет запускаться согласно расписанию.

Изменение режима защиты

Постоянная защита позволяет обнаруживать угрозы в открытых файлах, а также проверять приложения во время их установки на устройство в режиме реального времени. Для обеспечения защиты в автоматическом режиме используются антивирусные базы и облачная служба Kaspersky Security Network (Облачная защита).

Чтобы изменить режим защиты устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security в панели быстрого запуска нажмите → **Настройки** → **Антивирус** → **Постоянная защита**.
2. Выберите режим защиты устройства:
   - **Выключена**. Защита выключена.
   - **Рекомендуемый**. Антивирус проверяет только установленные приложения и файлы из папки "Загрузки". Антивирус проверяет новые приложения один раз, сразу после их установки.
   - **Расширенный**. Антивирус проверяет на наличие вредоносных объектов все файлы на устройстве при любом действии с ними (например, сохранении, перемещении или изменении). Также Антивирус проверяет новые приложения сразу после их установки.

Информация о действующем режиме защиты отображается под описанием компонента.

Доступ к настройкам постоянной защиты может быть ограничен вашим администратором.

Чтобы включить Облачную защиту (KSN), выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите → **Настройки** → **Антивирус**.

2. Включите переключатель **Облачная защита (KSN)**.

   Переключатель **Облачная защита (KSN)** управляет использованием Kaspersky Security Network только для постоянной защиты устройства. Если флажок выключен, Kaspersky Endpoint Security продолжает использовать KSN для работы других компонентов приложения.

В результате приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в антивирусные базы, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Антивируса и снижает вероятность ложных срабатываний. Полностью выключить использование Kaspersky Security Network может только ваш администратор.

Чтобы настроить постоянную защиту, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security в панели быстрого запуска нажмите → **Настройки** → **Антивирус** → **Постоянная защита**.

2. Если вы хотите, чтобы во время проверки приложение обнаруживало рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или вашим данным, включите переключатель **Реклама, автодозвон и другое**.

3. Нажмите **Действие при обнаружении угрозы** и выберите действие приложения по умолчанию:

   - **Карантин**

     Карантин хранит файлы в упакованном виде, в котором они не могут нанести вред устройству. Карантин предоставляет возможность удалить или восстановить файлы, помещенные в изолированное хранилище.

   - **Удалить**

     Обнаруженные объекты будут удалены автоматически. Никаких дополнительных действий не требуется. Перед удалением Kaspersky Endpoint Security отобразит временное уведомление об обнаружении объекта.

   - **Пропустить**

     Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security предупреждает вас о проблемах в защите устройства. Информация о пропущенных объектах отображается в разделе **Статус** приложения. Для каждой пропущенной угрозы приведены действия, которые вы можете выполнить для ее устранения. Список пропущенных объектов может измениться, например, если вредоносный файл был удален или перемещен. Чтобы получить актуальный список угроз, запустите полную проверку устройства. Для надежной защиты ваших данных устраните все обнаруженные объекты.

Информация об обнаруженных угрозах и выполненных над ними действиях записывается в отчеты приложения (→ **Настройки** → **Отчеты**). Вы можете выбрать отображение отчетов по работе Антивируса.

Обновление антивирусных баз

Чтобы обновить антивирусные базы приложения,

в главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите **Обновление баз**.

Обновление баз по расписанию

Приложение может автоматически обновлять антивирусные базы по заданному расписанию.

Чтобы настроить расписание обновления, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите → **Настройки** → **Антивирус** → **Обновление баз**.
2. Нажмите **Расписание** и выберите периодичность запуска обновления:
   - **Раз в неделю;**
   - **Раз в день;**
   - **Выключено;**
3. Нажмите **День запуска** и выберите день недели, в который нужно запускать обновление.
4. Нажмите **Время запуска** и укажите время запуска обновления.

Обновление антивирусных баз будет запускаться согласно расписанию.

Действия в случае кражи или потери устройства

В случае кражи или потери устройства обратитесь к системному администратору. Администратор дистанционно запустит на устройстве функции Анти-Вора в соответствии с требованиями корпоративной безопасности.

Если на устройство отправлена команда сброса настроек до заводских, контроль над устройством будет потерян, и остальные команды Анти-Вора выполняться не будут.

Веб-Фильтр

Для работы Веб-Фильтра необходимо выполнение следующих условий:

- Приложение Kaspersky Endpoint Security включено в качестве службы Специальных возможностей.
- Принято Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре). Kaspersky Endpoint Security использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN.

  Администратор вашей сети может принять Положение о Веб-Фильтре в Kaspersky Security Center. В этом случае вам не потребуется выполнять никаких действий.

  Если администратор вашей сети не принял Положение о Веб-Фильтре и направил вам запрос на принятие Положения, прочитайте и примите Положение о Веб-Фильтре в настройках приложения.

  Если администратор вашей сети не принял Положение о Веб-Фильтре, Веб-Фильтр будет недоступен.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome, Huawei Browser и Samsung Internet Browser. В браузере Samsung Internet Browser Веб-Фильтр не блокирует сайты на мобильных устройствах, если используется рабочий профиль и Веб-Фильтр включен только для рабочего профиля.

Для постоянного использования Веб-Фильтра для проверки сайтов во время работы в интернете, назначьте Google Chrome или Samsung Internet Browser браузером по умолчанию.

Чтобы назначить поддерживаемый браузер браузером по умолчанию и использовать Веб-Фильтр для постоянной проверки веб-сайтов, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите → **Настройки** → **Веб-Фильтр**
2. Включите переключатель **Веб-Фильтр**.
3. Нажмите **Установить браузер по умолчанию**. Эта кнопка отображается, если Веб-Фильтр включен, но поддерживаемый браузер не установлен в качестве браузера по умолчанию.

   Запустится мастер выбора браузера по умолчанию.
4. Следуйте указаниям мастера.

В результате работы мастера Google Chrome, Huawei Browser или Samsung Internet Browser будет назначен браузером по умолчанию. Веб-Фильтр будет постоянно проверять веб-сайты во время работы в интернете.

Контроль установленных приложений

Контроль приложений – проверка установленных на мобильное устройство приложений на соответствие требованиям корпоративной безопасности. Администратор создает в Kaspersky Security Center списки разрешенных, запрещенных, обязательных и рекомендованных приложений в соответствии с требованиями корпоративной безопасности. В результате работы Контроля приложений Kaspersky Endpoint Security предложит установить обязательные и рекомендованные приложения, а также удалить запрещенные. Запустить запрещенные приложения на мобильном устройстве невозможно.

Чтобы установить обязательные и рекомендованные приложения или удалить запрещенные, выполните следующие действия:

1. Перейдите в раздел **Статус** Kaspersky Endpoint Security.
2. Выберите задачи Контроля приложений.
3. Выполните предложенные варианты действий.

Получение сертификата

Чтобы получить сертификат для доступа к ресурсам сети организации, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите → **Настройки** → **Дополнительно** → **Получение сертификата**.

2. Укажите ваши учетные данные в сети организации.

3. Если вы получили от администратора одноразовый пароль, установите флажок **Одноразовый пароль** и введите полученный пароль.

   Запустится мастер установки сертификата.

4. Следуйте указаниям мастера.

Синхронизация с Kaspersky Security Center

Синхронизация мобильного устройства с системой удаленного администрирования Kaspersky Security Center необходима для защиты и настройки вашего устройства в соответствии с требованиями корпоративной безопасности. Синхронизация устройства с Kaspersky Security Center выполняется автоматически. Можно также запускать синхронизацию вручную. После первой синхронизации ваше устройство добавляется в список мобильных устройств, управляемых через Kaspersky Security Center. После этого администратор может настраивать ваше устройство в соответствии с требованиями корпоративной безопасности.

Вы можете задать значения параметров синхронизации во время работы мастера первоначальной настройки или в настройках Kaspersky Endpoint Security. Параметры синхронизации требуется настраивать, если вы установили Kaspersky Endpoint Security с помощью Google Play. Для получения значений параметров синхронизации обратитесь к администратору.

Изменяйте параметры синхронизации устройства с системой удаленного администрирования Kaspersky Security Center только по указанию администратора.

Чтобы синхронизировать устройство с Kaspersky Security Center, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите → **Настройки** → **Синхронизация**.

2. В разделе **Параметры синхронизации** укажите значения следующих параметров:

   - **Сервер**
   - **Порт**
   - **Группа**
   - **Адрес корпоративной электронной почты**

   Параметры синхронизации могут быть скрыты администратором.

3. Нажмите **Синхронизировать**.

Обновление приложения

Kaspersky Endpoint Security можно обновить следующими способами:

- Самостоятельно с помощью Google Play. Вы загружаете с Google Play новую версию приложения и устанавливаете приложение на ваше устройство.
- С помощью администратора. Администратор дистанционно обновляет версию приложения на вашем устройстве с помощью системы удаленного администрирования Kaspersky Security Center.

Обновление с помощью Google Play

Администратор может запретить вам обновлять приложение с помощью Google Play.

Обновление с помощью Google Play выполняется обычным способом, принятым для платформы Android. Для обновления приложения должны быть выполнены следующие условия:

- У вас должна быть учетная запись Google;
- Устройство должно быть привязано к учетной записи Google;
- На устройстве должно быть установлено соединение с интернетом.

Подробная информация о создании учетной записи Google, привязке устройства к учетной записи и работе с приложением Google Play Маркет приведена на сайте технической поддержки Google.

Обновление с помощью Kaspersky Security Center

Обновление приложения с помощью Kaspersky Security Center состоит из следующих этапов:

1. Администратор отправляет на ваше мобильное устройство дистрибутив приложения, версия которого удовлетворяет требованиям корпоративной безопасности.

   На мобильном устройстве вы увидите уведомление о необходимости обновить Kaspersky Endpoint Security.

2. Примите условия обновления.

   Новая версия приложения будет установлена на ваше устройство. Дополнительная настройка приложения после обновления не требуется.

Удаление приложения

Администратор может запретить вам самостоятельно удалять приложение. В этом случае удаление Kaspersky Endpoint Security невозможно.

Kaspersky Endpoint Security можно удалить следующими способами:

- Самостоятельно в настройках приложения.
- Самостоятельно в настройках устройства.

- С помощью администратора. Администратор дистанционно удаляет приложение на вашем устройстве с помощью системы удаленного администрирования Kaspersky Security Center.

Удаление в настройках приложения

Чтобы удалить Kaspersky Endpoint Security с вашего устройства, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security на панели быстрого запуска нажмите → **Удалить приложение**.

   Запустится мастер удаления приложения.

2. Следуйте указаниям мастера.

Удаление в настройках устройства

Удаление приложения выполняется обычным способом, принятым для платформы Android. Для удаления приложения требуется выключить права администратора для Kaspersky Endpoint Security в настройках безопасности устройства.

На устройствах под управлением операционной системы Android версии 7.0 и выше, если администратор запретил удаление, при попытке удалить приложение в настройках Android устройство будет заблокировано. Для разблокирования устройства обратитесь к вашему администратору.

Удаление с помощью Kaspersky Security Center

Удаление приложения с помощью Kaspersky Security Center состоит из следующих этапов:

1. Администратор отправляет на ваше мобильное устройство команду удаления приложения.

   На мобильном устройстве вы увидите уведомление с запросом на подтверждение удаления Kaspersky Endpoint Security.

2. Подтвердите удаление приложения.

   Приложение будет удалено с вашего устройства.

Приложения с "портфелем"

Значок приложения в рабочем профиле Android

Приложения, отмеченные значком портфеля (корпоративные приложения), находятся на вашем устройстве в рабочем профиле Android (далее также "Рабочий профиль"). *Рабочий профиль Android* – это безопасная среда на вашем устройстве, в которой администратор может управлять приложениями и учетными записями, не ограничивая ваши возможности работы с персональными данными.

Рабочий профиль позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений. При создании рабочего профиля на вашем устройстве в рабочий профиль автоматически устанавливаются следующие корпоративные приложения: Google Play Маркет, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие.

Приложение KNOX

Значок KNOX

Приложение KNOX открывает KNOX-контейнер на вашем устройстве. *KNOX-контейнер* – безопасная среда на вашем устройстве с отдельным рабочим столом, панелью запуска, приложениями, виджетами. Администратор может управлять приложениями и учетными записями в KNOX-контейнере, не ограничивая ваши возможности работы с персональными данными.

KNOX-контейнер позволяет хранить корпоративные данные отдельно от персональных данных. Это обеспечивает конфиденциальность корпоративных данных и их защиту от вредоносных приложений.

В KNOX-контейнере вам доступны корпоративный почтовый ящик, контактные данные сотрудников организации, хранилище файлов и другие приложения.

Подробная информация о работе с KNOX приведена на *сайте Службы технической поддержки Samsung*.

Нагрузка на сеть

Этот раздел содержит информацию об объеме сетевого трафика, которым обмениваются между собой мобильные устройства и Kaspersky Security Center во время работы.

Расход трафика

Задача	Исходящий трафик	Входящий трафик	Общий трафик
Первоначальное развертывание приложения, МБ	0.08	17.76	17.84
Первоначальное обновление антивирусных баз (объем трафика может отличаться из-за размера антивирусных баз), МБ	0.04	2.21	2.25
Синхронизация мобильного устройства с Kaspersky Security Center, МБ	0.03	0.02	0.05
Регулярное обновление антивирусных баз (объем трафика может отличаться из-за размера антивирусных баз), МБ	0.08	3.06	3.14
Выполнение команд Анти-Вора. Определение местоположения (объем трафика может отличаться из-за характеристик встроенной камеры и качества изображений), МБ	0.09	0.8	0.17
Выполнение команд Анти-Вора. Фотографирование, МБ	1.0	0.02	1.02
Выполнение команд Анти-Вора. Блокировка устройства, МБ	0.06	0.05	0.11
Средний расход за сутки, МБ	0.22	6.96	7.18

Участие в Kaspersky Security Network

Чтобы повысить эффективность защиты мобильных устройств, Kaspersky Endpoint Security для Android использует данные, полученные от пользователей со всего мира. Для обработки этих данных предназначена сеть *Kaspersky Security Network*.

Kaspersky Security Network (KSN) – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Использование данных Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Ваше участие в Kaspersky Security Network позволяет "Лаборатории Касперского" оперативно получать информацию о типах и источниках новых угроз, разрабатывать способы их нейтрализации, уменьшать количество ложных срабатываний Kaspersky Endpoint Security для Android. Кроме того, участие в Kaspersky Security Network обеспечивает доступ к данным о репутации программ и веб-сайтов.

Когда вы участвуете в Kaspersky Security Network, определенная статистика, полученная в результате работы Kaspersky Endpoint Security для Android, автоматически отправляется в "Лабораторию Касперского". Эта информация позволяет отслеживать угрозы в режиме реального времени. Также для дополнительной проверки в "Лабораторию Касперского" могут отправляться файлы (или их части), в отношении которых существует риск использования их злоумышленником для нанесения вреда компьютеру или данным пользователя.

Использование Kaspersky Security Network необходимо для работы Kaspersky Endpoint Security для Android. KSN используется для работы основных компонентов приложения: Антивирус, Веб-Фильтр и Контроль приложений. Отказ от участия в KSN снижает уровень защиты устройства, что может привести к заражению устройства и потере информации. Чтобы начать использование Kaspersky Security Network, вы должны принять условия Лицензионного соглашения при установке приложения. В Лицензионном соглашении вы можете ознакомиться с тем, какие данные Kaspersky Endpoint Security для Android передает в Kaspersky Security Network.

