kaspersky

Kaspersky Secure Mobility Management

© 2023 АО "Лаборатория Касперского"

Содержание

Справка Kaspersky Security для мобильных устройств

Что нового

Сравнение функций приложения в зависимости от средств управления

Комплект поставки

Работа в Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

- Об управлении мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console
  - Основные функции управления мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console
  - О приложении Kaspersky Endpoint Security для Android
  - О приложении Kaspersky Security для iOS
  - О плагине Kaspersky Security for Mobile (Devices)
  - О плагине Kaspersky Security for Mobile (Policies)
  - Аппаратные и программные требования
  - Известные проблемы и рекомендации
- Развертывание решения для управления мобильными устройствами в Kaspersky Security Center Web Console или Cloud Console
  - Сценарии развертывания
  - Подготовка Kaspersky Security Center Web Console и Cloud Console к развертыванию
    - Настройка Сервера администрирования для подключения мобильных устройств
    - Настройка шлюза соединения для подключения мобильных устройств к Серверу администрирования Kaspersky Security Center
    - Создание группы администрирования
    - Создание правила автоматического перемещения устройств в группу администрирования
  - Развертывание плагинов управления
    - Установка плагинов управления из списка доступных дистрибутивов
    - Установка плагинов управления из дистрибутива
  - Развертывание мобильного приложения
    - Развертывание мобильного приложения с помощью Kaspersky Security Center Web Console или Cloud Console
    - Активация мобильного приложения
    - Предоставление необходимых разрешений приложению Kaspersky Endpoint Security для Android
  - Управление сертификатами
    - Просмотр списка сертификатов
    - Задание параметров сертификата
    - Создание сертификата
    - Обновление сертификата
    - Удаление сертификата
  - Обмен информацией с Firebase Cloud Messaging
- Управление мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console
  - Подключение мобильных устройств к Kaspersky Security Center
  - Перемещение нераспределенных мобильных устройств в группы администрирования
  - Отправка команд на мобильные устройства
  - Удаление мобильных устройств из Kaspersky Security Center
- Управление групповыми политиками
  - Групповые политики для управления мобильными устройствами
  - Просмотр списка групповых политик

Просмотр результатов применения политики
Создание групповой политики
Изменение групповой политики
Копирование групповой политики
Перенос политики в другую группу администрирования
Удаление групповой политики
Определение параметров политики
Настройка антивирусной защиты
Настройка постоянной защиты
Настройка автоматического запуска антивирусной проверки мобильного устройства
Настройка обновления антивирусных баз
Задание параметров разблокировки устройства
Настройка защиты данных при потере или краже устройства
Настройка контроля приложений
Настройка контроля соответствия мобильных устройств требованиям корпоративной безопасности
Включение и отключение правил соответствия
Редактирование правил соответствия
Добавление правил соответствия
Удаление правил соответствия
Список критериев несоответствия
Список действий при обнаружении несоответствия
Настройка доступа пользователей к веб-сайтам
Настройка ограничений функций
Защита Kaspersky Endpoint Security для Android от удаления
Настройка синхронизации мобильных устройств с Kaspersky Security Center
Kaspersky Security Network
Обмен информацией с Kaspersky Security Network
Включение и отключение Kaspersky Security Network
Обмен информацией с Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics
Настройка уведомлений на мобильных устройствах
Обнаружение взлома устройства
Задание параметров лицензирования
Настройка событий
Настройка событий, связанных с установкой, обновлением и удалением приложений на устройствах пользователей
Нагрузка на сеть
Работа с Консолью администрирования на базе MMC
Основные сценарии использования
О Kaspersky Security для мобильных устройств
Основные функции управления мобильными устройствами в Консоли администрирования на базе MMC
О приложении Kaspersky Endpoint Security для Android
О Kaspersky Device Management для iOS
О плагине управления Kaspersky Endpoint Security для Android
О плагине управления Kaspersky Device Management для iOS
Аппаратные и программные требования
Известные проблемы и рекомендации

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
  - Настройка шлюза соединения для подключения мобильных устройств к Серверу администрирования Kaspersky Security Center
  - Отображение папки "Управление мобильными устройствами" в Консоли администрирования
  - Создание группы администрирования
  - Создание правила автоматического переноса устройств в группу администрирования
  - Создание мобильного сертификата
- Установка Kaspersky Endpoint Security для Android
  - Разрешения
  - Установка Kaspersky Endpoint Security для Android по ссылке на Google Play
  - Установка Kaspersky Endpoint Security для Android в режиме device owner
  - 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 приложения Kaspersky Endpoint Security для Android
- 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
  - Удаление данных на Android-устройствах после неудачных попыток ввода пароля
- Настройка надежности пароля разблокировки устройства
  - Настройка надежности пароля разблокировки Android-устройства
  - Настройка надежности пароля разблокировки iOS MDM-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 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 соответствия iOS MDM-устройств требованиям корпоративной безопасности
- Контроль приложений
  - Контроль приложений на Android-устройствах
  - Контроль приложений на iOS MDM-устройствах
- Установка и удаление приложений для группы iOS MDM-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)
- Установка корневых сертификатов на Android-устройствах
- 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
Режим device owner
Ограничение функций Android на устройствах
Управление настройками Google Chrome
Настройка режима киоска
Управление Exchange ActiveSync для Gmail
Подключение к NDES/SCEP-серверу
Команды для мобильных устройств
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
Нагрузка на сеть
Участие в Kaspersky Security Network
Обмен информацией с Kaspersky Security Network
Включение и выключение использования Kaspersky Security Network
Использование Kaspersky Private Security Network
Предоставление данных сторонним сервисам
Обмен информацией с Firebase Cloud Messaging
Обмен информацией с Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics
Принятие дополнительных Положений глобально администратором
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

- Приложения
  - Права на настройку групповых политик
  - Категории приложений
- Использование приложения Kaspersky Endpoint Security для Android
  - Возможности приложения
  - Обзор главного окна
  - Значок в строке состояния
  - 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
  - Получение сертификата
  - Синхронизация с Kaspersky Security Center
  - Активация Kaspersky Endpoint Security для Android без использования Kaspersky Security Center
  - Установка приложения в режиме device owner
  - Включение специальных возможностей на Android 13 или выше
  - Обновление приложения
  - Удаление приложения
  - Приложения с "портфелем"
  - Приложение KNOX
- Использование приложения Kaspersky Security для iOS
  - Возможности приложения
  - Установка приложения
  - Активация приложения
  - Активация приложения с помощью кода активации
  - Обзор главного окна
  - Обновление приложения
  - Удаление приложения
- Лицензирование программы
  - О Лицензионном соглашении
  - О лицензии
  - О подписке
  - О ключе
  - О коде активации
  - О файле ключа
  - Предоставление данных в Kaspersky Endpoint Security для Android
  - Предоставление данных в Kaspersky Security для iOS
- Обращение в Службу технической поддержки
  - Способы получения технической поддержки
  - Техническая поддержка через Kaspersky CompanyAccount
- Источники информации о программе
- Глоссарий
  - Apple Push Notification service (APNs) сертификат
  - IMAP

iOS MDM-профиль
iOS MDM-устройство
Kaspersky Private Security Network (KPSN)
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
Контроль соответствия
Лицензионное соглашение
Лицензия
Плагин управления программой
Подписка
Политика
Прокси-сервер
Рабочее место администратора
Рабочий профиль Android
Сервер iOS MDM
Сервер администрирования
Серверы обновлений "Лаборатории Касперского"
Срок действия лицензии
Устройство в режиме supervised
Файл ключа
Фишинг
Информация о стороннем коде
Уведомления о товарных знаках

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Справка Kaspersky Security для мобильных устройств

Решение Kaspersky Security для мобильных устройств предназначено для защиты и управления корпоративными мобильными устройствами, а также личными мобильными устройствами, используемыми сотрудниками компании в корпоративных целях.

Компоненты и функции Kaspersky Security для мобильных устройств зависят от консоли Kaspersky Security Center, используемой в качестве интерфейса защиты и управления мобильными устройствами.

Выберите нужный раздел справки в зависимости от используемой консоли Kaspersky Security Center:

- Консоль администрирования на базе Консоли управления Microsoft (MMC)
- Kaspersky Security Center Web Console или Kaspersky Security Center Cloud Console

В отдельных разделах справки описаны функции и операции, доступные пользователям приложений Kaspersky Endpoint Security для Android и Kaspersky Security для iOS.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Что нового

Kaspersky Secure Mobility Management 1.0

В этом релизе мы обновили плагины Консоли администрирования на базе MMC, добавив множество функций для настройки контроля корпоративных мобильных устройств.

В плагин для управления Android-устройствами были добавлены следующие функции:

- Приложение Kaspersky Endpoint Security для Android теперь поддерживает устройства, работающие в режиме device owner. Вы можете сгенерировать QR-код для установки приложения в режиме device owner, позволяющем настраивать различные параметры устройства.
- Функции для Android-устройств в режиме device owner:
  - Ограничения функций операционной системы Android. Ограничения затрагивают:
    - функции устройства (например, сброс настроек до заводских, снимки экрана, вызовы и SMS-сообщения);
    - приложения (например, использование различных приложений и параметры установки приложений);
    - память (например, установка внешних носителей и передача файлов через USB);
    - сеть (например, сети Wi-Fi, мобильные сети и настройки VPN);
    - службы геолокации (использование местоположения и изменение настроек местоположения).
  - Управление настройками Google Chrome.
  - Режим киоска (с одним или несколькими приложениями).
  - Управление настройками Exchange ActiveSync для Gmail.
  - Подключение к NDES/SCEP-серверу.
  - Установка корневых сертификатов на устройствах.
  - Тихая установка обязательных приложений и удаление запрещенных приложений, указанных в правилах Контроля приложений.
  - Возможность удалять приложения, заблокированные Контролем приложений.
- Функции для настройки паролей разблокировки экрана на Android-устройствах:
  - Можно задавать различные требования к паролю.
  - Можно управлять использованием биометрических методов разблокировки.

    - Можно определять срок использования пароля и количество неповторяющихся паролей в журнале.
    - Можно задавать пароль разблокировки в Консоли администрирования и принудительно изменять его на устройстве.
- Новые опции для устройств Samsung KNOX:
    - Запрет режим разработчика.
    - Запрет отправки отчетов о сбоях в Google.
- Новые функции для настройки сетей Wi-Fi:
    - Поддержка протокола безопасности 802.1.x EAP и возможность настройки его параметров защиты (например, метода EAP).
    - Можно определить список сетей Wi-Fi, к которым разрешено подключаться автоматически и скрыть остальные сети на устройстве пользователя.
- Новые опции для удаления всех данных на потерянном или украденном Android-устройстве после нескольких неудачных попыток ввода пароля разблокировки.
- Добавление веб-клипов на устройствах.

В этом релизе также добавлены новые функции в плагин для управления iOS MDM-устройствами:

- Новый компонент Контроль соответствия, который позволяет контролировать соблюдение требований корпоративной безопасности на iOS MDM-устройствах и принимать различные меры.
- Можно управлять приложениями на iOS MDM-устройствах на основании списков разрешенных и запрещенных приложений.
- Добавлены новые команды:
    - Сбросить пароль.
    - Запланировать обновление ОС.
    - Настроить Bluetooth.
- Новые функции для настройки VPN-соединений:
    - Поддержка протокола IKEv2.
    - Можно настроить включение VPN-соединения для избранных доменов веб-сайтов в Safari.
- Новая опция для настройки принудительного использования пароля на устройстве.
- Новые опции для управления функциями операционной системы на устройствах в режиме supervised:
    - Отложенное обновление операционной системы.
    - Управление доступом к USB-устройствам.

- Управление настройками Wi-Fi, VPN и Персональной точки доступа.
- Управление использованием NFC.

Начиная с релиза 1.0, Kaspersky Security для мобильных устройств больше не поддерживает управление мобильными устройствами с помощью протокола Exchange ActiveSync (управление EAS-устройствами). Вместо этого вы можете обеспечить взаимодействие с Сервером Exchange через настройки политики для Android-устройств и iOS MDM-устройств. Если вы хотите продолжать управлять устройствами с помощью протокола Exchange ActiveSync, используйте более ранние версии решения Kaspersky Security для мобильных устройств.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Сравнение функций приложения в зависимости от средств управления

Для управления мобильными устройствами в Kaspersky Security Center можно используя следующие средства:

- Консоль администрирования Kaspersky Security Center на базе Microsoft Management Console (MMC)
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

В следующей таблице приведено сравнение функций, доступных для каждого из средств управления.

Доступность функций приложения в зависимости от средств управления

	Консоль администрирования	Web Console	Cloud Console
Общие			
Управление устройствами Android	Доступно	Доступно	Доступно
Управление устройствами iOS	Доступно (с помощью сертификата APNs)	Доступно (с помощью приложения Kaspersky Security для iOS)	Доступно (с помощью приложения Kaspersky Security для iOS)
Управление мобильными устройствами			
Добавление устройств по ссылке на Google Play	Доступно	Доступно	Доступно
Добавление устройств с помощью ссылки в App Store	Не доступно	Доступно	Доступно
Добавление устройств iOS с помощью профиля iOS MDM	Доступно	Не доступно	Не доступно
Добавление устройств путем создания инсталляционного пакета	Доступно	Не доступно	Не доступно
Отправка команд на мобильные устройства	Доступно	Доступно (за исключение команды Сфотографировать)	Доступно (за исключение команды Сфотографировать)
Удаление мобильных устройств из Kaspersky Security Center	Доступно	Доступно (Только удаление из списка устройств. Приложение необходимо удалить с устройства вручную.)	Доступно (Только удаление из списка устройств. Приложение необходимо удалить с устройства вручную.)
Управление сертификатами			
Выпуск почтовых сертификатов	Доступно	Не доступно	Не доступно
Выпуск VPN-сертификатов	Доступно	Не доступно	Не доступно
Выпуск мобильных сертификатов	Доступно	Доступно	Доступно
Выпуск мобильных сертификатов средствами Сервера администрирования	Доступно	Доступно	Доступно
Выбор файлов сертификатов	Доступно	Не доступно	Не доступно
Интеграция с инфраструктурой открытых ключей	Доступно	Не доступно	Не доступно
Управление политиками			

	Консоль администрирования	Web Console	Cloud Console
Доступ к параметрам групповых политик на основе ролей	Доступно	Не доступно	Не доступно
Настройка синхронизации мобильных устройств с Kaspersky Security Center	Доступно	Доступно	Доступно
Настройка антивирусной проверки на мобильных устройствах	Доступно	Доступно	Доступно
Настройка защиты мобильных устройств	Доступно	Доступно	Доступно
Настройка обновления антивирусных баз	Доступно	Доступно	Доступно
Настройка защиты данных при потере или краже устройства	Доступно	Доступно	Доступно
Настройка доступа пользователей к веб-сайтам	Доступно	Доступно	Доступно
Настройка контроля приложений	Доступно	Доступно	Доступно
Настройка контроля соответствия	Доступно	Доступно	Доступно
Настройка рабочих профилей Android	Доступно	Не доступно	Не доступно
Настройка подключения к сети Wi-Fi	Доступно	Не доступно	Не доступно
Samsung KNOX	Доступно	Не доступно	Не доступно
Прочие функции			
Централизованное принятие условий Лицензионного соглашения в Kaspersky Security Center	Доступно	Не доступно	Не доступно
Настройка Kaspersky Private Security Network	Доступно	Не доступно	Не доступно

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Комплект поставки

В состав дистрибутива Kaspersky Security для мобильных устройств могут входить различные компоненты в зависимости от выбранной версии программы.

Управление мобильными устройствами в Kaspersky Security Center Web Console

- `on_prem_ksm_devices_xx.x.x.x.zip`

  Архив, содержащий файлы, необходимые для установки плагина Kaspersky Security for Mobile (Devices):

  - `plugin.zip`

    Архив, содержащий плагин Kaspersky Security for Mobile (Devices).

  - `signature.txt`

    Файл, содержащий подпись плагина Kaspersky Security for Mobile (Devices).

- `on_prem_ksm_policies_xx.x.x.x.zip`

  Архив, содержащий файлы, необходимые для установки плагина Kaspersky Security for Mobile (Policies):

  - `plugin.zip`

    Архив, содержащий плагин Kaspersky Security for Mobile (Policies).

  - `signature.txt`

    Файл, содержащий подпись плагина Kaspersky Security for Mobile (Policies).

Управление мобильными устройствами в Kaspersky Security Center Cloud Console

Для управления мобильными устройствами в Kaspersky Security Center Cloud Console не нужно скачивать дистрибутив. Нужно только создать учетную запись в Kaspersky Security Center Cloud Console. Дополнительная информация о создании учетной записи приведена в *Справке Kaspersky Security Center Cloud Console*.

Управление мобильными устройствами в Консоли администрирования на базе MMC

- `Klcfginst_en.exe`

  Файл для установки плагина управления Kaspersky Endpoint Security для Android, предназначенного для управления программой с помощью системы удаленного администрирования Kaspersky Security Center.

- `Klmdminst.exe`

  Файл для установки плагина управления Kaspersky Device Management для iOS, предназначенного для управления программой с помощью системы удаленного администрирования Kaspersky Security Center.

Файл приложения Kaspersky Endpoint Security для Android

`KES10_xx_xx_xxx.apk` – пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

Дополнительные файлы

- `sc_package_xx.exe`

  Самораспаковывающийся архив, содержащий файлы, необходимые для установки Kaspersky Endpoint Security для Android путем создания инсталляционных пакетов:

  - `adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll`

    Файлы, необходимые для создания инсталляционных пакетов.

  - `installer.ini`

    Конфигурационный файл с параметрами подключения к Серверу администрирования.

  - `KES10_xx_xx_xxx.apk`

    Пакетный файл Android для приложения Kaspersky Endpoint Security для Android.

  - `kmlisten.exe`

    Утилита для доставки инсталляционных пакетов с компьютера администратора.

  - `kmlisten.ini`

    Конфигурационный файл, содержащий параметры утилиты `kmlisten.exe`.

  - `kmlisten.kpd`

    Файл, содержащий описание программы.

- `SigningUtility.zip`

  Архив, содержащий утилиту для подписания дистрибутивов приложения Kaspersky Endpoint Security для Android и контейнеров для iOS-устройств.

Комплект документации

- Справка для Kaspersky Security для мобильных устройств.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Работа в Kaspersky Security Center Web Console и Kaspersky Security Center Cloud Console

В этом разделе справки описана защита и управление мобильными устройствами с помощью Kaspersky Security Center Web Console (далее также Web Console) и Kaspersky Security Center Cloud Console (далее также Cloud Console).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Об управлении мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console

Вы можете управлять мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console, используя следующие компоненты:

- **Приложение Kaspersky Endpoint Security для Android**

  Приложение Kaspersky Endpoint Security для Android обеспечивает защиту мобильных устройств от веб-угроз, вирусов и других программ, представляющих угрозы.

- **Приложение Kaspersky Security для iOS**

  Приложение Kaspersky Security для iOS обеспечивает защиту мобильных устройств от фишинга и веб-угроз.

- **Плагин Kaspersky Security for Mobile (Devices)**

  Плагин Kaspersky Security for Mobile (Devices) предоставляет интерфейс для управления мобильными устройствами и установленными на них мобильными приложениями с помощью Kaspersky Security Center Web Console и Cloud Console.

- **Плагин Kaspersky Security for Mobile (Policies)**

  Плагин Kaspersky Security for Mobile (Policies) позволяет определять параметры конфигурации устройств, подключенных к Kaspersky Security Center, с помощью групповых политик.

Плагины интегрируются в *систему удаленного администрирования Kaspersky Security Center*. Вы можете использовать Kaspersky Security Center Web Console или Cloud Console для управления мобильными устройствами, а также клиентскими компьютерами и виртуальными системами. После подключения мобильных устройств к Серверу администрирования они становятся управляемыми. Вы можете удаленно контролировать управляемые устройства.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Основные функции управления мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console

Kaspersky Security для мобильных устройств предоставляет следующие функции:

- Рассылка сообщений электронной почты для подключения мобильных устройств Android к Kaspersky Security Center с использованием ссылок для загрузки приложения Kaspersky Endpoint Security для Android из Google Play.
- Рассылка сообщений электронной почты для подключения мобильных устройств iOS к Kaspersky Security Center с использованием ссылок для загрузки приложения Kaspersky Security для iOS из App Store.
- Дистанционное подключение мобильных устройств к Kaspersky Security Center и другим сторонним EMM-системам (например, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Удаленная настройка мобильного приложения, а также удаленная настройка сервисов, приложений и функций мобильных устройств.
- Дистанционная настройка мобильных устройств согласно требованиям корпоративной безопасности.
- Предотвращение утечек корпоративной информации, хранящейся на мобильных устройствах, в случае их кражи или потери (Анти-Вор). Поддерживается только для устройств Android.
- Контроль соблюдения требований корпоративной безопасности (Контроль соответствия). Поддерживается только для устройств Android.
- Контроль защиты от онлайн-угроз и контроль использования интернета на мобильных устройствах (Веб-Фильтр).
- Настройка уведомлений, отображаемых пользователю в приложениях Kaspersky Endpoint Security для Android и Kaspersky Security для iOS.
- Уведомление администратора о статусе и событиях в работе приложений Kaspersky Endpoint Security для Android и Kaspersky Security для iOS в Kaspersky Security Center или по электронной почте.
- Контроль изменений параметров политики (история ревизий).

Kaspersky Security для мобильных устройств включает следующие компоненты защиты и управления:

- Антивирус (для Android-устройств).
- Анти-Вор (для Android-устройств).
- Веб-Фильтр (для Android и iOS-устройств).
- Контроль приложений (для Android-устройств).

- Контроль соответствия (для Android-устройств).
- Обнаружение root-прав на устройствах Android и обнаружение jailbreak на устройствах iOS.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 следующие компоненты:

- **Антивирус**. Этот компонент обнаруживает и устраняет угрозы на устройствах, используя антивирусные базы и облачную службу Kaspersky Security Network. В состав Антивируса входят следующие компоненты:
  - **Защита**. Обнаруживает угрозы в открытых файлах, проверяет новые приложения и предотвращает 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:
  - **Определение местоположения**. Получение координат местоположения устройства.
  - **Воспроизведение звукового сигнала**. Устройство издает громкий сигнал тревоги.
  - **Удаление данных**. 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 перед открытием, 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.

Вы можете настроить компоненты приложения Kaspersky Endpoint Security для Android в Kaspersky Security Center Web Console и Cloud Console, задав параметры групповых политик.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О приложении Kaspersky Security для iOS

Приложение Kaspersky Security для iOS обеспечивает защиту мобильных устройств от фишинга и веб-угроз.

Kaspersky Security для iOS предоставляет следующие ключевые функции:

- **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 перед открытием, используя облачную службу Kaspersky Security Network. По результатам проверки Веб-Фильтр разрешает загрузку веб-сайтов, признанных надежными, и блокирует веб-сайты, признанные вредоносными. Вы можете настроить этот компонент в Kaspersky Security Center Web Console и Cloud Console, определив настройки групповых политик.

- **Обнаружение модификации прошивки (jailbreak)**. Если приложение Kaspersky Security для iOS обнаруживает модификацию прошивки (jailbreak), то отображает критическое сообщение и информирует вас о проблеме.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О плагине Kaspersky Security for Mobile (Devices)

Плагин Kaspersky Security for Mobile (Devices) предоставляет интерфейс для управления мобильными устройствами и установленными на них мобильными приложениями с помощью Kaspersky Security Center Web Console и Cloud Console. Плагин Kaspersky Security for Mobile (Devices) позволяет выполнять следующие действия:

- подключать мобильные устройства к Kaspersky Security Center;
- управлять сертификатами мобильных устройств;
- настраивать Firebase Cloud Messaging (только для устройств Android);
- отправлять команды на мобильные устройства (только для устройств Android).

Плагин Kaspersky Security for Mobile (Devices) можно установить при настройке Kaspersky Security Center Web Console. При использовании Kaspersky Security Center Cloud Console, вам не нужно устанавливать этот плагин. Дополнительная информация о сценариях развертывания для различных типов консолей приведена в разделе Сценарии развертывания.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О плагине Kaspersky Security for Mobile (Policies)

Плагин Kaspersky Security for Mobile (Policies) позволяет определять параметры конфигурации устройств, подключенных к Kaspersky Security Center, с помощью групповых политик. Плагин Kaspersky Security for Mobile (Policies) позволяет выполнять следующие действия:

- создавать групповые политики безопасности мобильных устройств;
- удаленно настраивать параметры работы приложения на мобильных устройствах пользователей;
- получать отчеты и статистику о работе приложения на мобильных устройствах пользователей.

Плагин Kaspersky Security for Mobile (Policies) можно установить при настройке Kaspersky Security Center Web Console. При использовании Kaspersky Security Center Cloud Console, вам не нужно устанавливать этот плагин. Дополнительная информация о сценариях развертывания для различных типов консолей приведена в разделе Сценарии развертывания.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Аппаратные и программные требования

В этом разделе перечислены аппаратные и программные требования к компьютеру администратора, используемому для установки плагинов Kaspersky Security for Mobile (Devices) и Kaspersky Security for Mobile (Policies) в Kaspersky Security Center Web Console и Cloud Console, а также аппаратные и программные требования мобильных приложений.

Аппаратные и программные требования к компьютеру администратора

Для установки плагинов Kaspersky Security for Mobile (Devices) и Kaspersky Security for Mobile (Policies), компьютер администратора должен соответствовать аппаратным требованиям Kaspersky Security Center. Дополнительная информация об аппаратных и программных требованиях для Kaspersky Security Center приведена в следующих документах:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Для использования плагинов Kaspersky Security for Mobile (Devices) и Kaspersky Security for Mobile (Policies) в Kaspersky Security Center Web Console, эта консоль должна быть установлена на компьютере администратора.

Для использования плагинов Kaspersky Security for Mobile (Devices) и Kaspersky Security for Mobile (Policies) в Kaspersky Security Center Cloud Console необходимо создать учетную запись в Kaspersky Security Center Cloud Console. Дополнительная информация о создании учетной записи приведена в *Справке Kaspersky Security Center Cloud Console*.

Также приложение Kaspersky Endpoint Security для Android может работать в составе следующих 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 установки 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 5.0–13 (включая Android 12L, исключая Go Edition);
- 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 установки Kaspersky Security для iOS

Приложение Kaspersky Security для iOS имеет следующие аппаратные требования:

- iPhone 6S или более поздней версии
- iPad Air 2 или более поздней версии

Приложение Kaspersky Security для iOS имеет следующие программные требования:

- iOS 14.1 или более поздней версии
- iPadOS 14.1 или более поздней версии

Приложение Kaspersky Security для iOS не может работать корректно, если на мобильном устройстве одновременно запущен VPN-клиент с активным VPN-подключением.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Известные проблемы и рекомендации

Kaspersky Endpoint Security для Android и Kaspersky Security для iOS имеют некоторые известные проблемы, которые не являются критичными для работы этих приложений.

Известные ошибки Kaspersky Security для iOS

- Приложение Kaspersky Security для iOS не может работать корректно, если на мобильном устройстве одновременно запущен VPN-клиент с активным VPN-подключением.

Известные ошибки Kaspersky Endpoint Security для Android

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 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.

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.
- Иногда обновление антивирусных баз с Сервера администрирования может завершиться ошибкой на мобильных устройствах. В этом случае запустите задачу обновления антивирусных баз на Сервере администрирования.
- На некоторых устройствах Kaspersky Endpoint Security для Android не обнаруживает устройства, подключенные по USB OTG. Выполнить антивирусную проверку таких устройств невозможно.
- На устройствах с операционной системой Android 11 и выше приложение Kaspersky Endpoint Security для Android не может сканировать папки Android/data и Android/obb и обнаруживать в них вредоносные программы из-за технических ограничений.

- На устройствах с операционной системой Android 11 и выше пользователю необходимо предоставить разрешение "Разрешить доступ на управление всеми файлами".

- 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 7.0 при выполнении задачи постоянной защиты в расширенном режиме не выполняется обнаружение угроз в файлах, хранящихся на внешней SD-карте.

- 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 (включая функцию Custom Tabs), Huawei Browser и Samsung Internet Browser.

- 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.

- На некоторых устройствах Xiaomi для работы Веб-Фильтра должны быть предоставлены разрешения "Отображать всплывающие окна" и "Отображать всплывающие окна во время работы в фоновом режиме".

- 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`).

- Если для Веб-Фильтра выбран режим **Запрещены все веб-сайты**, то Kaspersky Endpoint Security для Android не блокирует поиск в виджете Google Поиск. Вместо этого блокируется доступ к результатам поиска.

- Если в рабочем профиле для Веб-Фильтра выбран режим **Запрещены все веб-сайты**, то Kaspersky Endpoint Security для Android постоянно перезагружает главную страницу Google Chrome, блокирует браузер и мешает работе устройства.

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.

Известные проблемы в работе Контроля приложений

- Для работы Контроля приложений Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Не применимо к режиму device owner.

- 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 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 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 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.

- На некоторых устройствах Xiaomi и Huawei защита Kaspersky Endpoint Security для Android от удаления не работает. Проблема связана с особенностями прошивки MIUI 7 и 8 на Xiaomi и прошивки EMUI на Huawei.

Известные проблемы при настройке ограничений устройства

- На устройствах под управлением Android 10.0 и выше запрет на использование сетей Wi-Fi не поддерживается.

- На устройствах под управлением Android 10 и выше использование камеры нельзя запретить полностью.

- На устройствах с операционной системой Android 11 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 не удастся ограничить использование камеры.

Известные проблемы при отправке команд на мобильные устройства

- На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой.

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 устройствах Huawei под управлением Android 5.X после установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей отображается неверное сообщение об отсутствии соответствующих 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 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 устройствах Honor и Huawei 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.

- На устройствах Blackview пользователь может очистить память для приложения Kaspersky Endpoint Security для Android. В результате защита и управление устройством отключается, все заданные параметры становятся недействительными, а приложение Kaspersky Endpoint Security для Android удаляется из специальных возможностей. Это связано с тем, что устройства этого производителя предоставляют приложению "Недавние экраны" (Recent screens) расширенные права. Приложение может переопределять значения параметров Kaspersky Endpoint Security для Android, и его нельзя заменить, поскольку оно является частью операционной системы Android.

- На некоторых устройствах Google Pixel под управлением Android 11 и ниже сразу после запуска приложения Kaspersky Endpoint Security для Android происходит его сбой. Это связано с проблемой в Android.

- На устройствах Samsung серий Galaxy S23 и S24 может не работать постоянная защита.

Известные проблемы при работе на Android 13

- На Android 13 пользователь может использовать Диспетчер задач ОС, чтобы остановить работу Kaspersky Endpoint Security в фоновом режиме. Это связано с известной проблемой в Android 13.

- На Android 13 разрешение на отправку уведомлений запрашивается в начале настройки приложения. Это связано с особенностями операционной системы Android 13.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Развертывание решения для управления мобильными устройствами в Kaspersky Security Center Web Console или Cloud Console

Для управления мобильными устройствами с помощью Kaspersky Security Center Web Console или Cloud Console необходимо развернуть решение для управления мобильными устройствами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Сценарии развертывания

Развертывание в Kaspersky Security Center Web Console

Развертывание решения для управления мобильными устройствами в Kaspersky Security Center Web Console состоит из следующих шагов:

1. **Подготовка Kaspersky Security Center Web Console к развертыванию**
2. **Развертывание плагинов управления**
3. **Развертывание мобильного приложения**
4. **(Необязательно, только для Android) Настройка обмена данными с Firebase Cloud Messaging**

   Этот шаг рекомендуется выполнить для своевременной доставки команд на мобильные устройства и принудительной синхронизации при изменении параметров политики.