Для повышения качества работы приложения вы можете дополнительно отправлять в Kaspersky Security Network статистические данные. Участие в Kaspersky Security Network для обработки статистических данных является добровольным. Чтобы начать использование Kaspersky Security Network, вы должны принять условия специального соглашения – *Положения о Kaspersky Security Network*. Вы можете в любой момент отказаться от участия в Kaspersky Security Network. В Положении о Kaspersky Security Network вы можете прочитать о том, какие данные Kaspersky Endpoint Security для Android передает в Kaspersky Security Network.

Обмен информацией с Kaspersky Security Network

Для повышения уровня оперативной защиты Kaspersky Security для мобильных устройств использует облачную службу Kaspersky Security Network в работе следующих компонентов:

- **Антивирус.** Приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в антивирусные базы, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Антивируса и снижает вероятность ложных срабатываний.

- **Веб-Фильтр.** Приложение выполняет проверку веб-сайтов до их открытия с учетом данных, полученных от KSN. Также приложение определяет категорию веб-сайта для контроля доступа пользователей в сети

Интернет на основе списков разрешенных и запрещенных категорий (например, категория "Общение в сети").

- **Контроль приложений.** Приложение определяет категорию приложения для ограничения запуска приложения, которые не удовлетворяют требованиям корпоративной безопасности, на основе списков разрешенных и запрещенных категорий (например, категория "Игры").

Информация о типах данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы мобильного приложения Kaspersky Endpoint Security для Android, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать перечисленную ниже информацию. Чтобы установить приложение, пользователь должен принять условия Лицензионного соглашения.

В целях выявления новых и сложных для обнаружения угроз информационной безопасности и их источников, угроз вторжения, а также повышения уровня защиты информации, хранимой и обрабатываемой на устройстве, вы можете расширить участие в Kaspersky Security Network.

Для обмена данными с KSN в целях повышения качества работы приложения должны быть выполнены следующие условия:

- Администратор или пользователь устройства должен прочитать и принять условия Положения о Kaspersky Security Network. Если выбран вариант, при котором Положение принимается пользователями, на главном экране приложения отобразится уведомление с предложением принять условия Положения. Пользователи также могут принять Положение в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

Если выбран вариант, при котором Положения принимаются глобально, версии Положений, принимаемые в Kaspersky Security Center, должны совпадать с версиями, уже принятыми пользователями. В противном случае пользователи будут проинформированы об этой проблеме, и им будет предложено принять ту версию Положения, которая соответствует версии, принятой администратором глобально. Статус устройства в плагине управления Kaspersky Endpoint Security для Android изменится на *Предупреждение*.

- Администратор должен разрешить передачу статистических данных в KSN в настройках групповой политики (см. ниже).

Пользователи могут в любой момент отказаться от отправки статистических данных в KSN. Информация о типах статистических данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы мобильного приложения Kaspersky Endpoint Security для Android, приведена в Положении о Kaspersky Security Network.

Предоставление данных в KSN в рамках Лицензионного соглашения

Если для активации ПО применяется Код активации, с целью проверки правомерности использования ПО Пользователь соглашается периодически предоставлять Правообладателю следующую информацию: тип, версию и локализацию установленного ПО, версии установленных Обновлений ПО, идентификатор Компьютера и идентификатор установки ПО на Компьютере, код активации и уникальный идентификатор активации текущей лицензии, дату и время активации, тип, версию и разрядность операционной системы, название виртуальной среды, если ПО установлено в виртуальной среде, идентификаторы компонентов ПО, активных на момент предоставления информации, веб-адрес и IP-адрес службы активации, контрольную сумму сертификата, тип сертификата и содержание сертификата службы активации.

Для защиты Компьютера от угроз информационной безопасности Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- адрес веб-сайта, посещаемого в текущий момент пользователем, номер порта, протокол передачи данных, адрес веб-сайта, с которого был осуществлен переход;
- информация о проверяемых файлах (имя файла, контрольная сумма (MD5) APK-файла);
- название обнаруженного объекта согласно классификации "Лаборатории Касперского", репутация объекта, дата и время выпуска баз, идентификатор записи антивирусной базы, на основе которой определена репутация объекта;
- имена пакетов мобильных приложений, название интернет-магазина, из которого установлено приложение, открытый ключ и контрольная сумма сертификата, которым подписан APK-файл.

Если получение Обновлений выполняется с серверов обновления Правообладателя, то для целей улучшения качества работы механизма обновления Пользователь соглашается периодически предоставлять Правообладателю следующую информацию: идентификатор, версию и локализацию установленного ПО, идентификаторы обновляемых компонентов ПО, идентификатор установки ПО на компьютере, тип, версию и разрядность операционной системы, уникальный идентификатор запуска задачи обновления, идентификатор текущей лицензии. Правообладатель может также использовать такую информацию для получения статистической информации о распространении и использовании ПО.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год) или по запросу Пользователя. Данные общей статистики хранятся бессрочно.

Предоставление данных в KSN в рамках Положения о Kaspersky Security Network

Использование KSN может повысить эффективность защиты, предоставляемой ПО, от угроз информационной и сетевой безопасности.

Если вы используете лицензию на 5 и более узлов, Правообладатель автоматически получает и обрабатывает следующие данные во время использования KSN:

- Идентификатор сработавшей записи в антивирусных базах ПО; отметка времени сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; дата и время выпуска баз данных ПО; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновлений ОС; характеристики обнаружения; контрольная сумма (MD5) обрабатываемого объекта; название обрабатываемого объекта; флаг, указывающий, является ли обрабатываемый объект PE-файлом; контрольная сумма (MD5) маски, заблокировавшей веб-сервис; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; код типа объекта; решение ПО касательно обрабатываемого объекта; путь к обрабатываемому объекту; код каталога; версия компонента ПО; версия отправляемой статистики; адрес веб-сервиса (URL, IP), к которому осуществлялся доступ; тип клиента, используемого для доступа к веб-сервису; IPv4-адресу веб-сервиса, к которому осуществлялся доступ; IPv6-адресу веб-сервиса, к которому осуществлялся доступ; веб-адрес источника запроса веб-сервиса (referer); обрабатываемый веб-адрес.
- Информация о проверяемых объектах (версия приложения из AndroidManifest.xml; решение ПО касательно приложения; метод, используемый для получения решения ПО касательно приложения; имя пакета установщика магазина; имя пакета (или имя комплекта) из AndroidManifest.xml; категория Google SafetyNet; флаг, указывающий, включен ли SafetyNet на устройстве; значение SHA256 из ответа Google SafetyNet; схема подписи APK для сертификата APK; код версии установленного ПО; серийный номер сертификата, используемого для подписи APK-файла; имя установленного APK-файла; путь к установленному APK-файлу; издатель сертификата, используемого для подписи APK-файла; открытый ключ, используемый для подписи APK-файла; контрольная сумма сертификата, используемого для подписи APK-файла; дата и время истечения срока действия сертификата; дата и время выпуска сертификата; версия отправляемой статистики; алгоритм расчета отпечатка цифрового сертификата; контрольная сумма MD5 установленного APK-файла; MD5-хэш файла DEX, находящегося в APK-файле;

разрешения, динамически предоставляемые приложению; версия стороннего ПО; флаг, показывающий, является ли приложение SMS-мессенджером по умолчанию; флаг, показывающий, есть ли у приложения права администратора устройства; флаг, показывающий, присутствует ли приложение в системном каталоге; флаг, показывающий, использует ли приложение службы специальных возможностей).

- Информация обо всех потенциально вредоносных объектах и действиях (фрагмент содержимого обрабатываемого объекта; дата и время истечения срока действия сертификата; дата и время выпуска сертификата; идентификатор ключа из хранилища ключей, используемого для шифрования; протокол, используемый для обмена данными с KSN; порядок фрагментов в обрабатываемом объекте; данные внутреннего журнала, формируемого антивирусным программным модулем для обрабатываемого объекта; имя издателя сертификата; открытый ключ сертификата; алгоритм расчета открытого ключа сертификата; серийный номер сертификата; дата и время подписания объекта; имя и параметры владельца сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм расчета контрольной суммы; дата и время последнего изменения обрабатываемого объекта; дата и время создания обрабатываемого объекта; обрабатываемые объекты или их части; описание обрабатываемого объекта, как определено в свойствах объекта; формат обрабатываемого объекта; тип контрольной суммы обрабатываемого объекта; контрольная сумма (MD5) обрабатываемого объекта; имя обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; имя поставщика ПО; решение ПО касательно обрабатываемого объекта; версия обрабатываемого объекта; источник решения по обрабатываемому объекту; контрольная сумма обрабатываемого объекта; название родительского приложения; путь к обрабатываемому объекту; информация о результатах проверки подписи файлов; ключ сеанса входа в систему; алгоритм шифрования ключа сеанса входа в систему; время хранения обрабатываемого объекта; алгоритм расчета отпечатка цифрового сертификата).

- Тип сборки, например, "пользователь" или "rus"; полное имя продукта; производитель продукта / оборудования; можно ли установить приложения не из Google Play; статус облачного сервиса для проверки приложений Google; статус облачного сервиса для проверки приложений Google, установленных через ADB; текущее кодовое имя разработки или "REL" для производственных сборок; инкрементный номер сборки; строка версии, отображаемая для пользователя; имя пользовательского устройства; идентификатор сборки ПО, отображаемый для пользователя; отпечаток прошивки; идентификатор прошивки; флаг, указывающий, имеются ли на устройстве root-права; операционная система; название ПО; тип используемой лицензии на ПО.

- Информация о качестве услуг KSN (протокол, используемый для обмена данными с KSN; идентификатор службы KSN, к которой имеет доступ ПО; дата и время прекращения получения статистики; количество подключений к KSN, полученных из кеша; количество запросов, для которых ответ был найден в локальной базе данных запросов; количество неудачных подключений к KSN; количество неудачных транзакций KSN; распределение отмененных запросов к KSN по времени; распределение неудачных подключений к KSN по времени; распределение неудачных транзакций KSN по времени; распределение успешных подключений к KSN по времени; распределение успешных KSN транзакций по времени; распределение успешных запросов к KSN по времени; распределение по времени запросов к KSN, для которых истекло время ожидания; количество новых подключений к KSN; количество неудачных запросов к KSN, вызванных ошибками маршрутизации; количество неудачных запросов, вызванных тем, что KSN отключено в настройках ПО; количество неудачных запросов к KSN, вызванных проблемами сети; количество успешных подключений к KSN; количество успешных транзакций KSN; общее количество запросов к KSN; дата и время начала получения статистики).

- Идентификатор устройства; полная версия ПО; идентификатор обновления ПО; идентификатор установки ПО (PCID); тип установленного ПО.

- Высота экрана устройства; ширина экрана устройства; информация о перекрывающем приложении: MD5-хеш APK-файла; информация о перекрывающем приложении: MD5-хеш файла classes.dex; информация о перекрывающем приложении: имя APK-файла; информация о перекрывающем приложении: путь к APK-файлу без имени файла; высота перекрытия; информация о перекрытом ПО: MD5-хеш APK-файла; информация о перекрытом приложении: MD5-хеш файла classes.dex; информация о перекрытом приложении: имя APK-файла; информация о перекрытом приложении: путь к APK-файлу без имени файла; информация о перекрытом приложении: имя пакета приложения (для перекрытого приложения: если реклама отображается на пустом рабочем столе, значение должно быть "средство запуска"); дата и время

возникновения перекрытия; информация о перекрывающем приложении: имя пакета приложения; ширина перекрытия.

- Параметры используемой точки доступа Wi-Fi (тип обнаруженного устройства; параметры DHCP (контрольные суммы локального IPv6 шлюза, DHCP IPv6, DNS1 IPv6, DNS2 IPv6; контрольная сумма длины префикса сети; контрольная сумма локального адреса IPv6); параметры DHCP (контрольные суммы локального IP-адреса шлюза, DHCP IP, DNS1 IP, DNS2 IP и маски подсети); флаг, показывающий, имеется ли домен DNS; контрольная сумма назначенного локального адреса IPv6; контрольная сумма назначенного локального адреса IPv4; флаг, показывающий, подключено ли устройство; тип аутентификации сети Wi-Fi; список доступных сетей Wi-Fi и их параметры; контрольная сумма (MD5 с солью) MAC-адреса точки доступа; контрольная сумма (SHA256 с солью) MAC-адреса точка доступа; типы подключения, поддерживаемые точкой доступа Wi-Fi; тип шифрования сети Wi-Fi; местное время начала и окончания подключения к сети Wi-Fi; идентификатор сети Wi-Fi на основе MAC-адреса точки доступа; идентификатор сети Wi-Fi на основе имени сети Wi-Fi; идентификатор сети Wi-Fi на основе имени сети Wi-Fi и MAC-адреса точки доступа; мощность сигнала Wi-Fi; имя сети Wi-Fi; набор протоколов аутентификации, поддерживаемых данной конфигурацией; протокол аутентификации, используемый для соединения WPA-EAP; внутренний протокол аутентификации; набор групповых шифров, поддерживаемых данной конфигурацией; набор протоколов управления ключами, поддерживаемых данной конфигурацией; окончательная категория конфиденциальности сети в ПО; окончательная категория безопасности сети в ПО; набор блочных шифров для WPA, поддерживаемых данной конфигурацией; набор протоколов безопасности, поддерживаемых данной конфигурацией).

Также для достижения заявленной цели повышения эффективности защиты, предоставляемой ПО, Правообладатель может получать объекты (файл или его часть, служебная информация), в отношении которых существует риск их использования злоумышленниками для нанесения вреда устройству и создания угроз информационной безопасности.

Участие в Kaspersky Security Network для обработки статистических данных является добровольным.

Чтобы запретить обмен данными с KSN, повышающий эффективность защиты, выполните следующие действия:

1. Откройте окно настройки параметров политики управления мобильными устройствами, на которых установлено приложение Kaspersky Endpoint Security для Android.
2. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
3. В блоке **Передача данных** снимите флажок **Разрешить передачу статистических данных в KSN**.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

   Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Включение и выключение использования Kaspersky Security Network

Kaspersky Security Network используется в Kaspersky Endpoint Security для Android следующими компонентами:

- Антивирус. Приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в антивирусные базы, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Антивируса и снижает вероятность ложных срабатываний.

- Веб-Фильтр. Компонент блокирует вредоносные веб-сайты, цель которых – распространить вредоносный код, а также поддельные (фишинговые) веб-сайты, цель которых – украсть конфиденциальные данные пользователя и получить доступ к его финансовым счетам.

- Контроль приложений (категории приложений). Компонент блокирует запуск приложений из запрещенных категорий.

Для работы компонентов, использующих Kaspersky Security Network, приложение отправляет в облачные службы запросы. Запросы содержит следующие данные:

- данные о проверяемых объектах и действиях над ними (Антивирус);

- адрес веб-сайта, посещаемого в текущий момент пользователем, для определения репутации веб-адреса (Веб-Фильтр);

- имена пакетов мобильных приложений, запускаемых на устройствах пользователей для определения категорий приложений (Контроль приложений).

Если использование Kaspersky Security Network на устройстве выключено, компоненты Облачная защита, Веб-Фильтр и Контроль приложений автоматически выключаются.

Также "Лаборатория Касперского" использует Kaspersky Security Network для получения следующих статистических данных:

- данные о работе приложения Kaspersky Endpoint Security для Android (например, версия приложения Kaspersky Endpoint Security для Android);

- данные для выявления новых и сложных для обнаружения угроз информационной безопасности и их источников (например, результаты антивирусной проверки);

- данные для оптимизации методов проверки и снижения количества ложных срабатываний при проверке установленных приложений и загруженных файлов (например, название установленного приложения).

Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:

1. Откройте окно параметров политики управления мобильными устройствами, на которых установлено приложение Kaspersky Endpoint Security для Android.

2. В политике, в окне **Свойства** выберите раздел **Дополнительно**.

3. В блоке **Параметры Kaspersky Security Network (KSN)** настройте параметры использования Kaspersky Security Network:

   - Установите флажок **Использовать Kaspersky Security Network** для работы следующих компонентов: Антивирус (Облачная защита), Веб-Фильтр, Контроль приложения (категории приложений).

   - Установите флажок **Разрешить передачу статистических данных в KSN** для передачи данных в "Лабораторию Касперского". Данные позволят увеличить скорость реакции приложения Kaspersky Endpoint Security для Android на угрозы, улучшить производительность компонентов защиты, снизить вероятность ложных срабатываний.

4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. После применения политики компоненты, использующие Kaspersky Security Network, будут выключены и настройка компонентов будет недоступна.

Предоставление данных в сервисы Google

Kaspersky Endpoint Security для Android использует сервисы Google™: Firebase Cloud Messaging и Google Analytics для Firebase™. Kaspersky Endpoint Security для Android использует сервис Firebase Cloud Messaging (FCM) для своевременной доставки команд на мобильные устройства и принудительной синхронизации при изменении параметров политики. Kaspersky Endpoint Security для Android использует сервис Google Analytics для Firebase для повышения качества работы приложения и эффективного формирования "Лабораторией Касперского" маркетинговых материалов.

Обмен информацией с Firebase Cloud Messaging

Kaspersky Endpoint Security для Android использует сервис Firebase Cloud Messaging (FCM) для своевременной доставки команд на мобильные устройства и принудительной синхронизации при изменении параметров политики. При этом приложение использует механизм push-уведомлений.

Для использования сервиса Firebase Cloud Messaging необходимо настроить параметры сервиса в Kaspersky Security Center. Подробная информация о настройке Firebase Cloud Messaging в Kaspersky Security Center приведена в *справке Kaspersky Security Center*. Если параметры Firebase Cloud Messaging не настроены, команды на мобильном устройстве и параметры политики будут доставлены на устройства во время синхронизации устройства с Kaspersky Security Center по расписанию, установленному в политике (например, каждые 24 ч.). Т.е. команды и параметры политики будут доставлены с задержкой.

В целях обеспечения основной функциональности продукта Вы соглашаетесь в автоматическом режиме предоставлять в сервис Firebase Cloud Messaging уникальный идентификатор установки приложения (Instance ID), а также следующие данные:

- информация об установленном ПО: версия приложения, идентификатор приложения, версия сборки приложения, название пакета приложения;
- информация о компьютере, на котором установлено ПО: версия ОС, идентификатор устройства, версия сервисов Google;
- информация о FCM: идентификатор приложения в FCM, идентификатор пользователя FCM, версия протокола.

Передача данных в сервисы Firebase осуществляется по защищенному каналу. Доступ к информации и ее защита регулируется соответствующими условиями использования сервисов Firebase: https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

Чтобы запретить обмен информацией с сервисом Firebase Cloud Messaging, выполните следующие действия:

1. В дереве консоли выберите **Управление мобильными устройствами → Мобильные устройства**.
2. В контекстном меню папки **Мобильные устройства** выберите пункт **Свойства**.
3. В окне свойств папки **Мобильные устройства** выберите раздел **Параметры Google Firebase Cloud Messaging**.
4. Нажмите на кнопку **Сбросить параметры**.

Обмен информацией с Google Analytics для Firebase

Если при использовании плагина управления более ранней версии вы включили обмен данными с сервисом Google Analytics, Kaspersky Endpoint Security для Android Service Pack 4 Maintenance Release 3 будет выполнять обмен данными с сервисом Google Analytics для Firebase. Поддержка Google Analytics прекращена.

Kaspersky Security для мобильных устройств выполняет обмен данными с сервисом Google Analytics для Firebase по следующим причинам:

- В целях повышения качества работы приложения.

  Для обмена данными с сервисом Google Analytics для Firebase в целях повышения качества работы приложения должны быть выполнены следующие условия:

  - Администратор или пользователь устройства должен прочитать и принять условия Положения о Kaspersky Security Network. Если выбран вариант, при котором Положение принимается пользователями, на главном экране приложения отобразится уведомление с предложением принять условия Положения. Пользователи также могут принять Положение в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

Если выбран вариант, при котором Положения принимаются глобально, версии Положений, принимаемые в Kaspersky Security Center, должны совпадать с версиями, уже принятыми пользователями. В противном случае пользователи будут проинформированы об этой проблеме, и им будет предложено принять ту версию Положения, которая соответствует версии, принятой администратором глобально. Статус устройства в плагине управления Kaspersky Endpoint Security для Android изменится на *Предупреждение*.

- Администратор должен разрешить передачу статистических данных в KSN в настройках групповой политики (см. ниже).

- В целях эффективного формирования "Лабораторией Касперского" маркетинговых материалов.

  Для обмена данными с сервисом Google Analytics для Firebase в целях эффективного формирования "Лабораторией Касперского" маркетинговых материалов должны быть выполнены следующие условия:

  - Администратор или пользователь устройства должен прочитать и принять условия Положения об обработке данных для маркетинговых целей. Если выбран вариант, при котором Положение принимается пользователями, они могут принять условия Положения при установке приложения или в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

  - Администратор должен разрешить передачу данных в Google Analytics для Firebase в настройках групповой политики (см. ниже).

Предоставление данных в Google Analytics для Firebase в рамках Положения об обработке данных для маркетинговых целей

Правообладатель использует для обработки данных информационные системы третьих лиц. Обработка данных в информационных системах третьих лиц регулируется соответствующими политиками конфиденциальности таких систем. Правообладатель использует следующие сервисы для обработки перечисленных данных:

- Google Analytics для Firebase

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Google Analytics для Firebase для их обработки для заявленных целей:

- данные о приложении (версия приложения, идентификатор приложения, идентификатор приложения в сервисе Firebase, идентификатор экземпляра в сервисе Firebase, название магазина, в котором было куплено приложение, время первого запуска);
- об идентификаторе установки приложения на устройство и способе установки на устройство;
- о регионе и языковой локализации;
- о разрешении экрана устройства;
- данные о получении root-прав пользователем;
- диагностическая информация об устройстве из сервиса SafetyNet Attestation;
- данные об установке Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей;
- данные о переходах между значками приложения;
- данные о протоколе отправки данных в сервис Firebase, его версии и идентификаторе используемого метода отправки данных;
- информация о типе и параметрах события, в отношении которого происходит отправка данных;
- данные о лицензии на приложение, ее наличии, количестве устройств;
- информация о частоте обновления антивирусных баз и синхронизации с Сервером администрирования;
- данные о консоли администрирования (Kaspersky Security Center или сторонних EMM-систем);
- идентификатор Android;
- рекламный идентификатор (Advertising ID);
- информация о пользователе: возрастная категория и пол, идентификатор страны проживания и список интересов;
- информация о компьютере пользователя, на котором установлено ПО: название производителя компьютера, тип компьютера, модель, версия и язык (локаль) операционной системы;
- информация о программах, которые открывались в первый раз в течение последних 7 дней, и о программах, которые открывались в первый раз более 7 дней назад.

Передача данных в сервис Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase доступна по адресу https://firebase.google.com/support/privacy.

- SafetyNet Attestation.

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис SafetyNet Attestation для их обработки для заявленных целей:

- Время проверки устройства;
- Информация о ПО, название и данные о сертификатах ПО;
- Результаты проверки устройства;
- Случайный идентификатор проверки для верификации результатов проверки устройства.

Передача данных в сервис SafetyNet Attestation осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе SafetyNet Attestation доступна по адресу https://policies.google.com/privacy.

Предоставление вышеуказанной информации для обработке в маркетинговых целях является добровольным.

Чтобы запретить обмен данными с сервисом Google Analytics для Firebase, выполните следующие действия:

1. Откройте окно настройки параметров политики управления мобильными устройствами, на которых установлено приложение Kaspersky Endpoint Security для Android.
2. В политике, в окне **Свойства** выберите раздел **Дополнительно**.
3. В блоке **Передача данных** снимите флажок **Разрешить передачу данных в Google Analytics для Firebase**.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

   Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Известные проблемы и рекомендации

Kaspersky Endpoint Security для Android имеет ряд проблем, не критичных для работы.

Известные проблемы при установке программы

- Kaspersky Endpoint Security для Android устанавливается только в основную память устройства.
- На устройствах под управлением Android 7.0 при попытке выключить права администратора для Kaspersky Endpoint Security для Android в настройках устройства может произойти сбой, если для Kaspersky Endpoint Security для Android запрещено наложение поверх других окон. Проблема связана с известным дефектом в Android 7.
- Приложение Kaspersky Endpoint Security для Android на устройствах под управлением Android 7.0 и выше не поддерживает многооконный режим.
- Kaspersky Endpoint Security для Android не работает на Chromebook-устройствах под управлением операционной системы Chrome.
- Kaspersky Endpoint Security для Android не работает на устройствах Samsung с операционной системой Android версии Go Edition.
- При использовании приложения Kaspersky Endpoint Security для Android со сторонними EMM-системами (например, VMWare AirWatch) доступны только компоненты Антивирус и Веб-Фильтр. Администратор может настраивать параметры Антивируса и Веб-Фильтра в консоли EMM-системы. При этом уведомления о работе приложения доступны только в интерфейсе приложения Kaspersky Endpoint Security для Android (Отчеты).

Известные проблемы при обновлении версии приложения

- Вы можете обновить Kaspersky Endpoint Security для Android только до более новой версии приложения. Обновить Kaspersky Endpoint Security для Android до более старой версии невозможно.
- Для обновления Kaspersky Endpoint Security для Android с помощью автономного пакета установки на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников.
- Обновление с помощью Google Play доступно, если Kaspersky Endpoint Security для Android установлен из Google Play. Если приложение установлено другим способом, обновление с помощью Google Play невозможно.
- Можно выполнить обновление с помощью Kaspersky Security Center, если приложение Kaspersky Endpoint Security для Android было установлено с помощью Kaspersky Security Center. Если приложение установлено из Google Play, обновление с помощью Kaspersky Security Center невозможно.

Известные проблемы в работе Антивируса

- Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает такие файлы и не уведомляет вас, если такие файлы были пропущены.
- Для дополнительной проверки устройства на новые угрозы, информация о которых еще не вошла в антивирусные базы, требуется включить использование Kaspersky Security Network. *Kaspersky Security*

Network (KSN) – инфраструктура облачных служб, предоставляющая доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов, веб-ресурсов и программного обеспечения. Для использования KSN требуется подключение мобильного устройства к интернету.

- На некоторых устройствах Kaspersky Endpoint Security для Android не обнаруживает устройства, подключенные по USB OTG. Выполнить антивирусную проверку таких устройств невозможно.

- На устройствах под управлением Android 7.0 и выше может некорректно отображаться окно настройки расписания запуска антивирусной проверки (не отображаются элементы управления). Проблема связана с известным дефектом в Android 7.

- На устройствах под управлением Android 6.0 Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносного файла в память устройства. Вредоносный файл может быть обнаружен Антивирусом при запуске файла или во время антивирусной проверки устройства. Проблема связана с известным дефектом в Android 6.0. Для обеспечения безопасности устройства рекомендуется настроить запуск антивирусной проверки по расписанию.

Известные проблемы в работе Веб-Фильтра

- Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome, Huawei Browser и Samsung Internet Browser. В браузере Samsung Internet Browser Веб-Фильтр не блокирует сайты на мобильных устройствах, если используется рабочий профиль и Веб-Фильтр включен только для рабочего профиля.

- Kaspersky Endpoint Security в рабочем профиле проверяет только домен веб-сайта в HTTPS-трафике. Вредоносные и фишинговые веб-сайты могут оставаться разблокированными, если приложение установлено в рабочем профиле. Если домен является доверенным, Веб-Фильтр может пропустить угрозу (например, `https://trusted.domain.com/phishing/`). Если домен не является доверенным, Веб-Фильтр блокирует вредоносные и фишинговые веб-сайты.

- Для работы Веб-Фильтра требуется включить использование Kaspersky Security Network. Веб-Фильтр блокирует веб-сайты на основе данных о репутации и категории веб-сайтов, которые содержатся в KSN.

- На устройствах под управлением Android 6.0 с установленным браузером Google Chrome версии 51 или более ранних версий запрещенные веб-сайты могут не блокироваться Веб-Фильтром, если веб-сайт открыт следующими способами (проблема связана с известным дефектом в Google Chrome):

  - из результатов поискового запроса;
  - из списка закладок;
  - из истории поисковых запросов;
  - при использовании функции автозаполнения веб-адреса;
  - при открытии веб-сайта на новой вкладке в Google Chrome.

- Запрещенные веб-сайты могут не блокироваться в браузере Google Chrome версии 50 или более ранних версий, если веб-сайт открыт из результатов поискового запроса Google и в настройках браузера включена функция **Объединить вкладки и приложения**. Проблема связана с известным дефектом в Google Chrome.

- Веб-сайты из запрещенных категорий могут не блокироваться в Google Chrome, если пользователь открывает их из сторонних приложений, например, из приложения IM-клиента. Проблема связана с особенностями работы службы Специальных возможностей с функцией Chrome Custom Tabs.

- Запрещенные веб-сайты могут не блокироваться в Samsung Internet Browser, если пользователь открывает их в фоновом режиме из контекстного меню или из сторонних приложений, например, из приложения IM-клиента.

- Для работы Веб-Фильтра Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.

- При вводе адреса веб-сайта в параметрах Веб-Фильтра соблюдайте следующие правила:

  - Для Android-устройств указывайте адрес в формате регулярных выражений (например, `http:\/\/www\.example\.com.*`).

  - Для iOS MDM-устройств указывайте протокол передачи данных HTTP или HTTPS (например, `http://www.example.com`).

- Разрешенные веб-сайты могут блокироваться в Samsung Internet Browser в режиме Веб-Фильтра **Разрешить только перечисленные веб-сайты** при обновлении страницы. Веб-сайты блокируются, если регулярное выражение содержит дополнительные параметры (например, `^https?:\/\/example\.com\/pictures\/`). Рекомендуется использовать регулярные выражения без дополнительных параметров (например, `^https?:\/\/example\.com`).

Известные проблемы в работе Анти-Вора

- Для своевременной доставки команд на Android-устройства приложение использует сервис Firebase Cloud Messaging (FCM). Если FCM не настроен, команды будут доставлены на устройство только при синхронизации с Kaspersky Security Center по расписанию, заданному в политике, например, каждые 24 часа.

- Для блокирования устройства Kaspersky Endpoint Security для Android должен быть установлен в качестве администратора устройства.

- На устройствах под управлением операционной системы Android версии 7.0 и выше для блокирования устройства Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.

- На некоторых устройствах команды Анти-Вора не могут быть выполнены, если на устройстве включен режим энергосбережения. Этот дефект подтвержден на Alcatel 5080X.