Развертывание в Kaspersky Security Center Cloud Console

Развертывание решения для управления мобильными устройствами в Kaspersky Security Center Cloud Console состоит из следующих шагов:

1. **Подготовка Kaspersky Security Center Cloud Console к развертыванию**
2. **Развертывание мобильного приложения**

3. (Необязательно, только для Android) Настройка обмена данными с Firebase Cloud Messaging

Этот шаг рекомендуется выполнить для своевременной доставки команд на мобильные устройства и принудительной синхронизации при изменении параметров политики.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Подготовка Kaspersky Security Center Web Console и Cloud Console к развертыванию

В этом разделе приведены инструкции по подготовке Kaspersky Security Center Web Console и Cloud Console к развертыванию.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка Сервера администрирования для подключения мобильных устройств

Чтобы мобильные устройства могли подключаться к Серверу администрирования, перед установкой приложения на мобильные устройства необходимо задать параметры подключения.

- Если вы используете Kaspersky Security Center Web Console, настройте свойства, как описано ниже.
- Если вы используете Kaspersky Security Center Cloud Console, параметры подключения определяются при первоначальной настройке Kaspersky Security Center Cloud Console. Дополнительная информация приведена в справке Kaspersky Security Center.

Чтобы настроить свойства Kaspersky Security Center Web Console для подключения мобильного устройства:

1. В главном окне Kaspersky Security Center Web Console нажмите на кнопку **Настройка** ().

   Откроется окно свойств Сервера администрирования.

2. Настройте порты Сервера администрирования, используемые для мобильных устройств:

   a. Выберите раздел **Дополнительные порты**.

   b. Включите переключатель **Открывать порт для мобильных устройств**.

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

По умолчанию указан порт 13292.

Если переключатель **Открывать порт для мобильных устройств** выключен или порт для подключения указан неверно, мобильные устройства не смогут подключаться к Серверу администрирования.

d. В поле **Порт для активации мобильных устройств** укажите порт для подключения мобильных устройств к Серверу администрирования для активации мобильного приложения.

По умолчанию указан порт 17100.

Если указан неверный порт подключения, пользователи мобильных устройств не смогут активировать приложение с помощью Сервера администрирования.

3. При необходимости измените сертификат, используемый мобильными устройствами для подключения к Серверу администрирования.

По умолчанию используется сертификат, созданный при установке Сервера администрирования. При необходимости замените сертификат, выданный Сервером администрирования, на другой сертификат или перевыпустите его.

Чтобы изменить сертификат, выполните следующие действия:

a. Выберите раздел **Сертификаты**.

b. Задайте необходимые параметры.

Подробная информация о сертификатах приведена в *Справке Kaspersky Security Center*.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить измененные параметры и закрыть окно свойств Сервера администрирования.

После настройки параметров подключения мобильных устройств можно установить приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS на мобильные устройства и подключить их к Серверу администрирования, используя указанные параметры.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка шлюза соединения для подключения мобильных устройств к Серверу администрирования Kaspersky Security Center

В этом разделе описывается настройка шлюза соединения для подключения мобильных устройств к Серверу администрирования Kaspersky Security Center. Настройка включает в себя следующие шаги:

1. Установка Агента администрирования в качестве шлюза соединения на хосте.

2. Настройка шлюза соединения на Сервере администрирования Kaspersky Security Center.

Эта статья содержит обзор сценария. Более подробная информация приведена в документации Kaspersky Security Center.

Требования

Чтобы шлюз соединения корректно работал с мобильными устройствами, должны соблюдаться следующие требования:

- Порт 13292 должен быть открыт на хосте со шлюзом соединения.
- Порт 13000 должен быть открыт между шлюзом соединения и Kaspersky Security Center. Его открытие наружу из демилитаризованной зоны не требуется.
- Хост должен иметь статический адрес, доступный из интернета.

Установка Агента администрирования на хост, выполняющий роль шлюза соединения

Сначала необходимо установить Агент администрирования на выбранном устройстве-хосте, который будет выступать в качестве шлюза соединения. Вы можете загрузить полный инсталляционный пакет Kaspersky Security Center или установить Kaspersky Security Center локально.

По умолчанию установочный файл расположен по следующему пути: `\\<server name>\KLSHARE\PkgInst\NetAgent_<version number>`

Чтобы установить Агент администрирования в роли шлюза соединения:

1. Запустите Мастер установки Агента администрирования и следуйте его указаниям, оставляя настройки по умолчанию для всех параметров, пока не откроется окно **Выбор Сервера администрирования**.
2. В окне **Выбор Сервера администрирования** настройте следующие параметры:
   - Введите адрес устройства с установленным Сервером администрирования.
   - Оставьте значения по умолчанию в полях **Порт**, **SSL-порт** и **UDP-порт**.
   - Установите флажок **Использовать SSL для соединения с Сервером администрирования**, чтобы установить соединение с Сервером администрирования через защищенный порт с использованием SSL.

     Рекомендуется не снимать этот флажок, чтобы соединение оставалось защищенным.
   - Установите флажок **Разрешить Агенту администрирования открыть UDP-порт**, чтобы управлять клиентскими устройствами и получать о них информацию.
3. Нажмите **Далее** и пройдите все шаги мастера до появления окна **Шлюз соединения**, оставляя настройки по умолчанию.
4. В окне **Шлюз соединения** выберите **Использовать в качестве шлюза соединения в демилитаризованной зоне**.

   Этот режим одновременно активирует Агент администрирования в роли шлюза соединения и переключает его на ожидание подключений от Сервера администрирования, а не на установку подключения к Серверу администрирования.
5. Нажмите **Далее** и начните установку.

Теперь Агент администрирования установлен и настроен в качестве шлюза соединения.

Настройка шлюза соединения на Сервере администрирования Kaspersky Security Center

После установки Агента администрирования в качестве шлюза соединения необходимо подключить его к Серверу администрирования. Сервер администрирования пока не отображает устройство со шлюзом соединения в списке управляемых устройств, поскольку шлюз соединения еще не подключался к Серверу администрирования. По этой причине необходимо добавить шлюз соединения как точку распространения, чтобы убедиться, что Сервер администрирования инициирует подключение к шлюзу соединения.

Чтобы настроить шлюз соединения на Сервере администрирования:

1. Добавьте шлюз соединения как точку распространения в Kaspersky Security Center.

   a. В дереве консоли выберите узел **Сервер администрирования**.

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

   c. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.

   d. Нажмите на кнопку **Добавить**.

   Откроется окно **Добавление точки распространения**.

   e. В окне **Добавление точки распространения** выполните следующие действия:

   - Укажите IP-адрес устройства с установленным Агентом администрирования в поле **Устройство, которое будет выполнять роль точки распространения**. Для этого выберите пункт **Добавить шлюз соединения, находящийся в демилитаризованной зоне, по адресу** в раскрывающемся списке.

     Введите IP-адрес шлюза соединения или имя шлюза соединения, если к нему можно получить доступ по имени.

   - В поле **Область действия точки распространения**, в раскрывающемся списке выберите группу, на которую будет распространяться шлюз соединения, а затем нажмите **ОК**.

   f. В разделе **Точки распространения** нажмите **ОК**, чтобы сохранить внесенные изменения.

   Шлюз соединения будет сохранен как новая запись под именем **Временная запись для шлюза соединения**.

   Сервер администрирования практически сразу попытается подключиться к шлюзу соединения по указанному вами адресу. При удачном подключении имя записи изменится на имя устройства шлюза соединения. Этот процесс занимает до 5 минут.

   Пока временная запись для шлюза соединения переводится в именованную запись, шлюз соединения также отображается в группе **Нераспределенные устройства**.

2. Создайте новую группу в группе **Управляемые устройства**. В эту группу будут входить внешние управляемые устройства.

3. Переместите шлюз соединения из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

4. Настройте свойства шлюза соединения, который вы развернули:

    1. В свойствах Сервера администрирования, в разделе **Точки распространения** выберите шлюз соединения и нажмите **Свойства**.

    2. В разделе **Общие**, в свойстве **Имена DNS-доменов точки распространения, под которыми она будет доступна мобильным устройствам (включаются в сертификат)** укажите DNS-имя шлюза соединения, которое будет использоваться для подключения к мобильному устройству.

    3. В разделе **Шлюз соединения** установите следующие флажки, оставляя номера портов по умолчанию:

        - **Открыть порт для мобильных устройств (аутентификация SSL только для Сервера администрирования).**

        - **Открыть порт для мобильных устройств (двусторонняя аутентификация SSL).**

    4. Нажмите **OK**, чтобы сохранить внесенные изменения.

Шлюз соединения настроен. Теперь вы можете добавлять новые мобильные устройства, указав адрес шлюза соединения. Новые устройства появятся на Сервере администрирования.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Создание группы администрирования

Групповые политики используются для централизованной настройки приложений Kaspersky Endpoint Security для Android и Kaspersky Security для iOS, установленных на мобильных устройствах пользователей.

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 главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Иерархия групп**.

2. В структуре групп администрирования выберите группу администрирования, в которую будет добавлена новая группа администрирования.

3. Нажмите на кнопку **Добавить**.

4. В открывшемся окне **Имя новой группы администрирования** укажите название группы и нажмите на кнопку **Добавить**.

В иерархии групп администрирования появится новая группа администрирования с указанным именем.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Создание правила автоматического перемещения устройств в группу администрирования

Мобильные устройства, на которых установлено приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS, отображаются на странице **Обнаружение и развертывание** > **Нераспределенные устройства** в Kaspersky Security Center Web Console или Cloud Console. Для управления новыми подключенными устройствами можно вручную переместить их в группу администрирования или создать правило автоматического распределения устройств по группам администрирования.

Чтобы создать правило автоматического распределения мобильных устройств по группам администрирования, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Обнаружение и развертывание** > **Развертывание и назначение** > **Правила перемещения**.
2. В открывшемся окне **Новое правило** нажмите на кнопку **Добавить**.
3. В поле **Имя правила** укажите название правила.
4. В поле **Группа администрирования** выберите группу администрирования, в которую будут перемещены мобильные устройства после установки на них приложения.
5. В разделе **Применение правила** выберите вариант **Выполняется один раз для каждого устройства**.
6. Установите флажок **Перемещать только устройства, не принадлежащие группам администрирования**, чтобы в результате применения правила мобильные устройства, принадлежащие другим группам администрирования, не были перемещены в выбранную группу.
7. Установите флажок **Включить правило**, чтобы правило применялось сразу после создания.

   Правило можно включить позже в любое время, используя переключатель на странице **Правила перемещения**.
8. Выберите **Условия правила** > **Приложения** и выполните следующие действия:

   a. Включите переключатель **Версия операционной системы**.

   b. В открывшемся списке операционных систем выберите **Android** или **iOS**.

   Правило будет применяться к соответствующим устройствам. Для создания правила необходимо указать хотя бы одно условие.
9. Нажмите на кнопку **Сохранить**, чтобы создать правило.

Новое созданное правило отобразится на странице **Правила перемещения**. Согласно правилу, Kaspersky Security Center помещает все новые подключенные устройства в выбранную группу администрирования.

Подробная информация об управлении группами администрирования и действиях с нераспределенными устройствами приведена в следующих документах:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Развертывание плагинов управления

Для управления мобильными устройствами с помощью Kaspersky Security Center Web Console должны быть установлены следующие плагины управления:

- Плагин Kaspersky Security for Mobile (Devices).
- Плагин Kaspersky Security for Mobile (Policies).

При использовании Kaspersky Security Center Cloud Console плагины управления устанавливать не нужно. Нужно только создать учетную запись в Kaspersky Security Center Cloud Console. Дополнительная информация о создании учетной записи приведена в *Справке Kaspersky Security Center Cloud Console*.

Плагины управления можно установить следующими способами:

- С помощью Мастера первоначальной настройки Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console 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.

  Более подробная информация о Мастере первоначальной настройки Kaspersky Security Center приведена в *справке Kaspersky Security Center*.

- С помощью списка доступных дистрибутивов в Kaspersky Security Center Web Console.

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

- Загрузите дистрибутивы из внешнего источника и добавьте плагины управления Kaspersky Security Center Web Console.

  Например, дистрибутивы плагинов управления можно загрузить с сайта "Лаборатории Касперского".

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка плагинов управления из списка доступных дистрибутивов

Чтобы установить плагины управления, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console выберите **Параметры консоли** > **Веб-плагины**.
2. Нажмите на кнопку **Добавить**.

   Откроется список актуальных версий приложений "Лаборатории Касперского".
3. Установите плагины управления:
   a. В списке доступных приложений раскройте раздел **Мобильные устройства**.
   b. Выберите плагин **Kaspersky Security for Mobile (Devices)** и нажмите **Установить плагин**.
   c. Выберите плагин **Kaspersky Security for Mobile (Policies)** и нажмите **Установить плагин**.

Будут загружены дистрибутивы и установлены плагины. После установки и добавления плагинов в Kaspersky Security Center Web Console, отобразится окно подтверждения.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка плагинов управления из дистрибутива

Вы можете загрузить дистрибутив на сайте "Лаборатории Касперского".

Чтобы установить плагин Kaspersky Security for Mobile (Devices) из дистрибутива, выполните следующие действия:

1. Скопируйте файлы `plugin.zip` и `signature.txt` из архива дистрибутива `on_prem_ksm_devices_xx.x.x.x.zip` на рабочее место администратора.
2. В главном окне Kaspersky Security Center Web Console выберите **Параметры консоли** > **Веб-плагины**.
3. Нажмите на кнопку **Импортировать**.
4. В открывшемся окне **Импортировать** нажмите **Загрузить ZIP-файл** и выберите файл `plugin.zip`.
5. Нажмите на кнопку **Загрузить подпись** и выберите файл `signature.txt`.
6. Нажмите на кнопку **Добавить**.

Плагин Kaspersky Security for Mobile (Devices) будет установлен и добавлен в Kaspersky Security Center Web Console.

Чтобы установить плагин Kaspersky Security for Mobile (Policies) из дистрибутива, выполните следующие действия:

1. Скопируйте файлы `plugin.zip` и `signature.txt` из архива дистрибутива `on_prem_ksm_policies_xx.x.x.x.zip` на рабочее место администратора.
2. В главном окне Kaspersky Security Center Web Console выберите **Параметры консоли** > **Веб-плагины**.
3. Нажмите на кнопку **Импортировать**.
4. В открывшемся окне **Импортировать** нажмите **Загрузить ZIP-файл** и выберите файл `plugin.zip`.
5. Нажмите на кнопку **Загрузить подпись** и выберите файл `signature.txt`.
6. Нажмите на кнопку **Добавить**.

   Плагин Kaspersky Security for Mobile (Policies) будет установлен и добавлен в Kaspersky Security Center Web Console.

Вы можете проверить, установлены ли плагины управления, просмотрев список установленных плагинов на странице **Параметры консоли** > **Веб-плагины**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Развертывание мобильного приложения

Для управления мобильными устройствами в Kaspersky Security Center Web Console или Cloud Console необходимо развернуть приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS на мобильных устройствах. Приложения на мобильных устройствах можно развернуть с помощью Kaspersky Security Center Web Console или Cloud Console.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Развертывание мобильного приложения с помощью Kaspersky Security Center Web Console или Cloud Console

Развертывание мобильного приложения выполняется на мобильных устройствах пользователей, учетные записи которых добавлены в Kaspersky Security Center. Дополнительная информация об учетных записях пользователей в Kaspersky Security Center приведена в:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Вы можете использовать плагин Kaspersky Security for Mobile (Devices), чтобы установить приложение из Kaspersky Security Center Web Console и Cloud Console, отправив ссылку для установки на мобильное устройство.

- На устройстве Android пользователь получает ссылку на Google Play для загрузки приложения Kaspersky Endpoint Security для Android. Установка выполняется обычным способом, принятым для платформы Android. После установки приложения пользователю необходимо предоставить необходимые разрешения.

  У некоторых устройств Huawei и Honor отсутствуют сервисы Google и, следовательно, нет доступа 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.

- На устройстве iOS пользователь получает ссылку из App Store для загрузки приложения Kaspersky Security для iOS. Установка выполняется обычным способом, принятым для платформы iOS.

  Перед подключением устройства iOS отправьте адрес Kaspersky Security Center пользователю устройства, чтобы повысить безопасность подключения. Пользователь увидит этот адрес во время установки приложения и сможет отменить соединение, если отображаемый адрес не совпадает с адресом, который вы отправили.

Ссылка содержит следующие данные:

- параметры синхронизации с Kaspersky Security Center;
- мобильный сертификат.

Чтобы развернуть приложение на мобильном устройстве:

1. Запустите Мастер подключения мобильного устройства:
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**, а затем нажмите на кнопку **Добавить**.
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Пользователи и роли** > **Пользователи**. Выберите имя пользователя или группы пользователей, которым вы хотите отправить ссылку для подключения мобильного устройства, а затем выберите **Устройства.** Нажмите на кнопку **Добавить мобильное устройство**. В этом случае пропустите шаг 3.

Пройдите все шаги мастера, нажимая на кнопку **Далее**.

2. Выберите операционную систему устройств, которые вы хотите добавить:

   - **Android**
   - **iOS и iPadOS**

3. Выберите пользователей и группы пользователей, которым вы хотите отправить ссылку для подключения мобильного устройства.

4. Выберите адреса электронной почты, на которые следует отправить ссылку:

   - **Все адреса электронной почты**
   - **Основной адрес электронной почты**
   - **Дополнительный адрес электронной почты**
   - **Другой адрес электронной почты**

     Если вы выбрали этот вариант, ниже укажите адрес электронной почты.

5. Отображается итоговый вид ссылки.

   Убедитесь, что все параметры ссылки верны, и нажмите на кнопку **Отправить**.

6. Откроется окно с подтверждением отправки ссылки для добавления мобильного устройства.

   Нажмите на кнопку **ОК**, чтобы завершить работу Мастера.

Когда пользователь устанавливает приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS, устройство пользователя появится на закладке **Устройства** > **Мобильные** > **Устройства** в Web Console или Cloud Console. После установки приложения на мобильные устройства пользователей вы сможете настраивать параметры устройств и приложений с помощью групповых политик. Вы также сможете отправлять на мобильные устройства команды (только для устройств Android) для защиты данных в случае потери или кражи устройств.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Активация мобильного приложения

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования приложения Kaspersky Endpoint Security для Android или Kaspersky Security для iOS 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.

Дополнительная информация о лицензировании Kaspersky Security Center и вариантах лицензирования приведена в:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Активация приложения Kaspersky Endpoint Security для Android или Kaspersky Security для iOS на мобильном устройстве осуществляется путем предоставления приложению информации о действующей лицензии. Информация о лицензии передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

Если мобильное приложение не было активировано в течение 30 дней с момента установки на мобильное устройство, оно 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 приложение не было активировано в течение 30 дней с момента установки, пользователю необходимо вручную выполнить синхронизацию устройства с Kaspersky Security Center.

Если Kaspersky Security Center не развернут в вашей организации или недоступен для мобильных устройств, пользователи могут активировать мобильное приложение на своих устройствах вручную.

Чтобы активировать мобильное приложение:

1. Откройте окно свойств политики:
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.
2. На странице свойств политики выберите **Параметры приложений** > **Лицензии**.
3. С помощью раскрывающегося списка выберите требуемый лицензионный ключ в хранилище ключей Сервера администрирования.

   Подробная информация о лицензионном ключе отображается в полях ниже.

   Если выбрать файл ключа из хранилища ключей Kaspersky Security Center и отправить его на устройство, Kaspersky Security для iOS не сможет его обработать, потому что не поддерживает такой формат активации. Чтобы активировать Kaspersky Security для iOS, добавьте в Kaspersky Security Center лицензию в виде кода активации.

Вы можете заменить существующий ключ активации на мобильном устройстве, если он отличается от ключа, выбранного в раскрывающемся списке. Для этого установите флажок **Если на устройстве используется другой ключ, замените его этим ключом**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Предоставление необходимых разрешений приложению Kaspersky Endpoint Security для Android

Для доступа к некоторым функциям приложения Kaspersky Endpoint Security для Android требуются разрешения. Kaspersky Endpoint Security для Android запрашивает обязательные разрешения во время установки, а также после установки и перед использованием отдельных функций. 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 этот список, Kaspersky Endpoint Security для Android прекращает выполнять все свои функции после перезагрузки мобильного устройства.

На устройствах с операционной системой Android 11 и выше необходимо отключить системную настройку **Удалить разрешения, если приложение не используется**. В противном случае, если приложение не используется в течение нескольких месяцев, система автоматически сбрасывает разрешения, предоставленные приложению пользователем.

Разрешения, запрашиваемые Kaspersky Endpoint Security для Android

Разрешение	Функция приложения
Телефон (для Android 5.0 – 9.X)	Подключение к Kaspersky Security Center (идентификатор устройства)
Память (обязательно)	Антивирус
Доступ на управление всеми файлами (для Android 11 или более поздней версии)	Антивирус
Устройства Bluetooth поблизости (Android 12 или более поздней версии)	Ограничение использования Bluetooth
Уведомления (для Android 13)	Уведомление пользователя о проблемах безопасности и событиях приложения
Разрешение на работу в фоновом режиме (Android 12 или более поздней версии)	Обеспечение непрерывной работы приложения. Если разрешение не предоставлено, приложение может быть выгружено из памяти и не сможет перезапуститься.

Разрешение	Функция приложения
Администратор устройства (обязательно)	Анти-Вор – блокировка устройства (только для Android 5.0 – 6.X)
	Анти-Вор – выполнение снимка фронтальной камерой Создание снимков не поддерживается в Kaspersky Security Center Web Console и Cloud Console, однако приложению Kaspersky Endpoint Security для Android требуется это разрешение, чтобы обеспечить возможность управлять приложением со всех консолей Kaspersky Security Center.
	Анти-Вор – воспроизведение звукового сигнала
	Анти-Вор – сброс настроек до заводских
	Защита паролем
	Защита приложения от удаления
	Установка сертификатов безопасности
	Контроль приложений
	Ограничение использования камеры, Bluetooth, Wi-Fi
Камера	Анти-Вор – выполнение снимка фронтальной камерой Создание снимков не поддерживается в Kaspersky Security Center Web Console и Cloud Console, однако приложению Kaspersky Endpoint Security для Android требуется это разрешение, чтобы обеспечить возможность управлять приложением со всех консолей Kaspersky Security Center. 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 возможности	Анти-Вор – блокировка устройства (только для Android 7.0 и выше)
	Веб-Фильтр
	Контроль 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)
	Ограничение использования камеры (только для Android 11 и выше)
Отображать всплывающее окно (на некоторых устройствах Xiaomi)	Веб-Фильтр
Отображать всплывающие окна при работе в фоновом режиме (на некоторых устройствах Xiaomi)	Веб-Фильтр

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Управление сертификатами

Мобильные сертификаты используются для идентификации пользователей мобильных устройств на Сервере администрирования.

В Kaspersky Security Center Web Console и Cloud Console можно выполнять следующие действия с мобильными сертификатами пользователей:

- Просматривать сертификаты и их статусы.
- Создавать новые сертификаты.
- Обновлять сертификаты с истекающим сроком действия.
- Удалять сертификаты.

Дополнительная информация о сертификатах Kaspersky Security Center приведена в:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Просмотр списка сертификатов

В Kaspersky Security Center Web Console и Cloud Console можно просматривать используемые мобильные сертификаты пользователей, их статусы и свойства.

Чтобы просмотреть список используемых мобильных сертификатов пользователей, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.
2. Выберите **Управление сертификатами**.

   Откроется страница **Мобильные сертификаты** с информацией об используемых мобильных сертификатах пользователей. Вы можете просмотреть информацию о сертификате, выбрав его в столбце **Имя пользователя**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Задание параметров сертификата

Вы можете использовать Kaspersky Security Center Web Console или Cloud Console, чтобы настроить срок действия, автоматическое обновление и защиту паролем для мобильных сертификатов.

Чтобы задать параметры мобильного сертификата, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.
2. Выберите **Управление сертификатами**.
3. Выберите **Параметры сертификатов**.
4. В открывшемся окне **Создать мобильные сертификаты** можно настроить следующие параметры:

   - **Срок действия сертификата (дней)**

     Срок действия сертификата в днях. По умолчанию срок действия сертификата составляет 365 дней. По истечении этого срока мобильное устройство не сможет подключиться к Серверу администрирования.

   - **Перевыпустить, когда до окончания срока действия сертификата останется (дней)**

     Количество дней до истечения срока действия текущего сертификата, в течение которых Сервер администрирования должен выпустить новый сертификат. Например, если указано значение 4, Сервер администрирования выпускает новый сертификат за четыре дня до окончания срока действия текущего. По умолчанию указано значение 1.

   - **По возможности перевыпустить сертификат автоматически**

     По возможности перевыпуск сертификатов будет выполняться автоматически. Если этот параметр отключен, сертификаты должны перевыпускаться вручную по мере истечения срока их действия. По умолчанию этот параметр отключен.

   - **Запрос пароля при установке сертификата**

     При установке сертификата на мобильное устройство пользователю будет предложено ввести пароль. Пароль используется только один раз: при установке сертификата на мобильное устройство. Пароль автоматически формируется Сервером администрирования и отправляется пользователю по электронной почте. Можно указать длину пароля в поле **Длина пароля**.

5. Нажмите на кнопку **Сохранить**, чтобы применить изменения и закрыть окно.

Указанные параметры будут использоваться Kaspersky Security Center для создания, обновления и защиты мобильных сертификатов.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Создание сертификата

В Kaspersky Security Center Web Console и Cloud Console можно создавать мобильные сертификаты для идентификации пользователей мобильных устройств.

Чтобы создать мобильный сертификат, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.

2. Выберите **Управление сертификатами**.

3. В открывшемся окне **Мобильные сертификаты** нажмите на кнопку **Добавить**, чтобы запустить **Мастер создания мобильного сертификата**. Пройдите все шаги мастера, нажимая на кнопку **Далее**.

4. Выберите пользователей и группы пользователей, для управления мобильными устройствами которых будет использоваться новый сертификат.

5. Укажите **Параметры публикации**:

   - Чтобы уведомить пользователей о новом сертификате, установите флажок **Уведомить пользователя о новом сертификате**.

   - Чтобы разрешить использование одного сертификата несколько раз на одном устройстве, установите флажок **Разрешить использование одного сертификата несколько раз на одном устройстве (только для устройств с Kaspersky Endpoint Security для Android)**.

6. Выберите **Тип аутентификации**:

   - Выберите **Учетные данные (доменная авторизация или имя пользователя)**, чтобы пользователи получали доступ к сертификату, используя свои учетные данные.

   - Выберите **Одноразовый пароль**, чтобы пользователи получали доступ к сертификату с помощью одноразового пароля.

     Этот вариант доступен, если на предыдущем шаге вы не установили флажок **Разрешить использование одного сертификата несколько раз на одном устройстве (только для устройств с Kaspersky Endpoint Security для Android)**.

   - Выберите **Пароль**, чтобы пользователи получали доступ к сертификату с помощью пароля.

     Этот вариант доступен, если на предыдущем шаге вы установили флажок **Разрешить использование одного сертификата несколько раз на одном устройстве (только для устройств с Kaspersky Endpoint Security для Android)**.

7. В поле **Доставка сертификата** укажите способ доставки сертификата:

   - Если на предыдущем шаге вы выбрали **Одноразовый пароль**, выберите один из следующих вариантов:

     - Чтобы отправить пароль по электронной почте, выберите **Уведомить пользователя по электронной почте**.

       Затем выберите используемый адрес электронной почты или вариант **Другой адрес электронной почты** и укажите другой адрес электронной почты.

     - Чтобы уведомить пользователей о пароле другими способами, выберите **Показать пароль после завершения работы мастера**.

   - Если на предыдущем шаге вы выбрали **Учетные данные (доменная авторизация или имя пользователя)**, выберите используемый адрес электронной почты или вариант **Другой адрес электронной почты** и укажите другой адрес электронной почты.

8. Отображается итоговый вид сертификата.

   Убедитесь, что все параметры верны, и нажмите на кнопку **Создать**.

В результате, **Мастер создания мобильного сертификата** сформирует сертификат, который пользователи смогут установить на мобильные устройства. Сертификат будет доступен после следующей синхронизации мобильных устройств с Kaspersky Security Center.

Дополнительная информация о создании сертификатов и настройке правил их выпуска приведена в следующих документах:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обновление сертификата

Если срок действия используемого мобильного сертификата скоро истечет, его можно обновить с помощью Kaspersky Security Center Web Console или Cloud Console.

Чтобы обновить мобильный сертификат, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.
2. Выберите **Управление сертификатами**.
3. Выберите сертификат, который вы хотите обновить, и нажмите на кнопку **Перевыпустить**.

   Статус сертификата изменится на **Сертификат перевыпущен**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Удаление сертификата

Вы можете удалять мобильные сертификаты с помощью Kaspersky Security Center Web Console или Cloud Console.

После удаления мобильного сертификата устройство не синхронизируется с Сервером администрирования и им невозможно управлять с помощью Kaspersky Security Center. Чтобы восстановить управление мобильным устройством, необходимо переустановить на нем приложение Kaspersky Endpoint Security для Android.

Чтобы удалить мобильный сертификат, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.
2. Выберите **Управление сертификатами**.
3. Выберите сертификат, который вы хотите удалить, и нажмите на кнопку **Удалить**.

   Сертификат будет удален и исчезнет из списка сертификатов.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Для использования сервиса Firebase Cloud Messaging необходимо задать параметры сервиса в Kaspersky Security Center Web Console или Cloud Console.

Чтобы включить Firebase Cloud Messaging в Kaspersky Security Center Web Console или Cloud Console, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Синхронизация Android-устройств**.

   Откроется окно **Синхронизация Android-устройств**

2. В полях **Идентификатор отправителя** и **Ключ сервера** укажите параметры Firebase Cloud Messaging: SENDER_ID и API Key.

Firebase Cloud Messaging включен.

Чтобы получить идентификатор отправителя и ключ сервера, выполните следующие действия:

1. Зарегистрируйтесь на портале Google.
2. Перейдите в Google Cloud Platform.
3. Создайте новый проект.

   Подождите, пока проект будет создан.
4. Найдите соответствующий идентификатор SENDER_ID проекта.
5. Включите Google Firebase Cloud Messaging для Android.
6. Следуйте инструкциям на экране, чтобы создать учетные данные.
7. Скопируйте ключ API из свойств созданных учетных данных.

Подробная информация об операциях в Google Cloud Platform приведена в соответствующей документации.

Теперь у вас есть значения параметров **Идентификатор отправителя** и **Ключ сервера** для настройки Firebase Cloud Messaging.

Если параметры Firebase Cloud Messaging не заданы, 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 часа). То есть 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 регулируются условиями использования соответствующих сервисов Firebase: Условия обработки данных и безопасности Firebase, Конфиденциальность и безопасность в Firebase.

Чтобы запретить обмен информацией с сервисом Firebase Cloud Messaging, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Синхронизация Android-устройств**.

   Откроется окно **Синхронизация Android-устройств**

2. Нажмите на кнопку **Сброс**.

3. В открывшемся окне нажмите на кнопку **OK**, чтобы подтвердить сброс.

Настройки Firebase Cloud Messaging будут сброшены.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Управление мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console

Вы можете управлять мобильными устройствами в Kaspersky Security Center Web Console и Cloud Console, используя групповые политики и отправляя команды на мобильные устройства (только для устройств Android).

Для управления мобильными устройствами в Kaspersky Security Center Web Console необходимо установить плагины управления.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Подключение мобильных устройств к Kaspersky Security Center

Для управления мобильным устройством с помощью Kaspersky Security Center Web Console или Cloud Console устройства должны быть подключены к Kaspersky Security Center. Вы можете просмотреть список мобильных устройств, подключенных к Kaspersky Security Center, в Web Console или Cloud Console на закладке **Устройства** > **Мобильные** > **Устройства**.

Перед подключением устройства iOS отправьте адрес Kaspersky Security Center пользователю устройства, чтобы повысить безопасность подключения. Пользователь увидит этот адрес во время установки приложения и сможет отменить соединение, если отображаемый адрес не совпадает с адресом, который вы отправили.