- Чтобы определить местоположение устройства с операционной системой Android 10.0 и выше, необходимо предоставить разрешение "Всегда" для доступа к местоположению устройства.

- Чтобы выполнить снимок с помощью устройства с операционной системой Android 11.0 и выше, необходимо предоставить разрешение "При использовании приложения" для доступа к камере.

Известные проблемы в работе Контроля приложений

- Для работы Контроля приложений на мобильных устройствах под управлением операционной системы Android версии 5.0 и выше Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.

- Для работы Контроля приложений (категории приложений) требуется включить использование Kaspersky Security Network. Контроль приложений определяет категорию приложения на основе данных, которые содержатся в KSN. Для использования KSN требуется подключение мобильного устройства к интернету. Для работы Контроля приложений вы можете добавить отдельные приложения в списки запрещенных и разрешенных приложений. В этом случае KSN не требуется.

- При настройке Контроля приложений рекомендуется снять флажок **Блокировать системные приложения**. Блокировка системных приложений может привести к сбоям в работе устройства.

Известные проблемы при настройке электронной почты

Дистанционная настройка почтового ящика доступна только на следующих устройствах:

- iOS MDM-устройства;
- Samsung-устройства под управлением операционной системы Android версии 5.0 или выше (Exchange ActiveSync);
- Android-устройства с установленным почтовым клиентом TouchDown.

В предыдущих версиях Kaspersky Endpoint Security для Android вы можете удаленно настраивать параметры профиля TouchDown на устройстве пользователя с помощью Kaspersky Security Center. В Kaspersky Endpoint Security для Android Service Pack 4 поддержка TouchDown прекращена. Более подробная информация приведена на *сайте Службы технической поддержки Symantec*.

После обновления плагина управления Kaspersky Endpoint Security для Android параметры TouchDown в политике будут скрыты, но сохранены. При подключении новых устройств параметры TouchDown будут настроены после применения политики.

После изменения и сохранения политики параметры TouchDown будут удалены. Параметры TouchDown на устройствах пользователей будут сброшены после применения политики.

Известные проблемы при настройке надежности пароля разблокировки устройства

- На устройствах под управлением Android 10.0 и выше Kaspersky Endpoint Security приводит требования надежности пароля к одному из системных значений: средний или высокий.

  Если требуемая длина пароля составляет от 1 до 4 символов, приложение предлагает пользователю установить пароль средней надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей (например, 1234), либо буквенно-цифровым. PIN-код или пароль должны состоять не менее чем из 4 символов.

  Если требуемая длина пароля составляет не менее 5 символов, приложение предлагает пользователю установить пароль высокой надежности. Он должен быть либо цифровым (PIN-код) без повторяющихся или упорядоченных последовательностей, либо буквенно-цифровым (пароль). PIN-код должен состоять не менее чем из 8 цифр; пароль должен состоять не менее чем из 6 символов.

- На устройствах под управлением Android 10.0 и выше управлять использованием отпечатка пальца для разблокировки экрана можно только в рабочем профиле.

- На устройствах под управлением Android 7.1.1 при несоответствии пароля разблокировки требованиям корпоративной безопасности (Контроль соответствия) системное приложение Настройки может работать некорректно при попытке изменить пароль разблокировки из Kaspersky Endpoint Security для Android. Проблема связана с известным дефектом в Android 7.1.1. Для изменения пароля разблокировки в этом случае используйте только системное приложение Настройки.

- На некоторых устройствах под управлением Android 6.0 и выше может произойти сбой при вводе пароля разблокировки экрана, если данные на устройстве зашифрованы. Проблема связана с особенностями

работы Службы специальных возможностей на устройствах с прошивкой MIUI.

Известные проблемы, связанные с рабочим профилем Android

Использование рабочих профилей Android доступно только на устройствах под управлением операционной системы Android версии 5.0 или выше.

Известные проблемы при настройке Wi-Fi

На устройствах с операционной системой Android версии 8.0 или выше настроить параметры прокси-сервера для сети Wi-Fi с помощью политики невозможно. Вы можете настроить параметры прокси-сервера для сети Wi-Fi на мобильном устройстве вручную.

Известные проблемы при настройке APN

- Дистанционная настройка APN доступна только на iOS MDM-устройствах или Samsung-устройствах под управлением операционной системы Android версии 5.0 или выше.
- Настраивайте APN для iOS MDM-устройств в разделе **Сотовая связь**. Раздел **APN** устарел. Перед настройкой параметров APN убедитесь, что флажок **Применить на устройстве** в разделе **APN** снят.

Известные проблемы при работе с сетевым экраном

Использование Сетевого экрана доступно только на Samsung-устройствах под управлением операционной системы Android версии 5.0 или выше.

Известные проблемы при настройке VPN

Дистанционная настройка VPN доступна только на следующих устройствах:

- iOS MDM-устройства;
- Samsung-устройства под управлением операционной системы Android версии 5.0 или выше.

Известные проблемы при работе с контейнерами

- В Kaspersky Security для мобильных устройств Service Pack 3 Maintenance Release 2 поддержка создания контейнеров для мобильных приложений прекращена. Однако вы можете добавлять на Android-устройства контейнеры, созданные в более ранних версиях программы.
- Для установки приложений в контейнерах на мобильном устройстве пользователя должна быть разрешена установка приложений из неизвестных источников. Подробная информация об установке приложений без использования Google Play приведена в *справке Android*.
- Не поддерживается контейнеризация приложений для Android-устройств, содержащих более 65,536 методов (multidex configuration).

Известные проблемы, связанные с защитой от удаления приложения

- Kaspersky Endpoint Security для Android должен быть установлен в качестве администратора устройства.

- На устройствах под управлением операционной системы Android версии 7.0 и выше для защиты приложения от удаления Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей.

Известные проблемы, связанные с определенными моделями устройств

- На некоторых устройствах (например, Huawei, Meizu, Xiaomi) требуется предоставить приложению Kaspersky Endpoint Security для Android разрешение на автоматический запуск или вручную добавить его в список приложений, запускаемых при загрузке операционной системы. Если приложение не добавлено в список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства. Также, если устройство было заблокировано, разблокировать устройство с помощью команды невозможно. Вы можете разблокировать устройство только с помощью одноразового кода разблокировки.

- На некоторых устройствах (например, Meizu, Asus) под управлением Android 6.0 и выше после шифрования данных и перезагрузки устройства Android требует ввести цифровой пароль для разблокировки устройства. Если пользователь использует графический пароль для разблокировки, требуется перевести графический пароль в цифровой. Подробнее о переводе графического пароля в цифровой см. на сайте Службы технической поддержки компании-производителя мобильного устройства. Проблема связана с особенностями работы службы Специальных возможностей.

- На некоторых Huawei-устройствах под управлением Android 5.X после установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей отображается неверное сообщение об отсутствии этих прав. Чтобы скрыть это сообщение, включите приложение как защищенное в настройках устройства.

- На некоторых Huawei-устройствах под управлением Android 5.X и 6.X при включенном режиме энергосбережения для Kaspersky Endpoint Security для Android пользователь может самостоятельно завершить работу приложения. При этом устройство пользователя не защищено. Проблема связана с особенностями программного обеспечения Huawei. Чтобы восстановить защиту устройства, запустите Kaspersky Endpoint Security для Android вручную. Рекомендуется отключить режим энергосбережения для приложения Kaspersky Endpoint Security для Android в настройках устройства.

- На Huawei-устройствах с прошивкой EMUI под управлением Android 7.0 пользователь может скрыть уведомление о статусе защиты Kaspersky Endpoint Security для Android. Проблема связана с особенностями программного обеспечения Huawei.

- На некоторых Xiaomi-устройствах при установке в политике длины пароля больше 5 символов пользователю будет предложено изменить пароль разблокировки экрана, а не PIN-код. Установить PIN-код длиной более 5 символов невозможно. Проблема связана с особенностями программного обеспечения Xiaomi.

- На Xiaomi-устройствах с прошивкой MIUI под управлением Android 6.0 значок Kaspersky Endpoint Security для Android в строке состояния может быть скрыт. Проблема связана с особенностями программного обеспечения Xiaomi. Рекомендуется разрешить отображение значков уведомлений в настройках уведомлений.

- На некоторых Nexus-устройствах под управлением Android 6.0.1 во время работы мастера первоначальной настройки Kaspersky Endpoint Security для Android невозможно выдать необходимые права для корректной работы. Проблема связана с известным дефектом в Security Patch для Android от Google. Для корректной работы приложения требуется вручную выдать необходимые права в настройках устройства.

- На некоторых Samsung-устройствах под управлением операционной системы Android 7.0 и выше при попытке пользователя настроить неподдерживаемые способы разблокировки устройства (например, графический пароль) устройство может быть заблокировано, если выполнены следующие условия:

включена защита Kaspersky Endpoint Security для Android от удаления и заданы требования к надежности пароля разблокировки экрана. Для разблокировки устройства требуется отправить на устройство специальную команду.

- На некоторых Samsung-устройствах невозможно запретить использование отпечатков пальцев для разблокировки экрана.

- На некоторых Samsung-устройствах под управлением операционной системы Android 5.0 и выше не работает Веб-Фильтр, если устройство подключено к сети 3G/4G, на устройстве включен режим энергосбережения и ограничены фоновые данные. Рекомендуется выключить функцию отключения фоновых процессов в настройках режима энергосбережения.

- Также на некоторых Samsung-устройствах при несоответствии пароля разблокировки требованиям корпоративной безопасности Kaspersky Endpoint Security для Android не запрещает использование отпечатков пальцев для разблокировки экрана.

- На некоторых Samsung-устройствах после выполнения команд Анти-Вора (поиск, блокирование, разблокирование и фотографирование) общий сертификат и VPN-сертификат могут удалиться. Для продолжения работы требуется заново установить сертификаты. Проблема связана со стандартом безопасности MDFPP (Mobile Device Fundamentals Protection Profile).

- На некоторых Samsung-устройствах под управлением Android 4.4 невозможно изменять язык ввода на стандартной клавиатуре Samsung, если Kaspersky Endpoint Security для Android не установлен в качестве службы Специальных возможностей.

- На мобильном устройстве Samsung S3 Neo GT-I9310(x) под управлением Android 4.4.2 недоступны функции Анти-Вора. Проблема связана с известным дефектом в системном программном обеспечении Samsung.

- На мобильном устройстве Huawei P20 невозможно ограничить использование Bluetooth. При попытке приложения Kaspersky Endpoint Security для Android ограничить использование Bluetooth операционная система показывает уведомление с вариантами действий: отклонить или разрешить это ограничение. Таким образом, пользователь может отклонить ограничение и продолжить использование Bluetooth. Проблема связана с особенностями прошивки EMUI.

- На некоторых устройствах Xiaomi и Huawei защита Kaspersky Endpoint Security для Android от удаления не работает. Проблема связана с особенностями прошивки MIUI на Xiaomi и прошивки EMUI на Huawei.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security для мобильных устройств.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать Kaspersky Security для мобильных устройств.

Рекомендуется внимательно ознакомиться с условиями и положениями Лицензионного соглашения перед началом работы с Kaspersky Security для мобильных устройств.

Условия и положения Лицензионного соглашения можно посмотреть следующими способами:

- Во время установки компонентов Kaspersky Security для мобильных устройств.
- Прочитав документ license.txt. Документ включен в комплект поставки Kaspersky Security для мобильных устройств.
- В разделе **О приложении** в Kaspersky Endpoint Security для Android.
- В разделе **Дополнительно → Принятые лицензионные соглашения** в свойствах Сервера администрирования. Эта функция доступна в Kaspersky Security Center версии 12.1.

Вы принимаете условия и положения Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки компонентов Kaspersky Security для мобильных устройств. Если вы не согласны с условиями Лицензионного соглашения, следует прервать установку компонентов Kaspersky Security для мобильных устройств и отказаться от их использования.

О лицензии

Лицензия – это ограниченное по времени право на использование комплексного решения Kaspersky Security для мобильных устройств, предоставляемое вам на основе Лицензионного соглашения.

Лицензия включает в себя право на получение следующих видов услуг:

- использование приложений на мобильных устройствах в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Объем предоставляемых услуг и срок использования мобильных приложений зависят от типа лицензии, по которой были активированы приложения.

Предусмотрены следующие типы лицензий:

- *Пробная* – бесплатная лицензия, предназначенная для ознакомления с Kaspersky Security для мобильных устройств.

Пробная лицензия имеет срок 30 дней. По истечении срока действия пробной лицензии мобильное приложение Kaspersky Endpoint Security для Android прекращает выполнять все свои функции кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

- *Коммерческая* – платная лицензия, предоставляемая при приобретении Kaspersky Security для мобильных устройств.

  По истечении срока действия коммерческой лицензии мобильное приложение продолжает работу, но с ограниченной функциональностью. В режиме ограниченной функциональности в приложении Kaspersky Endpoint Security для Android доступны следующие компоненты:

  - **Антивирус**: постоянная защита и антивирусная проверка устройства, но обновление антивирусных баз недоступно.
  - **Анти-Вор**: отправка команд на мобильное устройство.
  - **Синхронизация с Сервером администрирования**.

  Остальные компоненты приложения Kaspersky Endpoint Security для Android недоступны пользователю устройства. Администратор может управлять этими компонентами в режиме ограниченной функциональности с помощью групповых политик. Настроить остальные компоненты приложения с помощью групповых политик невозможно.

Приложение Kaspersky Endpoint Security для Android прекращает обмен информацией с Kaspersky Security Network и Google Analytics для Firebase в случае блокировки ключа "Лабораторией Касперского", по истечении срока действия пробной лицензии и при отсутствии лицензии (код активации удален из групповой политики).

Чтобы продолжить использование приложения в режиме полной функциональности, вам нужно продлить срок действия коммерческой лицензии. Рекомендуется продлевать срок действия лицензии или приобретать новую лицензию не позднее даты ее окончания, чтобы обеспечить максимальную защиту от всех угроз компьютерной безопасности.

О подписке

Подписка на Kaspersky Security для мобильных устройств – это заказ на использование мобильного приложения с выбранными параметрами (дата окончания подписки, количество защищаемых мобильных устройств). Подписку на Kaspersky Security для мобильных устройств можно зарегистрировать у поставщика услуг (например, у интернет-провайдера). Подписку можно продлевать вручную или в автоматическом режиме, или отказаться от нее. Управление подпиской доступно на веб-сайте поставщика услуг.

Подписка может быть ограниченной (например, на один год) или неограниченной (без даты окончания). Для продолжения работы Kaspersky Security для мобильных устройств после окончания ограниченной подписки ее требуется продлевать. Неограниченная подписка продлевается автоматически при условии своевременного внесения предоплаты поставщику услуг.

Если подписка ограничена, по ее истечении может предоставляться льготный период для продления подписки, в течение которого функциональность приложений сохраняется. Наличие и длительность льготного периода определяет поставщик услуг.

Чтобы использовать Kaspersky Security для мобильных устройств по подписке, требуется применить код активации, предоставленный поставщиком услуг. После применения кода активации устанавливается ключ для лицензии на использование приложений по подписке.

В зависимости от поставщика услуг, наборы возможных действий для управления подпиской могут различаться. Поставщик услуг может не предоставлять льготный период для продления подписки, в течение которого функциональность приложений сохраняется.

Коды активации, приобретенные по подписке, не могут быть использованы для активации предыдущих версий Kaspersky Security для мобильных устройств.

О ключе

Ключ – последовательность битов, с помощью которой вы можете активировать и затем использовать комплексное решение Kaspersky Security для мобильных устройств в соответствии с условиями Лицензионного соглашения. Ключ создается специалистами "Лаборатории Касперского".

Вы можете добавить ключ в мобильное приложение с помощью файла ключа или кода активации:

- Если в вашей организации развернут программный комплекс Kaspersky Security Center, требуется применить файл ключа и распространить его на мобильные приложения. Ключ отображается в интерфейсе Kaspersky Security Center и интерфейсе мобильного приложения в виде уникальной буквенно-цифровой последовательности.

- Если ваша организация не использует программный комплекс Kaspersky Security Center, требуется добавить код активации в дистрибутив мобильного приложения. Ключ отображается в интерфейсе мобильного приложения в виде уникальной буквенно-цифровой последовательности, после того как вы добавили его в программу.

После добавления ключей вы можете заменять их другими.

Ключ может быть заблокирован "Лабораторией Касперского", если, например, условия Лицензионного соглашения нарушены. Если ключ заблокирован, мобильное приложение Kaspersky Endpoint Security для Android прекращает выполнять все свои функции, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно добавить другой ключ.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий Kaspersky Endpoint Security для Android. Вы получаете код активации по указанному вами адресу электронной почты после приобретения комплексного решения Kaspersky Security для мобильных устройств или после заказа пробной версии Kaspersky Security для мобильных устройств.

Чтобы активировать мобильное приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского".

Если код активации был потерян после активации мобильного приложения, вы можете восстановить код активации. Вам может потребоваться код активации, например, для регистрации в Kaspersky CompanyAccount. Для восстановления кода активации требуется обратиться в Службу технической поддержки "Лаборатории Касперского".

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего мобильные приложения.

Вы получаете файл ключа по указанному вами адресу электронной почты после приобретения комплексного решения Kaspersky Security для мобильных устройств или после заказа пробной версии Kaspersky Security для мобильных устройств.

Чтобы активировать приложения с помощью файла ключа, не требуется подключение к серверам активации "Лаборатории Касперского".

Если файл ключа был случайно удален, вы можете его восстановить. Файл ключа может потребоваться вам, например, для регистрации в Kaspersky CompanyAccount.

Для восстановления файла ключа вам нужно выполнить одно из следующих действий:

- Обратиться к продавцу лицензии;
- Получить файл ключа на веб-сайте "Лаборатории Касперского" с помощью имеющегося кода активации.

Принятие дополнительных Положений глобально администратором

Чтобы включить защиту, обеспечиваемую Kaspersky Endpoint Security для Android, необходимо принять условия Лицензионного соглашения и дополнительных Положений (см. ниже). Для этого необходимо настроить политику для принятия перечисленных ниже Положений глобально для всех пользователей. Пользователям не будет предложено читать и принимать условия следующих Соглашений и Положений, принятых глобально:

- Положение о Kaspersky Security Network.
- Положение об обработке данных для использования Веб-Фильтра.
- Положение об обработке данных для маркетинговых целей.

Если выбран вариант, при котором Положения принимаются глобально, версии Положений, принимаемые в Kaspersky Security Center, должны совпадать с версиями, уже принятыми пользователями. В противном случае пользователи будут проинформированы об этой проблеме, и им будет предложено принять ту версию Положения, которая соответствует версии, принятой администратором глобально. Статус устройства в плагине управления Kaspersky Endpoint Security для Android изменится на *Предупреждение*.

Чтобы выбрать, как должны приниматься условия Положений: глобально или пользователями путем применения групповой политики, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Дополнительно**.

5. В разделе **Передача данных** выберите, как будет приниматься Положение об обработке данных в маркетинговых целях: глобально администратором или пользователями.

6. В разделе **Параметры Kaspersky Security Network (KSN)** выберите, как будет приниматься Положение о Kaspersky Security Network: глобально администратором или пользователями.

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Пользователь может в любой момент принять условия Положения или отказаться от них в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

Предоставление данных

Kaspersky Security для мобильных устройств соответствует Общим нормам защиты данных (GDPR).

Чтобы установить приложение, администратору или пользователю устройства необходимо прочитать и принять условия Лицензионного соглашения. Можно также настроить политику для принятия перечисленных ниже Положений глобально для всех пользователей. В противном случае у пользователей на главном экране приложения будет отображаться уведомление с предложением принять следующие Положения об обработке персональных данных:

- Положение о Kaspersky Security Network.
- Положение об обработке данных для использования Веб-Фильтра.
- Положение об обработке данных для маркетинговых целей.

Если выбран вариант, при котором Положения принимаются глобально, версии Положений, принимаемые в Kaspersky Security Center, должны совпадать с версиями, уже принятыми пользователями. В противном случае пользователи будут проинформированы об этой проблеме, и им будет предложено принять ту версию Положения, которая соответствует версии, принятой администратором глобально. Статус устройства в плагине управления Kaspersky Endpoint Security для Android изменится на *Предупреждение*.

Пользователь может в любой момент принять условия Положения или отказаться от них в разделе **О приложении** в настройках Kaspersky Endpoint Security для Android.

Предоставление данных в рамках Лицензионного соглашения

Для повышения уровня оперативной защиты Kaspersky Security для мобильных устройств использует облачную службу Kaspersky Security Network в работе следующих компонентов:

- **Антивирус.** Приложение получает доступ к оперативной базе знаний "Лаборатории Касперского" о репутации файлов и приложений. Проверка производится на угрозы, информация о которых еще не вошла в антивирусные базы, но уже содержится в KSN. Облачная служба Kaspersky Security Network обеспечивает полноценную работу Антивируса и снижает вероятность ложных срабатываний.
- **Веб-Фильтр.** Приложение выполняет проверку веб-сайтов до их открытия с учетом данных, полученных от KSN. Также приложение определяет категорию веб-сайта для контроля доступа пользователей в сети Интернет на основе списков разрешенных и запрещенных категорий (например, категория "Общение в сети").

- **Контроль приложений.** Приложение определяет категорию приложения для ограничения запуска приложения, которые не удовлетворяют требованиям корпоративной безопасности, на основе списков разрешенных и запрещенных категорий (например, категория "Игры").

Информация о типах данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы мобильного приложения Kaspersky Endpoint Security для Android, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать перечисленную ниже информацию.

Если для активации ПО применяется Код активации, с целью проверки правомерности использования ПО Пользователь соглашается периодически предоставлять Правообладателю следующую информацию: тип, версию и локализацию установленного ПО, версии установленных Обновлений ПО, идентификатор Компьютера и идентификатор установки ПО на Компьютере, код активации и уникальный идентификатор активации текущей лицензии, дату и время активации, тип, версию и разрядность операционной системы, название виртуальной среды, если ПО установлено в виртуальной среде, идентификаторы компонентов ПО, активных на момент предоставления информации, веб-адрес и IP-адрес службы активации, контрольную сумму сертификата, тип сертификата и содержание сертификата службы активации.

Для защиты Компьютера от угроз информационной безопасности Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- адрес веб-сайта, посещаемого в текущий момент пользователем, номер порта, протокол передачи данных, адрес веб-сайта, с которого был осуществлен переход;
- информация о проверяемых файлах (имя файла, контрольная сумма (MD5) APK-файла);
- название обнаруженного объекта согласно классификации "Лаборатории Касперского", репутация объекта, дата и время выпуска баз, идентификатор записи антивирусной базы, на основе которой определена репутация объекта;
- имена пакетов мобильных приложений, название интернет-магазина, из которого установлено приложение, открытый ключ и контрольная сумма сертификата, которым подписан APK-файл.

Если получение Обновлений выполняется с серверов обновления Правообладателя, то для целей улучшения качества работы механизма обновления Пользователь соглашается периодически предоставлять Правообладателю следующую информацию: идентификатор, версию и локализацию установленного ПО, идентификаторы обновляемых компонентов ПО, идентификатор установки ПО на компьютере, тип, версию и разрядность операционной системы, уникальный идентификатор запуска задачи обновления, идентификатор текущей лицензии. Правообладатель может также использовать такую информацию для получения статистической информации о распространении и использовании ПО.

Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями. Исходная полученная информация хранится в зашифрованном виде и уничтожается по мере накопления (два раза в год) или по запросу Пользователя. Данные общей статистики хранятся бессрочно.

Предоставление данных в рамках Положения о Kaspersky Security Network

Использование KSN может повысить эффективность защиты, предоставляемой ПО, от угроз информационной и сетевой безопасности.

Если вы используете лицензию на 5 и более узлов, Правообладатель автоматически получает и обрабатывает следующие данные во время использования KSN:

- Идентификатор сработавшей записи в антивирусных базах ПО; отметка времени сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; дата и время выпуска баз данных ПО; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация

о редакции ОС; версия пакета обновлений ОС; характеристики обнаружения; контрольная сумма (MD5) обрабатываемого объекта; название обрабатываемого объекта; флаг, указывающий, является ли обрабатываемый объект PE-файлом; контрольная сумма (MD5) маски, заблокировавшей веб-сервис; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; код типа объекта; решение ПО касательно обрабатываемого объекта; путь к обрабатываемому объекту; код каталога; версия компонента ПО; версия отправляемой статистики; адрес веб-сервиса (URL, IP), к которому осуществлялся доступ; тип клиента, используемого для доступа к веб-сервису; IPv4-адресу веб-сервиса, к которому осуществлялся доступ; IPv6-адресу веб-сервиса, к которому осуществлялся доступ; веб-адрес источника запроса веб-сервиса (referer); обрабатываемый веб-адрес.

- Информация о проверяемых объектах (версия приложения из AndroidManifest.xml; решение ПО касательно приложения; метод, используемый для получения решения ПО касательно приложения; имя пакета установщика магазина; имя пакета (или имя комплекта) из AndroidManifest.xml; категория Google SafetyNet; флаг, указывающий, включен ли SafetyNet на устройстве; значение SHA256 из ответа Google SafetyNet; схема подписи APK для сертификата APK; код версии установленного ПО; серийный номер сертификата, используемого для подписи APK-файла; имя установленного APK-файла; путь к установленному APK-файлу; издатель сертификата, используемого для подписи APK-файла; открытый ключ, используемый для подписи APK-файла; контрольная сумма сертификата, используемого для подписи APK-файла; дата и время истечения срока действия сертификата; дата и время выпуска сертификата; версия отправляемой статистики; алгоритм расчета отпечатка цифрового сертификата; контрольная сумма MD5 установленного APK-файла; MD5-хэш файла DEX, находящегося в APK-файле; разрешения, динамически предоставляемые приложению; версия стороннего ПО; флаг, показывающий, является ли приложение SMS-мессенджером по умолчанию; флаг, показывающий, есть ли у приложения права администратора устройства; флаг, показывающий, присутствует ли приложение в системном каталоге; флаг, показывающий, использует ли приложение службы специальных возможностей).

- Информация обо всех потенциально вредоносных объектах и действиях (фрагмент содержимого обрабатываемого объекта; дата и время истечения срока действия сертификата; дата и время выпуска сертификата; идентификатор ключа из хранилища ключей, используемого для шифрования; протокол, используемый для обмена данными с KSN; порядок фрагментов в обрабатываемом объекте; данные внутреннего журнала, формируемого антивирусным программным модулем для обрабатываемого объекта; имя издателя сертификата; открытый ключ сертификата; алгоритм расчета открытого ключа сертификата; серийный номер сертификата; дата и время подписания объекта; имя и параметры владельца сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм расчета контрольной суммы; дата и время последнего изменения обрабатываемого объекта; дата и время создания обрабатываемого объекта; обрабатываемые объекты или их части; описание обрабатываемого объекта, как определено в свойствах объекта; формат обрабатываемого объекта; тип контрольной суммы обрабатываемого объекта; контрольная сумма (MD5) обрабатываемого объекта; имя обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; имя поставщика ПО; решение ПО касательно обрабатываемого объекта; версия обрабатываемого объекта; источник решения по обрабатываемому объекту; контрольная сумма обрабатываемого объекта; название родительского приложения; путь к обрабатываемому объекту; информация о результатах проверки подписи файлов; ключ сеанса входа в систему; алгоритм шифрования ключа сеанса входа в систему; время хранения обрабатываемого объекта; алгоритм расчета отпечатка цифрового сертификата).

- Тип сборки, например, "пользователь" или "rus"; полное имя продукта; производитель продукта / оборудования; можно ли установить приложения не из Google Play; статус облачного сервиса для проверки приложений Google; статус облачного сервиса для проверки приложений Google, установленных через ADB; текущее кодовое имя разработки или "REL" для производственных сборок; инкрементный номер сборки; строка версии, отображаемая для пользователя; имя пользовательского устройства; идентификатор сборки ПО, отображаемый для пользователя; отпечаток прошивки; идентификатор прошивки; флаг, указывающий, имеются ли на устройстве root-права; операционная система; название ПО; тип используемой лицензии на ПО.

- Информация о качестве услуг KSN (протокол, используемый для обмена данными с KSN; идентификатор службы KSN, к которой имеет доступ ПО; дата и время прекращения получения статистики; количество подключений к KSN, полученных из кеша; количество запросов, для которых ответ был найден в локальной базе данных запросов; количество неудачных подключений к KSN; количество неудачных транзакций KSN;

распределение отмененных запросов к KSN по времени; распределение неудачных подключений к KSN по времени; распределение неудачных транзакций KSN по времени; распределение успешных подключений к KSN по времени; распределение успешных KSN транзакций по времени; распределение успешных запросов к KSN по времени; распределение по времени запросов к KSN, для которых истекло время ожидания; количество новых подключений к KSN; количество неудачных запросов к KSN, вызванных ошибками маршрутизации; количество неудачных запросов, вызванных тем, что KSN отключено в настройках ПО; количество неудачных запросов к KSN, вызванных проблемами сети; количество успешных подключений к KSN; количество успешных транзакций KSN; общее количество запросов к KSN; дата и время начала получения статистики).

- Идентификатор устройства; полная версия ПО; идентификатор обновления ПО; идентификатор установки ПО (PCID); тип установленного ПО.

- Высота экрана устройства; ширина экрана устройства; информация о перекрывающем приложении: MD5-хеш APK-файла; информация о перекрывающем приложении: MD5-хеш файла classes.dex; информация о перекрывающем приложении: имя APK-файла; информация о перекрывающем приложении: путь к APK-файлу без имени файла; высота перекрытия; информация о перекрытом ПО: MD5-хеш APK-файла; информация о перекрытом приложении: MD5-хеш файла classes.dex; информация о перекрытом приложении: имя APK-файла; информация о перекрытом приложении: путь к APK-файлу без имени файла; информация о перекрытом приложении: имя пакета приложения (для перекрытого приложения: если реклама отображается на пустом рабочем столе, значение должно быть "средство запуска"); дата и время возникновения перекрытия; информация о перекрывающем приложении: имя пакета приложения; ширина перекрытия.