Чтобы подключить мобильное устройство к Kaspersky Security Center, выполните следующие действия:

1. Запустите Мастера подключения мобильного устройства:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**, а затем нажмите на кнопку **Добавить**.
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Пользователи и роли** > **Пользователи**. Выберите имя пользователя или группы пользователей, которым вы хотите отправить ссылку для подключения мобильного устройства, а затем выберите **Устройства.** Нажмите на кнопку **Добавить мобильное устройство**. В этом случае пропустите шаг 3.

   Пройдите все шаги мастера, нажимая на кнопку **Далее**.

2. Выберите операционную систему устройств, которые вы хотите добавить:

   - **Android**
   - **iOS и iPadOS**

3. Выберите пользователей и группы пользователей, которым вы хотите отправить ссылку для подключения мобильного устройства.

4. Выберите адреса электронной почты, на которые следует отправить ссылку:

   - **Все адреса электронной почты**
   - **Основной адрес электронной почты**
   - **Дополнительный адрес электронной почты**

- **Другой адрес электронной почты**

  Если вы выбрали этот вариант, ниже укажите адрес электронной почты.

5. Отображается итоговый вид ссылки.

   Убедитесь, что все параметры ссылки верны, и нажмите на кнопку **Отправить**.

6. Откроется окно с подтверждением отправки ссылки для добавления мобильного устройства.

   Нажмите на кнопку **ОК**, чтобы завершить работу Мастера.

Когда пользователь устанавливает приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS, устройство пользователя появится на закладке **Устройства** > **Мобильные** > **Устройства** в Web Console или Cloud Console.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Перемещение нераспределенных мобильных устройств в группы администрирования

Мобильные устройства, на которых установлено приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS, отображаются на странице **Обнаружение и развертывание** > **Нераспределенные устройства** в Kaspersky Security Center Web Console или Cloud Console. Для управления новыми подключенными устройствами можно создать правило автоматического распределения устройств по группам администрирования или вручную переместить их в группу администрирования.

Чтобы переместить нераспределенное мобильное устройство в группу администрирования, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Обнаружение и развертывание** > **Нераспределенные устройства**.

2. Выберите устройство, которое вы хотите переместить в группу администрирования, и нажмите **Переместить в группу**.

3. В появившемся дереве групп администрирования выберите группу, куда вы хотите переместить устройство.

   Можно создать новую группу администрирования, выбрав существующую группу и нажав **Добавить вложенную группу**.

4. Нажмите на кнопку **Переместить**.

Устройство будет перемещено в указанную группу администрирования, и к нему применится групповая политика.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Отправка команд на мобильные устройства

Вы можете отправлять команды на мобильные устройства Android, например, для защиты данных на потерянном или украденном устройстве, или для выполнения принудительной синхронизации устройства с Kaspersky Security Center.

Вы не можете отправлять команды на iOS-устройства.

Поддерживаются следующие команды:

- **Заблокировать устройство**

  Мобильное устройство заблокировано.

- **Разблокировать устройство**

  Мобильное устройство разблокировано. На устройствах под управлением операционной системы Android версии 5.0 – 6.X после разблокировки мобильного устройства пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.

- **Сбросить настройки до заводских**

  Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до установленных по умолчанию.

- **Удалить корпоративные данные**

  Удалены данные в контейнерах и учетная запись корпоративной электронной почты.

- **Определить местоположение устройства**

  Местоположение устройства определено и показано на Google Картах. Оператор мобильной связи может взимать плату за доступ в интернет.

  На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой.

- **Воспроизвести звуковой сигнал**

  Мобильное устройство воспроизводит звуковой сигнал. Звуковой сигнал воспроизводится в течение 5 минут (при низком уровне заряда батареи – 1 минуты).

- **Синхронизировать устройство**

  Выполняется синхронизация мобильного устройства с Kaspersky Security Center.

Для выполнения команд приложению Kaspersky Endpoint Security для Android требуются определенные разрешения. 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 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 Анти-Вора работать не будут. Пользователю будет показано 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.

Чтобы отправить команды на мобильное устройство, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.
2. Выберите устройство, на которое требуется отправить команду, а затем нажмите **Контроль** или **Управление**.
3. В списке **Доступные команды** выберите нужную команду и нажмите кнопку **OK**.
4. Нажмите **OK**, если предлагается подтвердить операцию.

Указанная команда будет отправлена на мобильное устройство, также отобразится окно подтверждения.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Удаление мобильных устройств из Kaspersky Security Center

Если управлять определенным мобильным устройством больше не требуется, его можно удалить из Kaspersky Security Center с помощью Web Console или Cloud Console.

Чтобы удалить мобильное устройство из Kaspersky Security Center, выполните следующие действия:

1. Удалите мобильное приложение с устройства или убедитесь, что пользователь удалил приложение с нужного устройства.
2. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**.

3. Выберите мобильное устройство, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

4. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Устройство будет удалено из Kaspersky Security Center.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Управление групповыми политиками

В этом разделе описано управление групповыми политиками в Kaspersky Security Center Web Console и Cloud Console.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

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.

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 Android в актуальном состоянии, вы можете контролировать соответствие устройств пользователей требованиям корпоративной безопасности.

Дополнительная информация об управлении политиками и группами администрирования в Kaspersky Security Center Web Console и Cloud Console приведена в следующих документах:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Просмотр списка групповых политик

В Kaspersky Security Center Web Console и Cloud Console можно просматривать групповые политики, их статусы и свойства.

Чтобы просмотреть список групповых политик,

В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**.

Откроется список групповых политик с краткой информацией о групповых политиках. На этой странице вы можете создавать, изменять, копировать, перемещать и удалять групповые политики.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Просмотр результатов применения политики

В Kaspersky Security Center Web Console и Cloud Console можно просматривать диаграмму распространения групповой политики и информацию обо всех устройствах, подпадающих под действие политики.

Чтобы просмотреть результаты распространения групповой политики, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**.
2. В открывшемся списке групповых политик установите флажок рядом с названием политики, для которой вы хотите просмотреть результаты распространения, и нажмите **Распространение**.

Откроется страница с результатами распространения политики. Она содержит общую информацию о политике, диаграмму распространения политики и таблицу с информацией обо всех устройствах, подпадающих под действие этой политики. Вы можете открыть окно свойств политики, нажав на кнопку **Настроить политику**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Создание групповой политики

В Kaspersky Security Center Web Console и Cloud Console можно создавать групповые политики для управления мобильными устройствами.

Чтобы создать групповую политику, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**.
2. В открывшемся списке групповых политик Kaspersky Security Center нажмите **Текущий путь** и выберите группу администрирования, для которой требуется создать политику.

   По умолчанию новая групповая политика применяется к группе **Управляемые устройства**.
3. Нажмите на кнопку **Добавить**, чтобы запустить Мастер создания политики. Пройдите все шаги мастера, нажимая на кнопку **Далее**.
4. Выберите **Kaspersky Security for Mobile (Policies)**.
5. В поле **Имя** укажите имя новой политики. Если вы укажете имя уже существующей политики, к нему автоматически будет добавлено окончание (1).
6. Выберите статус политики:

   - **Активна**

     Мастер сохраняет созданную политику на Сервере администрирования. При следующей синхронизации мобильного устройства с Сервером администрирования политика будет использоваться на устройстве в качестве действующей.

   - **Неактивна**

     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.

7. Можно включить или отключить два параметра наследования: **Наследовать параметры родительской политики** и **Принудительное наследование параметров для дочерних политик**:

   - Если для дочерней группы администрирования включен параметр **Наследовать параметры родительской политики**, а в родительской политике заблокированы отдельные параметры, их нельзя будет изменить в политике для дочерней группы. Однако можно менять параметры, не заблокированные в родительской политике.

   - Если параметр **Наследовать параметры родительской политики** отключен для дочерней группы администрирования, можно менять все параметры политики для дочерней группы, даже если некоторые их них заблокированы в родительской политике.

   - Если в родительской группе администрирования включен параметр **Принудительное наследование параметров для дочерних политик**, для каждой дочерней политики будет включен параметр **Наследовать параметры родительской политики**. В этом случае не удастся отключить этот параметр для дочерних политик. Все параметры, заблокированные в родительской политике, принудительно наследуются в дочерних группах, где их невозможно изменить.

   - В политиках для группы **Управляемые устройства** параметр **Наследовать параметры родительской политики** ни на что не влияет, поскольку группа **Управляемые устройства** не имеет вышестоящих групп и, следовательно, не наследует никаких политик.

   По умолчанию параметр **Наследовать параметры родительской политики** включен, а параметр **Принудительное наследование параметров для дочерних политик** отключен.

8. При необходимости можно задать параметры для новой созданной политики. Для этого перейдите на закладку **Параметры приложений** и выполните действия, описанные в разделе Определение параметров политики.

   Это также можно сделать позже.

9. Нажмите на кнопку **Сохранить**, чтобы создать политику.

Будет создана новая групповая политика для управления мобильными устройствами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Изменение групповой политики

В Kaspersky Security Center Web Console и Cloud Console можно изменять параметры групповых политик.

Чтобы изменить групповую политику, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. В окне свойств политики выберите **Параметры программы**, а затем задайте параметры политики, как описано в разделе Определение параметров политики.

   Можно также настроить общие параметры, наследование параметров, запись событий и уведомления, профили политик и просмотреть историю изменений политики. Дополнительная информация приведена в *справке Kaspersky Security Center*.

3. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Копирование групповой политики

В Kaspersky Security Center Web Console и Cloud Console можно создавать копии групповых политик.

Чтобы создать копию групповой политики, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**.

2. В открывшемся списке групповых политик установите флажок рядом с названием политики, для которой вы хотите создать копию, и нажмите **Копировать**.

3. В появившемся дереве групп администрирования выберите группу, в которой вы хотите создать копию политики.

   Можно создать новую группу администрирования, выбрав существующую группу и нажав **Добавить вложенную группу**.

4. Нажмите на кнопку **Копировать**.

5. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

В целевой группе будет создана копия политики с тем же именем. Статус каждой скопированной или перемещенной политики в целевой группе будет **Неактивна**. В любое время можно изменить статус на **Активна**.

Если в целевой группе уже существует политика с именем, совпадающем с именем новой созданной или перемещенной политики, к имени новой созданной или перемещенной политики добавляется индекс (<порядковый номер>), например: (1).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Перенос политики в другую группу администрирования

В Kaspersky Security Center Web Console и Cloud Console можно перенести политику в другую группу администрирования.

Чтобы перенести политику в другую группу администрирования, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**.

2. В открывшемся списке групповых политик установите флажок рядом с названием политики, которую вы хотите перенести в другую группу администрирования, и нажмите **Переместить**.

3. В появившемся дереве групп администрирования выберите группу, куда вы хотите переместить политику.

   Можно создать новую группу администрирования, выбрав существующую группу и нажав **Добавить вложенную группу**.

4. Нажмите на кнопку **Переместить**.

5. Нажмите на кнопку **OK**, чтобы подтвердить операцию.

Результат зависит от свойств наследования политики:

- Если политика не наследовалась в исходной группе, она будет перемещена в целевую группу.
- Если политика наследовалась в исходной группе, она не будет перемещена. Вместо этого в целевой группе будет создана копия перемещаемой политики.

Статус каждой скопированной или перемещенной политики в целевой группе будет **Неактивна**. В любое время можно изменить статус на **Активна**.

Если в целевой группе уже существует политика с именем, совпадающем с именем новой созданной или перемещенной политики, к имени новой созданной или перемещенной политики добавляется индекс (<порядковый номер>), например: (1).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Удаление групповой политики

В Kaspersky Security Center Web Console и Cloud Console можно удалять групповые политики.

Можете удалять только политики, которые не наследуются в текущей группе администрирования. Если политика наследуется, ее можно удалить только в группе верхнего уровня, для которой она была создана.

Чтобы удалить групповую политику, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**.
2. В открывшемся списке групповых политик установите флажок рядом с названием политики, которую вы хотите удалить, и нажмите **Удалить**.
3. Нажмите на кнопку **ОК**, чтобы подтвердить операцию.

Групповая политика будет удалена.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Определение параметров политики

В этом разделе описано, как задать параметры политик Kaspersky Security Center для управления мобильными устройствами.

Параметры политики можно задать как при создании, так и при изменении политики.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка антивирусной защиты

Вы можете определить эти параметры политики только для устройств Android.

Для своевременного обнаружения угроз, вирусов и других вредоносных приложений следует настроить постоянную защиту 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.

Из-за технических ограничений Kaspersky Endpoint Security для Android не может проверять файлы размером 2 ГБ и более. Во время проверки приложение пропускает файлы большого размера и не уведомляет о том, что такие файлы были пропущены.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка постоянной защиты

Вы можете определить эти параметры политики только для устройств Android.

Чтобы настроить постоянную защиту, выполните следующие действия:

1. Откройте окно свойств политики:
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.
2. В окне свойств политики выберите **Параметры приложений** > **Базовая защита**.

3. В разделе **Антивирус** настройте защиту файловой системы мобильного устройства:

- Чтобы включить постоянную защиту мобильного устройства от угроз, установите флажок **Включить постоянную защиту от вирусов**.
- Укажите уровень защиты:
  - Чтобы приложение Kaspersky Endpoint Security для Android проверяло только новые приложения и файлы из папки Загрузки, выберите **Проверять только новые приложения**.
  - Чтобы включить расширенную защиту мобильного устройства от угроз, выберите **Проверять все приложения и контролировать действия с файлами**.

    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 с операционной системой 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 с использованием облачной службы Kaspersky Security Network, установите флажок **Дополнительная защита со стороны Kaspersky Security Network**.
- Чтобы заблокировать рекламные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламные приложения, средства автодозвона и другие приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя**.

4. В разделе **Параметры антивируса** выберите действие, выполняемое при обнаружении угрозы:

- **Удалить и сохранить резервную копию файла в карантине**

  Обнаруженные объекты будут удалены автоматически. От пользователя не требуется никаких дополнительных действий. Перед удалением объекта Kaspersky Endpoint Security для Android создает резервную копию файла и сохраняет ее в карантине.

- **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. 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.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка автоматического запуска антивирусной проверки мобильного устройства

Вы можете определить эти параметры политики только для устройств Android.

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

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. В окне свойств политики выберите **Параметры приложений** > **Базовая защита**.

3. Чтобы заблокировать рекламные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламные приложения, средства автодозвона и другие приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя** в разделе **Проверка устройства**.

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

   - **Удалить и сохранить резервную копию файла в карантине**

     Обнаруженные объекты будут удалены автоматически. От пользователя не требуется никаких дополнительных действий. Перед удалением объекта Kaspersky Endpoint Security для Android создает резервную копию файла и сохраняет ее в карантине.

   - **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. 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.

- **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.

5. В разделе **Проверка по расписанию** можно настроить автоматическую полную проверку файловой системы устройства.

   Выберите один из следующих вариантов:

   - **Выключена**

     Проверка файловой системы устройства не запускается автоматически.

   - **После обновления баз**

     Файловая система устройства будет проверяться автоматически при каждом обновлении антивирусных баз.

   - **Раз в день**

     Файловая система устройства будет проверяться автоматически каждый день.

     При выборе этого варианта можно также указать время проверки в поле **Время запуска**.

   - **Еженедельно по**

     Файловая система устройства будет проверяться автоматически один раз в неделю.

     При выборе этого варианта в раскрывающемся списке можно также выбрать день недели, когда будет запускаться проверка, и указать проверки в поле **Время запуска**.

На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка обновления антивирусных баз

Вы можете определить эти параметры политики только для устройств Android.

Чтобы настроить обновления антивирусных баз, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. В окне свойств политики выберите **Параметры приложений** > **Обновление баз**.

3. В разделе **Обновление баз** настройте расписание автоматического обновления баз на устройстве пользователя.

   Выберите один из следующих вариантов:

   - **Выключено**

     Автоматическое обновление антивирусных баз отключено.

   - **Раз в день**

     Обновление антивирусных баз выполняется каждый день.

     При выборе этого варианта можно также указать время обновления в поле **Время обновления**.

   - **Раз в неделю**

     Обновление антивирусных баз выполняется раз в неделю.

     При выборе этого варианта можно также указать время обновления в поле **Время обновления** и день недели, когда будет запускаться обновление, в раскрывающемся списке **День недели**.

На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

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

   - **Серверы "Лаборатории Касперского"**

     Kaspersky Endpoint Security для Android использует сервер обновлений "Лаборатории Касперского" в качестве источника обновлений для загрузки антивирусных баз на устройство пользователя.

   - **Сервер администрирования**

     Доступен только при использовании Kaspersky Security Center Web Console.

     Kaspersky Endpoint Security для Android использует хранилище Сервера администрирования Kaspersky Security Center в качестве источника обновлений для загрузки антивирусных баз на устройство пользователя.

   - **Другой источник**

     Kaspersky Endpoint Security для Android использует сторонний сервер в качестве источника обновлений для загрузки антивирусных баз на устройство пользователя.

     При выборе этого варианта укажите адрес HTTP-сервера в поле **Использовать другой сервер в качестве источника обновлений антивирусных баз**.

5. Чтобы приложение Kaspersky Endpoint Security для Android загружало обновления антивирусных баз по заданному расписанию, когда устройство пользователя находится в роуминге, в разделе **Разрешать обновление баз в роуминге** установите флажок **Обновление антивирусных баз в роуминге**.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Задание параметров разблокировки устройства

Вы можете определить эти параметры политики только для устройств Android.

Для обеспечения безопасности мобильного устройства настройте 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.

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 надежность пароля разблокировки устройства, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. В окне свойств политики выберите **Параметры приложений** > **Базовая защита**.

3. Чтобы приложение проверяло наличие пароля разблокировки, в разделе **Защита паролем** установите флажок **Требовать установить пароль разблокировки экрана**.

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

4. Укажите 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 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.

5. Если вы хотите, чтобы у пользователя была возможность использовать отпечатки пальцев для разблокировки экрана, установите флажок **Разрешить использование отпечатков пальцев (для устройств с Android 9 и ниже)**. 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 использование отпечатка пальца для разблокировки экрана не поддерживается.

   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.

6. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка защиты данных при потере или краже устройства

Вы можете определить эти параметры политики только для устройств Android.

Для защиты корпоративных данных в случае потери или кражи мобильного устройства необходимо настроить защиту от несанкционированного доступа.

Для защиты данных на украденном или утерянном устройстве 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.

Чтобы настроить защиту данных при потере или краже устройства, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. В окне свойств политики выберите **Параметры приложений** > **Базовая защита**.

3. В разделе **Анти-Вор** настройте блокировку устройства:

   - Укажите количество символов в коде разблокировки.

   - Укажите текст, отображаемый, если устройство заблокировано.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка контроля приложений

Вы можете определить эти параметры политики только для устройств Android.

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 пользователю установить обязательные и рекомендованные приложения, а также удалить запрещенные. Запустить запрещенные приложения на мобильном устройстве пользователя невозможно.

В Kaspersky Security Center Web Console и Cloud Console можно управлять приложениями на устройствах пользователей, применяя заданные заранее правила. **Контроль приложений** позволяет настроить два типа правил: для приложений и для категорий.

Правило для приложений применяется к определенному приложению, а **Правило для категорий** применяется ко всем приложениям из заранее определенной категории. Категории приложений определяются специалистами "Лаборатории Касперского".

*Чтобы настроить **Контроль приложений**, выполните следующие действия:*

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В таблице в разделе **Контроль приложений** добавьте правила, определяющие контролируемые приложения.

   - Чтобы добавить правило для определенного приложения:

     a. В таблице выберите пункт **Правило для приложений**.

     b. В открывшемся окне **Правило для приложений** выберите действие, выполняемое над приложениями, на которые распространяется созданное правило.

     c. Укажите приложение, на которое будет распространяться правило, заполнив поля **Ссылка на инсталляционный пакет (например, https://play.google.com/store/apps/details?id=com.kaspersky.kes)**, **Название пакета (например, katana.facebook.com)** и **Название приложения**.

     d. Нажмите на кнопку **Сохранить**.

   Правило будет добавлено в список правил компонента **Контроль приложений**.

- Чтобы добавить правило для категории приложений:

  a. В таблице в разделе **Контроль приложений** выберите пункт **Правило для категорий**.

  b. В открывшемся окне **Правило для категорий** выберите категорию приложения из раскрывающегося списка.

  Приложения, относящиеся к выбранной категории, будут подпадать под действие созданного правила.

  c. В разделе **Режим работы** выберите действие, выполняемое при попытке запуска любого приложения из выбранной категории: **Запрещенные приложения** или **Разрешенные приложения**.

  d. При необходимости заполните поле **Дополнительный комментарий, отображаемый на устройстве пользователя при обнаружении приложения указанной категории**.

  e. Нажмите на кнопку **Сохранить**.

  Правило будет добавлено в список правил компонента **Контроль приложений**.

4. В разделе **Действия с запрещенными приложениями** выберите действие, выполняемое над запрещенными приложениями:

   - Чтобы Kaspersky Endpoint Security для Android блокировал запуск запрещенных приложений на мобильном устройстве пользователя, выберите **Блокировать запуск приложений**.

   - Чтобы Kaspersky Endpoint Security для Android отправлял данные о запрещенных приложениях в журнал событий, не блокируя их, выберите **Не блокировать запрещенные приложения, только сообщать**.

5. В разделе **Режим работы** выберите, какие приложения будут определены добавляемыми правилами: разрешенные или запрещенные.

   - Чтобы правила определяли, какие приложения разрешены, выберите **Запрещенные приложения**.

     Чтобы Kaspersky Endpoint Security для Android блокировал запуск системных приложений на мобильном устройстве пользователя (например, Календарь, Камера, Настройки) в режиме **Запрещенные приложения**, установите флажок **Блокировать системные приложения**.

     > Специалисты "Лаборатории Касперского" не рекомендуют блокировать системные приложения, так как это может привести к сбоям в работе устройства.

   - Чтобы правила определяли, какие приложения запрещены, выберите **Разрешенные приложения**.

6. Чтобы получать информацию обо всех приложениях, установленных на мобильных устройствах, в разделе **Отчет о приложениях** установите флажок **Отправить список установленных приложений на все мобильные устройства**.

   Kaspersky Endpoint Security для Android отправляет данные в журнал событий каждый раз после установки или удаления приложения с устройства.

7. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка контроля соответствия мобильных устройств требованиям корпоративной безопасности

Вы можете определить эти параметры политики только для устройств Android.

Контроль соответствия позволяет контролировать соблюдения требований корпоративной безопасности на Android-устройствах и принимать меры в случае их несоблюдения. 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 несоответствия устройства.
- Действие, выполняемое с устройством, если пользователь не устранит несоответствие в течение указанного времени.
- Время, выделенное пользователю устройства для устранения несоответствия (например, 24 часа).

  По истечении указанного периода времени на устройстве пользователя будет выполнено выбранное действие.

  На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

Для настройки контроля соответствия можно выполнить следующие действия:

- Включить или отключить существующие правила соответствия.
- Измените существующие правила соответствия.
- Добавить новое правило.
- Удалить правило.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Включение и отключение правил соответствия

Вы можете определить эти параметры политики только для устройств Android.

Чтобы включить или отключить правила контроля соответствия мобильных устройств требованиям корпоративной безопасности, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Контроль соответствия** включите или отключите существующие правила соответствия с помощью переключателей в столбце **Статус**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Редактирование правил соответствия

Вы можете определить эти параметры политики только для устройств Android.

Чтобы изменить правило контроля соответствия мобильных устройств требованиям корпоративной безопасности, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Контроль соответствия** выберите правило, которое вы хотите изменить, и нажмите на кнопку **Изменить**.

4. В открывшемся окне **Правило** отредактируйте правило следующим образом:

   a. В столбце **Действие** настройте список действий, которые будут выполняться в случае несоблюдения правила, добавив, изменив или удалив требуемые действия.

   b. При необходимости укажите период времени, в течение которого пользователь должен исправить несоответствие, в столбце **Время на устранение** для каждого действия.

   c. Нажмите на кнопку **Сохранить**, чтобы сохранить правило.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Добавление правил соответствия

Вы можете определить эти параметры политики только для устройств Android.

Чтобы добавить правило контроля соответствия мобильных устройств требованиям корпоративной безопасности, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Контроль соответствия** перейдите по ссылке **Правило**.

4. В открывшемся окне **Правило** определите правило следующим образом:

   a. Выберите критерий несоответствия правилу.

   b. Нажмите на кнопку **Добавить**, а затем в столбце **Действие** выберите действие, которое будет выполняться в случае несоблюдения правила.

      Вы можете добавить несколько действий.

   c. Укажите период времени, в течение которого пользователь должен исправить несоответствие, в столбце **Время на устранение** для каждого действия.

   d. Нажмите на кнопку **Сохранить**, чтобы сохранить правило.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Удаление правил соответствия

Вы можете определить эти параметры политики только для устройств Android.

Чтобы удалить правило контроля соответствия мобильных устройств требованиям корпоративной безопасности, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Контроль соответствия** выберите правило, которое вы хотите удалить, и нажмите на кнопку **Удалить**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Список критериев несоответствия

Вы можете определить эти параметры политики только для устройств Android.

Чтобы убедиться, что Android-устройство соответствует требованиям корпоративной безопасности, Kaspersky Endpoint Security для Android может проверить устройство по следующим критериям:

- **Постоянная защита выключена**.

  Постоянная защита должна быть включена.

  Дополнительная информация о настройке постоянной защиты приведена в разделе Настройка постоянной защиты.

- **Антивирусные базы устарели**.

  Антивирусные базы Kaspersky Endpoint Security для Android должны регулярно обновляться.

  Дополнительная информация о настройке параметров обновления антивирусных баз приведена в разделе Настройка антивирусной защиты.

- **Установлены запрещенные приложения**.

  На устройстве не должно быть установлено приложений, имеющих статус **Блокировать запуск** согласно классификации в разделе **Контроль приложений**.

Дополнительная информация о создании правил для приложений приведена в разделе Настройка контроля приложений.

- **Установлены приложения запрещенных категорий**.

  На устройстве не должно быть установлено приложений, принадлежащих категории со статусом **Блокировать запуск** согласно классификации в разделе **Контроль приложений**.

  Дополнительная информация о создании правил для категорий приложений приведена в разделе Настройка контроля приложений.

- **Не установлены все обязательные приложения**.

  На устройстве должны быть установлены специальные приложения, имеющие статус **Обязательно к установке** согласно классификации в разделе **Контроль приложений**.

  Дополнительная информация о создании правил для приложений приведена в разделе Настройка контроля приложений.

- **Версия операционной системы устарела**.

  На устройстве должна быть установлена разрешенная версия операционной системы.

  Для использования этого критерия несоответствия необходимо указать диапазон допустимых версий операционной системы в раскрывающихся списках **Минимальная версия ОС** и **Максимальная версия ОС**.

- **Устройство давно не синхронизировалось**.

  Устройство необходимо регулярно синхронизировать с Сервером администрирования.

  Для использования этого критерия несоответствия необходимо указать максимальный интервал времени между операциями синхронизации устройств в раскрывающемся списке **Период синхронизации**.

- **На устройстве получены root-права**

  На устройстве на должны предоставляться root-права.

  Дополнительная информация приведена в разделе Обнаружение взлома устройства (root).

- **Пароль разблокировки экрана не соответствует требованиям безопасности**.

  Устройство должно быть защищено паролем разблокировки, соответствующим требованиям к надежности пароля разблокировки.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Список действий при обнаружении несоответствия

Вы можете определить эти параметры политики только для устройств Android.

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).

- **Сброс устройства до заводских настроек**.

  Удалены все данные с мобильного устройства, настройки мобильного устройства сброшены до заводских.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка доступа пользователей к веб-сайтам

Вы можете настроить эти параметры политики для устройств Android и iOS.

Чтобы защитить личные и корпоративные данные, хранящиеся на мобильных устройствах, во время просмотра веб-страниц, можно настроить доступ пользователей к веб-сайтам с помощью Веб-Фильтра. Веб-Фильтр проверяет веб-сайты до их открытия пользователем, а затем блокирует веб-сайты, распространяющие вредоносный код, и фишинговые веб-сайты, предназначенные для кражи конфиденциальных данных и получения доступа к финансовым счетам.

Для устройств Android эта функция также поддерживает фильтрацию веб-сайтов по категориям, определенным в облачной службе Kaspersky Security Network. Фильтрация позволяет вам ограничить доступ к отдельным веб-сайтам или категориям веб-сайтов (например, к веб-сайтам из категории **Азартные игры, лотереи, тотализаторы** или **Общение в сети**).

Чтобы включить Веб-Фильтр на iOS-устройствах, пользователь должен разрешить приложению Kaspersky Security для iOS добавить конфигурацию VPN.

Чтобы включить Веб-Фильтр на Android-устройствах:

- Приложение Kaspersky Endpoint Security включено в качестве службы Специальных возможностей.

- Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) должно быть принято. Kaspersky Endpoint Security использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN.

Вы можете принять Положение о Веб-Фильтре в Kaspersky Security Center. В этом случае пользователю не потребуется выполнять никаких действий.

Если вы не приняли Положение о Веб-Фильтре и направили пользователю запрос на принятие Положения, пользователь должен прочитать и принять Положение о Веб-Фильтре в настройках приложения.

Если вы не приняли Положение о Веб-Фильтре, Веб-Фильтр будет недоступен.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome (включая функцию Custom Tabs), 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 настроить доступ пользователей к веб-сайтам, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Веб-Фильтр** установите флажок **Включить Веб-Фильтр**, чтобы включить эту функцию.

4. Для устройств Android вы можете выбрать одну из следующих опций:

   - Чтобы ограничить доступ пользователей к веб-сайтам на основе их содержимого:

     a. Выберите **Блокировать сайты указанных категорий**.

     b. Установите флажки, соответствующие категориями веб-сайтов, доступ к которым будет заблокирован.

     Если Веб-Фильтр включен, доступ пользователей к веб-сайтам категорий **Фишинг** и **Сайты с вредоносным ПО** всегда запрещен.

- Чтобы указать список разрешенных веб-сайтов:

  a. Выберите **Разрешить только указанные 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:

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

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

- Чтобы заблокировать доступ пользователей ко всем веб-сайтам, выберите **Блокировать все веб-сайты**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка ограничений функций

Вы можете определить эти параметры политики только для устройств Android.

Kaspersky Security Center Web Console позволяет настроить доступ пользователей к следующим функциям мобильных устройств:

- Wi-Fi
- Камера
- 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. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Управление функциями** настройте использование Wi-Fi, камеры, Bluetooth:

   - Чтобы выключить модуль Wi-Fi на мобильном устройстве пользователя, установите флажок **Запретить использование Wi-Fi (только для устройств с Android 9 и ниже)**.

     На устройствах под управлением Android 10.0 и выше запрет на использование сетей Wi-Fi не поддерживается.

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

     На устройствах под управлением Android 10 и выше использование камеры нельзя запретить полностью.

     На устройствах с операционной системой Android 11 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 не удастся ограничить использование камеры.

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

     На Android 12 или более поздней версии использование Bluetooth может быть отключено, только если пользователь устройства предоставил разрешение **Устройства Bluetooth поблизости**. Пользователь может предоставить это разрешение во время работы Мастера первоначальной настройки или позже.

На личных устройствах под управлением Android 13 или выше нельзя отключить использование Bluetooth.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 пользователю отобразится запрос на выключение прав администратора для Kaspersky Endpoint Security для Android. После выключения прав мобильное устройство будет заблокировано.

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

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Контроль безопасности**.

3. В разделе **Управление приложениями на мобильном устройстве** снимите флажок **Разрешить удаление приложения Kaspersky Endpoint Security для Android на устройстве**.

   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.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

При попытке удаления приложения мобильное устройство будет заблокировано.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка синхронизации мобильных устройств с Kaspersky Security Center

Вы можете настроить эти параметры политики для устройств Android и iOS.

Для управления мобильными устройствами и получения отчетов и статистики от мобильных устройств настройте параметры синхронизации. Синхронизация мобильных устройств 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 свойствах политики. Изменение параметров политик, команд и задач выполняется при синхронизации мобильных устройств с Kaspersky Security Center по расписанию, то есть с задержкой. По умолчанию мобильные устройства автоматически синхронизируются с Kaspersky Security Center каждые шесть часов.