- Параметры используемой точки доступа Wi-Fi (тип обнаруженного устройства; параметры DHCP (контрольные суммы локального IPv6 шлюза, DHCP IPv6, DNS1 IPv6, DNS2 IPv6; контрольная сумма длины префикса сети; контрольная сумма локального адреса IPv6); параметры DHCP (контрольные суммы локального IP-адреса шлюза, DHCP IP, DNS1 IP, DNS2 IP и маски подсети); флаг, показывающий, имеется ли домен DNS; контрольная сумма назначенного локального адреса IPv6; контрольная сумма назначенного локального адреса IPv4; флаг, показывающий, подключено ли устройство; тип аутентификации сети Wi-Fi; список доступных сетей Wi-Fi и их параметры; контрольная сумма (MD5 с солью) MAC-адреса точки доступа; контрольная сумма (SHA256 с солью) MAC-адреса точка доступа; типы подключения, поддерживаемые точкой доступа Wi-Fi; тип шифрования сети Wi-Fi; местное время начала и окончания подключения к сети Wi-Fi; идентификатор сети Wi-Fi на основе MAC-адреса точки доступа; идентификатор сети Wi-Fi на основе имени сети Wi-Fi; идентификатор сети Wi-Fi на основе имени сети Wi-Fi и MAC-адреса точки доступа; мощность сигнала Wi-Fi; имя сети Wi-Fi; набор протоколов аутентификации, поддерживаемых данной конфигурацией; протокол аутентификации, используемый для соединения WPA-EAP; внутренний протокол аутентификации; набор групповых шифров, поддерживаемых данной конфигурацией; набор протоколов управления ключами, поддерживаемых данной конфигурацией; окончательная категория конфиденциальности сети в ПО; окончательная категория безопасности сети в ПО; набор блочных шифров для WPA, поддерживаемых данной конфигурацией; набор протоколов безопасности, поддерживаемых данной конфигурацией).

Также для достижения заявленной цели повышения эффективности защиты, предоставляемой ПО, Правообладатель может получать объекты (файл или его часть, служебная информация), в отношении которых существует риск их использования злоумышленниками для нанесения вреда устройству и создания угроз информационной безопасности.

Участие в Kaspersky Security Network для обработки статистических данных является добровольным. Вы можете в любой момент отказаться от участия в Kaspersky Security Network.

Предоставление данных в рамках Положения об обработке данных для использования Веб-Фильтра

В соответствии с Положением о Веб-Фильтре, Правообладатель обрабатывает данные в целях обеспечения работы Веб-Фильтра. Заявленная цель включает обнаружение веб-угроз и определение категорий посещаемых веб-сайтов с помощью облачного сервиса Kaspersky Security Network (KSN).

С вашего согласия, следующие данные будут автоматически регулярно отправляться Правообладателю в соответствии с Положением о Веб-Фильтре:

- версия продукта, уникальный идентификатор устройства, идентификатор установки, тип продукта;
- адрес веб-сайта, посещаемого в текущий момент пользователем, номер порта, протокол передачи данных, адрес веб-сайта, с которого был осуществлен переход;

Предоставление данных в рамках Положения об обработке данных для маркетинговых целей

Правообладатель использует для обработки данных информационные системы третьих лиц. Обработка данных в информационных системах третьих лиц регулируется соответствующими политиками конфиденциальности таких систем. Правообладатель использует следующие сервисы для обработки перечисленных данных:

- Google Analytics для Firebase

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Google Analytics для Firebase для их обработки для заявленных целей:

- данные о приложении (версия приложения, идентификатор приложения, идентификатор приложения в сервисе Firebase, идентификатор экземпляра в сервисе Firebase, название магазина, в котором было куплено приложение, время первого запуска);
- об идентификаторе установки приложения на устройство и способе установки на устройство;
- о регионе и языковой локализации;
- о разрешении экрана устройства;
- данные о получении root-прав пользователем;
- диагностическая информация об устройстве из сервиса SafetyNet Attestation;
- данные об установке Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей;
- данные о переходах между значками приложения;
- данные о протоколе отправки данных в сервис Firebase, его версии и идентификаторе используемого метода отправки данных;
- информация о типе и параметрах события, в отношении которого происходит отправка данных;
- данные о лицензии на приложение, ее наличии, количестве устройств;
- информация о частоте обновления антивирусных баз и синхронизации с Сервером администрирования;
- данные о консоли администрирования (Kaspersky Security Center или сторонних EMM-систем);

- идентификатор Android;
- рекламный идентификатор (Advertising ID);
- информация о пользователе: возрастная категория и пол, идентификатор страны проживания и список интересов;
- информация о компьютере пользователя, на котором установлено ПО: название производителя компьютера, тип компьютера, модель, версия и язык (локаль) операционной системы;
- информация о программах, которые открывались в первый раз в течение последних 7 дней, и о программах, которые открывались в первый раз более 7 дней назад.

Передача данных в сервис Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase доступна по адресу https://firebase.google.com/support/privacy.

- SafetyNet Attestation.

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис SafetyNet Attestation для их обработки для заявленных целей:

- Время проверки устройства;
- Информация о ПО, название и данные о сертификатах ПО;
- Результаты проверки устройства;
- Случайный идентификатор проверки для верификации результатов проверки устройства.

Передача данных в сервис SafetyNet Attestation осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе SafetyNet Attestation доступна по адресу https://policies.google.com/privacy.

Предоставление вышеуказанной информации для обработке в маркетинговых целях является добровольным.

Samsung KNOX

Samsung KNOX – мобильное решение для настройки и защиты мобильных устройств Samsung под управлением операционной системы Android. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

Установка приложения Kaspersky Endpoint Security для Android с помощью KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) является частью мобильного решения Samsung KNOX и используется для массовой установки и первоначальной настройки приложений на новых устройствах Samsung, приобретенных у официальных поставщиков.

Установка приложения Kaspersky Endpoint Security для Android через KNOX Mobile Enrollment состоит из следующих этапов:

1. **Создание профиля KNOX MDM с приложением Kaspersky Endpoint Security для Android.**
2. **Добавление устройств в KNOX Mobile Enrollment.**
3. **Установка приложения Kaspersky Endpoint Security для Android на мобильных устройствах пользователя.**

Подробная информация о работе с KNOX Mobile Enrollment приведена в *Руководстве пользователя KNOX Mobile Enrollment*.

Схема развертывания через KNOX Mobile Enrollment доступна только для Samsung-устройств под управлением операционной системы Android версии 5.0 и выше. Список поддерживаемых устройств приведен на *сайте Службы технической поддержки Samsung*.

Создание профиля KNOX MDM

Профиль KNOX MDM – профиль, который содержит ссылки на приложения для их быстрого развертывания и первоначальной настройки на мобильных устройствах.

Чтобы создать профиль KNOX MDM, выполните следующие действия:

1. Войдите в консоль Samsung KNOX → **KNOX Mobile Enrollment**.
2. Выберите раздел **Профили MDM**.
3. Нажмите на кнопку **Добавить**.

   Запустится мастер создания профиля KNOX MDM.
4. На шаге **Подключение сервера MDM** выберите **URI сервера не требуется для моего сервиса MDM** и нажмите на кнопку **Далее**.
5. На шаге **Сведения о профиле MDM** выполните следующие действия:

a. Введите общую информацию о профиле KNOX MDM: **Название профиля** и **Описание**.

b. Введите путь к установочному файлу APK по кнопке **Добавить приложения MDM**.

Установочный файл Kaspersky Endpoint Security для Android входит в комплект поставки Kaspersky Security для мобильных устройств. Предварительно разместите установочный файл APK на Веб-сервере Kaspersky Security Center или на другом сервере, доступном для загрузки с устройства.

c. Введите параметры подключения устройства к Kaspersky Security Center в поле **Пользовательские данные JSON** в формате:
`{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`.

Подключение устройства к Kaspersky Security Center требуется для активации приложения, настройки устройства и отправки команд.

d. Установите флажок **Добавление соглашений, связанных с Knox**.

Для установки Kaspersky Endpoint Security для Android через KNOX Mobile Enrollment пользователь мобильного устройства должен принять условия Лицензионного соглашения Samsung. Вы можете ознакомиться с условиями Лицензионного соглашения Samsung в блоке **Лицензионные соглашения с конечным пользователем, условия обслуживания и пользовательские соглашения**. Также вы можете добавить другие юридические документы вашей компании, необходимые для развертывания профиля KNOX MDM, по кнопке **Добавить пользовательское соглашение**.

e. Снимите флажок **Привяжите лицензию Knox к этому профилю**.

Информация о лицензии Samsung KNOX передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

6. Нажмите на кнопку **Сохранить**.

В результате новый профиль KNOX MDM с приложением Kaspersky Endpoint Security для Android будет добавлен в список в консоли KME.

Добавление устройств в KNOX Mobile Enrollment

Добавление устройств в консоли KNOX Mobile Enrollment (KME) может быть выполнено следующими способами:

- Поставщик автоматически добавляет устройства в консоль KME после приобретения устройства.

  Выберите этот способ, если ваша организация сотрудничает с официальным поставщиком Samsung-устройств.

- Администратор устанавливает приложение KNOX Deployment из Google Play на свое мобильное устройство и переносит профиль KNOX MDM на устройства пользователей с помощью Bluetooth или NFC (Near Field Communication). После разворачивания профиля KNOX MDM устройство автоматически будет добавлено в консоль KME.

  Выберите этот способ, если Samsung-устройства приобретены не у официального поставщика.

Добавление устройства поставщиком

Официальный поставщик Samsung-устройств зарегистрирован в Samsung KNOX. Список официальных поставщиков приведен на *сайте Службы технической поддержки Samsung*. Поставщик автоматически добавляет устройства в консоль KME для вашей учетной записи Samsung сразу после приобретения устройств. Для добавления устройств поставщиком требуется зарегистрировать поставщика в консоли KME для вашей учетной записи Samsung. Для добавления поставщика Samsung-устройств в консоль KME вам потребуется идентификатор посредника. Для получения идентификатора посредника вам необходимо отправить запрос поставщику. В запросе укажите ваш идентификатор клиента KNOX.

Чтобы просмотреть ваш идентификатор клиента KNOX, выполните следующие действия:

1. Войдите в консоль Samsung KNOX → **KNOX Mobile Enrollment**.
2. Выберите раздел **Посредники**.
3. В поле **Идентификатор клиента KNOX** отображается ваш идентификатор.

После получения ответа от поставщика с идентификатором посредника зарегистрируйте поставщика в консоли KME. Перед регистрацией поставщика вы можете создать профиль KNOX MDM для автоматического разворачивания профиля при добавлении новых устройств.

Чтобы зарегистрировать официального поставщика в консоли KME, выполните следующие действия:

1. Войдите в консоль Samsung KNOX → **KNOX Mobile Enrollment**.
2. Выберите раздел **Посредники**.
3. Нажмите на кнопку **Зарегистрировать торгового посредника**.

   Откроется окно регистрации поставщика устройств.
4. В поле **Идентификатор посредника** введите идентификатор, полученный от официального поставщика Samsung-устройств.
5. Если вы создали профиль KNOX MDM, в окне регистрации поставщика выберите KNOX MDM профиль.

   При добавлении новых устройств автоматически устанавливается профиль KNOX MDM.
6. В списке **Предпочитаемый способ подтверждения загрузок** выберите способ подтверждения добавления устройства для поставщика.

   - **Все загрузки должны быть подтверждены**. При добавлении устройства поставщиком вам потребуется подтвердить операцию.
   - **Автоматически подтверждать все загрузки этого посредника**. Устройства поставщика будут добавлены в консоль KME автоматически.
7. Нажмите кнопку **OK**.

Поставщик Samsung-устройств будет добавлен в список поставщиков в консоли KME.

После приобретения новых устройств у официального поставщика на устройства автоматически будет установлено приложение Kaspersky Endpoint Security для Android после подключения устройств к сети Интернет. Подробная информация о работе с KNOX Mobile Enrollment приведена в *Руководстве пользователя KNOX Mobile Enrollment*. Если у вас уже сформирован список устройств в консоли KME, добавьте на устройство профиль KNOX MDM с приложением KNOX MDM.

Чтобы доставить профиль KNOX MDM на устройства, выполните следующие действия:

1. Войдите в консоль Samsung KNOX → **KNOX Mobile Enrollment**.
2. Выберите раздел **Устройства** → **Все устройства**.
3. Выберите устройства, на которых вы хотите установить профиль KNOX MDM.
4. Нажмите на кнопку **Настроить**.

   Откроется окно **Информация об устройстве**.
5. В списке **Профиль MDM** выберите профиль KNOX MDM с приложением Kaspersky Endpoint Security для Android.
6. В поле **Теги** введите теги для группировки и маркировки устройств, а также для оптимизации поиска в консоли KME.
7. Введите учетные данные пользователя устройства в поля **Идентификатор пользователя** и **Пароль**.

   Учетные данные требуются для получения общего сертификата. Идентификатор пользователя и пароль должны совпадать с учетными данными пользователя в Kaspersky Security Center (Полное имя и Пароль в свойствах учетной записи).
8. Выберите профиль KNOX MDM для остальных устройств.
9. Нажмите на кнопку **Сохранить**.

В результате после подключения устройства к сети Интернет пользователю будет предложено установить профиль KNOX MDM.

Добавление устройства с помощью приложения KNOX Deployment

Если вы приобрели Samsung-устройство не у официального поставщика, вы можете добавить устройство в KNOX Mobile Enrollment с помощью Bluetooth или NFC. Для этого потребуется мобильное устройство администратора, с помощью которого будет выполняться доставка профилей KNOX MDM на мобильные устройства пользователей.

Для добавления устройств с помощью приложения KNOX Deployment должны быть выполнены следующие условия:

- На мобильных устройствах должны быть включены модули Bluetooth или NFC в зависимости от выбранного режим доставки.
- Мобильные устройства должны быть подключены к сети Интернет.

Чтобы доставить KNOX MDM профиль с помощью приложения KNOX Deployment, выполните следующие действия:

1. Установите на мобильное устройство администратора приложение KNOX Deployment из Google Play.
2. Запустите приложение KNOX Deployment.
3. Введите данные вашей учетной записи Samsung.
4. В окне **KNOX Deployment** настройте параметры развертывания KNOX MDM профиля:
   - Выберите профиль KNOX MDM.

- Выберите режим развертывания: **Bluetooth** или **NFC**.

  При использовании Bluetooth вы можете добавлять профиль KNOX MDM сразу на несколько устройств.

5. Нажмите **Начать развертывание**:

   - **Bluetooth**. На мобильном устройстве пользователя откройте веб-сайт https://configure.samsungknox.com.

     Запустится мастер регистрации устройства в Samsung KNOX. Следуйте указаниям на экране.

     В результате после установки профиля KNOX MDM в консоли KME будет добавлено новое устройство с тегом **Bluetooth**.

   - **NFC**. Поднесите мобильное устройство администратора к мобильному устройству пользователя и передайте профиль KNOX MDM.

     В результате на мобильном устройстве пользователя ему будет предложено установить профиль KNOX MDM. В консоли KME будет добавлено новое устройство с тегом **NFC**.

Установка приложения

Перед установкой приложения Kaspersky Endpoint Security для Android выпишите в Консоли администрирования Kaspersky Security Center общий сертификат для пользователей мобильных устройств. Общий сертификат требуется для идентификации пользователя мобильного устройства в Консоли администрирования Kaspersky Security Center.

После начала развертывания профиля KNOX MDM на мобильном устройстве автоматически будет загружен установочный файл APK. Установка приложения Kaspersky Endpoint Security для Android запустится автоматически. Пользователю требуется принять Лицензионное соглашение Samsung KNOX и Лицензионное соглашение Kaspersky Endpoint Security для Android. Дополнительной настройки приложения не требуется. После установки приложения синхронизация с Kaspersky Security Center будет выполнена автоматически. В результате мобильное устройство будет добавлено в Консоль администрирования Kaspersky Security Center в группу администрирования, указанную в параметрах профиля KNOX MDM (`groupName`).