  На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

- **Принудительно** (для Android-устройств). 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 FCM.

Чтобы настроить синхронизацию мобильного устройства с Kaspersky Security Center, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Синхронизация**.

3. В разделе **Синхронизация с Сервером администрирования** в раскрывающемся списке **Период синхронизации** выберите период синхронизации.

   По умолчанию синхронизация выполняется каждые шесть часов.

4. Вы можете отключить синхронизацию для устройств Android, когда устройство находится в роуминге. Для этого установите флажок **Выключить синхронизацию в роуминге**.

   По умолчанию синхронизация в роуминге включена.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Kaspersky Security Network

Чтобы повысить эффективность защиты мобильных устройств, Kaspersky Endpoint Security для Android и Kaspersky Security для iOS используют данные, полученные от пользователей во всем мире. 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. Кроме того, участие в Kaspersky Security Network обеспечивает доступ к данным о репутации программ и веб-сайтов.

Когда вы участвуете в Kaspersky Security Network, статистика, полученная в результате работы мобильного приложения, 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.

Следующие компоненты приложений используют облачную службу Kaspersky Security Network:

- Компоненты Антивирус, Веб-Фильтр и Контроль приложений в приложении Kaspersky Endpoint Security для Android.
- Компонент Веб-Фильтр в приложении Kaspersky Security для iOS.

Чтобы начать использовать KSN, вы должны принять условия Лицензионного соглашения. Подробнее об отправке данных в KSN читайте в разделе Обмен информацией с Kaspersky Security Network.

Отказ от участия в KSN снижает уровень защиты устройства, что может привести к заражению устройства и потере информации.

Для повышения качества работы мобильного приложения вы можете также отправлять в Kaspersky Security Network статистические данные.

Предоставление информации в Kaspersky Security Network является добровольным.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обмен информацией с Kaspersky Security Network

Обмен информацией в Kaspersky Endpoint Security для Android

Для повышения уровня постоянной защиты Kaspersky Endpoint Security для Android 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 перед открытием с учетом данных, полученных от KSN. Также приложение определяет категорию веб-сайта для контроля доступа пользователей в интернет на основе списков разрешенных и запрещенных категорий (например, категория "Общение в сети").

- **Контроль приложений.** Приложение определяет категории для ограничения запуска приложений, 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 компонентов Антивирус и Контроль приложений, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать следующую информацию.

Информация о типах данных, передаваемых в "Лаборатории Касперского" при использовании KSN во время работы Веб-Фильтра, доступна в Положении об обработке данных для использования Веб-Фильтра. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

Подробнее о предоставлении данных в KSN см. в разделе Предоставление данных в Kaspersky Endpoint Security для Android.

Предоставление данных в KSN является добровольным. При желании можно отключить обмен данными с KSN.

Обмен информацией в Kaspersky Security для iOS.

Для повышения уровня постоянной защиты Kaspersky Security для iOS использует облачную службу Kaspersky Security Network в работе компонента **Веб-Фильтр**. Приложение выполняет проверку веб-ресурсов перед открытием с учетом данных, полученных от KSN.

Информация о типах данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы компонента Веб-Фильтр, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать следующую информацию.

Подробнее о предоставлении данных в KSN см. в разделе Предоставление данных в Kaspersky Security для iOS.

Предоставление данных в KSN является добровольным. При желании можно отключить обмен данными с KSN.

Отправка статистики в KSN от приложений для Android и iOS

Для обмена данными с KSN в целях повышения качества работы приложения должны быть выполнены следующие условия:

- Пользователь устройства должен прочитать и принять условия Положения о Kaspersky Security Network.
- Необходимо разрешить передачу статистики в KSN в параметрах групповой политики.

Вы можете 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, приведена в Положении о Kaspersky Security Network.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Включение и отключение Kaspersky Security Network

По умолчанию использование Kaspersky Security Network включено.

Если использование Kaspersky Security Network отключено, Веб-Фильтр, Контроль приложений и дополнительная защита в Kaspersky Security Network автоматически отключаются, а их настройки становятся недоступными.

Чтобы включить или выключить использование Kaspersky Security Network, выполните следующие действия:

1. Откройте окно свойств политики:
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.
   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.
2. На странице свойств политики выберите **Параметры приложений** > **KSN и статистика**.
3. Чтобы включить или отключить использование Kaspersky Security Network, установите или снимите флажок **Использовать Kaspersky Security Network**.

4. Если использование Kaspersky Security Network включено и вы согласны отправлять данные в "Лабораторию Касперского", установите флажок **Разрешить отправку статистики в Kaspersky Security Network**. Данные позволят увеличить скорость реакции мобильного приложения на угрозы, улучшить производительность компонентов защиты, снизить вероятность ложных срабатываний.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обмен информацией с Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics

Вы можете определить эти параметры политики только для устройств Android.

Kaspersky Endpoint Security для Android обменивается данными с сервисами Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics для улучшения качества, внешнего вида и производительности программного обеспечения, продуктов, услуг и инфраструктуры "Лаборатории Касперского", анализируя работу пользователей, функции, статус и используемые настройки устройств.

Обмен информацией с сервисами Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics по умолчанию отключен.

Чтобы включить обмен данными, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **KSN и статистика**.

3. В разделе **Отправка статистики в сторонние сервисы** установите флажок **Разрешить передачу данных, чтобы помочь улучшить качество работы, интерфейс и производительность приложения**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка уведомлений на мобильных устройствах

Вы можете определить эти параметры политики только для устройств 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. Пользователь устройства может нажать на статус защиты устройства и посмотреть список проблем в приложении.

- **Уведомления приложения**. Уведомления информируют пользователя устройства о приложении (например, об обнаружении угрозы).

- **Всплывающие сообщения**. Всплывающие сообщения требуют внимания со стороны пользователя устройства (например, предпринять действия при обнаружении угрозы).

По умолчанию все уведомления Kaspersky Endpoint Security для Android включены.

На Android 13 пользователь устройства должен предоставить разрешение на отправку уведомлений во время работы Мастера начальной настройки или позже.

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 на мобильном устройстве, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Уведомления и отчеты**.

3. В разделе **Уведомления** настройте отображение уведомлений:

   - Чтобы скрыть все уведомления и всплывающие сообщения, отключите переключатель **Отображать уведомления, если Kaspersky Endpoint Security 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. Приложение также отображает уведомления, когда пользователь работает с приложением (например, обновляет антивирусные базы вручную).

     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.

   - В разделе **Список проблем безопасности, отображаемый на устройствах пользователей** выберите проблемы Kaspersky Endpoint Security для Android, которые должны отображаться на мобильных устройствах пользователей.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обнаружение взлома устройства

Kaspersky Security Center Web Console позволяет обнаруживать взлом устройства (получение root-прав) на устройствах Android и модификацию прошивки (jailbreak) на устройствах iOS. 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.

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

- *Встроенная служба Kaspersky Endpoint Security для Android*. Служба "Лаборатории Касперского", которая 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 выявляет другие проблемы безопасности. Подробная информация о работе SafetyNet Attestation приведена на веб-сайте Службы технической поддержки Android.

Kaspersky Security для iOS использует следующие службы для обнаружения модифицированной прошивки (jailbreak):

- *Встроенная служба Kaspersky Security для iOS*. Служба "Лаборатории Касперского", которая проверяет, модифицирована ли прошивка мобильного устройства (Kaspersky Mobile Security SDK).

При взломе устройства вы получите уведомление. Вы можете просмотреть уведомления о взломах в Kaspersky Security Center Web Console на закладке **Мониторинг и отчетность** > **Панель мониторинга**. Вы также можете выключить уведомление о взломе в параметрах уведомлений о событиях.

На Android-устройствах можно установить ограничения на действия пользователя в случае взлома устройства (например, заблокировать устройство). Вы можете установить ограничения с помощью компонента Контроль соответствия. Для этого создайте правило соответствия с критерием **На устройстве получены root-права**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Задание параметров лицензирования

Вы можете настроить эти параметры политики для устройств Android и iOS.

Для управления мобильными устройствами в Kaspersky Security Center Web Console или Cloud Console необходимо активировать мобильное приложение на мобильных устройствах. Активация приложения Kaspersky Endpoint Security для Android или Kaspersky Security для iOS на мобильном устройстве осуществляется путем предоставления приложению информации о действующей лицензии. Информация о лицензии передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

Если мобильное приложение не было активировано в течение 30 дней с момента установки на мобильное устройство, оно 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 приложение не было активировано в течение 30 дней с момента установки, пользователю необходимо вручную выполнить синхронизацию устройства с Kaspersky Security Center.

Чтобы задать параметры лицензирования для групповой политики, выполните следующие действия:

1. Откройте окно свойств политики:

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Политики и профили**. В открывшемся списке групповых политик выберите политику, которую вы хотите настроить.

   - В главном окне Kaspersky Security Center Web Console или Cloud Console выберите **Устройства** > **Мобильные** > **Устройства**. Выберите мобильное устройство, подпадающее под действие политики, которую вы хотите настроить, а затем выберите политику на закладке **Активные политики и профили политик**.

2. На странице свойств политики выберите **Параметры приложений** > **Лицензии**.

3. С помощью раскрывающегося списка выберите требуемый лицензионный ключ в хранилище ключей Сервера администрирования.

   Подробная информация о лицензионном ключе отображается в полях ниже.

   Вы можете заменить существующий ключ активации на мобильном устройстве, если он отличается от ключа, выбранного в раскрывающемся списке. Для этого установите флажок **Если на устройстве используется другой ключ, замените его этим ключом**.

4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка событий

Вы можете настроить эти параметры политики для устройств Android и iOS.

Вы можете задать параметры хранения и уведомления о событиях, которые происходят на устройствах пользователей и отправляются в Kaspersky Security Center.

Настраивать события можно только при изменении политики.

События распределяются по следующим закладкам в зависимости от уровней важности:

- **Критическое**

  Критическое событие указывает на проблему, которая может привести к потере данных, сбоям в работе или критической ошибке.

- **Отказ функционирования**

  Отказ функционирования указывает на серьезную проблему, ошибку или неисправность, возникшую во время работы приложения.

- **Предупреждение**

  Предупреждение не обязательно является серьезным событием, однако указывает на возможную проблему.

- **Информационное**

  Информационное событие уведомляет об успешном завершении операции или процедуры и о корректной работе приложения.

В каждом разделе списка перечислены типы событий и установленный по умолчанию срок хранения событий в Kaspersky Security Center (в днях).

В списке событий можно выполнять следующие действия:

- Добавлять или удалять типы событий из списка типов событий, отправляемых в Kaspersky Security Center.
- Определять параметры хранения и уведомления для каждого типа событий, например: как долго события определенного типа должны храниться в базе данных Сервера администрирования и будут ли отправляться уведомления о событиях определенного типа по электронной почте.

Дополнительная информация о настройке событий в Kaspersky Security Center Web Console и Cloud Console приведена в следующих документах:

- Если вы используете Kaspersky Security Center Web Console – в *Справке Kaspersky Security Center*.
- Если вы используете Kaspersky Security Center Cloud Console – в *Справке Kaspersky Security Center Cloud Console*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка событий, связанных с установкой, обновлением и удалением приложений на устройствах пользователей

Вы можете настроить эти параметры политики для устройств Android и iOS.

Если вы используете Kaspersky Security Center Cloud Console, список типов событий, происходящих на устройствах пользователей и отправляемых в Kaspersky Security Center, не включает события, связанные с установкой, обновлением и удалением приложений на устройствах. Это связано с тем, что такие события происходят часто, и могут заменить другие важные события в базе Kaspersky Security Center при достижении ограничения на количество событий. Они также могут влиять на производительность Сервера администрирования и базы данных и на пропускную способность интернет-соединения с Kaspersky Security Center Cloud Console.

Если существует необходимость сохранять события этого типа и получать о них уведомления, выполните действия, описанные в этом разделе.

Чтобы настроить события, связанные с установкой, обновлением и удалением приложений на устройствах пользователей, выполните следующие действия:

1. В параметрах политики на закладке **Настройка событий** добавьте информационное событие с типом **Установлено или удалено приложение (список установленных приложений)** в список событий, хранящихся в базе данных Сервера администрирования.

   Подробная информация о настройке событий приведена в *Справке Kaspersky Security Center Cloud Console*.

2. Включите параметр **Отправить список установленных приложений на все мобильные устройства**.

   События, связанные с установкой, обновлением и удалением приложений на устройствах пользователей будут храниться в базе Kaspersky Security Center. Вы будете получать уведомления об этих событиях.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Работа с Консолью администрирования на базе MMC

В этом разделе справки описана защита и управление мобильными устройствами с помощью Консоли администрирования Kaspersky Security Center на базе MMC.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Основные сценарии использования



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?

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О Kaspersky Security для мобильных устройств

Kaspersky Security для мобильных устройств – это комплексное решение, предназначенное для защиты и управления корпоративными мобильными устройствами, а также личными мобильными устройствами, используемыми сотрудниками компании в корпоративных целях.

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 определять параметры конфигурации устройств, подключенных к Kaspersky Security Center через протокол iOS MDM (далее также «iOS MDM-устройства»), без использования iPhone Configuration Utility.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Основные функции управления мобильными устройствами в Консоли администрирования на базе MMC

Kaspersky Security для мобильных устройств предоставляет следующие функции:

- Рассылка сообщений электронной почты со ссылками на Google Play для подключения устройств под управлением Android к Kaspersky Security Center.
- Дистанционное подключение мобильных устройств к Kaspersky Security Center и другим сторонним EMM-системам (например, VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Дистанционная настройка Kaspersky Endpoint Security для Android, а также сервисов, приложений и функций Android-устройств.
- Дистанционная настройка мобильных устройств согласно требованиям корпоративной безопасности.
- Предотвращение утечек корпоративной информации, хранящейся на мобильных устройствах, в случае их кражи или потери (Анти-Вор).
- Контроль соблюдения требований корпоративной безопасности (Контроль соответствия).
- Контроль использования интернета на мобильных устройствах (Веб-Фильтр).
- Настройка корпоративной почты на мобильных устройствах, в том числе в организациях, в которых развернут почтовый сервер Microsoft Exchange (только для устройств iOS и Samsung).
- Настройка параметров корпоративных сетей (Wi-Fi, VPN) для использования VPN на мобильных устройствах. VPN можно настроить только на устройствах iOS и Samsung.
- Настройка отображения статуса мобильного устройства в Kaspersky Security Center при нарушении правил политики: Критический, Предупреждение, OK.
- Настройка уведомлений, отображаемых пользователю в Kaspersky Endpoint Security для Android.
- Настройка параметров на устройствах с поддержкой Samsung KNOX 2.6 и выше.
- Настройка параметров устройств, поддерживающих рабочие профили Android.
- Настройка параметров мобильных Android-устройств в режиме device owner.
- Развертывание Kaspersky Endpoint Security для Android с помощью консоли Samsung KNOX Mobile Enrollment. Samsung KNOX Mobile Enrollment предназначен для массовой установки и первоначальной настройки приложений на Samsung-устройствах, приобретенных у официальных поставщиков.
- Обновление Kaspersky Endpoint Security для Android до заданной версии с помощью политик Kaspersky Security Center.
- Уведомление администратора о статусе и событиях в работе Kaspersky Endpoint Security для Android в Kaspersky Security Center или по электронной почте.
- Контроль изменений параметров политики (история ревизий).

- Команды для удаленного управления мобильными устройствами. Например, в случае потери или кражи мобильного устройства вы можете отправить команды, чтобы определить местоположение устройства или удалить корпоративные данные с устройства.
- Настройка параметров пароля разблокировки экрана для мобильных устройств.
- Настройка параметров сети Wi-Fi для мобильных устройств.
- Добавление веб-клипов для открытия веб-сайтов с главного экрана мобильных устройств.

Kaspersky Security для мобильных устройств включает следующие компоненты защиты и управления:

- Антивирус (для Android-устройств).
- Анти-Вор (для Android-устройств).
- Веб-Фильтр (для Android и iOS-устройств).
- Контроль приложений (для Android-устройств).
- Контроль соответствия (для Android и iOS-устройств).
- Обнаружение root-прав на устройствах (для Android-устройств).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 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.** Позволяет проверять управляемые устройства на соответствие требованиям корпоративной безопасности и накладывать ограничения на определенные функции несовместимых устройств.

Приложение Kaspersky Endpoint Security для Android также можно установить в режиме device owner. Режим device owner обеспечивает полный контроль над корпоративными Android-устройствами и позволяет вам настроить множество функций устройства. В режиме device owner вы можете:

- Ограничить функции операционной системы Android.
- Задать настройки Google Chrome.
- Задать настройки запуска приложений в Контроле приложений.
- Ограничить набор приложений, доступных пользователю устройства в режиме киоска.
- Задать настройки Exchange ActiveSync для Gmail.
- Настроить подключение к NDES/SCEP-серверу.
- Установить корневые сертификаты на устройствах.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 устройстве в режиме supervised.
- **Ограничения функций.** Этот компонент позволяет проверять управляемые устройства на соответствие требованиям корпоративной безопасности и накладывать ограничения на определенные функции несовместимых устройств.
- **Контроль соответствия.** Этот компонент контролирует соблюдение требований корпоративной безопасности на iOS MDM-устройствах и принимает меры в случае их несоблюдения. Контроль соответствия работает на основе списка правил. Каждое правило содержит следующие компоненты:
  - статус (правило включено или выключено);
  - критерии проверки устройства (например, отсутствие указанных приложений или версия операционной системы на устройстве);
  - действия, выполняемые на устройстве в случае несоответствия (например, удалить корпоративные данные или отправить пользователю сообщение электронной почты).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О плагине управления Kaspersky Device Management для iOS

Плагин управления Kaspersky Device Management для iOS обеспечивает интерфейс управления мобильными устройствами, подключенными по протоколу iOS MDM 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 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 протоколу iOS MDM 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 12 и выше.

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

- Консоль администрирования Kaspersky Security Center 12 и выше;
- 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 12 и 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 установки 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 5.0–13 (включая Android 12L, исключая Go Edition);
- 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 10–16 или iPadOS 13–15;
- подключение к интернету.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Известные проблемы и рекомендации

Следующие известные проблемы не являются критичными для работы решения.

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 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.
- После обновления плагинов управления до Технического релиза 33 необходимо также обновить приложение Kaspersky Endpoint Security для Android до Технического релиза 33. В противном случае на некоторых устройствах пользователей не получится активировать Samsung KNOX.

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.
- Иногда обновление антивирусных баз с Сервера администрирования может завершиться ошибкой на мобильных устройствах. В этом случае запустите задачу обновления антивирусных баз на Сервере администрирования.
- На некоторых устройствах Kaspersky Endpoint Security для Android не обнаруживает устройства, подключенные по USB OTG. Выполнить антивирусную проверку таких устройств невозможно.

- На устройствах с операционной системой Android 11 и выше приложение Kaspersky Endpoint Security для Android не может сканировать папки Android/data и Android/obb и обнаруживать в них вредоносные программы из-за технических ограничений.

- На устройствах с операционной системой Android 11 и выше пользователю необходимо предоставить разрешение "Разрешить доступ на управление всеми файлами".

- 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 7.0 при выполнении задачи постоянной защиты в расширенном режиме не выполняется обнаружение угроз в файлах, хранящихся на внешней SD-карте.

- 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 (включая функцию Custom Tabs), 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.

- На некоторых устройствах Xiaomi для работы Веб-Фильтра должны быть предоставлены разрешения "Отображать всплывающее окно" и "Отображать всплывающие окна во время работы в фоновом режиме".

- При вводе адреса веб-сайта в параметрах Веб-Фильтра соблюдайте следующие правила:

  - Для Android-устройств указывайте адрес в формате регулярных выражений (например, `https://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`).

- Если для Веб-Фильтра выбран режим **Запрещены все веб-сайты**, то Kaspersky Endpoint Security для Android не блокирует поиск в виджете Google Поиск. Вместо этого блокируется доступ к результатам поиска.

- Если в рабочем профиле для Веб-Фильтра выбран режим **Запрещены все веб-сайты**, то Kaspersky Endpoint Security для Android постоянно перезагружает главную страницу Google Chrome, блокирует браузер и мешает работе устройства.

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 Kaspersky Endpoint Security для Android должен быть установлен в качестве службы Специальных возможностей. Не применимо к режиму device owner.
- 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.
- На iOS MDM-устройствах, если вы добавите приложения, которые разрешено устанавливать на устройство, в список разрешенных приложений, то все приложения, кроме добавленных в список и системных приложений, будут скрыты с экрана устройства.

Известные проблемы при настройке сертификатов в политике iOS MDM

- При добавлении сертификата в политику iOS MDM попытка сохранить или закрыть политику может привести к сбою Консоли администрирования Kaspersky Security Center на базе MMC, при этом сертификат сохранится в настройках политики.

Известные проблемы при настройке электронной почты

- Дистанционная настройка почтового ящика доступна только на следующих устройствах:
  - iOS MDM-устройства;
  - Samsung-устройства (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 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 и Samsung-устройствах.

- 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.

Известные проблемы при настройке VPN

- Дистанционная настройка VPN доступна только на следующих устройствах:
  - iOS MDM-устройства;
  - Samsung-устройства.
- При настройке VPN-соединения для избранных доменов в Safari, если изменить значение опции **Подключаться автоматически**, изменения не будут применены на устройстве. По умолчанию флажок **Подключаться автоматически** установлен, и его не рекомендуется снимать, если вы хотите автоматически включать VPN для указанных доменов.

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.
- На некоторых устройствах Xiaomi и Huawei защита Kaspersky Endpoint Security для Android от удаления не работает. Проблема связана с особенностями прошивки MIUI 7 и 8 на Xiaomi и прошивки EMUI на Huawei.

Известные проблемы при настройке ограничений устройства

- На устройствах под управлением Android 10.0 и выше запрет на использование сетей Wi-Fi не поддерживается.
- На устройствах под управлением Android 10 и выше использование камеры нельзя запретить полностью.
- На устройствах с операционной системой Android 11 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 не удастся ограничить использование камеры.

Известные проблемы при отправке команд на мобильные устройства

- На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой.

Известные проблемы, связанные с рабочим профилем Android

- Если вы создаете рабочий профиль Android с помощью политики, пользователь должен предоставить разрешение "Разрешить доступ на управление всеми файлами" программе Kaspersky Endpoint Security для Android, установленной на устройствах под управлением Android 11 или более поздней версии и связанной с рабочим профилем.

- Функция рабочего профиля Android **Запретить включать режим отладки по USB** не работает на устройствах под управлением Android 13. Это связано с проблемой в Android 13.

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 устройствах Huawei под управлением Android 5.X после установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей отображается неверное сообщение об отсутствии соответствующих 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 пользователь может использовать Диспетчер задач ОС, чтобы остановить работу Kaspersky Endpoint Security для Android в фоновом режиме. Проблема связана с особенностями программного обеспечения Xiaomi.

- 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 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) мобильный 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 устройствах Honor и Huawei 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.

- На некоторых устройствах Samsung после установки или обновления Kaspersky Endpoint Security из автономного инсталляционного пакета активация профиля KNOX MDM недоступна.

- На устройствах Blackview пользователь может очистить память для приложения Kaspersky Endpoint Security для Android. В результате защита и управление устройством отключается, все заданные параметры становятся недействительными, а приложение Kaspersky Endpoint Security для Android удаляется из специальных возможностей. Это связано с тем, что устройства этого производителя предоставляют приложению "Недавние экраны" (Recent screens) расширенные права. Приложение может переопределять значения параметров Kaspersky Endpoint Security для Android, и его нельзя заменить, поскольку оно является частью операционной системы Android.

- На некоторых устройствах Google Pixel под управлением Android 11 и ниже сразу после запуска приложения Kaspersky Endpoint Security для Android происходит его сбой. Это связано с проблемой в Android.

- На некоторых устройствах TECNO пользователь может разблокировать устройство с помощью сканирования лица, даже если этот метод биометрической разблокировки запрещен политикой.

- На некоторых устройствах Sony и Google Pixel под управлением Android 13 или выше справка Kaspersky Endpoint Security с информацией о включении специальных возможностей отображается неправильно.

- На устройствах Samsung серий Galaxy S23 и S24 может не работать постоянная защита.

Известные проблемы при работе на Android 13

- На Android 13 пользователь может использовать Диспетчер задач ОС, чтобы остановить работу Kaspersky Endpoint Security в фоновом режиме. Это связано с известной проблемой в Android 13.

- На Android 13 разрешение на отправку уведомлений запрашивается в начале настройки приложения. Это связано с особенностями операционной системы Android 13.

Известные проблемы при добавлении веб-клипов

- Максимальное количество веб-клипов, которые можно добавить на Android-устройство, зависит от типа устройства. Когда это количество достигнуто, веб-клипы перестают добавляться на Android-устройство.

Известные проблемы в режиме device owner

- На устройствах под управлением Android 10 или ниже, если при настройке ограничений для приложений установлен флажок **Запретить изменение приложений через Настройки** и применена политика, пользователь по-прежнему может сбрасывать настройки приложений по умолчанию и останавливать приложения через настройки. Это связано с особенностями операционной системы Android.

- Управление настройками обновлений на мобильных устройствах является вендор-специфичным. На некоторых Android-устройствах ограничения на установку обновлений операционной системы вручную пользователем могут работать некорректно.

- Приложение Kaspersky Endpoint Security для Android не может быть установлено в режиме device owner на следующих устройствах: Honor 30i (Android 10), Huawei y8p, Huawei Y5 (Android 8), Huawei Mate 40 PRO (Android 10), Xiaomi Redmi 4X (Android 7.1), Honor 5c (Android 7.0, EMUI 5.0). Это связано со спецификой прошивки устройств: сканер QR-кода недоступен после сброса устройства до заводских настроек.

- На устройствах под управлением Android 10 при выдаче разрешения на определение местоположения автоматически устанавливается значение **Разрешить только во время использования приложения** вместо **Разрешить в любом режиме**. Это значение не может быть изменено администратором или пользователями. Проблема связана с известной ошибкой в Android 10.

- Ограничение **Запретить снимки экрана** не блокирует снимки экрана в настройках устройства.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

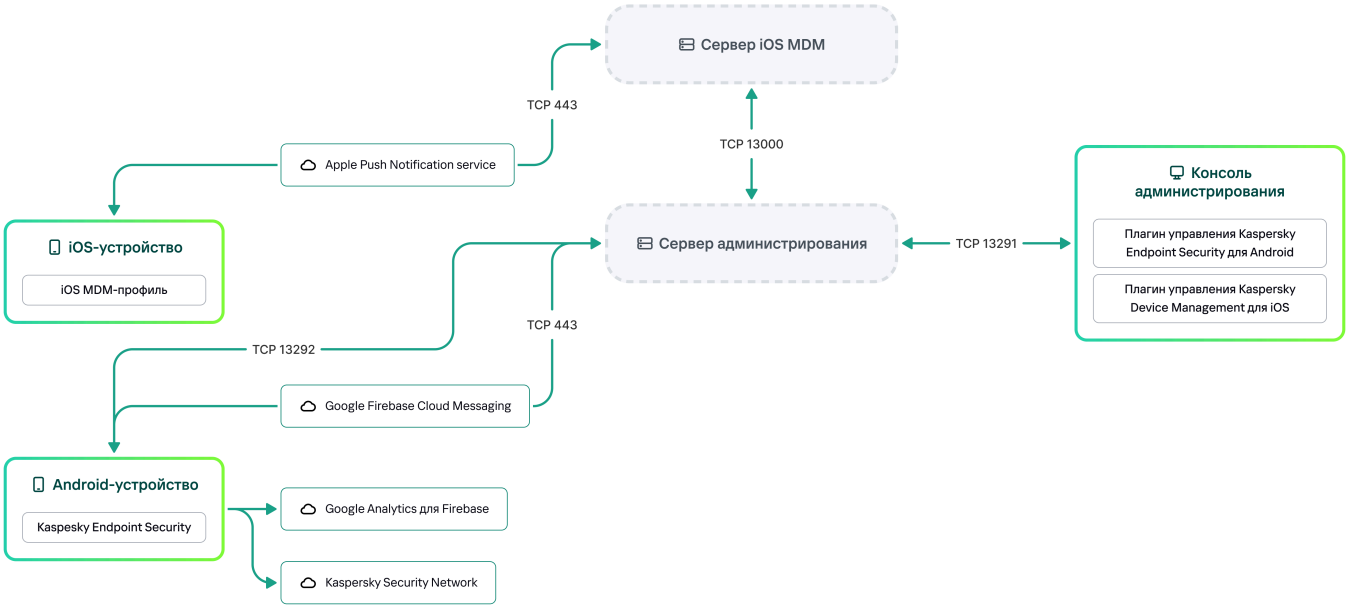
- Плагин управления Kaspersky Endpoint Security для Android

  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 протоколу iOS MDM, 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 и Сервере iOS MDM приведена в *справке Kaspersky Security Center*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 на персональных устройствах

На *персональных устройствах* 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 инсталляционный пакет в Kaspersky Security Center.

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

Для развертывания Kaspersky Endpoint Security для Android с помощью инсталляционного пакета выполните следующие действия:

1. Создайте и настройте инсталляционный пакет приложения.
2. Создайте автономный инсталляционный пакет.
3. Отправьте пользователям Android-устройств сообщения со ссылкой на загрузку автономного инсталляционного пакета. Доступна массовая рассылка.

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

Схемы развертывания Kaspersky Endpoint Security для Android через Kaspersky Security Center на корпоративных устройствах (режим device owner)

На *корпоративных устройствах (режим device owner)*, развертывание Kaspersky Endpoint Security для Android через Kaspersky Security Center может быть выполнено следующим способом:

- С помощью рассылки QR-кода со ссылкой на общую версию приложения (установочный файл APK).
- С помощью рассылки QR-кода со ссылкой на инсталляционный пакет в Kaspersky Security Center.

Для развертывания Kaspersky Endpoint Security для Android в режиме device owner через общую версию приложения выполните следующие действия:

1. Создайте QR-код для установки приложения из Консоли администрирования.
2. Выполните предварительную настройку мобильного устройства и установите Kaspersky Endpoint Security для Android с использованием QR-кода.

Для развертывания Kaspersky Endpoint Security для Android в режиме device owner с помощью инсталляционного пакета выполните следующие действия:

1. Создайте и настройте инсталляционный пакет приложения.
2. Создайте автономный инсталляционный пакет.
3. Создайте QR-код для установки приложения с использованием инсталляционного пакета.
4. Выполните предварительную настройку мобильного устройства и установите Kaspersky Endpoint Security для Android с использованием QR-кода.

Схема развертывания Kaspersky Endpoint Security для Android из Google Play

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 мобильного 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 устройстве дополнительно требуется установить мобильный сертификат.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Подготовка Консоли администрирования к развертыванию комплексного решения

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 17100.

6. Нажмите кнопку **ОК**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка шлюза соединения для подключения мобильных устройств к Серверу администрирования Kaspersky Security Center

В этом разделе описывается настройка шлюза соединения для подключения мобильных устройств к Серверу администрирования Kaspersky Security Center. Настройка включает в себя следующие шаги:

1. Установка Агента администрирования в качестве шлюза соединения на хосте.
2. Настройка шлюза соединения на Сервере администрирования Kaspersky Security Center.

> Эта статья содержит обзор сценария. Более подробная информация приведена в документации Kaspersky Security Center.

Требования

Чтобы шлюз соединения корректно работал с мобильными устройствами, должны соблюдаться следующие требования:

- Порт 13292 должен быть открыт на хосте со шлюзом соединения.
- Порт 13000 должен быть открыт между шлюзом соединения и Kaspersky Security Center. Его открытие наружу из демилитаризованной зоны не требуется.
- Хост должен иметь статический адрес, доступный из интернета.

Установка Агента администрирования на хост, выполняющий роль шлюза соединения

Сначала необходимо установить Агент администрирования на выбранном устройстве-хосте, который будет выступать в качестве шлюза соединения. Вы можете загрузить полный инсталляционный пакет Kaspersky Security Center или установить Kaspersky Security Center локально.

По умолчанию установочный файл расположен по следующему пути: `\\<server name>\KLSHARE\PkgInst\NetAgent_<version number>`

Чтобы установить Агент администрирования в роли шлюза соединения:

1. Запустите Мастер установки Агента администрирования и следуйте его указаниям, оставляя настройки по умолчанию для всех параметров, пока не откроется окно **Выбор Сервера администрирования**.
2. В окне **Выбор Сервера администрирования** настройте следующие параметры:
   - Введите адрес устройства с установленным Сервером администрирования.
   - Оставьте значения по умолчанию в полях **Порт**, **SSL-порт** и **UDP-порт**.

- Установите флажок **Использовать SSL для соединения с Сервером администрирования**, чтобы установить соединение с Сервером администрирования через защищенный порт с использованием SSL.

  Рекомендуется не снимать этот флажок, чтобы соединение оставалось защищенным.

- Установите флажок **Разрешить Агенту администрирования открыть UDP-порт**, чтобы управлять клиентскими устройствами и получать о них информацию.

3. Нажмите **Далее** и пройдите все шаги мастера до появления окна **Шлюз соединения**, оставляя настройки по умолчанию.

4. В окне **Шлюз соединения** выберите **Использовать в качестве шлюза соединения в демилитаризованной зоне**.

   Этот режим одновременно активирует Агент администрирования в роли шлюза соединения и переключает его на ожидание подключений от Сервера администрирования, а не на установку подключения к Серверу администрирования.

5. Нажмите **Далее** и начните установку.

Теперь Агент администрирования установлен и настроен в качестве шлюза соединения.

Настройка шлюза соединения на Сервере администрирования Kaspersky Security Center

После установки Агента администрирования в качестве шлюза соединения необходимо подключить его к Серверу администрирования. Сервер администрирования пока не отображает устройство со шлюзом соединения в списке управляемых устройств, поскольку шлюз соединения еще не подключался к Серверу администрирования. По этой причине необходимо добавить шлюз соединения как точку распространения, чтобы убедиться, что Сервер администрирования инициирует подключение к шлюзу соединения.

Чтобы настроить шлюз соединения на Сервере администрирования:

1. Добавьте шлюз соединения как точку распространения в Kaspersky Security Center.

   a. В дереве консоли выберите узел **Сервер администрирования**.

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

   c. В окне свойств Сервера администрирования выберите раздел **Точки распространения**.

   d. Нажмите на кнопку **Добавить**.

      Откроется окно **Добавление точки распространения**.

   e. В окне **Добавление точки распространения** выполните следующие действия:

      - Укажите IP-адрес устройства с установленным Агентом администрирования в поле **Устройство, которое будет выполнять роль точки распространения**. Для этого выберите пункт **Добавить шлюз соединения, находящийся в демилитаризованной зоне, по адресу** в раскрывающемся списке.

        Введите IP-адрес шлюза соединения или имя шлюза соединения, если к нему можно получить доступ по имени.

      - В поле **Область действия точки распространения**, в раскрывающемся списке выберите группу, на которую будет распространяться шлюз соединения, а затем нажмите **ОК**.

   f. В разделе **Точки распространения** нажмите **ОК**, чтобы сохранить внесенные изменения.

Шлюз соединения будет сохранен как новая запись под именем **Временная запись для шлюза соединения**.

Сервер администрирования практически сразу попытается подключиться к шлюзу соединения по указанному вами адресу. При удачном подключении имя записи изменится на имя устройства шлюза соединения. Этот процесс занимает до 5 минут.

Пока временная запись для шлюза соединения переводится в именованную запись, шлюз соединения также отображается в группе **Нераспределенные устройства**.

2. Создайте новую группу в группе **Управляемые устройства**. В эту группу будут входить внешние управляемые устройства.

3. Переместите шлюз соединения из группы **Нераспределенные устройства** в группу, которую вы создали для внешних устройств.

4. Настройте свойства шлюза соединения, который вы развернули:

    1. В свойствах Сервера администрирования, в разделе **Точки распространения** выберите шлюз соединения и нажмите **Свойства**.

    2. В разделе **Общие**, в свойстве **Имена DNS-доменов точки распространения, под которыми она будет доступна мобильным устройствам (включаются в сертификат)** укажите DNS-имя шлюза соединения, которое будет использоваться для подключения к мобильному устройству.

    3. В разделе **Шлюз соединения** установите следующие флажки, оставляя номера портов по умолчанию:

        - **Открыть порт для мобильных устройств (аутентификация SSL только для Сервера администрирования).**

        - **Открыть порт для мобильных устройств (двусторонняя аутентификация SSL).**

    4. Нажмите **OK**, чтобы сохранить внесенные изменения.

Шлюз соединения настроен. Теперь вы можете добавлять новые мобильные устройства, указав адрес шлюза соединения. Новые устройства появятся на Сервере администрирования.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 **OK**.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Создание мобильного сертификата

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

Чтобы создать мобильный 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 **Мобильный сертификат**.
4. В окне мастера **Выбор пользователя** укажите пользователей, для которых вы хотите создать мобильный сертификат.
5. В окне мастера **Источник сертификата** укажите способ создания мобильного сертификата.
   - Чтобы создать мобильный 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 мобильный 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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка Kaspersky Endpoint Security для Android

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

На устройствах с операционной системой Android 11 и выше необходимо отключить системную настройку **Удалить разрешения, если приложение не используется**. В противном случае, если приложение не используется в течение нескольких месяцев, система автоматически сбрасывает разрешения, предоставленные приложению пользователем.

Разрешения, запрашиваемые Kaspersky Endpoint Security для Android

Разрешение	Функция приложения
Телефон (для Android 5.0 – 9.X)	Подключение к Kaspersky Security Center (идентификатор устройства)
Память (обязательно)	Антивирус
Доступ на управление всеми файлами (для Android 11 или более поздней версии)	Антивирус
Устройства Bluetooth поблизости (Android 12 или более поздней версии)	Ограничение использования Bluetooth
Уведомления (для Android 13)	Уведомление пользователя о проблемах безопасности и событиях приложения
Разрешение на работу в фоновом режиме (Android 12 или более поздней версии)	Обеспечение непрерывной работы приложения. Если разрешение не предоставлено, приложение может быть выгружено из памяти и не сможет перезапуститься.

Разрешение	Функция приложения
Администратор устройства (обязательно)	Анти-Вор – блокировка устройства (только для Android 5.0 – 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 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 возможности	Анти-Вор – блокировка устройства (только для Android 7.0 и выше)
	Веб-Фильтр
	Контроль 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)
	Ограничение использования камеры (только для Android 11 и выше)
Отображать всплывающее окно (на некоторых устройствах Xiaomi)	Веб-Фильтр
Отображать всплывающие окна при работе в фоновом режиме (на некоторых устройствах Xiaomi)	Веб-Фильтр

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.
- Мобильный 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 разделе **Операционная система** выберите **Android**.
4. В разделе **Тип устройства** выберите **Персональное устройство**.

   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.
5. На странице **Способ установки Kaspersky Endpoint Security для Android** выберите **Ссылка на версию приложения в Google Play.**

6. 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.

7. 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.

8. 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 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.

9. 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка Kaspersky Endpoint Security для Android в режиме device owner

Режим device owner – это режим работы корпоративных Android-устройств. Этот режим позволяет вам осуществлять полный контроль над устройством и настраивать множество функций. Режим device owner поддерживается на Android 7.0 или выше.

Kaspersky Security Center позволяет установить приложение Kaspersky Endpoint Security для Android в режиме device owner с помощью сгенерированного QR-кода для установки приложения на устройство.

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.

Способы установки приложения

Приложение Kaspersky Endpoint Security для Android можно установить с помощью QR-кода, который содержит один из вариантов ссылки:

- **Ссылку на общую версию приложения.**

  Выберите этот способ для мобильных устройств, которые имеют доступ в интернет, чтобы загрузить установочный файл APK с сайта "Лаборатории Касперского". После этого приложение будет обновляться с помощью Google Play или Huawei AppGallery.

- **Ссылку на инсталляционный пакет в Kaspersky Security Center.**

  Выберите этот способ для мобильных устройств без доступа к интернету. Инсталляционный пакет приложения будет загружен с сервера Kaspersky Security Center. Приложение также будет обновляться через Kaspersky Security Center с помощью настроек политики.

  Чтобы использовать этот способ, перед генерацией QR-кода выполните следующие шаги:

  1. Создайте и настройте инсталляционный пакет приложения.
  2. Создайте автономный инсталляционный пакет.

Генерация QR-кода для установки приложения

Чтобы сгенерировать QR-код для установки приложения в режиме device owner:

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 разделе **Операционная система** выберите **Android**.
4. В разделе **Тип устройства** выберите **Корпоративное устройство (режим device owner)**.
5. В разделе **Дополнительно** выберите необходимые параметры:

   - Установите флажок **Включить все системные приложения**, если вы хотите, чтобы системные приложения на устройстве были включены. Если флажок снят, все системные приложения отключены.
   - Установите флажок **Разрешить использовать мобильную сеть для загрузки Kaspersky Endpoint Security**, если вы хотите использовать мобильную сеть для загрузки приложения Kaspersky Endpoint Security для Android. Опция поддерживается на устройствах с Android версии 8 и выше. Если флажок снят, приложение будет загружено при подключении устройства к Wi-Fi.

6. Нажмите **Далее**.

   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.

7. На странице **Способ установки Kaspersky Endpoint Security для Android в режиме device owner** выберите способ установки:

   - **Ссылка на общую версию приложения.**
   - **Ссылка на инсталляционный пакет в Kaspersky Security Center.**

     При выборе этого варианта, оставьте флажок **Разрешить использование HTTP для загрузки приложения в режиме device owner** установленным, чтобы убедиться, что приложение будет загружено. В противном случае приложение будет загружено через HTTPS, только если сертификат Веб-сервера Kaspersky Security Center был выдан доверенным центром сертификации.

   Подробная информация об этих способах установки доступна в разделе **Способы установки приложения**.

8. 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.

9. 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.

10. На странице **Способ уведомления пользователей** укажите адреса электронной почты. Убедитесь, что в параметрах учетных записей пользователей в Kaspersky Security Center указан адрес электронной почты.

11. Проверьте информацию на странице **Результат** и сохраните QR-код.

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

Для установки Kaspersky Endpoint Security для Android в режиме device owner необходима дополнительная настройка Android-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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 мобильный сертификат для пользователя мобильного устройства.

4. Пользователь получает автоматическое уведомление с предложением установить мобильный сертификат. После подтверждения мобильный 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 мобильного 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

  > На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

- **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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Активация приложения Kaspersky Endpoint Security для Android

В Kaspersky Security Center лицензия может распространяться на различные группы функциональности. Для полноценного функционирования Kaspersky Endpoint Security для Android 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*.

Активация приложения Kaspersky Endpoint Security для Android на мобильном устройстве осуществляется путем предоставления приложению информации о действующей лицензии. Информация о лицензии передается на мобильное устройство вместе с политикой при синхронизации устройства с Kaspersky Security Center.

Если приложение Kaspersky Endpoint Security для Android не было активировано в течение 30 дней с момента установки на мобильное устройство, 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 приложение не было активировано в течение 30 дней с момента установки, пользователю необходимо вручную выполнить синхронизацию устройства с Kaspersky Security Center.

Если Kaspersky Security Center не развернут в вашей организации или недоступен для мобильных устройств, пользователи могут активировать приложение Kaspersky Endpoint Security для Android на своих устройствах вручную.

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 разделе **Лицензирование** 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 – персональные 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.

Устройства в режиме supervised

iOS-устройства в режиме supervised – 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 устройствах в режиме supervised 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 iOS-устройствами в режиме supervised и неконтролируемыми iOS-устройствами на Сервер iOS MDM должен быть установлен APNs-сертификат, а на мобильных устройствах пользователей – iOS MDM-профиль.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 разделе **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 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 протоколу iOS MDM 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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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**).

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Чтобы удалить Kaspersky Endpoint Security для Android с устройства, работающего в режиме device owner:

1. Отправьте на устройство команду **Сбросить настройки до заводских** из Консоли администрирования. Эта команда удаляет все данные с устройства и сбрасывает настройки устройства до заводских.

2. Вручную удалите устройство из списка управляемых устройств в Консоли администрирования.

   Если устройство не будет удалено из Консоли администрирования, то при последующей установке приложений "Лаборатории Касперского" на устройство могут возникнуть проблемы.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Информация об удалении Kaspersky Endpoint Security для Android с устройств, работающих в режиме device owner, приведена в разделе **Удаление приложения в режиме device owner**.

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 Kaspersky Endpoint Security для Android** установите флажок **Удалить с устройства приложение Kaspersky Endpoint Security для Android**.

   Этот параметр неприменим для устройств, работающих в режиме device owner.

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 с устройства приложение Kaspersky Endpoint Security для Android**.

   Этот параметр неприменим для устройств, работающих в режиме device owner.

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.

Удаление приложения в режиме device owner

Чтобы удалить Kaspersky Endpoint Security для Android с устройства, работающего в режиме device owner:

1. В дереве консоли выберите **Управление мобильными устройствами → Мобильные устройства**.
2. В списке устройств выберите устройство, на котором вы хотите удалить приложение.
3. Щелкните правой кнопкой мыши по устройству.
4. В контекстном меню выберите **Управление мобильными устройствами → Сбросить настройки до заводских**.

   Команда **Сбросить настройки до заводских** отправлена на устройство. Эта команда удаляет все данные с устройства и сбрасывает настройки устройства до заводских.
5. В списке устройств щелкните правой кнопкой мыши по устройству и нажмите **Удалить**.

   Устройство удалено из списка управляемых устройств в Консоли администрирования.

   Если устройство не будет удалено из Консоли администрирования, то при последующей установке приложений "Лаборатории Касперского" на устройство могут возникнуть проблемы.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

На устройствах, работающих в режиме device owner, приложение Kaspersky Endpoint Security для Android может быть удалено только администратором. Дополнительная информация приведена в разделе Дистанционное удаление приложения.

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**.

   Этот параметр неприменим для устройств, работающих в режиме device owner.

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**.

   Этот параметр неприменим для устройств, работающих в режиме device owner.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 или устройство работает в режиме device owner.

   > На устройствах, работающих в режиме device owner, приложение Kaspersky Endpoint Security для Android может быть удалено только администратором. Дополнительная информация приведена в разделе Дистанционное удаление приложения.

2. Подтвердить удаление Kaspersky Endpoint Security для Android.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Начало работы

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Создание групповой политики

В этом разделе описано создание групповых политик для устройств, на которых установлено мобильное приложение Kaspersky Endpoint Security для Android, а также политик для 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 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

  На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

- **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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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. Он содержит следующую информацию:

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Защита

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 уведомлениях 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 заблокировать рекламные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламное ПО, средства автодозвона и приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя**.

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. 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 заблокировать рекламные программы, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя, установите флажок **Обнаруживать рекламное ПО, средства автодозвона и приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя**.

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. 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.

   На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

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.

   На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

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

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 (включая функцию Custom Tabs), 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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).

Способ подключения к Kaspersky Security Center	Команда	Результат выполнения команды
Kaspersky Endpoint Security для Android	Заблокировать	Мобильное устройство заблокировано.
	Разблокировать	На устройствах под управлением операционной системы Android версии 5.0 – 6.X после разблокировки мобильного устройства пароль разблокировки экрана 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	Получены координаты местоположения мобильного устройства на карте. На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой.
	Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства при попытке разблокировать устройство. На устройствах с выдвижной фронтальной камерой фотография будет черной, если камера закрыта. При попытке разблокировки устройства пользователь автоматически соглашается на фотографирование. Если разрешение на использование камеры было отозвано, на мобильном устройстве отображается уведомление, предлагающее предоставить это разрешение. Если разрешение на использование камеры было отозвано из панели быстрых настроек на мобильном устройстве под управлением Android 12 или более поздней версии, уведомление не отображается, но сделанная фотография будет черной.
	Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал. Звуковой сигнал воспроизводится 5 мин (при низком уровне заряда батареи – 1 мин).
	Удалить корпоративные данные	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.
	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	Заблокировать	Мобильное устройство заблокировано.
	Сбросить пароль	Сброшен пароль для разблокировки экрана мобильного устройства, пользователю предложено установить новый пароль в соответствии с требованиями политики.
	Удалить корпоративные данные	Будут 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.

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 Анти-Вора 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.

Полный список доступных команд приведен в разделе Команды для мобильных устройств. Подробная информация об отправке команд из Консоли администрирования приведена в справке Kaspersky Security Center.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 5.0 – 6.X после разблокировки мобильного устройства пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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**).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Удаление данных на Android-устройствах после неудачных попыток ввода пароля

Вы можете настроить удаление всех данных на Android-устройстве (то есть сброс настроек устройства до заводских) после того, как пользователь неправильно ввел пароль разблокировки экрана слишком много раз.

Эти настройки применимы для устройств, работающих в режиме device owner, и персональных устройств, на которых приложение Kaspersky Endpoint Security для Android включено в качестве администратора устройства.

Чтобы настроить удаление всех данных:

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 **Анти-Вор**.

5. В блоке **Удаление данных на устройстве** установите флажок **Удалить все данные после неудачных попыток ввода пароля разблокировки**.

6. В поле **Максимальное количество попыток ввода пароля разблокировки** укажите количество попыток разблокировать устройство, которые может совершить пользователь. По умолчанию указано значение 8. Максимальное доступное значение – 20.

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

Параметры на мобильном устройстве будут настроены после очередной синхронизации устройства с Kaspersky Security Center. Если указанное количество попыток ввести правильный пароль разблокировки экрана будет превышено пользователем, приложение Kaspersky Endpoint Security для Android удалит все данные на устройстве.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 политике, в окне **Свойства** 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. При необходимости укажите следующие параметры:

   - **Минимальное количество символов**

     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.

   - **Минимальные требования к паролю разблокировки (для режима device owner, Android 12 или ниже)**

     Определяет минимальные требования к паролю разблокировки. Требования применяются только к новым паролям пользователя. Доступны следующие значения:

     - **Числовой**

       Пользователь может установить пароль, включающий в себя цифры, или любой более надежный пароль (например, буквенный или буквенно-цифровой).

       Этот параметр выбран по умолчанию.

     - **Буквенный**

       Пользователь может установить пароль, включающий в себя буквы (или другие нечисловые символы), или любой более надежный пароль (например, буквенно-цифровой).

     - **Буквенно-цифровой**

       Пользователь может установить пароль, включающий в себя цифры и буквы (или другие нечисловые символы), или любой более надежный сложный пароль.

     - **Любой**

       Пользователь может установить любой пароль.

- **Сложный**

  Пользователь должен установить сложный пароль в соответствии с указанными свойствами пароля:

  - **Минимальное количество букв**
  - **Минимальное количество цифр**
  - **Минимальное количество специальных символов**
  - **Минимальное количество заглавных букв**
  - **Минимальное количество строчных букв**
  - **Минимальное количество небуквенных символов**

- **Сложный числовой**

  Пользователь может установить пароль, включающий в себя числа без повторений (например, 4444) или упорядоченных последовательностей (например, 1234, 4321, 2468), или любой более надежный сложный пароль.

- **Слабый биометрический**

  Пользователь может использовать биометрические методы разблокировки или установить более надежный сложный пароль.

Этот параметр применим только для устройств под управлением операционной системы Android версии 12 и выше в режиме device owner.

- **Срок действия пароля, в днях**

Определяет количество дней до истечения срока действия пароля. При применении новый срок действия будет установлен для текущего пароля.

По умолчанию указано значение 0. Это означает, что срок действия пароля не ограничен.

- **Количество дней, за которое уведомлять об истечении срока действия пароля (для режима device owner)**

Определяет количество дней, за которое уведомлять пользователя об истечении срока действия пароля.

По умолчанию указано значение 0. Это означает, что пользователь не будет уведомлен об истечении срока действия пароля.

Этот параметр применим только для устройств, работающих в режиме device owner.

- **Количество неповторяющихся паролей в журнале**

Определяет максимальное количество ранее использованных пользователем паролей, которые не могут быть установлены в качестве нового пароля.

По умолчанию указано значение 0. Это означает, что новый пароль пользователя может совпадать с любым ранее использованным паролем, кроме текущего.

- **Период неактивности для блокировки устройства, в секундах**

  Определяет период неактивности перед блокировкой экрана устройства. После окончания этого периода экран устройства будет заблокирован.

  По умолчанию указано значение 0. Это означает, что экран устройства не будет блокироваться после окончания какого-либо периода.

- **Период разблокировки без пароля, в минутах (для режима device owner, Android 8.0+)**

  Определяет период для разблокировки устройства без пароля. В течение этого периода пользователь может использовать биометрические методы для разблокировки экрана. После окончания этого периода пользователь может разблокировать экран только с помощью пароля.

  По умолчанию указано значение 0. Это означает, что пользователю не придется разблокировать устройство с помощью пароля после истечения какого-либо периода.

  Этот параметр применим только для устройств под управлением операционной системы Android версии 8 и выше в режиме device owner.

- **Разрешить биометрические методы разблокировки (Android 9+)**

  Если флажок установлен, использование биометрических методов разблокировки на мобильном устройстве разрешено.

  Если флажок снят, Kaspersky Endpoint Security для Android запрещает использовать биометрические методы для разблокировки экрана. Пользователь может разблокировать экран только с помощью пароля.

  По умолчанию флажок установлен.

  Этот параметр применим только для устройств под управлением Android 9 и выше.

- **Разрешить использование отпечатков пальцев**

  Использование отпечатков пальцев для разблокировки экрана. Флажок не ограничивает использование сканера отпечатков пальцев при входе в приложения или подтверждении покупок.

  На устройствах под управлением Android 10.0 и выше управлять использованием отпечатков пальцев для разблокировки экрана можно только в рабочих профилях.

  Если флажок установлен, использование отпечатков пальцев на мобильном устройстве разрешено. Если пароль разблокировки не соответствует требованиям корпоративной безопасности, пользователь не может использовать сканер отпечатков пальцев для разблокировки экрана.

Если флажок снят, Kaspersky Endpoint Security для Android блокирует возможность использовать отпечатки пальцев для разблокировки экрана. Пользователь может разблокировать экран только с помощью пароля. В настройках Android пункт установки отпечатков пальцев будет недоступен (**Настройки Android** > **Безопасность** > **Блокировка экрана** > **Отпечатки пальцев**).

Флажок доступен только если установлен флажок **Разрешить биометрические методы разблокировки (Android 9+)**.

По умолчанию флажок установлен.

- **Разрешить распознавание лица (Android 9+)**

  Если флажок установлен, использование распознавания лица на мобильном устройстве разрешено.

  Если флажок снят, Kaspersky Endpoint Security для Android запрещает использовать распознавание лица для разблокировки экрана.

  Флажок доступен только если установлен флажок **Разрешить биометрические методы разблокировки (Android 9+)**.

  По умолчанию флажок установлен.

  Этот параметр применим только для устройств под управлением Android 9 и выше.

- **Разрешить распознавание по радужной оболочке глаза (Android 9+)**

  Если флажок установлен, использование распознавания по радужной оболочке глаза на мобильном устройстве разрешено.

  Если флажок снят, Kaspersky Endpoint Security для Android запрещает использовать распознавание по радужной оболочке глаза для разблокировки экрана.

  Флажок доступен только если установлен флажок **Разрешить биометрические методы разблокировки (Android 9+)**.

  По умолчанию флажок установлен.

  Этот параметр применим только для устройств под управлением Android 9 и выше.

- **Принудительно использовать пароль при запуске**

  Если флажок установлен, пользователю не требуется вводить пароль при запуске устройства.

  После того как флажок установлен, невозможно отключить запрос пароля при запуске устройства без сброса настроек до заводских.

  Если флажок снят, требования, касающиеся запуска устройства, остаются без изменений.

  По умолчанию флажок снят.

- **Пароль разблокировки**

  Этот параметр позволяет установить пароль на устройстве пользователя.

  На устройствах под управлением операционной системы Android версии 11 и выше этот параметр применим, только если устройство находится в режиме device owner.

  После сохранения политики настройка применяется на устройстве в результате отправки команды с указанным паролем. Поле ввода будет очищено, указанный пароль не сохранится в Консоли администрирования.

  - Если устройство не защищено паролем или работает под управлением операционной системы Android версии 10 или ниже, Kaspersky Endpoint Security для Android сразу устанавливает пароль.
  - Если устройство работает под управлением операционной системы Android версии 11 или выше, Kaspersky Endpoint Security для Android предлагает пользователю применить новый пароль.

  Если вы оставите пустое значение, изменений на устройстве не будет.

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

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка виртуальной частной сети (VPN)

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 11 и ниже.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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. Протокол VPN IKEv2 также позволяет настроить VPN-соединение для избранных доменов веб-сайтов в Safari.

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.

   - **IKEv2** (Internet Key Exchange версии 2). Соединение устанавливает между двумя сетевыми объектами атрибут Ассоциация безопасности (SA) и поддерживает аутентификацию с использованием EAP (Extensible Authentication Protocols), общих ключей и сертификатов.

   - **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. Информацию об этих параметрах можно получить в контекстной справке плагина управления.

11. Для соединения **IKEv2** при необходимости настройте VPN-соединение для избранных доменов в Safari:

    a. Установите флажок **Настроить VPN-соединение для доменов (только для Safari)**, чтобы указать домены веб-сайтов, которые активируют VPN-соединение.

    b. Установите флажок **Подключаться автоматически**, если хотите, чтобы на устройстве автоматически включалось VPN-соединение, когда ассоциированные домены инициируют передачу данных по сети. Если флажок снят, пользователю необходимо включить VPN-соединение вручную, прежде чем ассоциированные домены инициируют передачу данных по сети.

    c. Укажите в таблице домены, которые активируют VPN-соединение в Safari. Все домены необходимо указывать в формате "www.example.com".

12. 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 **OK**.

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

13. Нажмите кнопку **OK**.

    Новая сеть VPN 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 VPN-сети.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Контроль

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка ограничений

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 политике, в окне **Свойства** 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**.

     На устройствах под управлением Android 10.0 и выше запрет на использование сетей Wi-Fi не поддерживается.

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

     На устройствах под управлением Android 10 и выше использование камеры нельзя запретить полностью.

     На устройствах с операционной системой Android 11 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 не удастся ограничить использование камеры.

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

     На Android 12 или более поздней версии использование Bluetooth может быть отключено, только если пользователь устройства предоставил разрешение **Устройства Bluetooth поблизости**. Пользователь может предоставить это разрешение во время работы мастера начальной настройки или позже.

На личных устройствах под управлением Android 13 или выше нельзя отключить 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка ограничений для iOS MDM-устройств

Для выполнения требований корпоративной безопасности следует настроить ограничения в работе iOS MDM-устройства. Информацию о доступных ограничениях можно получить в контекстной справке плагина управления.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка доступа пользователей к веб-сайтам

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Для работы Веб-Фильтра необходимо выполнение следующих условий:

- Приложение Kaspersky Endpoint Security включено в качестве службы Специальных возможностей.
- Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) должно быть принято. Kaspersky Endpoint Security использует Kaspersky Security Network (KSN) для проверки веб-сайтов. Положение о Веб-Фильтре содержит условия обмена данными с KSN.

  Вы можете принять Положение о Веб-Фильтре в Kaspersky Security Center. В этом случае пользователю не потребуется выполнять никаких действий.

  Если вы не приняли Положение о Веб-Фильтре и направили пользователю запрос на принятие Положения, пользователь должен прочитать и принять Положение о Веб-Фильтре в настройках приложения.

  Если вы не приняли Положение о Веб-Фильтре, Веб-Фильтр будет недоступен.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome (включая функцию Custom Tabs), 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:

      - `https://example.com.*` – разрешены все страницы веб-сайта (например, `https://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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 устройств в режиме supervised.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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).

  На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

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 пользователя об этом.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Контроль соответствия iOS MDM-устройств требованиям корпоративной безопасности

Контроль соответствия позволяет контролировать соблюдение требований корпоративной безопасности на iOS MDM-устройствах и принимать меры в случае обнаружения несоответствия требованиям. Контроль соответствия работает на основе списка правил. Каждое правило содержит следующие компоненты:

- статус (правило включено или выключено);
- критерии несоответствия (например, отсутствие указанных приложений или версия операционной системы на устройстве);
- действия, выполняемые на устройстве, если обнаружено несоответствие (например, удалить корпоративные данные или отправить пользователю сообщение электронной почты).

Чтобы создать правило:

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 **Контроль соответствия**.

5. В разделе **Правила Контроля соответствия** нажмите **Добавить**.

   Запустится мастер создания правила контроля соответствия.

6. Установите флажок **Включить правило**, если хотите включить правило. Если флажок снят, правило выключено.

7. На закладке **Критерии несоответствия** нажмите **Добавить критерий** и выберите критерий несоответствия для правила. Вы можете добавить несколько критериев. Их можно объединить с помощью логического оператора AND.

   Доступны следующие критерии:

   - **Список приложений на устройстве**

     Проверяет список приложений на устройстве на наличие запрещенных приложений или на отсутствие обязательных приложений.

     Для этого критерия необходимо выбрать тип проверки (**содержит** или **не содержит**) и указать идентификаторы приложений.

   - **Версия операционной системы**

     Проверяет версию операционной системы на устройстве.

     Для этого критерия необходимо выбрать оператор сравнения (**равно**, **не равно**, **меньше** или **больше**) и указать версию iOS.

     Операторы **равно** и **не равно** проверяют полное соответствие версии операционной системы указанному значению. Например, если в правиле указать версию 15, а устройство работает на iOS 15.2, то условие **равно** не будет выполнено. Если необходимо указать диапазон версий, вы можете создать два критерия, использовав операторы **меньше** и **больше**.

   - **Режим управления**

     Проверяет режим управления устройством.

     Для этого критерия необходимо выбрать режим (**Устройство в режиме supervised** или **Неконтролируемое устройство**).

8. На закладке **Действия** укажите действия, которые будут выполняться на устройстве при обнаружении всех указанных критериев несоответствия. Добавить действие можно одним из следующих способов:

   - Нажмите кнопку **Добавить действие**, если действие должно быть выполнено на устройстве сразу после обнаружения несоответствия.

   - Нажмите кнопку **Добавить отложенное действие**, если вы хотите установить период времени, в течение которого пользователь может устранить несоответствие. Если несоответствие не будет устранено в течение указанного периода, на устройстве будет выполнено действие.

Доступны следующие действия:

- **Отправить сообщение пользователю**

  Пользователь устройства будет проинформирован о несоответствии по электронной почте.

  Для этого действия необходимо указать адрес(-а) электронной почты пользователя и сообщение электронной почты.

- **Установить профиль**

  Конфигурационный профиль будет установлен на устройстве. Действие выполняется с помощью отправки команды **Установить профиль**.

  Для этого действия необходимо указать идентификатор устанавливаемого конфигурационного профиля.

- **Удалить профиль**

  Конфигурационный профиль будет удален с устройства. Действие выполняется с помощью отправки команды **Удалить профиль**.

  Для этого действия необходимо указать идентификатор удаляемого конфигурационного профиля.

- **Удалить все профили**

  Все ранее установленные конфигурационные профили будут удалены с устройства.

- **Удалить корпоративные данные**

  Будут удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**. Действие выполняется с помощью отправки команды **Удалить корпоративные данные**.

9. Нажмите кнопку **Сохранить**, чтобы сохранить правило и закрыть мастер.

   Новое правило появится в списке в разделе **Правила Контроля соответствия**.

10. Нажмите на кнопку **Применить**, чтобы сохранить изменения, внесенные в политику, и закрыть окно свойств политики.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Контроль приложений

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Контроль приложений на Android-устройствах

Компонент Контроль приложений позволяет управлять приложениями на Android-устройствах, чтобы обеспечивать безопасность этих устройств.

- 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 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.

В режиме device owner вам доступен расширенный контроль над устройством. Контроль приложений работает, не уведомляя об этом пользователя устройства:

- Обязательные приложения устанавливаются автоматически в фоновом режиме. Для тихой установки приложений необходимо указать ссылку на APK-файл обязательного приложения в настройках политики.