Настройка KNOX-контейнеров

Этот раздел содержит информацию о работе с KNOX-контейнерами на Samsung-устройствах под управлением операционной системы Android.

Использование KNOX-контейнеров доступно только на Samsung-устройствах под управлением операционной системы Android версии 6.0 или выше.

О KNOX-контейнере

KNOX-контейнер – безопасная среда на устройстве пользователя с отдельным рабочим столом, панелью запуска, приложениями, виджетами. KNOX-контейнер позволяет изолировать корпоративные приложения и данные от персональных. KNOX-контейнер является компонентом мобильного решения Samsung KNOX.

Samsung KNOX – мобильное решение для настройки и защиты мобильных устройств Samsung под управлением операционной системы Android. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

KNOX-контейнеры позволяют разделить персональные и корпоративные данные на мобильном устройстве. Например, невозможно отправить файл, расположенный в KNOX-контейнере, с помощью личного почтового ящика. Рекомендуется разворачивать KNOX-контейнер, если для работы с корпоративными данными используются личные мобильные устройства сотрудников.

Для использования KNOX-контейнеров требуется активировать Samsung KNOX. После синхронизации устройства с Kaspersky Security Center пользователю мобильного устройства будет предложено установить KNOX-контейнер. Перед установкой KNOX-контейнера пользователь должен принять условия Лицензионного соглашения от компании Samsung.

После установки KNOX-контейнера на рабочий стол мобильного устройства будет добавлен значок KNOX  . Или рабочая область будет добавлена в список приложений на мобильном устройстве. Для работы с корпоративными данными пользователю нужно запустить приложение из KNOX-контейнера.

Kaspersky Endpoint Security для Android не устанавливается в KNOX-контейнер и не защищает корпоративные данные. Kaspersky Endpoint Security для Android не обнаруживает загрузку вредоносных файлов и не блокирует вредоносные сайты в KNOX-контейнере. В KNOX-контейнере невозможно контролировать загрузку приложений и запретить использование камеры. Kaspersky Endpoint Security для Android защищает только личные данные. Корпоративные данные можно защитить с помощью инструментов Samsung KNOX. Подробная информация о Samsung KNOX приведена на *сайте Службы технической поддержки Samsung*.

Активация Samsung KNOX

Чтобы использовать KNOX-контейнер на мобильном устройстве пользователя, требуется активировать Samsung KNOX. Для активации Samsung KNOX нужно получить ключ KNOX License Manager (далее KLM-ключ) от компании Samsung. *Ключ KNOX License Manager* – уникальный код, который используется системой лицензирования Samsung KNOX. KLM-ключ можно приобрести в Магазине KNOX (KNOX Marketplace). Также вы можете получить KLM-ключ у торгового посредника или менеджера по работе с клиентами Samsung. Более подробная информация о KLM-ключе приведена на сайте технической поддержки Samsung KNOX.

Без KLM-ключа настроить параметры KNOX-контейнера на мобильном устройстве невозможно.

Использование KNOX-контейнеров возможно только для Samsung-устройств под управлением операционной системы Android версии 6.0 и выше.

Чтобы активировать Samsung KNOX, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.

5. В поле **Ключ KNOX License Manager** введите KLM-ключ, полученный от компании Samsung.

6. Установите атрибут "замок" в закрытое положение .

7. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Samsung KNOX будет активирован после очередной синхронизации устройства с Kaspersky Security Center. Пользователю будет предложено принять условия Лицензионного соглашения от компании Samsung и установить KNOX-контейнер.

Чтобы деактивировать Samsung KNOX, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.

2. В рабочей области группы выберите закладку **Политики**.

3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.

5. В поле **Ключ KNOX License Manager** удалите ключ, полученный от компании Samsung.

6. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Samsung KNOX будет активирован после очередной синхронизации устройства с Kaspersky Security Center. Доступ в KNOX-контейнер будет заблокирован.

Ограничения Samsung KNOX

- Использование KNOX-контейнеров доступно только на Samsung-устройствах под управлением операционной системы Android версии 5.0 или выше.
- Для использования KNOX-контейнеров требуется приобрести ключ KNOX License Manager (KLM-ключ) в Магазине KNOX. Без KLM-ключа настроить параметры KNOX-контейнера на мобильном устройстве невозможно.
- На Samsung-устройствах с поддержкой KNOX 2.6, 2.7 и 2.7.1 в KNOX-контейнере не работает Веб-Фильтр и Контроль приложений. Проблема связана с отсутствием необходимых прав в KNOX-контейнере (служба Специальных возможностей). На устройствах с поддержкой KNOX 2.8 и выше все компоненты приложения работают без ограничений.
- Kaspersky Endpoint Security для Android версии ниже, чем Service Pack 4 Maintenance Release 3 Update 2 может работать нестабильно на устройствах Samsung с операционной системой Android 10 из-за обновлений Samsung KNOX. Рекомендуется обновить Kaspersky Endpoint Security для Android до версии Service Pack 4 Maintenance Release 3 Update 2.

Настройка Сетевого экрана в KNOX

Для контроля сетевых соединений в KNOX-контейнере следует настроить параметры Сетевого экрана.

Чтобы настроить Сетевой экран в KNOX-контейнере, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.
4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.
5. В блоке **Сетевой экран** нажмите на кнопку **Настроить**.

   Откроется окно **Сетевой экран**.
6. Выберите режим работы Сетевого экрана:

   - Чтобы разрешить все входящие и исходящие соединения, переместите ползунок в положение **Разрешать все**.
   - Чтобы блокировать любую сетевую активность, кроме приложений из списка исключений, переместите ползунок в положение **Блокировать все, кроме исключений**.
7. Если вы выбрали режим работы Сетевого экрана **Блокировать все, кроме исключений**, сформируйте список исключений:

   a. Нажмите на кнопку **Добавить**.

   Откроется окно **Исключение для Сетевого экрана**.

   b. В поле **Название приложения** введите название мобильного приложения.

   c. В поле **Имя пакета** введите системное имя пакета мобильного приложения (например, `com.mobileapp.example`).

   d. Нажмите кнопку **ОК**.
8. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Настройка почтового ящика Exchange в KNOX

Для работы с корпоративной почтой, контактами и календарем в KNOX-контейнере следует настроить параметры почтового ящика Exchange.

Чтобы настроить почтовый ящик Exchange в KNOX-контейнере, выполните следующие действия:

1. В дереве консоли в папке **Управляемые устройства** выберите группу администрирования, в которую входят Android-устройства.
2. В рабочей области группы выберите закладку **Политики**.
3. Откройте окно свойств политики двойным щелчком мыши по любому столбцу.

4. В политике, в окне **Свойства** выберите раздел **Управление Samsung KNOX → KNOX-контейнеры**.

5. В блоке **Exchange ActiveSync** нажмите на кнопку **Настроить**.

   Откроется окно **Параметры почтового сервера Exchange**.

6. В поле **Адрес сервера** введите IP-адрес или DNS-имя сервера, на котором размещен почтовый сервер.

7. В поле **Домен** введите имя домена пользователя мобильного устройства в корпоративной сети.

8. В раскрывающемся списке **Периодичность синхронизации** выберите желаемый период синхронизации мобильного устройства с сервером Microsoft Exchange.

9. Чтобы использовать транспортный протокол передачи данных SSL, установите флажок **Использовать SSL-соединение**.

10. Чтобы использовать цифровые сертификаты для защиты передачи данных между мобильным устройством и сервером Microsoft Exchange, установите флажок **Проверять сертификат сервера**.

11. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о программе, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании программы.

"Лаборатория Касперского" обеспечивает поддержку этой программы в течение ее жизненного цикла (см. таблицу поддерживаемых продуктов). Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- Позвонить в Службу технической поддержки по телефону.
- Отправить запрос в Службу технической поддержки с портала Kaspersky CompanyAccount. https://companyaccount.kaspersky.com

Техническая поддержка предоставляется только пользователям, которые приобрели коммерческую лицензию. Пользователям, которые получили пробную лицензию, техническая поддержка не предоставляется.

Получение технической поддержки по телефону

В большинстве регионов по всему миру вы можете позвонить специалистам Службы технической поддержки. Информацию о способах получения технической поддержки в вашем регионе и контакты Службы технической поддержки приведены на веб-сайте Службы технической поддержки "Лаборатории Касперского".

Перед обращением в Службу технической поддержки ознакомьтесь с правилами предоставления технической поддержки.

Техническая поддержка через Kaspersky CompanyAccount

Kaspersky CompanyAccount – это портал для организаций, использующих программы "Лаборатории Касперского". Портал Kaspersky CompanyAccount предназначен для взаимодействия пользователей со специалистами "Лаборатории Касперского" с помощью электронных запросов. Kaspersky CompanyAccount можно также использовать для отслеживания статуса и хранения истории ваших онлайн-обращений.

Вы можете зарегистрировать всех сотрудников вашей организации в рамках одной учетной записи Kaspersky CompanyAccount. Одна учетная запись позволяет вам централизованно управлять электронными запросами от зарегистрированных сотрудников в "Лабораторию Касперского", а также управлять правами этих сотрудников в Kaspersky CompanyAccount.

Портал Kaspersky CompanyAccount доступен на следующих языках:

- английском;
- испанском;
- итальянском;
- немецком;
- польском;
- португальском;
- русском;
- французском;
- японском.

Более подробная информация о Kaspersky CompanyAccount приведена на веб-сайте Службы технической поддержки.

Другие источники информации о программе

Страница Kaspersky Security для мобильных устройств на веб-сайте "Лаборатории Касперского"

На странице Kaspersky Security для мобильных устройств приведена общая информация о программе, ее возможностях и особенностях работы.

Страница Kaspersky Security для мобильных устройств содержит ссылку на интернет-магазин. В нем вы можете приобрести программу или продлить право пользования программой.

Веб-страница Kaspersky Endpoint Security в Базе знаний

База знаний – это раздел веб-сайта Службы технической поддержки.

На странице Kaspersky Security для мобильных устройств в Базе знаний приведены статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании программы.

Статьи Базы знаний могут отвечать на вопросы, которые относятся не только к Kaspersky Security для мобильных устройств, но и к другим программам "Лаборатории Касперского". Статьи Базы знаний также могут содержать новости Службы технической поддержки.

Электронная справка

В состав электронной справки программы входят файлы справки.

В контекстной справке для плагинов управления Kaspersky Security для мобильных устройств вы можете найти информацию об окнах в Kaspersky Security Center: описание параметров Kaspersky Security для мобильных устройств и ссылки на описания задач, в которых используются эти параметры.

В полной справке для приложения Kaspersky Endpoint Security приведена информация о настройке и использовании мобильного приложения.

Обсуждение программ "Лаборатории Касперского" в сообществе пользователей

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями в нашем сообществе.

В сообществе вы можете просматривать темы обсуждений, добавлять свои комментарии, создавать новые темы для обсуждения.

Глоссарий

Apple Push Notification service (APNs) сертификат

Сертификат, подписанный компанией Apple, который позволяет использовать Apple Push Notification. С помощью Apple Push Notification Сервер iOS MDM может управлять iOS-устройствами.

EAS-устройство

Мобильное устройство, подключенное к Серверу администрирования по протоколу Exchange ActiveSync.

IMAP

Протокол для доступа к электронной почте. В отличие от протокола POP3, IMAP предоставляет расширенные возможности работы с почтовыми ящиками, такие как управление папками, манипуляция сообщениями без копирования их содержимого с почтового сервера. Протокол IMAP использует порт 134.

iOS MDM-профиль

Профиль, который содержит набор параметров для подключения мобильных устройств iOS к Серверу администрирования. iOS MDM-профиль позволяет рассылать конфигурационные профили iOS в фоновом режиме с помощью Сервера iOS MDM, а также получать расширенную диагностическую информацию о мобильных устройствах. Ссылку на iOS MDM-профиль необходимо отправлять пользователю для того, чтобы Сервер iOS MDM мог обнаружить и подключить его мобильное устройство под управлением iOS.

iOS MDM-устройство

Мобильное устройство на платформе iOS, находящееся под управлением Сервера iOS MDM.

Kaspersky Security Network (KSN)

Инфраструктура облачных служб, предоставляющая доступ к базе данных "Лаборатории Касперского" с постоянно обновляемой информацией о репутации файлов, веб-ресурсов и программного обеспечения. Kaspersky Security Network обеспечивает более высокую скорость реакции программ "Лаборатории Касперского" на угрозы, повышает эффективность работы некоторых компонентов защиты, а также снижает вероятность ложных срабатываний.

Manifest-файл

Файл в формате PLIST, содержащий ссылку на файл приложения (ipa-файл), расположенный на веб-сервере. Используется iOS-устройством для поиска, загрузки и установки приложений с веб-сервера.

POP3

Сетевой протокол получения сообщений почтовым клиентом с почтового сервера.

Provisioning-профиль

Набор параметров для работы программы на мобильных устройствах с операционной системой iOS. Provisioning-профиль содержит данные о лицензии и связан с определенной программой.

SSL

Протокол шифрования данных в локальных сетях и в интернете. Протокол SSL (Secure Sockets Layer) используется в веб-приложениях для создания защищенных соединений между клиентом и сервером.

Автономный пакет установки

Установочный файл программы Kaspersky Endpoint Security для операционной системы Android, содержащий параметры подключения программы к Серверу администрирования. Создается на основе инсталляционного пакета для этой программы и является частным случаем пакета мобильных приложений.

Администратор Kaspersky Security Center

Лицо, управляющее работой программы через систему удаленного централизованного администрирования Kaspersky Security Center.

Администратор устройства

Набор прав приложения на Android-устройстве, позволяющий приложению использовать политики управления устройством. Необходим для реализации полной функциональности Kaspersky Endpoint Security на Android-устройстве.

Активация программы

Перевод программы в полнофункциональный режим. Активация выполняется пользователем во время или после установки программы. Для активации программы необходим код активации или файл ключа.

Антивирусные базы

Базы данных, которые содержат информацию об угрозах компьютерной безопасности, известных "Лаборатории Касперского" на момент выпуска антивирусных баз. Записи в антивирусных базах позволяют обнаруживать вредоносный код в проверяемых объектах. Антивирусные базы формируются специалистами "Лаборатории Касперского" и обновляются каждый час.

Веб-сервер Kaspersky Security Center

Компонент Kaspersky Security Center, который устанавливается совместно с Сервером администрирования. Веб-сервер предназначен для передачи по сети автономных пакетов установки, iOS MDM-профилей, а также файлов из папки общего доступа.

Вирус

Программа, которая заражает другие программы – добавляет в них свой код, чтобы получить управление при запуске зараженных файлов. Это простое определение дает возможность выявить основное действие, выполняемое вирусом – заражение.

Группа администрирования

Набор управляемых устройств, например, мобильных устройств, объединенных в соответствии с их функциями и установленным на них набором программ. Управляемые устройства группируются с целью управления ими как единым целым. Например, в группу администрирования могут быть объединены мобильные устройства под управлением одной операционной системы. В состав группы могут входить другие группы администрирования. Для устройств в группах могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, назначенная для группы администрирования и выполняемая на всех управляемых устройствах, входящих в состав группы.

Запрос Certificate Signing Request

Файл с параметрами Сервера администрирования, который после подтверждения "Лабораторией Касперского" отправляется в Apple для получения APNs-сертификата.