- Запрещенные приложения можно удалять с устройства автоматически. Для тихого удаления приложений необходимо установить флажок **Автоматически удалять запрещенные приложения (только в режиме device owner)** в настройках политики.

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**. Приложение скроет значки заблокированных приложений.

   - Чтобы разрешить пользователю запускать только приложения, указанные в списке категорий и приложений как разрешенные, рекомендованные или обязательные, выберите режим **Разрешенные приложения**. Приложение скроет значки всех приложений, кроме тех, которые указаны в списке разрешенных, рекомендованных или обязательных приложений и системных приложений.

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. Если устройство находится в режиме device owner, установите флажок **Автоматически удалять запрещенные приложения (только в режиме device owner)**, чтобы удалить запрещенные приложения с устройства в фоновом режиме, не уведомляя об этом пользователя.

8. 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.

9. 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".

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

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

> Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Контроль приложений на iOS MDM-устройствах

Kaspersky Security Center позволяет управлять приложениями на iOS MDM-устройствах, чтобы поддерживать их безопасность. Вы можете создать список приложений, которые разрешено устанавливать на устройствах, и список приложений, которые запрещено отображать и запускать на устройствах.

> Ограничения применимы только для iOS MDM-устройств в режиме supervised.

Переход к разделу Ограничения приложений

Чтобы открыть настройки ограничений приложений на iOS MDM-устройствах:

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 приложений**.

Ограничение установки приложений

По умолчанию пользователь может устанавливать любые приложения на iOS MDM-устройстве в режиме supervised.

Чтобы ограничить список приложений, которые можно установить на устройстве:

1. Установите флажок **Разрешить установку приложений из списка (только для supervised)**.
2. В таблице нажмите **Добавить**, чтобы добавить приложение в список.
3. Укажите идентификатор пакета приложения. Получить идентификатор пакета приложения можно по инструкциям в документации Apple. Укажите значение *com.apple.webapp*, чтобы разрешить все веб-клипы.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

После применения политики к устройству на устройстве будут настроены указанные ограничения для приложений. Для установки будут доступны только приложения из списка и системные приложения. Любые другие приложения не могут быть установлены на устройстве.

Указанные приложения можно установить на устройстве следующими способами (если соответствующие параметры включены в разделе **Ограничения функций**):

- Установка из Apple Configurator или iTunes
- Установка из App Store
- Автоматическая загрузка

Добавление приложений в список запрещенных

По умолчанию на iOS MDM-устройстве в режиме supervised могут отображаться и запускаться все приложения.

Чтобы указать запрещенные приложения:

1. Установите флажок **Запретить отображение и запуск приложений из списка (только для supervised)**.
2. В таблице нажмите **Добавить**, чтобы добавить приложение в список.

3. Укажите идентификатор пакета приложения. Получить идентификатор пакета приложения можно по инструкциям в документации Apple. Укажите значение *com.apple.webapp*, чтобы запретить все веб-клипы.

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

После применения политики к устройству на устройстве будут настроены указанные ограничения для приложений. Приложения из списка будет запрещены для отображения и запуска на устройстве. Все остальные приложения будут отображаться, и их можно будет запускать.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка и удаление приложений для группы iOS MDM-устройств

Kaspersky Security Center позволяет устанавливать и удалять приложения на iOS MDM-устройствах с помощью отправки команд на устройства.

Выбор устройств

Чтобы выбрать iOS MDM-устройства, на которых необходимо установить или удалить приложения:

1. В дереве консоли, в папке **Управление мобильными устройствами** выберите подпапку **Мобильные устройства**.

   В рабочей области папки отображается список управляемых мобильных устройств.

2. Для отображения iOS MDM-устройств в рабочей области настройте фильтр по типу протокола (**iOS MDM**).

3. Выберите iOS MDM-устройство, на котором необходимо установить или удалить приложения.

   Вы можете выбрать несколько устройств и отправить команды одновременно. Выбрать группу устройств можно одним из следующих способов:

   - Чтобы выбрать все устройства в рабочей области, настройте необходимый фильтр для списка устройств и нажмите **Ctrl+A**.
   - Чтобы выбрать диапазон устройств, выберите первое и последнее устройство в диапазоне щелчком мыши, удерживая **Shift**.
   - Чтобы выбрать несколько отдельных устройств, выберите устройства, которые вы хотите включить в группу, щелчком мыши, удерживая **Ctrl**.

Установка приложений на устройствах

Перед установкой приложения на iOS MDM-устройстве, необходимо добавить приложение на Сервер iOS MDM. Дополнительная информация приведена в разделе Добавление управляемого приложения.

Чтобы установить приложения на выбранных iOS MDM-устройствах:

1. Щелкните правой кнопкой мыши по выбранным устройствам. В появившемся контекстном меню выберите **Все команды**, а затем **Установить приложение**.

   Если устройство только одно, в контекстном меню можно выбрать **Показать журнал команд**, перейти в раздел **Установить приложение** и нажать кнопку **Отправить команду**.

   Откроется окно **Выбор приложений** со списком управляемых приложений.

2. Выберите приложения, которые хотите установить на iOS MDM-устройствах. Чтобы выбрать диапазон приложений, используйте клавишу **Shift**. Чтобы выбрать несколько отдельных приложений, используйте клавишу **Ctrl**.

3. Нажмите **OK**, чтобы отправить команду на устройства.

   В результате выполнения команды на устройстве будут установлены выбранные приложения. Если команда выполнена успешно, в журнале команд ее текущий статус изменится на **Завершена**.

Удаление приложений с устройств

Чтобы удалить приложения с выбранных iOS MDM-устройств:

1. Щелкните правой кнопкой мыши по выбранным устройствам. В появившемся контекстном меню выберите **Все команды**, а затем **Удалить приложение**.

   Если устройство только одно, в контекстном меню можно выбрать **Показать журнал команд**, перейти в раздел **Удалить приложение** и нажать кнопку **Отправить команду**.

   Откроется окно **Удаление приложений** со списком ранее установленных приложений.

2. Выберите приложения, которые хотите установить на iOS MDM-устройствах. Чтобы выбрать диапазон приложений, используйте клавишу **Shift**. Чтобы выбрать несколько отдельных приложений, используйте клавишу **Ctrl**.

3. Нажмите **OK**, чтобы отправить команду на устройства.

   В результате выполнения команды с устройства будут удалены выбранные приложения. Если команда выполнена успешно, в журнале команд ее текущий статус изменится на **Завершена**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 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 (**OK**).

   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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Управление

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Подключение Android-устройств к сети Wi-Fi

Для автоматического подключения Android-устройства к доступной сети Wi-Fi и обеспечения безопасности данных следует настроить параметры подключения.

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. Установите флажок **Скрытая сеть**, если хотите скрыть сеть Wi-Fi в списке доступных сетей на устройстве. В этом случае для подключения к сети пользователю потребуется вручную ввести на мобильном устройстве идентификатор сети SSID, заданный в параметрах маршрутизатора Wi-Fi.

8. Установите флажок **Автоматическое подключение к сети**, если хотите чтобы устройство подключалось к сети Wi-Fi автоматически.

9. В блоке **Защита сети** выберите тип безопасности сети Wi-Fi (открытая или защищенная по протоколу WEP, WPA/WPA2 PSK, или 802.1.x EAP).

   Протокол безопасности 802.1.x EAP поддерживается только в приложении Kaspersky Endpoint Security для Android версии 10.48.1.1 или выше. Протокол шифрования WEP поддерживается только в Android версии 9.0 или ниже.

10. При выборе протокола безопасности 802.1.x EAP, задайте дополнительные настройки защиты сети (**Метод EAP**, **Корневой сертификат** и другие). Информацию об этих параметрах можно получить в контекстной справке плагина управления.

11. В поле **Пароль** задайте пароль для доступа к сети, если на шаге 9 вы выбрали защищенную сеть.

12. Выберите вариант **Использовать прокси-сервер**, если хотите использовать прокси-сервер для подключения к сети Wi-Fi. В противном случае выберите вариант **Не использовать прокси-сервер**.

13. При выборе варианта **Использовать прокси-сервер**, 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.

14. 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.

15. 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.

16. 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 **OK**.

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 **OK**.

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

13. Нажмите кнопку **OK**.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка электронной почты

Этот раздел содержит информацию о настройке почтовых ящиков на мобильных устройствах.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 **OK**.

    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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 (доступно только в Android 9 и ниже).

Настройка почтового ящика Exchange возможна только для Samsung-устройств.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка корневых сертификатов на Android-устройствах

Корневой сертификат – это сертификат открытого ключа, выпущенный доверенным центром сертификации (CA). Корневые сертификаты используются, чтобы проверять пользовательские сертификаты и гарантировать их подлинность.

Kaspersky Security Center позволяет добавлять корневые сертификаты для Android-устройств, работающих в режиме device owner. Такие корневые сертификаты автоматически устанавливаются в доверенное хранилище сертификатов на устройствах.

Чтобы добавить корневой сертификат в Kaspersky Security Center:

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 **Корневые сертификаты**.
5. В разделе **Корневые сертификаты** нажмите **Добавить**.

   Откроется проводник.
6. Выберите файл сертификата (**.cer**, **.pem** или **.key**) и нажмите **Открыть**.

   Откроется окно **Сертификат**.
7. Просмотрите информацию о сертификате и нажмите **Установить сертификат...**

   Запустится стандартный мастер импорта сертификатов.
8. Следуйте указаниям мастера.

   После завершения работы мастера корневой сертификат появится в списке сертификатов.

Добавленные корневые сертификаты будут установлены на Android-устройства в режиме device owner после следующей синхронизации с Kaspersky Security Center.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

На Android 13 пользователь устройства должен предоставить разрешение на отправку уведомлений во время работы Мастера начальной настройки или позже.

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 **ОК**.

   Kaspersky Endpoint Security для Android не будет отображать уведомления о проблемах. 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 (resource 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка точки доступа (APN)

Для подключения мобильного устройства к услугам передачи данных в мобильной сети следует настроить параметры APN (Access Point Name).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка APN на Android-устройствах (только Samsung)

Настройка APN возможна только для Samsung-устройств.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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. В раскрывающемся списке **Тип аутентификации** выберите тип аутентификации пользователя устройства на сервере мобильного оператора для доступа к сети (интернет и MMS).
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).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка рабочего профиля Android

Этот раздел содержит информацию о работе с рабочим профилем Android.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 включить Веб-Фильтр в рабочем профиле и отключить в личном профиле для браузера Google Chrome, установите флажок **Включить Веб-Фильтр только в рабочем профиле**.

     > Для Samsung Internet Browser и Huawei Browser флажок **Включить Веб-Фильтр только в рабочем профиле** должен быть снят. Эти браузеры не позволяют включить Веб-Фильтр только в рабочем профиле. Если установить этот флажок, Веб-Фильтр не будет работать в этих браузерах.

     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**.

- Чтобы также установить VPN-сертификат в личный профиль, установите флажок **Дублировать установку VPN-сертификата в личный профиль**. По умолчанию VPN-сертификаты, полученные из Kaspersky Security Center, устанавливаются в рабочий профиль. Эта опция применяется, когда выписывается новый VPN-сертификат.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 **ОК**.
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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 указывать значки веб-клипов, которые отображаются на экране.

Добавление веб-клипов на Android-устройствах

Чтобы добавить веб-клип на Android-устройство 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 устройством**.
5. В разделе **Добавление веб-клипов на главный экран устройства** нажмите **Добавить**.

   Откроется окно **Добавить веб-клип**.
6. В поле **Название** введите название веб-клипа, которое будет отображаться на главном экране Android-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. В поле **Значок** укажите изображение для значка веб-клипа: нажмите **Обзор...** и выберите файл изображения. Поддерживаются форматы файлов PNG и JPEG. Если вы не выберете изображение для веб-клипа, в качестве значка будет отображаться пустой квадрат.
9. Нажмите кнопку **ОК**.

   Новый веб-клип отобразится в списке.
10. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

После того, как к устройству будет применена политика, приложение Kaspersky Endpoint Security для Android будет показывать уведомления, предлагающие пользователю установить веб-клипы, которые вы создали. После того, как пользователь установит веб-клипы, соответствующие значки будут добавлены на главный экран устройства.

Максимальное количество веб-клипов, которые можно добавить на Android-устройство, зависит от типа устройства. Когда это количество достигнуто, веб-клипы перестают добавляться на Android-устройство.

Добавление веб-клипов на iOS MDM-устройствах

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 **OK**.

    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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Режим device owner

Этот раздел содержит информацию о том, как управлять настройками мобильных Android-устройств в режиме device owner. Информация о развертывании режима device owner доступна в этом разделе.

В режиме device owner доступны следующие функции для мобильных Android-устройств:

- Ограничения функций операционной системы Android
- Управление настройками Google Chrome
- Тихая установка обязательных приложений и удаление запрещенных приложений в разделе Контроль приложений
- Режим киоска
- Управление Exchange ActiveSync для Gmail
- Подключение NDES и SCEP

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Ограничение функций Android на устройствах

Вы можете ограничить функции операционной системы Android в режиме device owner. Например, вы можете ограничить сброс настроек до заводских, изменение учетных данных, использование Google Play и Google Chrome, передачу файлов по USB, изменение настроек местоположения и управлять обновлениями системы.

Вы можете ограничить функции Android в разделе **Ограничения функций**.

*Чтобы открыть раздел **Ограничения функций**:*

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 **Режим device owner** > **Ограничения функций**.

Ограничение функций устройства

На вкладке **Функции устройства** в разделе **Ограничения функций** вы можете включить или отключить следующие функции:

- **Запретить сброс к заводским настройкам**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства сбрасывать настройки устройства до заводских.

  По умолчанию флажок снят.

- **Запретить снимки экрана**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства делать снимки экрана.

  По умолчанию флажок снят.

- **Запретить исходящие звонки**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства совершать исходящие звонки на этом устройстве.

  По умолчанию флажок снят.

- **Запретить отправку и получение SMS-сообщений**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства отправлять и получать SMS-сообщения на этом устройстве.

  По умолчанию флажок снят.

- **Запретить изменение учетных данных**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства менять учетные данные в операционной системе.

  По умолчанию флажок снят.

- **Запретить строку состояния (Android версии 6.0 или выше)**

  Запрещает отображение строки состояния.

  Если флажок установлен, строка состояния не отображается на устройстве. Уведомления и быстрые настройки, доступные в строке состояния, также будут заблокированы.

  Если флажок снят, строка состояния отображается на устройстве.

  Ограничение поддерживается на устройствах с Android версии 6.0 и выше.

  По умолчанию флажок снят.

- **Запретить безопасную загрузку (Android версии 6.0 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства запускать устройство в безопасном режиме.

  Ограничение поддерживается на устройствах с Android версии 6.0 и выше.

  По умолчанию флажок снят.

- **Принудительно включать экран при подключении к сетевому зарядному устройству (Android версии 6.0 или выше)**

  Установка или снятие флажка определяет, будет ли экран устройства включен во время зарядки с помощью сетевого зарядного устройства.

  Ограничение поддерживается на устройствах с Android версии 6.0 и выше.

  По умолчанию флажок снят.

- **Принудительно включать экран при подключении к зарядному устройству USB (Android версии 6.0 или выше)**

  Установка или снятие флажка определяет, будет ли экран устройства включен во время зарядки с помощью зарядного устройства USB.

  Ограничение поддерживается на устройствах с Android версии 6.0 и выше.

  По умолчанию флажок снят.

- **Принудительно включать экран при подключении к беспроводному зарядному устройству (Android версии 6.0 или выше)**

  Установка или снятие флажка определяет, будет ли экран устройства включен во время зарядки с помощью беспроводного зарядного устройства.

  Ограничение поддерживается на устройствах с Android версии 6.0 и выше.

  По умолчанию флажок снят.

Ограничение функций приложений

На вкладке **Приложения** в разделе **Ограничения функций** вы можете включить или отключить следующие функции:

- **Запретить использование камеры**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать все имеющиеся на устройстве камеры.

  По умолчанию флажок снят.

- **Запретить переключение камеры (Android версии 12.0 или выше)**

  Запрещает пользователю устройства использовать переключатель камеры.

Если флажок установлен, пользователь устройства не может блокировать доступ к камере с помощью системного переключателя.

Если флажок снят, пользователю устройства разрешено использовать переключатель камеры.

Ограничение поддерживается на устройствах с Android версии 12.0 и выше.

По умолчанию флажок снят.

- **Запретить использование Google Play**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать Google Play.

  По умолчанию флажок снят.

- **Запретить использование Google Chrome**

  Запрещает использование Google Chrome.

  Если флажок установлен, пользователь устройства не может запускать Google Chrome или изменять его параметры в системных настройках.

  Если флажок снят, пользователю устройства разрешено использовать Google Chrome на устройстве.

  По умолчанию флажок снят.

- **Запретить использование Google Assistant**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать Google Assistant на устройстве.

  По умолчанию флажок снят.

- **Запретить установку приложений из неизвестных источников**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства устанавливать приложения из неизвестных источников.

  По умолчанию флажок снят.

- **Запретить изменение приложений через Настройки**

  Запрещает изменение приложений через Настройки.

  Если флажок установлен, пользователю устройства запрещены следующие действия:

  - удаление приложений;
  - отключение приложений;
  - очистка кеша приложений;
  - удаление данных приложений;
  - принудительная остановка приложений;

- сброс приложений по умолчанию.

  Если флажок снят, пользователю устройства разрешено изменять приложения через Настройки.

  По умолчанию флажок снят.

- **Запретить установку приложений**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства устанавливать приложения на устройстве.

  По умолчанию флажок снят.

- **Запретить удаление приложений**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства удалять приложения с устройства.

  По умолчанию флажок снят.

- **Запретить отключение проверки приложения**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства отключать проверку приложений.

  По умолчанию флажок снят.

Ограничение функций памяти

На вкладке **Память** в разделе **Ограничения функций** вы можете включить или отключить следующие функции:

- **Запретить функции отладки**

  Запрещает использование функций отладки.

  Если флажок установлен, пользователь устройства не может использовать функции отладки по USB и режим разработчика.

  Если флажок снят, пользователю устройства разрешено получать доступ к функциям отладки и режиму разработчика и включать их.

  По умолчанию флажок снят.

- **Запретить установку физических внешних носителей**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства устанавливать физические внешние носители, например, SD-карты и OTG-адаптеры.

  По умолчанию флажок снят.

- **Запретить передачу файлов через USB**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства передавать файлы через USB.

По умолчанию флажок снят.

- **Запретить сервис резервного копирования (Android версии 8.0 или выше)**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства включать или выключать сервис резервного копирования.

  Ограничение поддерживается на устройствах с Android версии 8.0 и выше.

  По умолчанию флажок снят.

Ограничение функций сети

На вкладке **Сеть** в разделе **Ограничения функций** вы можете включить или отключить следующие функции:

- **Запретить использование Wi-Fi**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать Wi-Fi и изменять его параметры в Настройках.

  По умолчанию флажок снят.

- **Запретить использование Bluetooth (Android версии 8.0 или выше)**

  Запрещает использование Bluetooth.

  Если флажок установлен, пользователь устройства не может включать Bluetooth и изменять его параметры в Настройках.

  Если флажок снят, пользователю устройства разрешено использовать Bluetooth.

  Ограничение поддерживается на устройствах с Android версии 8.0 и выше. Для предыдущих версий Android установите флажок **Запретить использование Bluetooth** в разделе **Управление устройством**.

  По умолчанию флажок снят.

- **Запретить изменение настроек Wi-Fi**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства настраивать точки доступа Wi-Fi в Настройках. Ограничение не затрагивает настройки Wi-Fi для режима модема.

  По умолчанию флажок снят.

- **Запретить изменение предварительно настроенных сетей Wi-Fi**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять конфигурации Wi-Fi, добавленные администратором в разделе Wi-Fi.

  По умолчанию флажок снят.

- **Запретить изменение настроек Bluetooth**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять параметры Bluetooth в Настройках.

По умолчанию флажок снят.

- **Запретить изменение настроек VPN**

  Запрещает изменение настроек VPN.

  Если флажок установлен, пользователь устройства не может настроить VPN в Настройках, запуск VPN запрещен.

  Если флажок снят, пользователю устройства разрешено изменять VPN в Настройках.

  По умолчанию флажок снят.

- **Запретить изменение настроек мобильной сети**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства изменять настройки мобильной сети.

  По умолчанию флажок снят.

- **Запретить использование Android Beam через NFC**

  Установка или снятие флажка определяет, разрешено ли на устройстве использовать NFC для передачи данных из приложений. Тем не менее, пользователь устройства может включать и выключать NFC.

  По умолчанию флажок снят.

- **Запретить использование модема**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства настраивать режим модема и точки доступа.

  По умолчанию флажок снят.

- **Запретить обмен данными через Bluetooth (Android версии 8.0 или выше)**

  Установка или снятие флажка определяет, разрешена ли на устройстве отправка данных через Bluetooth.

  Ограничение поддерживается на устройствах с Android версии 8.0 и выше.

  По умолчанию флажок снят.

Ограничение служб геолокации

На вкладке **Службы геолокации** в разделе **Ограничения функций** вы можете настроить следующие параметры:

- **Запретить отслеживание местоположения**

  Запрещает включение и выключение отслеживания местоположения.

  Если флажок установлен, пользователь устройства не может включать и выключать отслеживание местоположения. Поиск устройства в режиме Анти-Вор будет недоступен.

Если флажок снят, пользователь устройства может включать и выключать отслеживание местоположения.

По умолчанию флажок снят.

Если одновременно установлены флажки **Запретить отслеживание местоположения** и **Запретить изменение настроек местоположения (Android версии 9.0 или выше)**, отслеживание местоположения будет отключено, и пользователь устройства не сможет включить его.

- **Запретить изменение настроек местоположения (Android версии 9.0 или выше)**

  Запрещает изменение настроек местоположения.

  Если флажок установлен, пользователь устройства не может изменять настройки местоположения или отключать отслеживание местоположения.

  Если флажок снят, пользователь устройства может изменять настройки местоположения.

  Ограничение поддерживается на устройствах с Android версии 9.0 и выше.

  По умолчанию флажок снят.

  Если одновременно установлены флажки **Запретить отслеживание местоположения** и **Запретить изменение настроек местоположения (Android версии 9.0 или выше)**, отслеживание местоположения будет отключено, и пользователь устройства не сможет включить его.

Ограничение обновлений системы

Управление настройками обновлений на мобильных устройствах является вендор-специфичным. На некоторых Android-устройствах ограничения на установку обновлений операционной системы вручную пользователем могут работать некорректно.

На вкладке **Обновления** в разделе **Ограничения функций** вы можете настроить следующие параметры:

- **Установить политику обновления системы**

  Тип политики обновления системы.

  Если флажок установлен, применяется одна из политик обновления системы:

  - **Устанавливать обновления автоматически**. Устанавливает обновления системы сразу, без взаимодействия с пользователем. Этот параметр выбран по умолчанию.
  - **Устанавливать обновления в указанный период времени**. Устанавливает обновления системы во время ежедневного периода обслуживания без взаимодействия с пользователем.

    Администратору необходимо указать начало и завершение ежедневного периода обслуживания в полях **Время начала** и **Время окончания**.
  - **Отложить обновление на 30 дней**. Откладывает установку обновлений системы на 30 дней.

    После окончания указанного периода операционная система предложит пользователю устройства установить обновления. Если доступно новое обновление системы, период будет сброшен и отсчет начнется заново.

    Если флажок снят, политика обновления системы не применяется.

    По умолчанию флажок установлен.

Управление настройками обновлений на мобильных устройствах является вендор-специфичным. На некоторых Android-устройствах ограничения на установку обновлений операционной системы вручную пользователем могут работать некорректно.

- **Периоды приостановки обновления системы (Android версии 9.0 или выше)**

  В блоке **Периоды приостановки обновления системы (Android версии 9.0 или выше)** вы можете задать один или несколько периодов длительностью до 90 дней, во время которых обновления системы не будут устанавливаться на устройстве. Во время периода приостановки обновления системы устройство работает следующим образом:

  - устройство не получает уведомления о предстоящих обновлениях системы;
  - обновления системы не устанавливаются;
  - пользователь устройства не может вручную проверить наличие обновлений системы.

    Чтобы добавить период, нажмите **Добавить период** и задайте начало и окончание периода в полях **Время начала** и **Время окончания**.

    Примечание. Каждый период может длиться не более 90 дней, а интервал между соседними периодами должен составлять не менее 60 дней.

  Ограничение поддерживается на устройствах с Android версии 9.0 и выше.

  Управление настройками обновлений на мобильных устройствах является вендор-специфичным. На некоторых Android-устройствах ограничения на установку обновлений операционной системы вручную пользователем могут работать некорректно.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Управление настройками Google Chrome

Вы можете управлять настройками Google Chrome в разделе **Настройки Google Chrome** в режиме device owner.

*Чтобы открыть раздел **Настройки Google Chrome**:*

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 **Режим device owner** > **Настройки Google Chrome**.

Управление настройками контента

На вкладке **Контент** в разделе **Настройки Google Chrome** вы можете задать следующие настройки контента:

- **Задать настройки файлов cookie по умолчанию**

  Настройки файлов cookie по умолчанию.

  Если флажок установлен, по умолчанию ко всем сайтам будет применяться одна из следующих опций:

  - **Разрешить всем сайтам сохранять локальные данные** (по умолчанию)
  - **Запретить всем сайтам сохранять локальные данные**
  - **Хранить файлы cookie до конца сеанса**

    Если флажок снят, будут применяться персональные настройки пользователя.

    Этот параметр поддерживается в Google Chrome версии 30 или выше.

    По умолчанию флажок установлен.

    Между шаблонами URL, которые указываются в полях **Разрешить файлы cookie на этих сайтах**, **Блокировать файлы cookie на этих сайтах** и **Разрешить файлы cookie на этих сайтах только для одного сеанса** не должно быть конфликтов. Если URL не указан и установлен флажок **Задать настройки файлов cookie по умолчанию**, опция, выбранная в раскрывающемся списке, будет применяться для всех сайтов.

- **Разрешить файлы cookie на этих сайтах**

  Список сайтов, которым разрешено задавать настройки файлов cookie. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Блокировать файлы cookie на этих сайтах**

  Список сайтов, которым запрещено задавать настройки файлов cookie. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Разрешить файлы cookie на этих сайтах только для одного сеанса**

  Список сайтов, которым разрешено сохранять файлы cookie только для одного сеанса. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Задать настройки JavaScript по умолчанию**

  Настройки JavaScript по умолчанию.

Если флажок установлен, будет применяться одна из следующих опций, и пользователь не сможет ее изменить:

- **Разрешить всем сайтам запускать JavaScript** (по умолчанию)
- **Запретить всем сайтам запускать JavaScript**

  Если флажок снят, будут применяться персональные настройки пользователя.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок снят.

  Если параметры **Разрешить JavaScript на этих сайтах** и **Блокировать JavaScript на этих сайтах** не определены и установлен флажок **Задать настройки JavaScript по умолчанию**, выбранная опция будет применяться ко всем сайтам.

- **Разрешить JavaScript на этих сайтах**

  Список сайтов, которым разрешено запускать JavaScript. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  Если параметры **Разрешить JavaScript на этих сайтах** и **Блокировать JavaScript на этих сайтах** не определены и установлен флажок **Задать настройки JavaScript по умолчанию**, выбранная опция будет применяться ко всем сайтам.

- **Блокировать JavaScript на этих сайтах**

  Список сайтов, которым запрещено запускать JavaScript. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  Если параметры **Разрешить JavaScript на этих сайтах** и **Блокировать JavaScript на этих сайтах** не определены и установлен флажок **Задать настройки JavaScript по умолчанию**, выбранная опция будет применяться ко всем сайтам.

- **Задать настройки всплывающих окон по умолчанию**

  Настройка всплывающих окон по умолчанию.

  Если флажок установлен, для всплывающих окон применяется одна из следующих опций:

  - **Разрешить всем сайтам показывать всплывающие окна**. Позволяет всем сайтам открывать всплывающие окна. Это значение выбрано по умолчанию.
  - **Запретить всем сайтам показывать всплывающие окна**. Запрещает всем сайтам открывать всплывающие окна.

    Если флажок снят, всплывающие окна блокируются, но пользователь может изменить это в Настройках.

    Этот параметр поддерживается в Google Chrome версии 33 или выше.

    По умолчанию флажок снят.

Если параметры **Разрешить всплывающие окна на этих сайтах** и **Блокировать всплывающие окна на этих сайтах** не определены и установлен флажок **Задать настройки всплывающих окон по умолчанию**, выбранная опция будет применяться ко всем сайтам.

- **Разрешить всплывающие окна на этих сайтах**

  Список сайтов, которым разрешено показывать всплывающие окна. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 34 или выше.

  Если параметры **Разрешить всплывающие окна на этих сайтах** и **Блокировать всплывающие окна на этих сайтах** не определены и установлен флажок **Задать настройки всплывающих окон по умолчанию**, выбранная опция будет применяться ко всем сайтам.

- **Блокировать всплывающие окна на этих сайтах**

  Список сайтов, которым запрещено показывать всплывающие окна. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 34 или выше.

  Если параметры **Разрешить всплывающие окна на этих сайтах** и **Блокировать всплывающие окна на этих сайтах** не определены и установлен флажок **Задать настройки всплывающих окон по умолчанию**, выбранная опция будет применяться ко всем сайтам.

- **Задать настройки отслеживания местоположения пользователей**

  Настройки местоположения по умолчанию.

  Если флажок установлен, по умолчанию ко всем сайтам будет применяться одна из следующих опций:

  - **Разрешить всем сайтам отслеживать местоположение**
  - **Запретить всем сайтам отслеживать местоположение**
  - **Спрашивать, если сайт пытается отследить местоположение пользователя** (по умолчанию)

    Если флажок снят, будут применяться персональные настройки пользователя.

    Этот параметр поддерживается в Google Chrome версии 30 или выше.

    По умолчанию флажок снят.

Управление настройками прокси

На вкладке **Прокси** в разделе **Настройки Google Chrome** вы можете задать следующие настройки прокси:

- **Задать настройки прокси**

  Настройки прокси для Google Chrome и ARC-приложений.

Если флажок установлен, будет применяться одна из следующих опций, и пользователь не сможет изменить настройки прокси:

- **Никогда не использовать прокси**. Запрещает использование прокси, все остальные настройки прокси игнорируются. Этот параметр выбран по умолчанию.
- **Определять настройки прокси автоматически**. Определяет настройки прокси автоматически, все остальные опции игнорируются.
- **Использовать PAC-файл**. Использует PAC-файл прокси, указанный в поле **URL PAC-файла**.
- **Использовать фиксированные прокси-серверы**. Использует данные, указанные в полях **URL прокси-сервера** и **Список исключений**.
- **Использовать системные настройки прокси**. Использует системные настройки прокси.

  Если флажок снят, будут применяться персональные настройки пользователя.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок установлен.

- **URL прокси-сервера**

  URL прокси-сервера.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **URL PAC-файла**

  URL PAC-файла прокси.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Список исключений**

  Список хостов, для которых прокси будет игнорироваться.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

Управление настройками поиска

На вкладке **Поиск** в разделе **Настройки Google Chrome** вы можете задать следующие настройки поиска:

- **Разрешить быстрый поиск**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства использовать быстрый поиск, включать и выключать его.

  Этот параметр поддерживается в Google Chrome версии 40 или выше.

  По умолчанию флажок установлен.

- **Включить поисковую систему по умолчанию**

  Настройки поисковой системы по умолчанию.

  Если флажок установлен и пользователь вводит в адресную строку текст, не являющийся веб-адресом, используется поисковая система по умолчанию. Поисковая система по умолчанию зависит от настроек поисковой системы, расположенных под этим флажком:

  - Если в настройках поисковой системы оставить пустое значение, пользователь устройства сможет выбрать поисковую систему в настройках браузера.
  - Если задать настройки поисковой системы по умолчанию, всегда будет использоваться эта поисковая система, и пользователь устройства не сможет выбрать поисковую систему в браузере.