Инсталляционный пакет

Набор файлов, формируемый для удаленной установки программы "Лаборатории Касперского" с помощью системы удаленного администрирования. Инсталляционный пакет создается на основании специальных файлов, входящих в состав дистрибутива программы. Инсталляционный пакет содержит набор параметров, необходимых для установки программы и обеспечения ее работоспособности сразу после установки. Значения параметров в инсталляционном пакете соответствуют значениям параметров приложения по умолчанию.

Карантин

Папка, в которую программа "Лаборатории Касперского" перемещает обнаруженные возможно зараженные объекты. Объекты на карантине хранятся в зашифрованном виде во избежание их воздействия на компьютер.

Категории "Лаборатории Касперского"

Готовые категории данных, разработанные сотрудниками "Лаборатории Касперского". Категории могут обновляться при обновлении баз программы. Специалист по информационной безопасности не может изменять или удалять готовые категории.

Код активации

Код, который вы получаете, приобретая лицензию на Kaspersky Endpoint Security. Этот код необходим для активации программы.

Код активации представляет собой уникальную последовательность из двадцати букв и цифр, в формате xxxxx-xxxxx-xxxxx-xxxxx.

Код разблокировки

Код, который вы получаете на портале My Kaspersky. Он нужен, чтобы разблокировать устройство после выполнения команд **Блокирование и Поиск**, **Сирена** или **Тайное фото**, а также при срабатывании самозащиты.

Контролируемое устройство

iOS-устройство, параметры которого контролируются в Apple Configurator – программе для групповой настройки iOS-устройств. Контролируемое устройство имеет статус *supervised* в Apple Configurator. При каждом подключении контролируемого устройства к компьютеру Apple Configurator проверяет конфигурацию устройства на соответствие заданным эталонным параметрам и при необходимости настраивает ее. Контролируемое устройство не может быть синхронизировано с Apple Configurator, установленном на другом компьютере.

Для контролируемых устройств в политике Kaspersky Device Management для iOS можно переопределить больше параметров, чем для неконтролируемых. Например, можно настроить HTTP-прокси сервер для контроля интернет-трафика на устройстве в корпоративной сети. По умолчанию все мобильные устройства являются неконтролируемыми.

Контроль соответствия

Проверка соответствия параметров мобильного устройства и Kaspersky Endpoint Security для Android требованиям корпоративной безопасности. Требования корпоративной безопасности регламентируют использование устройства. Например, на устройстве должна быть включена постоянная защита, антивирусные базы должны быть актуальны, пароль устройства должен быть достаточно сложным. Контроль соответствия работает на основе списка правил. Правило соответствия состоит из следующих компонентов:

- критерий проверки устройства (например, отсутствие на устройстве запрещенных приложений);
- время, выделенное пользователю устройства для устранения несоответствия (например, 24 часа);
- действие, которое будет выполнено с устройством, если пользователь не устранит несоответствие в течение указанного времени (например, блокирование устройства).

Лицензионное соглашение

Юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать программу.

Лицензия

Ограниченное по времени право на использование приложения, предоставляемое на основании Лицензионного соглашения.

Плагин управления программой

Специализированный компонент, предоставляющий интерфейс для управления работой программы "Лаборатории Касперского" через Консоль администрирования. Для каждой программы существует свой плагин управления. Плагин управления входит в состав всех программ "Лаборатории Касперского", управление которыми можно осуществлять через Kaspersky Security Center.

Подписка

Позволяет использовать программу с выбранными параметрами (дата окончания, количество устройств). Можно приостанавливать и возобновлять подписку, продлевать ее в автоматическом режиме, а также отменить ее.

Политика

Набор параметров программы и мобильных приложений Kaspersky Endpoint Security, применяемый к устройствам в группах администрирования или к отдельным устройствам. К разным группам администрирования могут применяться разные политики. Политика включает в себя настроенные параметры всех функций мобильных приложений Kaspersky Endpoint Security.

Прокси-сервер

Служба в компьютерных сетях, позволяющая пользователям выполнять косвенные запросы к другим сетевым службам. Сначала пользователь подключается к прокси-серверу и запрашивает ресурс (например, файл), расположенный на другом сервере. Затем прокси-сервер либо подключается к указанному серверу и получает ресурс у него, либо возвращает ресурс из собственного кеша (в случаях, если прокси имеет свой кеш). В некоторых случаях запрос клиента или ответ сервера может быть изменен прокси-сервером в определенных целях.

Рабочее место администратора

Компьютер, на котором развернута Консоль администрирования Kaspersky Security Center. Если на рабочем месте администратора установлен плагин управления программой, то администратор может управлять мобильными приложениями Kaspersky Endpoint Security, развернутыми на устройствах пользователей.

Рабочий профиль Android;

Безопасная среда на устройстве пользователя, в которой администратор может управлять приложениями и учетными записями пользователя, не ограничивая его возможности при работе с персональными данными. При создании рабочего профиля на мобильном устройстве пользователя в рабочий профиль автоматически устанавливаются следующие корпоративные приложения: Google Play Маркет, Google Chrome, Загрузки, Kaspersky Endpoint Security для Android и другие. Корпоративные приложения, размещенные в рабочем профиле, а также уведомления этих приложений, отмечены красным значком портфеля. Для приложения Google Play Маркет требуется создать отдельную корпоративную учетную запись Google. Приложения, размещенные в рабочем профиле, отображаются в общем списке приложений.

Сервер iOS MDM

Компонент Kaspersky Endpoint Security, установленный на клиентское устройство и позволяющий подключать мобильные устройства iOS к Серверу администрирования и управлять ими с помощью Apple Push Notifications (APNs).

Сервер администрирования

Компонент программы Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации программах "Лаборатории Касперского" и управления ими.

Сервер мобильных устройств Exchange

Компонент Kaspersky Endpoint Security, который позволяет подключать мобильные устройства Exchange ActiveSync к Серверу администрирования.

Серверы обновлений "Лаборатории Касперского"

HTTP(S)-серверы "Лаборатории Касперского", с которых программы "Лаборатории Касперского" получают обновления баз и модулей программы.

Срок действия лицензии

Период времени, в течение которого вы можете пользоваться функциями программы и дополнительными услугами. Дополнительные услуги зависят от типа лицензии.

Файл ключа

Файл вида xxxxxxxx.key, который позволяет использовать программу "Лаборатории Касперского" по пробной или коммерческой лицензии. Программа формирует файл ключа на основе кода активации. Программу можно использовать только при наличии файла ключа.

Фишинг

Вид интернет-мошенничества, целью которого является получение неправомерного доступа к конфиденциальным данным пользователей.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Права на настройку групповых политик

Администраторы Kaspersky Security Center могут настраивать права доступа пользователей Консоли администрирования к различным функциям программы в зависимости от служебных обязанностей пользователей.

Для каждой функциональной области администратор может назначать следующие права доступа:

- **Разрешить изменение**. Пользователю Консоли администрирования разрешено изменять параметры политики в окне ее свойств.
- **Запретить изменение**. Пользователю Консоли администрирования запрещено изменять параметры политики в окне ее свойств. Закладки политики, входящие в функциональную область, для которой назначено это право, не отображаются в интерфейсе.

Права доступа к разделам плагина управления Kaspersky Endpoint Security

Функциональная область	Раздел политики
Android Enterprise	Рабочий профиль Android;
Анти-Вор	Анти-Вор
Контроль установленных приложений	Контроль установленных приложений
Защита	Защита, Проверка, Обновление
Контроль соответствия	Контроль соответствия
Контейнеры;	Контейнеры;
Параметры устройства	Управление устройством, Синхронизация
Управление устройствами Samsung	APN, Управление Samsung-устройствами, KNOX-контейнеры
Управление системой	Дополнительно, Wi-Fi
Веб-Фильтр	Веб-Фильтр

Права доступа к разделам плагина управления Kaspersky Device Management для iOS

Функциональная область	Раздел политики
Дополнительные	Веб-клипы, Шрифты, AirPlay, AirPrint
Exchange ActiveSync	Общие, Пароль, Синхронизация, Ограничения функций, Ограничения приложений
Общие	Общие, Единая учетная запись, Веб-Фильтр, Wi-Fi, Точка доступа (APN), Exchange ActiveSync, Электронная почта, Конфигурационные параметры
LDAP (календарь/ контакты)	LDAP, Календарь, Контакты, Подписки на календарь
Ограничения и безопасность	Ограничения функций, Ограничения приложений, Ограничения медиаконтента, Пароль, VPN, Глобальный HTTP-прокси, Сертификаты, SCEP

Категории приложений

Контроль приложений поддерживает категоризацию приложений. Режим работы, заданный для категории приложений, будет применен для всех приложений из этой категории. Категорию для каждого приложения определяет облачная служба Kaspersky Security Network.

Категории приложений

Категория	Описание
Развлечения	Приложения для интерактивных развлечений.
IM-клиенты, телефонные программы	Приложения для обмена мгновенными сообщениями, голосовой и видеосвязи через IP-телефонию.
Социальные сети	Приложения для работы с социальными сетями, блогами.
ПО для бизнеса	Приложения для подсчета налогов, управления банковскими операциями, работы с таблицами, бухгалтерского учета, а также другие приложения для бизнеса. Текстовые редакторы.
Дом, Семья, Хобби, Здоровье	Приложения, которые содержат рецепты, рекомендации по стилю. Приложения для фитнеса, ведения графика тренировок, получения рекомендаций по диете, здоровому питанию, технике безопасности, охране труда.
Медицина	Приложения, которые содержат справочники симптомов и лекарств, приложения для работников здравоохранения, журналы и новости о медицине.
Мультимедиа	Службы подписки на фильмы, мультимедийные и видеопроигрыватели. Музыкальные службы, проигрыватели, радиовещание.
ПО для графического дизайна	Приложения для работы с камерой, графические редакторы, приложения для управления фотографиями и их публикации.
Плагины для чтения новостных и RSS-лент	Приложения для чтения газет, журналов, блогов, агрегаторы новостей.
погода.	Приложения для отображения прогноза погоды.
Программы для образования	Приложения для чтения книг, справочники, учебники, словари, тезаурусы, энциклопедии. Приложения для подготовки к экзаменам, учебные материалы, словари, развивающие игры, средства изучения языков.
Онлайн-покупки	Приложения для совершения покупок в интернете и участия в аукционах, подарочные купоны, средства сравнения цен и ведения списка покупок, чтение отзывов о продуктах.
Утилиты для запуска	Приложения, предназначенные для изменения вида рабочего стола, виджетов, ярлыков.
Операционные системы и утилиты	Системные приложения, обеспечивающие управление операционной системой, взаимодействие с пользователем, управление оперативной памятью.
Программы для просмотра карт	Путеводители по городам, информация о местных компаниях, средства планирования поездки.
Другие	Библиотеки программного обеспечения, технические демоверсии приложений.

программы	Приложения, которые не попали ни в одну из категорий.
Транспорт	Приложения для использования общественного транспорта, средства навигации, вождения.
Игры	Аркады, Викторины, Гонки, Другое, Казино, Карточные, Музыка, Настольные игры, Обучающие, Пазлы, Приключения, Ролевые, Симуляторы, Словесные игры, Спортивные игры, Стратегии, Экшен.
Браузеры	Приложения для просмотра веб-сайтов, содержания веб-документов, файлов. Приложения для управления веб-приложениями.
Инструменты для разработки	Приложения, предназначенные для разработки программного обеспечения. Отладчики, компоновщики, редакторы кода, редакторы графического интерфейса.
Программы ОС	Приложения, которые поставляются совместно с операционной системой, и необходимые для обеспечения работы операционной системы.
ПО для работы в интернете	Менеджеры загрузок, почтовые клиенты, приложения для поиска в интернете, а также другие приложения для работы в интернете.
ПО для сетевой инфраструктуры	Приложения для управления серверами, устройствами для хранения данных сетевым оборудованием, программным обеспечением внутри корпоративной сети, автоматизации и интеграции инфраструктурного комплекса.
Сетевое ПО	Приложения, предназначенные для организации совместной работы группы пользователей на нескольких устройствах, коммуникации между устройствами.
Системные утилиты	Приложения, которые поставляются совместно с операционной системой: файловые менеджеры, архиваторы, утилиты для диагностики аппаратного и программного обеспечения, оптимизаторы памяти, деинсталляторы, утилиты управления процессорами.
ПО для защиты	Приложения для защиты данных на устройстве. Приложения для обнаружения и устранения угроз на устройстве. Сетевые экраны. Приложения для шифрования данных.
Менеджеры загрузок	Приложения для загрузки файлов из внешних источников.
Программы для хранения файлов в интернете	Приложения для работы с онлайн-хранилищами файлов, заметок, мультимедиа.
Справочные системы	Программы для чтения книг, справочники, учебники, словари, тезаурусы, вики-энциклопедии.
Почтовые программы	Приложения для отправки и получения электронных писем.

Информация о стороннем коде

Информация о стороннем коде содержится в файле legal_notices.txt, расположенном в папке установки комплексного решения Kaspersky Security для мобильных устройств.

На Android-устройствах информация о стороннем коде доступна в приложении Kaspersky Endpoint Security для Android по кнопке → **О приложении**.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

PostScript – товарный знак или зарегистрированный в Соединенных Штатах Америки и/или в других странах товарный знак Adobe Systems Incorporated.

AirDrop и AirPrint – товарные знаки Apple Inc.

Apple, Apple Configurator, AirPlay, AirPort Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPadOS, iPhone, iTunes, Keychain, OS X, Safari, Spotlight, Touch ID – товарные знаки Apple Inc., зарегистрированные в США и других странах.

Aruba Networks – товарный знак Aruba Networks, Inc. в США и некоторых других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect, IOS – товарные знаки или зарегистрированные в Соединенных Штатах Америки и в других странах товарные знаки Cisco Systems, Inc. и / или ее аффилированных компаний.

Aventail, SonicWALL, SonicWALL Mobile Connect – товарные знаки SonicWall, Inc.

SecurID – зарегистрированный товарный знак или товарный знак EMC Corporation в США и/или других странах.

Google, Android, Chrome, Chromebook, Chromium, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus, SPDY – товарные знаки Google, Inc.

Huawei и EMUI – товарные знаки Huawei Technologies Co., Ltd., зарегистрированные в Китае и в других странах.

IBM и Maas360 – товарные знаки International Business Machines Corporation, зарегистрированные во многих юрисдикциях по всему миру.

Juniper Networks, Juniper и JUNOS – товарные знаки или зарегистрированные в США и других странах товарные знаки Juniper Networks, Inc.

Microsoft, Active Directory, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile, Windows Phone – товарные знаки Microsoft Corporation, зарегистрированные в Соединенных Штатах Америки и в других странах.

Oracle и JavaScript – зарегистрированные товарные знаки компании Oracle и/или ее аффилированных компаний.

Товарный знак BlackBerry принадлежит Research In Motion Limited, зарегистрирован в США и может быть подан на регистрацию или зарегистрирован в других странах.

Samsung – товарный знак компании SAMSUNG в США или других странах.

SOTI и MobiControl – зарегистрированные в США и в других юрисдикциях товарные знаки SOTI Inc.

Symantec – товарный знак или зарегистрированный в США и других странах товарный знак Symantec Corporation или аффилированных компаний.

Владельцем товарного знака Symbian является Symbian Foundation Ltd.

VMware и VMware Workspace ONE – товарные знаки VMware, Inc. или зарегистрированные в США и/или других юрисдикциях товарные знаки VMware, Inc.