  По умолчанию флажок установлен, но настройки поисковой системы по умолчанию не заданы.

  > Если вы хотите выключить поиск в Google Chrome, мы рекомендуем оставить флажок **Включить поисковую систему по умолчанию** установленным и указать в параметре **Название поисковой системы** сайт, не являющийся поисковой системой. В некоторых версиях Google Chrome при снятии флажка в работе Google Chrome могут наблюдаться проблемы.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  Параметры поисковой системы по умолчанию:

  - **Название поисковой системы**
  - **Ключевое слово**
  - **URL поиска**
  - **URL запроса подсказок**
  - **URL значка**
  - **Кодировки**
  - **Дополнительные URL**
  - **URL изображений**
  - **URL страницы быстрого доступа**
  - **Параметры для запросов POST к URL-адресу для поиска**
  - **Параметры для запросов POST к URL-адресу для поиска предложений**
  - **Параметры для запросов POST к URL-адресу для поиска изображений**

- **Название поисковой системы**

  Имя поисковой системы по умолчанию.

Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Ключевое слово**

  Ключевое слово или ярлык, используемые в адресной строке для запуска поиска в поисковой системе.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **URL поиска**

  URL поисковой системы, используемой во время поиска по умолчанию.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **URL запроса подсказок**

  URL поисковой системы, предоставляющей поисковые подсказки.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **URL значка**

  URL значка поисковой системы по умолчанию.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Кодировки**

  Кодировки символов, поддерживаемые поисковой системой. Поддерживаемыми кодировками являются:

  - UTF-8
  - UTF-16
  - GB2312
  - ISO-8859-1

    Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Дополнительные URL**

  Список дополнительных URL для извлечения поисковых запросов из поисковой системы.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **URL изображений**

  URL поисковой системы, используемый для поиска изображений.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **URL страницы быстрого доступа**

  URL поисковой системы, используемый для открытия страницы быстрого доступа.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Параметры для запросов POST к URL-адресу для поиска**

  Параметры URL, используемые при поиске по URL-адресу методом POST. Параметры представляют собой разделенные запятыми пары ключ-значение. Если значением является параметр шаблона, например, '{searchTerms}', он заменяется фактическими поисковыми запросами. Например:

  q={searchTerms},ie=utf-8,oe=utf-8

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Параметры для запросов POST к URL-адресу для поиска предложений**

  Параметры URL для поисковых подсказок при использовании запросов методом POST. Параметры представляют собой разделенные запятыми пары ключ-значение. Если значением является параметр шаблона, например, '{searchTerms}', он заменяется фактическими поисковыми запросами. Например:

  q={searchTerms},ie=utf-8,oe=utf-8

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

- **Параметры для запросов POST к URL-адресу для поиска изображений**

  Параметры URL для поиска изображений при использовании запросов методом POST. Параметры представляют собой разделенные запятыми пары ключ-значение. Если значением является параметр шаблона, например, '{imageThumbnail}', он заменяется фактической миниатюрой изображения. Например:

  content={imageThumbnail},url={imageURL},sbisrc={SearchSource}

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

Управление настройками паролей

На вкладке **Пароли** в разделе **Настройки Google Chrome** вы можете задать следующие настройки паролей:

- **Включить сохранение паролей**

  Установка или снятие флажка определяет, будет ли Google Chrome запоминать пароли, вводимые пользователем, и предлагать их при следующем входе.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок установлен.

Управление настройками страниц

На вкладке **Страницы** в разделе **Настройки Google Chrome** вы можете задать следующие настройки страниц:

- **Включить дополнительные страницы с сообщениями об ошибках**

  Установка или снятие флажка определяет, разрешено ли Google Chrome использовать встроенные страницы с сообщениями об ошибках, такие как "Страница не найдена".

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок установлен.

- **Включить автозаполнение адресов**

  Настройки автозаполнения адресов.

  Если флажок установлен, пользователю устройства разрешено управлять автозаполнением адресов через интерфейс.

  Если флажок снят, автозаполнение не используется, а также не сохраняется дополнительная информация об адресах, вводимых пользователем во время работы в интернете.

  Этот параметр поддерживается в Google Chrome версии 69 или выше.

  По умолчанию флажок установлен.

- **Включить автозаполнение данных кредитных карт**

  Настройки автозаполнения данных кредитных карт.

  Если флажок установлен, пользователю устройства разрешено управлять предложениями автозаполнения для кредитных карт через интерфейс.

  Если флажок снят, автозаполнение не используется, а также не сохраняется дополнительная информация о кредитных картах, которую может вводить пользователь во время работы в интернете.

  Этот параметр поддерживается в Google Chrome версии 63 или выше.

  По умолчанию флажок установлен.

Управление другими настройками

На вкладке **Другое** в разделе **Настройки Google Chrome** вы можете задать следующие настройки:

- **Включить печать**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства производить печать в Google Chrome.

  Этот параметр поддерживается в Google Chrome версии 39 или выше.

  По умолчанию флажок установлен.

- **Задать настройки Безопасного просмотра Google**

  Уровень защиты Безопасного просмотра Google.

  Если флажок установлен, пользователю устройства разрешено управлять настройками Безопасного просмотра Google в Google Chrome и выбирать уровень защиты. Уровни защиты:

  - **Безопасный просмотр Google всегда отключен**. Полностью отключает Безопасный просмотр Google.
  - **Безопасный просмотр Google всегда включен в режиме стандартной защиты.** Безопасный просмотр Google будет всегда включен в режиме стандартной защиты. Этот параметр выбран по умолчанию.
  - **Безопасный просмотр Google всегда включен в режиме улучшенной защиты**. Безопасный просмотр Google будет всегда включен в режиме улучшенной защиты, но данные о работе пользователя устройства в интернете будут отправляться в Google.

    Если флажок снят, Безопасный просмотр Google будет работать в режиме стандартной защиты, и пользователю устройства будет разрешено изменять настройки Безопасного просмотра Google.

    Этот параметр поддерживается в Google Chrome версии 87 или выше.

    По умолчанию флажок установлен.

- **Отключить сохранение истории браузера**

  Установка или снятие флажка определяет, сохраняется ли история браузера и выполняется ли синхронизация вкладок.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок снят.

- **Отключить переход со страницы предупреждения Безопасного просмотра Google**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства переходить на опасные сайты со страниц предупреждений Безопасного просмотра Google, например, о вредоносном ПО или фишинге. Ограничение неприменимо для проблем, связанных с SSL-сертификатом, таких как недействительные сертификаты или сертификаты с истекшим сроком действия.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок снят.

- **Включить предварительное определение сети**

  Установка или снятие флажка определяет, будет ли Google Chrome предварительно определять такие действия в сети, как предзагрузка DNS, предварительное подключение по протоколам TCP и SSL, а также предварительная визуализация веб-страниц.

  Если флажок снят, предварительное определение сети отключено, но пользователь устройства может включить его.

  Этот параметр поддерживается в Google Chrome версии 38 или выше.

  По умолчанию флажок снят.

- **Включить принудительное использование Безопасного поиска Google**

  Установка или снятие флажка определяет, будет ли применяться Безопасный поиск Google для запросов в Google Поиске.

  Этот параметр поддерживается в Google Chrome версии 41 или выше.

  По умолчанию флажок снят.

- **Настроить Безопасный режим для YouTube**

  Минимальный требуемый уровень Безопасного режима для YouTube.

  Если флажок установлен, определяется минимальный требуемый уровень Безопасного режима для YouTube, и пользователь устройства не может выбрать менее безопасный режим. Уровни Безопасного режима:

  - **Отключить обязательное использование Безопасного режима**. Определяет, отключено ли обязательное использование Безопасного режима в Google Chrome. Тем не менее, Безопасный режим может обязательно применяться в соответствии с внешними политиками. Этот параметр выбран по умолчанию.

  - **Включить обязательное использование хотя бы Умеренного безопасного режима**. Позволяет пользователю устройства включить Умеренный и Строгий безопасный режим на YouTube, но запрещает отключение Безопасного режима.

  - **Включить обязательное использование Строгого безопасного режима**. Включает постоянное использование Строгого безопасного режима на YouTube.

    Если флажок снят, Google Chrome не требует использовать Безопасный режим для YouTube, но Безопасный режим может принудительно включаться на основании внешних правил, таких как правила YouTube.

    Этот параметр поддерживается в Google Chrome версии 55 или выше.

    По умолчанию флажок установлен.

- **Настроить доступность режима инкогнито**

  Доступность режима инкогнито в Google Chrome.

  Если флажок установлен, администратор может определять, разрешено ли пользователю устройства открывать страницы в режиме инкогнито, выбрав одну из следующих опций:

  - **Режим инкогнито доступен** (по умолчанию)

  - **Режим инкогнито отключен**

    Если флажок снят, пользователь устройства не может открывать страницы в режиме инкогнито в Google Chrome.

    Этот параметр поддерживается в Google Chrome версии 30 или выше.

    По умолчанию флажок установлен.

- **Включить поисковые подсказки**

  Установка или снятие флажка определяет, включены ли поисковые подсказки в адресной строке Google Chrome.

Этот параметр поддерживается в Google Chrome версии 30 или выше.

По умолчанию флажок установлен.

- **Задать настройки Переводчика**

  Включение функций перевода.

  Если флажок установлен, администратор может выбирать следующие опции для перевода:

  - **Всегда предлагать перевод**. Отображает интегрированную панель переводческих инструментов и пункт с командой на перевод в контекстном меню, которое открывается при нажатии правой кнопки мыши. Этот параметр выбран по умолчанию.
  - **Никогда не предлагать перевод**. Отключает все встроенные функции перевода.

    Если флажок снят, будут применяться персональные настройки пользователя.

    Этот параметр поддерживается в Google Chrome версии 30 или выше.

    По умолчанию флажок снят.

- **Включить возможность изменения закладок**

  Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять, удалять или изменять закладки.

  Этот параметр поддерживается в Google Chrome версии 30 или выше.

  По умолчанию флажок установлен.

- **Управляемые закладки**

  Список закладок, управляемых администратором. Список является словарем с ключами "name" и "url". То есть ключ содержит имя и адрес закладки. Вы можете настроить подпапку с ключом "children", в которой также содержится список закладок.

  По умолчанию папка с управляемыми закладками называется "Управляемые закладки". Вы можете изменить ее, добавив новый дополнительный словарь. Для этого укажите ключ "toplevel_name" с желаемым именем папки в качестве значения.

  Если вы укажете неполный URL в качестве адреса сайта для закладки, Google Chrome заменит его на URL так же, как при его вводе в адресной строке. Например, "kaspersky.ru" преобразуется в "https://www.kaspersky.ru".

  Например:

```
"ManagedBookmarks": [{
 //Изменяет имя папки по умолчанию
 "toplevel_name": "My managed bookmarks folder"
 },
 {
 //Добавляет закладку в папку с управляемыми закладками
 "name": "Kaspersky",
 "url": "kaspersky.com"
 },
 {
 "name": "Kaspersky products",
 "children": [{
 "name": "Kaspersky Endpoint Security",
 "url": "kaspersky.com/enterprise-security/endpoint"
```

```
 },
 {
 "name": "Kaspersky Security для почтовых серверов",
 "url": "kaspersky.com/enterprise-security/mail-server-security"
 }
 ]
 }
]
```

Этот параметр поддерживается в Google Chrome версии 37 или выше.

- **Заблокировать доступ к этим URL**

  Список запрещенных URL. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 86 или выше.

- **Разрешить доступ к этим URL (исключения для блокировки URL)**

  Список URL, которые являются исключениями из списка, указанного в пункте **Заблокировать доступ к этим URL**. Также вы можете задавать шаблоны URL, например: [*.]example.com.

  Этот параметр поддерживается в Google Chrome версии 86 или выше.

- **Задать минимально допустимую версию SSL**

  Минимально допустимая версия SSL.

  Если флажок установлен, Google Chrome не будет использовать SSL и TLS более ранних версий, чем выбранная. Доступные версии:

  - **TLS 1.0** (по умолчанию)
  - **TLS 1.1**
  - **TLS 1.2**

    Если флажок снят, Google Chrome будет сообщать об ошибке для протоколов TLS 1.0 и TLS 1.1, но у пользователя устройства будет возможность их проигнорировать.

    Этот параметр поддерживается в Google Chrome версии 66 или выше.

    По умолчанию флажок снят.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка режима киоска

Режим киоска это функция Kaspersky Endpoint Security для Android, которая позволяет ограничить набор приложений, доступных пользователю устройства, одним или несколькими приложениями. Также вы можете эффективно управлять некоторыми настройками устройства.

Настройки режима киоска применимы для устройств, управляемых через Kaspersky Endpoint Security для Android в режиме device owner.

Типы режима киоска

В Kaspersky Endpoint Security доступны следующие типы режима киоска:

- Режим одного приложения - режим киоска только с одним приложением. В этом режиме пользователю устройства разрешено открывать на устройстве только одно приложение, которое указано в настройках режима киоска.

  Если приложение, которое вы хотите добавить в режим киоска, не установлено на устройстве, режим киоска включается после установки этого приложения.

  На устройствах с Android версии 9.0 и выше для запуска приложение должно поддерживать функцию режима киоска и самостоятельно вызывать метод startLockTask().

  На устройствах с Android версии 9.0 или ниже приложение запускается напрямую в режиме киоска.

- Режим с несколькими приложениями - режим киоска, в котором доступно несколько приложений. В этом режиме пользователю устройства разрешено открывать на устройстве несколько приложений, которые указаны в настройках режима киоска.

Предварительная настройка

Предварительная настройка для режима киоска включает в себя следующие шаги:

- Перед тем, как указать приложения, которые разрешено запускать на устройстве в режиме киоска, сначала необходимо добавить эти приложения в **Контроль приложений** > **Список категорий и приложений** и отметить их как обязательные приложения. Затем они появятся в списке **Пакет приложения** режима киоска.

  > Недавно добавленные обязательные приложения могут не отображаться в списке **Пакет приложения**. Чтобы просмотреть все добавленные приложения и выбрать приложение для работы в режиме одного приложения, необходимо сохранить и закрыть политику, а затем открыть ее снова. Все добавленные приложения появятся в списке.

- Перед включением режима киоска рекомендуем запретить запуск Google Assistant, включив соответствующее ограничение в **Политика > Режим device owner > Ограничения функций > Приложения > Запретить использование Google Assistant**. В противном случае Google Assistant запустится в режиме киоска и позволяет открывать недоверенные приложения.

Переход в настройки режима киоска

Чтобы открыть настройки режима киоска:

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 **Режим device owner** > **Режим киоска**.

Настройка режима одного приложения

Чтобы настроить режим одного приложения:

1. В раскрывающемся списке **Режим киоска** выберите **Режим одного приложения**.
2. В раскрывающемся списке **Пакет приложения** выберите пакет приложения с приложением, которое разрешено запускать на устройстве.
3. Укажите любые необходимые ограничения. С доступными ограничениями можно ознакомиться в пункте **Ограничения режима киоска** ниже.
4. Установите флажок **Доверенные приложения**, если хотите добавить дополнительные приложения, разрешенные на устройстве. Чтобы узнать, как это сделать, ознакомьтесь с пунктом **Добавление доверенных приложений** ниже.
5. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Настройка режима с несколькими приложениями

Чтобы настроить режим с несколькими приложениями:

1. В раскрывающемся списке **Режим киоска** выберите **Режим с несколькими приложениями**.
2. Нажмите **Добавить**, выберите приложения, которые разрешено запускать на устройстве и нажмите **ОК**.
3. Укажите любые необходимые ограничения. С доступными ограничениями можно ознакомиться в пункте **Ограничения режима киоска** ниже.
4. Установите флажок **Разрешить переход в доверенные приложения**, если хотите добавить дополнительные приложения, разрешенные на устройстве. Чтобы узнать, как это сделать, ознакомьтесь с пунктом **Добавление доверенных приложений** ниже.
5. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Ограничения режима киоска

В режиме киоска вы можете установить следующие ограничения:

- **Запретить кнопку Обзор (Android версии 9.0 или выше)**

  Установка или снятие флажка определяет, будет ли скрыта кнопка Обзор. Ограничение поддерживается на устройствах с Android версии 9.0 и выше.

  По умолчанию флажок установлен.

- **Запретить кнопку Главный экран (Android версии 9.0 или выше)**

  Установка или снятие флажка определяет, будет ли скрыта кнопка Главный экран. Ограничение поддерживается на устройствах с Android версии 9.0 и выше.

  По умолчанию флажок установлен.

- **Запретить строку состояния (Android версии 9.0 или выше)**

  Установка или снятие флажка определяет, отображаются ли в строке состояния уведомления и индикаторы, такие как сеть, батарея, звук и вибрация. Ограничение поддерживается на устройствах с Android версии 9.0 и выше.

  По умолчанию флажок установлен.

- **Запретить показ системных уведомлений (Android версии 9.0 или выше)**

  Установка или снятие флажка определяет, будут ли скрыты системные уведомления. Ограничение поддерживается на устройствах с Android версии 9.0 и выше.

  По умолчанию флажок установлен.

- **Добавить Kaspersky Endpoint Security для Android как доверенное приложение**

  Установка или снятие флажка определяет, будет ли приложение Kaspersky Endpoint Security для Android добавлено в список доверенных приложений. Эта опция доступна, если установлен флажок **Разрешить переход в доверенные приложения**.

  По умолчанию флажок установлен.

Добавление доверенных приложений

Помимо настройки устройства для работы с одним или несколькими приложениями, вы также можете добавить доверенные приложения, в которые разрешено переходить пользователю устройства. Для этого в разделе **Режим киоска**:

1. Установите флажок **Разрешить переход в доверенные приложения**. Откроется список **Доверенные приложения**.
2. Нажмите **Добавить**, выберите необходимое имя пакета приложения и нажмите **OK**.
3. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Управление Exchange ActiveSync для Gmail

Вы можете управлять настройками Exchange ActiveSync для Gmail в режиме device owner.

*Чтобы открыть раздел **Exchange ActiveSync**:*

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 **Режим device owner** > **Exchange ActiveSync**.
5. Укажите следующие параметры:

   - **Адрес сервера Exchange ActiveSync**

     URL почтового сервера Exchange ActiveSync. Перед URL не обязательно использовать HTTP:// или HTTPS://.

   - **Принудительно использовать SSL**

     Установка или снятие флажка определяет, будет ли использоваться связь по протоколу SSL с портом сервера, который вы указали в поле **Адрес сервера Exchange ActiveSync**.

     По умолчанию флажок установлен.

   - **Отключить проверку SSL-сертификатов**

     Установка или снятие флажка определяет, будут ли осуществляться проверки SSL-сертификатов, используемых на серверах Exchange ActiveSync. Проверка полезна, если сертификаты являются самозаверенными.

     По умолчанию флажок снят.

   - **Разрешить неуправляемые учетные записи**

     Установка или снятие флажка определяет, разрешено ли пользователю устройства добавлять другие учетные записи в Gmail.

     По умолчанию флажок установлен.

- **Тип аутентификации**

  Тип аутентификации, используемый для проверки учетных данных почты пользователя устройства. Возможные значения:

  - **Современная аутентификация на основе токенов**. Использует метод аутентификации на основе токенов. Это значение выбрано по умолчанию.
  - **Базовая аутентификация**. Запрашивает у пользователя пароль и сохраняет его для использования в будущем.

- **Идентификатор устройства**

  Строка, используемая прокси Kaspersky Security Center или сторонним шлюзом для идентификации устройства и его подключения к Exchange ActiveSync. Вы можете ввести значение или выбрать его в раскрывающемся списке **Доступные макросы**.

- **Имя пользователя**

  Имя пользователя, которое будет использоваться для получения имени пользователя из Microsoft Active Directory. Оно может отличаться от адреса электронной почты пользователя. Вы можете ввести значение или выбрать его в раскрывающемся списке **Доступные макросы**.

- **адрес электронной почты;**

  Адрес электронной почты, который будет использоваться для получения адреса электронной почты пользователя из Microsoft Active Directory. Вы можете ввести значение или выбрать его в раскрывающемся списке **Доступные макросы**.

- **Доступные макросы**

  Макрос, который будет использоваться для замены значений в соответствующих полях. Возможные значения:

  - **%email%**. Определяет электронную почту пользователя, на которого зарегистрировано устройство. Значение может быть получено из мобильного сертификата.
  - **%email_domain%**. Определяет домен электронной почты пользователя, на которого зарегистрировано устройство. Значение может быть получено из мобильного сертификата.
  - **%email_user_name%**. Определяет имя пользователя из адреса электронной почты, на который зарегистрировано устройство. Значение может быть получено из мобильного сертификата.
  - **%user_name%**. Определяет имя пользователя, под которым зарегистрировано устройство. Значение может быть получено из мобильного сертификата.
  - **%device_id%**. Определяет идентификатор устройства.
  - **%group_id%**. Определяет идентификатор группы администрирования, в которую входит устройство.
  - **%device_platform%**. Определяет платформу устройства.

- **%device_model%**. Определяет модель устройства.
- **%os_version%**. Определяет версию операционной системы на устройстве.

- **Сертификат пользователя**

  Псевдоним строки, который представляет сертификат с закрытым ключом. Сертификатом может быть сертификат пользователя для аутентификации на серверах Exchange ActiveSync.

- **Интервал синхронизации по умолчанию**

  Используемый по умолчанию интервал синхронизации элементов почты на серверах Exchange ActiveSync с Gmail. Возможные значения:

  - 1 день
  - 3 дня
  - 1 неделя (по умолчанию)
  - 2 недели
  - 1 месяц

- **Подпись для электронной почты по умолчанию**

  Подпись для электронной почты по умолчанию, которая автоматически добавляется в конце электронных писем.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Подключение к NDES/SCEP-серверу

Вы можете настроить подключение к NDES/SCEP-серверу, чтобы получить сертификат от центра сертификации (CA) с помощью простого протокола регистрации сертификатов (SCEP). Для этого необходимо настроить подключение к центру сертификации (CA) с помощью SCEP и указать профиль сертификата.

Чтобы добавить подключение к центру сертификации и указать профиль сертификата:

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 **Режим device owner > NDES и SCEP**.

5. В разделе **Подключение к центру сертификации (CA)** нажмите **Добавить**.

   Откроется диалоговое окно **Подключение к центру сертификации**.

6. Укажите следующие параметры и нажмите **OK**:

   - **Имя соединения**

     Уникальное имя соединения.

   - **Тип протокола**

     Версия протокола. Возможные значения:

     - SCEP
     - NDES (по умолчанию)

   - **Веб-адрес SCEP-сервера**

     Веб-адрес SCEP-сервера.

     Веб-адрес для NDES имеет формат `http://<ServerName>/certsrv/mscep/mscep.dll`.

   - **Тип контрольной фразы**

     Тип контрольной фразы, необходимой для аутентификации. Возможные значения:

     - **Нет** - данные для аутентификации не требуются.
     - **Статическая** - требуется ввести фразу для аутентификации в поле **Статическая контрольная фраза**. Это значение установлено по умолчанию.

   - **Статическая контрольная фраза**

     Определяет фразу для аутентификации, которая используется при аутентификации устройства с помощью сертификата с веб-адресом SCEP-сервера.

7. В разделе **Профили сертификата** нажмите **Добавить**.

   Откроется диалоговое окно **Профиль сертификата**.

8. Укажите следующие параметры профиля сертификата и нажмите **OK**:

- **Имя профиля**

  Уникальное имя профиля сертификата.

- **Центр сертификации (CA)**

  Центр сертификации, который вы создали в блоке **Подключение к центру сертификации (CA)**.

- **Имя субъекта**

  Уникальный идентификатор, являющийся субъектом сертификата. Содержит информацию о сертификации, такую как, например, общее имя, организация, подразделение, код страны. Вы можете ввести значение или выбрать его в раскрывающемся списке **Доступные макросы**.

- **Длина личного ключа**

  Длина личного ключа сертификата. Возможные значения:

  - 1024
  - 2048 (по умолчанию)
  - 4096

- **Тип личного ключа**

  Тип личного ключа сертификата. Возможные значения:

  - Подпись (по умолчанию)
  - Шифрование
  - Подпись и шифрование

- **Альтернативное имя субъекта (SAN)**

  Альтернативное имя, которое представляет имя субъекта сертификата. Вы можете указать несколько альтернативных имен субъекта. Для этого нажмите **Добавить** и задайте параметры **Тип SAN** и **Значение SAN**.

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

Управление подключениями и профилями сертификата

Впоследствии вы можете изменять или удалять добавленные подключения и профили сертификата.

Чтобы изменить подключение или профиль сертификата:

1. Выберите необходимое подключение или профиль сертификата в соответствующем разделе.
2. Нажмите **Изменить**, внесите необходимые изменения и нажмите **ОК**.
3. Нажмите **Применить**, чтобы сохранить внесенные изменения.

Чтобы удалить подключение или профиль сертификата:

1. Выберите необходимое подключение или профиль сертификата в соответствующем разделе.
2. Нажмите **Удалить**, а затем **ОК**.

   Примечание. Если удалить соединение с центром сертификации, все профили сертификатов, которые используют это соединение, также будут удалены.

3. Нажмите **Применить**, чтобы сохранить внесенные изменения.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Команды для мобильных устройств

Kaspersky Security Center поддерживает команды для удаленного управления мобильными устройствами. Например, в случае потери или кражи мобильного устройства вы можете отправить команды, чтобы определить местоположение устройства или удалить корпоративные данные с устройства.

Вы можете отправлять команды на следующие типы управляемых мобильных устройств:

- Android-устройства, управляемые через приложение Kaspersky Endpoint Security для Android;
- iOS MDM-устройства.

Каждый тип устройств поддерживает свой набор команд. Информация об отправке команд из Консоли администрирования приведена в справке Kaspersky Security Center.

Команды для Android-устройств

Команды	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано.
Разблокировать	На устройствах под управлением операционной системы Android версии 5.0 – 6.X после разблокировки мобильного устройства пароль разблокировки экрана будет заменен на "1234". На устройствах под управлением операционной системы Android 7.0 и выше после разблокировки мобильного устройства пароль разблокировки экрана останется прежним.
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.

Удалить корпоративные данные	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.
Синхронизировать устройство	Данные с мобильного устройства синхронизированы с Сервером администрирования.
Определить местоположение устройства	Получены координаты местоположения мобильного устройства на карте. На устройствах с операционной системой Android 12 и выше, если пользователю предоставлено разрешение "Использовать приблизительное местоположение", Kaspersky Endpoint Security для Android сначала пытается определить точное местоположение устройства. Если это не удалось, определяется приблизительное местоположение устройства, но только в том случае, если данные о нем были получены не более 30 минут назад. В противном случае команда **Определить местоположение устройства** завершится с ошибкой.
Сфотографировать	Мобильное устройство заблокировано. Фотография выполнена фронтальной камерой устройства при попытке разблокировать устройство. На устройствах с выдвижной фронтальной камерой фотография будет черной, если камера закрыта. При попытке разблокировки устройства пользователь автоматически соглашается на фотографирование. Если разрешение на использование камеры было отозвано, на мобильном устройстве отображается уведомление, предлагающее предоставить это разрешение. Если разрешение на использование камеры было отозвано из панели быстрых настроек на мобильном устройстве под управлением Android 12 или более поздней версии, уведомление не отображается, но сделанная фотография будет черной.
Воспроизвести звуковой сигнал	Мобильное устройство воспроизводит звуковой сигнал. Звуковой сигнал воспроизводится 5 мин (при низком уровне заряда батареи – 1 мин).

Команды для iOS MDM-устройств

Команды	Результат выполнения команды
Заблокировать	Мобильное устройство заблокировано.
Сбросить пароль	Сброшен пароль для разблокировки экрана мобильного устройства, пользователю предложено установить новый пароль в соответствии с требованиями политики.
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.
Удалить корпоративные данные	Будут удалены все установленные конфигурационные профили, provisioning-профили, iOS MDM-профиль и приложения, для которых был установлен флажок **Удалять вместе с iOS MDM-профилем**.
Синхронизировать устройство	Данные с мобильного устройства синхронизированы с Сервером администрирования.
Установить профиль	Конфигурационный профиль установлен на мобильном устройстве.
Удалить профиль	Конфигурационный профиль удален с мобильного устройства.
Установить provisioning-профиль	Provisioning-профиль установлен на мобильном устройстве.
Удалить provisioning-профиль	Provisioning-профиль удален с мобильного устройства.
Установить приложение	Приложение установлено на мобильном устройстве.
Удалить приложение	Приложение удалено с мобильного устройства.
Ввести код погашения	Введен код погашения для платного приложения.

Команды	Результат выполнения команды
Запланировать обновление ОС	На мобильном устройстве запланированы обновления операционной системы в соответствии с указанными настройками обновлений. Эта команда поддерживается только на устройствах в режиме supervised.
Настроить параметры роуминга	Включение или выключение роуминга данных или роуминга голосовой связи.
Настроить Bluetooth	Включение или выключение Bluetooth на мобильном устройстве. Эта команда поддерживается только на устройствах в режиме supervised, работающих под управлением iOS 11.3 и выше.

Разрешения для выполнения команд

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 Анти-Вора 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

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 посещения 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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".

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 мобильный 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 правил 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.

В SOTI MobiControl вы можете использовать макрос %DEVICENAME% в поле `KscDeviceName`. Этот макрос позволяет автоматически получать имя устройства из консоли SOTI MobiControl в Kaspersky Security Center.

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** (Блокировка устройства);
- **Управление устройством** (Блокировка экрана);
- **Контроль приложений** (Блокировка запрещенных приложений);
- **Рабочий профиль Android;**
- **Управление Samsung KNOX.**

Способ развертывания рабочего профиля не позволяет применить параметры групповой политики из раздела **Рабочий профиль Android**. Эти параметры можно применить, только если рабочий профиль создан с помощью Kaspersky Security Center.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Файл AppConfig

Конфигурационный файл создается для настройки приложения в EMM-консоли. Параметры приложения в конфигурационном файле приведены в следующей таблице.

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`LicenseActivationCode`	Код активации приложения	String	Код активации приложения из 20 латинских букв и цифр. Чтобы активировать приложение с помощью кода активации, требуется доступ в интернет для подключения к серверам активации "Лаборатории Касперского". Если оставить поле пустым, приложение будет активировано по пробной лицензии. Пробная лицензия 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 нужно приобрести коммерческую лицензию.	
`EulaAcceptanceConfirmationV1`	<Ссылка на Лицензионное соглашение>	Choice	Этот параметр доступен только для VMware AirWatch. `Accepted` – я подтверждаю, что полностью прочитал(а), понимаю и принимаю положения и условия настоящего Лицензионного соглашения `Declined` – я не принимаю условия и положения настоящего Лицензионного соглашения. Чтобы принять условия и положения Лицензионного соглашения для всех мобильных устройств, необходим доступ в интернет для подключения к серверам "Лаборатории Касперского". Если вы выберете вариант `Declined`, приложение предложит пользователю принять условия и положения Лицензионного соглашения. Пользователи мобильных устройств могут принять эти условия в мастере первоначальной настройки.	
`EulaAcceptanceCodeV1`	Код Лицензионного соглашения	String	Эти параметры доступны только для VMware AirWatch. Используйте `EulaAcceptanceCodeV1`, чтобы принять одно лицензионное соглашение. Используйте `EulaAcceptanceCodesV2`, чтобы одновременно принять несколько лицензионных соглашений. Поле `EulaAcceptanceCodesV2` должно содержать список кодов EULA, разделенных точкой с запятой: "`<EULAid1>;<EULAid2>;<EULAid3>;...`". Код Лицензионного соглашения содержится в Лицензионном соглашении.	

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`EulaAcceptanceCodesV2`	Коды Лицензионных соглашений	String	*Чтобы просмотреть код Лицензионного соглашения, выполните следующие действия:* 1. Скопируйте ссылку на Лицензионное соглашение (`EulaAcceptanceConfirmationV1`) 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 Лицензионных соглашений для всех мобильных устройств, необходим доступ в интернет для подключения к серверам "Лаборатории Касперского". Если вы не заполните эти поля, приложение предложит пользователю принять условия и положения Лицензионных соглашений. Пользователь мобильного устройства может принять эти условия в мастере первоначальной настройки.	
`KscServer`	Адрес и порт Сервера администрирования Kaspersky Security Center	String	DNS-имя или IP-адрес Сервера администрирования Kaspersky Security Center и номер порта. Введите адрес следующим образом: `<адрес сервера>:<порт>`. Если вы ввели адрес сервера без указания порта, приложение использует порт по умолчанию 13292. Если вы укажете значения в обоих полях, будут приняты условия всех указанных в них лицензионных соглашений.	`<адрес сервера>:13292`
`DisableNotification`	Выключить уведомления приложения до подключения к Kaspersky Security Center	Boolean	`True` – Kaspersky Endpoint Security для Android скрывает все уведомления о работе приложения. Приложение Kaspersky Endpoint Security для Android скрывает уведомления до подключения устройства к Kaspersky Security Center. 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. Иначе пользователь может не получить уведомление об истечении срока действия лицензии. В этом случае приложение перестанет функционировать. `False` – Kaspersky Endpoint Security для Android показывает все уведомления о работе приложения.	`False`

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`ScanScheduleType`	Режим запуска проверки	Choice	`AfterUpdate` – запуск антивирусной проверки после обновления баз. Приложение обновляет антивирусные базы по сформированному расписанию (`UpdateScheduleType`). `Daily` – запуск антивирусной проверки раз в день. Настройте время запуска проверки (`ScanScheduleTime`). `Weekly` – запуск антивирусной проверки раз в неделю. Выберите день 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.	`AfterUpdate`
`ScanScheduleDay`	День запуска проверки	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Вы можете выбрать только одно значение параметра.	`Monday`
`ScanScheduleTime`	Время запуска проверки	String	Время в 24-часовом формате (например, 13:00) или 12-часовом (например, 10.30 pm).	`8:00`
`ScanScheduleLock`	Запретить настраивать режим запуска проверки	Boolean	`True` – параметры режима запуска антивирусной проверки недоступны для пользователя в настройках приложения. `False` – пользователь может настроить режим запуска антивирусной проверки и, например, выключить автоматический запуск антивирусной проверки.	`True`
`ScanOnlyExecutableFiles`	Типы файлов для проверки (Антивирусная проверка)	Choice	`AllFiles` – проверка всех файлов. `OnlyExecutables` – проверка только исполняемых файлов. К исполняемым 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 файлов.	`AllFiles`
`ScanArchives`	Проверять архивы с распаковкой	Boolean	`True` – приложение распаковывает архивы и проверяет их содержимое. `False` – приложение проверяет только файлы архивов. Приложение проверяет только архивы с расширением .zip (.apk). В Kaspersky Endpoint Security для Android Service Pack 4 Maintenance Release 1 невозможно выключить проверку содержимого архивов.	`True`

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`ScanActionOnThreatFound`	Действие при обнаружении угрозы (Антивирусная проверка)	Choice	`Quarantine` – приложение помещает обнаруженные объекты на 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. `Delete` – приложение удаляет обнаруженные объекты. `Skip` – приложение оставляет обнаруженные объекты без изменений. Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. При попытке обращения к объекту на устройстве (например, попытке скопировать или открыть) приложение блокирует доступ к нему. `AskUser` – приложение предлагает пользователю выбрать действие для каждого обнаруженного объекта: пропустить, поместить на карантин или удалить. При обнаружении нескольких объектов пользователь может применить выбранное действие ко всем объектам. Приложение записывает информацию об обнаруженных угрозах и выполненных действиях в отчеты приложения.	`Карантин`
`ScanLock`	Запретить настраивать параметры проверки	Boolean	`True` – следующие параметры проверки недоступны для пользователя в настройках приложения: тип файлов для проверки, проверка архивов, действие при обнаружении угрозы. `False` – пользователь может настроить параметры проверки и, например, выбрать действие `Skip` при обнаружении угрозы.	`True`
`ScanAndProtectionAdwareRiskware`	Блокировать рекламное ПО, средства автодозвона и приложения, которые могут использоваться злоумышленниками для нанесения вреда устройству и данным пользователя	Boolean	`True` – приложение обнаруживает рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству и данным пользователя. `False` – приложение пропускает рекламные приложения и приложения, которые могут быть использованы злоумышленниками для нанесения вреда устройству или данным пользователя.	`True`
`ProtectionMode`	Режим постоянной защиты	Choice	`Recommended` – приложение только однократно проверяет новые приложения (сразу после установки) и файлы из папки Загрузки. `Extended` – приложение проверяет все файлы, которые пользователь открывает, изменяет, копирует, запускает и сохраняет на устройстве. Также приложение проверяет новые приложения и файлы из папки Загрузки. `Disabled` – постоянная защита выключена.	`Recommended`

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`UseKsnMode`	Режим Kaspersky Security Network	Choice	`Recommended` – приложение обменивается данными с Kaspersky 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 Kaspersky Security Network и дополнительно отправляет в Вирусную лабораторию определенную статистику о работе Kaspersky Endpoint Security для Android. Эта информация позволяет отслеживать угрозы в режиме реального времени. Сбор, обработка и 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.	`Recommended`
`ProtectScanOnlyExecutableFiles`	Типы файлов для проверки (Постоянная защита)	Boolean	`AllFiles` – проверка всех файлов. `OnlyExecutables` – проверка только исполняемых файлов. К исполняемым 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 файлов.	`AllFiles`
`ProtectionActionOnThreatFound`	Действие при обнаружении угрозы (Постоянная защита)	Choice	`Quarantine` – приложение помещает обнаруженные объекты на 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. `Delete` – приложение удаляет обнаруженные объекты. `Skip` – приложение оставляет обнаруженные объекты без изменений. Если обнаруженные объекты были пропущены, Kaspersky Endpoint Security для Android предупреждает пользователя о проблемах в защите устройства. При попытке обращения к объекту на устройстве (например, попытке скопировать или открыть объект) приложение блокирует доступ к нему. Приложение записывает информацию об обнаруженных угрозах и выполненных действиях в отчеты приложения.	`Карантин`
`ProtectionLock`	Запретить настраивать параметры постоянной защиты	Boolean	`True` – следующие параметры постоянной защиты недоступны для пользователя в настройках приложения: режим постоянной защиты, тип файлов для проверки и действие при обнаружении угрозы. `False` – пользователь может настроить параметры постоянной защиты и, например, выбрать действие `Skip` при обнаружении угрозы.	`True`

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`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. Выберите день недели запуска обновления баз (`UpdateScheduleDay`) и настройте время (`UpdateScheduleTime`). `Off` – автоматическое обновление антивирусных баз выключено. При любом значении параметра пользователь устройства может запустить обновление антивирусных баз вручную.	`Раз в день`
`UpdateScheduleDay`	День запуска обновления баз	Choice	`Monday / Tuesday / Wednesday / Thursday / Friday / Saturday / Sunday` Вы можете выбрать только одно значение параметра.	`Monday`
`UpdateScheduleTime`	Время запуска обновления баз	String	Время в 24-часовом формате (например, 13:00) или 12-часовом (например, 10.30 pm).	`8:00`
`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 обновления баз и, например, выключить автоматический запуск обновления антивирусных баз.	`True`
`AllowUpdateInRoaming`	Обновлять базы в роуминге	Boolean	`True` – приложение загружает антивирусные базы, если устройство находится в зоне роуминга. Приложение загружает антивирусные базы по сформированному расписанию (`UpdateScheduleType`). `False` – приложение загружает антивирусные базы, только если устройство находится в домашней сети.	`False`

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию

`EnableWebFilter`	Веб-Фильтр	Boolean	`True` – приложение блокирует вредоносные и фишинговые веб-сайты в интернете с помощью компонента Веб-Фильтр. Веб-Фильтр работает только в Google Chrome.
			
			Вредоносные и фишинговые веб-сайты, использующие протокол HTTPS, разрешается не блокировать, если домен является доверенным. Если домен не является доверенным, Веб-Фильтр блокирует вредоносные и фишинговые веб-сайты.
			
			`False` – защита от вредоносных и фишинговых веб-сайтов выключена.
			
			Для работы Веб-Фильтра должны быть выполнены следующие условия:
			• Пользователи устройств приняли Политику конфиденциальности и Положение о Веб-Фильтре в мастере первоначальной настройки или параметрах приложения.
			• В параметрах браузера настроен прокси-сервер:
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128"`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled = false`
			Конфигурации прокси-сервера могут различаться в зависимости от версии Google Chrome. Подробная информация настройке Google Chrome приведена на веб-сайте проекта Chromium.
			После удаления приложения Kaspersky Endpoint Security для Android с мобильного устройства сбросьте настройки прокси-сервера.
			• В параметрах приложения включено использование KSN: `UseKsnMode = Recommended` или `UseKsnMode = Extended`.
			• В параметрах операционной системы рекомендуется выбрать Google Chrome в качестве браузера по умолчанию.
				`False`

`EnableWebFilterLock`	Запретить настраивать Веб-Фильтр	Boolean	`True` – параметры Веб-Фильтра недоступны для пользователя в настройках приложения. `False` – пользователь может настроить параметры Веб-Фильтра и, например, выключить защиту от вредоносных и фишинговых веб-сайтов в интернете.	`True`
`UpdateServer`	Адрес сервера источника обновлений баз	String	Адрес сервера источника обновлений баз, например, `http://update.server.com`. Если оставить поле пустым, Kaspersky Endpoint Security для Android использует серверы обновлений баз "Лаборатории Касперского".	

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`AllowGoogleAnalytics`	Передавать данные в сервисы Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics	Boolean	`True` – приложение автоматически передает данные о работе Kaspersky Endpoint Security для Android в сервисы Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics. Данные необходимы для повышения качества работы приложения и анализа удовлетворенности пользователей. Передача данных в сервисы Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics осуществляется по защищенному каналу. Доступ к данным и защита данных регулируются соответствующими условиями использования сервисов Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics. `False` – передача данных в сервисы Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics выключена.	`True`
`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 упрощает поиск и сортировку устройств в Kaspersky Security Center. • `{DeviceSerialNumber}` – серийный номер устройства. • `{DeviceUid}` – уникальный идентификатор устройства (UDID). • `{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 этих значений.	
`KscGroup`	Название группы устройств	String	Группы устройств можно указывать в EMM-консоли. При подключении устройства к Kaspersky Security Center, оно автоматически добавляется в подпапку папки "Нераспределенные устройства". Имя подпапки соответствует названию группы, указанному с помощью этого параметра. Затем можно создать правила автоматического перемещения устройств из подпапок папки "Нераспределенные устройства" в группы администрирования папки "Управляемые устройства". Если это поле не заполнено, устройство автоматически добавляется в корень папки "Нераспределенные устройства".	`KES10`

Ключ конфигурации	Описание	Тип	Значение	Значение по умолчанию
`KscCorporateEmail`	Корпоративная электронная почта пользователя	String	В консоли EMM можно указать корпоративные адреса электронной почты пользователей. Эти адреса электронной почты будут отображаться в Kaspersky Security Center. Строка должна представлять собой действующий адрес электронной почты. Другие значения будут игнорироваться.	
`KscDeviceName`	Имя устройства в Kaspersky Security Center	String	Этот параметр доступен только для SOTI MobiControl. Вы можете указать имя устройства, отображаемое в Kaspersky Security Center. Вы можете ввести любое имя или использовать макрос %DEVICENAME%, чтобы автоматически получить имя устройства из консоли SOTI MobiControl. Если оставить поле пустым, имя устройства будет сгенерировано в соответствии с форматом, указанным в групповой политике Kaspersky Security Center.	

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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, 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.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 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 компонентов Антивирус и Контроль приложений, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать следующую информацию.

Информация о типах данных, передаваемых в "Лаборатории Касперского" при использовании KSN во время работы Веб-Фильтра, доступна в Положении об обработке данных для использования Веб-Фильтра. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

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:

- Вам или пользователю устройства необходимо 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 Kaspersky Security for Mobile (Devices) изменится на *Предупреждение*.

- Необходимо разрешить передачу статистики в KSN в параметрах групповой политики.

Вы можете 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.

Подробная информация о предоставлении данных в KSN приведена в разделе Предоставление данных.

Предоставление данных в KSN является добровольным. При желании можно отключить обмен данными с KSN.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Включение и выключение использования Kaspersky Security Network

Для работы компонентов приложения Kaspersky Endpoint Security для Android, использующих Kaspersky Security Network, выполняется отправка запросов в облачные службы. Запросы содержат данные, описанные в разделе Предоставление данных.

Если использование Kaspersky Security Network на устройстве выключено, компоненты Облачная защита, Веб-Фильтр и Контроль приложений автоматически выключаются.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Использование Kaspersky Private Security Network

Kaspersky Private Security Network (далее также *KPSN*) – это решение, предоставляющее доступ к репутационным базам Kaspersky Security Network (KSN) без отправки данных с устройств пользователей в Kaspersky Security Network.

База данных репутации объектов (файлов или веб-адресов) хранится на сервере Kaspersky Private Security Network, а не на серверах Kaspersky Security Network. Репутационные базы данных KPSN хранятся в корпоративной сети и управляются администратором компании.

При включенном KPSN Kaspersky Endpoint Security не отправляет статистические данные с устройств пользователей в KSN.

Чтобы включить использование KPSN в Kaspersky Security Center, выполните следующие действия:

1. В главном окне Kaspersky Security Center Web Console или Cloud Console нажмите на кнопку **Настройка** ( ).

   Откроется окно свойств Сервера администрирования.

2. На закладке **Общие** перейдите в раздел **Параметры прокси-сервера KSN**.

3. Установите переключатель в положение **Использование Kaspersky Private Security Network включено**.

4. Нажмите на кнопку **Выбрать файл с параметрами прокси-сервера KSN**, а затем выберите файл конфигурации с расширением pkcs7 или pem (предоставляется "Лабораторией Касперского").

5. Нажмите кнопку **Открыть**.

6. Если в свойствах Сервера администрирования настроены параметры прокси-сервера, но для архитектуры сети требуется использовать KPSN напрямую, включите параметр **Игнорировать параметры прокси-сервера при подключении к Локальному KSN**. В противном случае запросы от управляемых программ не попадут в KPSN.

7. Нажмите на кнопку **Сохранить**.

После загрузки параметров в интерфейсе отобразится имя и контакты поставщика услуг, а также дата создания файла с параметрами KPSN. Параметры KPSN применятся к мобильным устройствам.

При переходе на KPSN компонент Контроль приложений не будет поддерживать категории приложений, доступные при использовании KSN. Категоризация приложений станет доступна при возврате к KSN.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Предоставление данных сторонним сервисам

Kaspersky Endpoint Security для Android использует сервисы Google™: Firebase Cloud Messaging, Google Analytics для Firebase™, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics. 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 сервисы Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics для повышения качества работы приложения и эффективного формирования "Лабораторией Касперского" маркетинговых материалов.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обмен информацией с Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics

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 сервисами Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics по следующим причинам:

- В целях повышения качества работы приложения.

Для обмена данными с сервисами Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics 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 Kaspersky Security for Mobile (Devices) 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 сервисами Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics 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, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics в настройках групповой политики (см. ниже).

Предоставление данных в Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics 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:

- информация о приложении: версия, идентификатор, название и идентификатор приложения в сервисе Firebase, уникальный идентификатор установки в сервисе Firebase, название магазина, из которого ПО было получено, время первого запуска ПО на устройстве;

- идентификатор установки приложения на устройство и способ установки на устройство;

- информация о регионе и языковой локализации;

- разрешение экрана устройства;
- информация о получении root -прав пользователем;
- диагностические данные об устройстве от сервиса SafetyNet Attestation;
- признак установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей;
- информация о переходах между окнами приложения, продолжительности сессии, начале и окончании сессии работы с экраном, названии экрана;
- информация 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;
- информация о лицензии на приложение, ее наличии, количестве устройств;
- интервалы обновления антивирусных баз и синхронизации с Сервером администрирования;
- информация о консоли администрирования (Kaspersky Security Center или сторонние EMM-системы);
- идентификатор Android ID;
- идентификатор Advertising ID;
- информация о пользователе: возрастная категория и половая принадлежность пользователя, идентификатор страны проживания, список интересов пользователя;
- информация о компьютере, на котором установлено ПО: название производителя компьютера, тип компьютера, модель устройства, версия и информация о языковой локализации ОС, информация о первом запущенном приложении за последнюю неделю и ранее.

  Передача данных в сервис Google Analytics для Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Google Analytics для 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.

Firebase Performance Monitoring

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Firebase Performance Monitoring для их обработки для заявленных целей:

- уникальный идентификатор установки;
- название пакета приложения;
- версия установленного ПО;
- уровень и статус заряда батареи;
- оператор связи;
- признак работы ПО в фоновом режиме;
- регион;
- IP-адрес;
- код языка устройства;
- информация о радио- и интернет-соединении;
- идентификатор-псевдоним экземпляра ПО;
- ОЗУ и размер диска;
- признак того, что на устройстве выполнена процедура рутинга или джейлбрейка;
- уровень сигнала;
- продолжительность автоматической трассировки;
- информация о сети и сопутствующая информация ответа: код ответа, размер полезной нагрузки в байтах, время отклика;
- описание устройства.

  Передача данных в сервис Firebase Performance Monitoring осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase Performance Monitoring доступна по адресу https://firebase.google.com/support/privacy.

Crashlytics

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Crashlytics для их обработки для заявленных целей:

- идентификатор ПО;
- версия установленного ПО;
- признак работы ПО в фоновом режиме;
- архитектура ЦП;
- уникальный идентификатор события;

- дата и время события;
- модель устройства;
- объем полного и используемого дискового пространства;
- название и версия ОС;
- объем полной и используемой оперативной памяти;
- признак того, что на устройстве выполнена процедура рутинга;
- ориентация экрана в момент события;
- производитель продукта / устройства;
- уникальный идентификатор установки;
- версия отправляемой статистики;
- тип исключения ПО;
- текст сообщения об ошибке;
- признак того, что исключение ПО вызвано исключением на вложенном уровне;
- идентификатор потока;
- признак того, что фрейм стал причиной ошибки ПО;
- признак того, что выполнение потока привело к неожиданному завершению работы ПО;
- данные о сигнале, который привел к неожиданному завершению работы ПО: название сигнала, код сигнала, адрес сигнала;
- для каждого фрейма, ассоциированного с потоком, исключением или ошибкой: имя файла фрейма, номер строки файла фрейма, отладочные символы, адрес и смещение в бинарном образе, отображаемое имя библиотеки, содержащей фрейм, тип фрейма, признак того, что фрейм стал причиной ошибки;
- идентификатор ОС;
- идентификатор проблемы, связанной с событием;
- информация о событиях, предшествующих неожиданному завершению работы ПО: идентификатор события, дата и время события, тип события и значение;
- значения регистра ЦП;
- тип события и значение.

  Передача данных в сервис Crashlytics осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Crashlytics доступна по адресу https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Предоставление вышеуказанной информации для обработки в маркетинговых целях является

добровольным.

Чтобы запретить обмен данными с сервисами Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics, 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 разделе **Передача данных** снимите флажок **Разрешить передачу данных, чтобы помочь улучшить качество работы, интерфейс и производительность приложения**.
4. Нажмите на кнопку **Применить**, чтобы сохранить внесенные изменения.

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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 в маркетинговых целях.

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 Kaspersky Security for Mobile (Devices) 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Развертывание через KNOX Mobile Enrollment возможно только для Samsung-устройств. Список поддерживаемых устройств приведен на *сайте Службы технической поддержки Samsung*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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, NFC (Near Field Communication) или QR-кода. 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 на 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 интернету. 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 мобильного 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 интернету 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, NFC или QR-кода. 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 интернету.

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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка приложения

Перед установкой приложения Kaspersky Endpoint Security для Android выпишите в Консоли администрирования Kaspersky Security Center мобильный сертификат для пользователей мобильных устройств. Мобильный 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`).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Активация Samsung KNOX

Чтобы использовать KNOX-контейнер на мобильном устройстве пользователя, требуется активировать Samsung KNOX. Процедура активации Samsung KNOX зависит от версии Kaspersky Endpoint Security для Android, установленной на устройствах пользователей:

- Если на устройствах установлена текущая версия Kaspersky Endpoint Security для Android, для активации Samsung KNOX ключи не требуются.
- Если на устройствах установлена устаревшая версия Kaspersky Endpoint Security для Android (10.8.3.174 или ниже), необходимо получить ключ KNOX License Manager (KLM-ключ) от Samsung. *Ключ KNOX License Manager* – уникальный код, который используется системой лицензирования Samsung KNOX. Более подробная информация о KLM-ключе приведена на сайте технической поддержки Samsung KNOX.

Использование KNOX-контейнеров возможно только на Samsung-устройствах.

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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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

5. В поле **Ключ KNOX License Manager** укажите следующие данные:

   - Если на устройствах установлена текущая версия Kaspersky Endpoint Security для Android, введите любой символ.

   - Если на устройствах установлена устаревшая версия Kaspersky Endpoint Security для Android (10.8.3.174 или ниже), введите KLM-ключ, полученный от 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.

   В течение 15 минут выполните следующие действия. По истечении этого времени при сохранении изменений политики может возникнуть ошибка.

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

5. Удалите значение, указанное в поле **Ключ KNOX License Manager**.

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

Samsung KNOX будет деактивирован после очередной синхронизации устройства с Kaspersky Security Center. Доступ в KNOX-контейнер будет заблокирован.

Ограничения Samsung KNOX

- Использование KNOX-контейнеров возможно только на Samsung-устройствах.

- 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Настройка почтового ящика Exchange в KNOX

Для работы с корпоративной почтой, контактами и календарем в KNOX-контейнере следует настроить параметры почтового ящика Exchange (доступно только в Android 9 и ниже).

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Приложения

Этот раздел содержит информацию, которая дополняет основной текст документа.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 приложений	Контроль приложений
Защита	Защита, Проверка, Обновление
Контроль соответствия	Контроль соответствия
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

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 программы	Библиотеки программного обеспечения, технические демоверсии приложений. 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Использование приложения Kaspersky Endpoint Security для Android

В этом разделе справки описаны функции и действия, доступные пользователям приложения Kaspersky Endpoint Security для Android.

Статьи в этом разделе содержат описание всех параметров, доступных и видимых на мобильных устройствах. Фактический внешний вид и работа приложения зависит от используемой системы удаленного администрирования и от того, как администратор настроил 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

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 с помощью соответствующего уведомления 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 перед открытием, используя облачную службу Kaspersky Security Network. Узнать больше.

Контроль 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 Kaspersky Endpoint Security должен быть установлен 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 с помощью соответствующего уведомления или в настройках устройства (**Настройки Android** → **Специальные возможности** → **Службы**).

Контроль соответствия

Компонент Контроль соответствия автоматически проверяет соответствие устройства требованиям корпоративной безопасности. Если ваше устройство не соответствует требованиям корпоративной безопасности, приложение показывает уведомление со следующей информацией:

- причина несоответствия (например, на устройстве были обнаружены запрещенные приложения или антивирусные базы устарели);
- 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, блокировка устройства);
- вариант действия для устранения несоответствия устройства требованиям корпоративной безопасности.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обзор главного окна

Вид главного окна для разных разрешений экрана незначительно отличается.

В главном окне отображается общий статус защиты вашего устройства. Этот статус определяет цвет окна:

- Зеленый цвет указывает на оптимальный уровень защиты устройства.
- Красный цвет указывает на критические проблемы с безопасностью устройства.

В главном окне приложения вы также можете:

- Просматривать уведомления, нажав на кнопку в правом верхнем углу. Они информируют вас о проблемах безопасности, проблемах в работе приложения, соответствии требованиям корпоративной безопасности и статусе вашей лицензии.
- Переходить между главным окном и настройками приложения с помощью кнопок внизу.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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).

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 уведомлениях 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 нажмите **Настройки → Настройки приложения → Антивирус → Запустить проверку**.

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, предназначенный 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 нажмите **Настройки → Настройки приложения → Антивирус → Настройки проверки**.

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, выполняемое приложением 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. 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 уведомлениях 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 нажмите **Настройки** → **Настройки приложения** → **Антивирус** → **Настройки проверки**.

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 требуется запускать полную проверку.

4. Нажмите **Время запуска** и укажите время запуска полной проверки.

Полная проверка устройства будет запускаться согласно расписанию.

На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 нажмите **Настройки** → **Настройки приложения** → **Антивирус** → **Режим постоянной защиты**.

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. Нажмите **Настройки** → **Настройки приложения** → **Антивирус** в главном окне Kaspersky Endpoint Security.

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 нажмите **Настройки** → **Настройки приложения** → **Антивирус** → **Настройки проверки**.

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, выполняемое приложением 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. 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обновление антивирусных баз

Чтобы обновить антивирусные базы приложения,

В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **Антивирус** → **Запустить обновление баз**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 нажмите **Настройки** → **Настройки приложения** → **Антивирус** → **Настройки обновления 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.

На Android 12 или более поздней версии приложение может выполнить эту задачу позже, чем указано, если устройство находится в режиме экономии заряда батареи.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Веб-Фильтр

Для включения Веб-Фильтра должны быть выполнены следующие условия:

- Приложение Kaspersky Endpoint Security включено в качестве службы Специальных возможностей.
- Положение об обработке данных в целях использования Веб-Фильтра (Положение о Веб-Фильтре) должно быть принято. 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.

Чтобы использовать Веб-Фильтр в приложении Telegram, выключите просмотр ссылок во встроенном браузере в настройках Telegram.

Веб-Фильтр на Android-устройствах работает только в браузерах Google Chrome (включая функцию Custom Tabs), 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 нажмите **Настройки** → **Настройки приложения** → **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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Получение сертификата

Чтобы получить сертификат для доступа к ресурсам сети организации, выполните следующие действия:

1. В главном окне Kaspersky Endpoint Security нажмите **Настройки** → **Настройки приложения** → **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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 нажмите **Настройки** → **Настройки приложения** → **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**.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Активация Kaspersky Endpoint Security для Android без использования Kaspersky Security Center

В большинстве случаев установленное на устройстве приложение Kaspersky Endpoint Security для Android активируется администратором централизованно с помощью системы удаленного администрирования Kaspersky Security Center. Если ваше устройство не подключено к Kaspersky Security Center, вы можете ввести код активации вручную. Для получения кода активации обратитесь к администратору.

Активируйте приложение вручную только по указанию администратора.

Чтобы ввести код активации, выполните следующие действия:

1. В сообщении об ошибке, в котором говорится, что срок действия вашей лицензии скоро истечет или уже истек, и что ваше устройство не подключено к Серверу администрирования, нажмите **Активировать**.
2. В окне активации введите код активации, предоставленный администратором, и нажмите **Активировать**.
3. Если код активации правильный, отображается уведомление об активации приложения, а также дата истечения срока действия лицензии.

Приложение Kaspersky Endpoint Security для Android на вашем устройстве будет активировано.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка приложения в режиме device owner

Режим device owner – это режим работы корпоративных Android-устройств. Этот режим позволяет администратору осуществлять полный контроль над устройством и настраивать множество функций. Режим device owner поддерживается на Android 7.0 или выше.

Для развертывания приложения в режиме device owner необходимо сбросить настройки устройства до заводских и установить приложение, используя QR-код, сгенерированный в Kaspersky Security Center. QR-код содержит все необходимые данные для настройки приложения.

Чтобы установить Kaspersky Endpoint Security для Android на устройство в режиме device owner:

1. Сбросьте настройки устройства до заводских.

   Устройство перезагрузится, откроется экран приветствия.
2. Шесть раз нажмите на пустое пространство на экране приветствия.

   Откроется утилита для считывания QR-кодов.
3. Отсканируйте QR-код, сгенерированный в Kaspersky Security Center, для установки приложения.
4. Выполните первоначальную настройку устройства. Операционная система установит приложение Kaspersky Endpoint Security для Android в фоновом режиме.

   После завершения настройки устройства на нем запустится Kaspersky Endpoint Security для Android.
5. Активируйте приложение, следуя указаниям мастера первоначальной настройки.

Приложение Kaspersky Endpoint Security для Android будет установлено и активировано на устройстве в режиме device owner.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Включение специальных возможностей на Android 13 или выше

На Android 13 или выше специальные возможности ограничены для приложений, загруженных не из Google Play или HUAWEI AppGallery. Если вы загрузили Kaspersky Endpoint Security для Android с сервера Kaspersky Security Center или с сайта "Лаборатории Касперского", вам необходимо вручную разрешить доступ к специальным возможностям.

Если вы обновили приложение Kaspersky Endpoint Security для Android с помощью инсталляционного пакета Kaspersky Security Center или APK-файла с сайта "Лаборатории Касперского", службы специальных возможностей будут выключены. Вам необходимо заново вручную включить службы специальных возможностей.

Специальные возможности используются для следующих целей:

- проверки веб-сайтов и приложений в Kaspersky Security Network;
- блокировки устройства в случае кражи;
- отображения уведомлений;
- блокировки камеры, если это запрещено администратором.

Чтобы включить специальные возможности для Kaspersky Endpoint Security, выполните следующие действия:

1. Откройте страницу **Специальные возможности** в настройках устройства и найдите Kaspersky Endpoint Security.
2. Включите переключатель Kaspersky Endpoint Security. В окне, в котором говорится, что доступ к специальным возможностям ограничен, нажмите **ОК**.

   Теперь вы можете предоставить Kaspersky Endpoint Security доступ к ограниченным настройкам.
3. Откройте страницу с информацией о Kaspersky Endpoint Security в настройках устройства. Например, перейдите в **Настройки** > **Приложения**, а затем найдите приложение в списке.
4. На странице с информацией о Kaspersky Endpoint Security нажмите ⋮ в правом верхнем углу и выберите пункт меню **Разрешить ограниченные настройки**.

   Теперь Kaspersky Endpoint Security имеет доступ к ограниченным настройкам.
5. Вернитесь на страницу **Специальные возможности** в настройках устройства и найдите Kaspersky Endpoint Security.
6. Включите переключатель **Kaspersky Endpoint Security**. В открывшемся окне предоставьте приложению полный контроль над вашим устройством.

Службы специальных возможностей теперь включены для Kaspersky Endpoint Security.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Чтобы включить специальные возможности для Kaspersky Endpoint Security, выполните следующие действия:

1. В окне включения служб специальных возможностей нажмите **Включить**.

   Откроется страница **Специальные возможности** в настройках устройства.

2. Включите переключатель Kaspersky Endpoint Security. В окне, в котором говорится, что доступ к специальным возможностям ограничен, нажмите **ОК**.

   Теперь вы можете предоставить Kaspersky Endpoint Security доступ к ограниченным настройкам.

3. Откройте страницу с информацией о Kaspersky Endpoint Security в настройках устройства. Например, перейдите в **Настройки** > **Приложения**, а затем найдите приложение в списке.

4. На странице с информацией о Kaspersky Endpoint Security нажмите ⋮ в правом верхнем углу и выберите пункт меню **Разрешить ограниченные настройки**.

   Теперь Kaspersky Endpoint Security имеет доступ к ограниченным настройкам.

5. Вернитесь в приложение и в окне включения специальных возможностей нажмите **Включить**.

   Откроется страница **Специальные возможности** в настройках устройства.

6. Включите переключатель **Kaspersky Endpoint Security**. В открывшемся окне предоставьте приложению полный контроль над вашим устройством.

Службы специальных возможностей теперь включены для Kaspersky Endpoint Security.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

   Отобразится запрос на установку Kaspersky Endpoint Security на ваше устройство.

2. Примите условия обновления.

   Новая версия приложения будет установлена на ваше устройство. Дополнительная настройка приложения после обновления не требуется.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 устройства.
- С помощью администратора. Администратор может дистанционно удалить приложение с вашего устройства с помощью системы удаленного администрирования Kaspersky Security Center.

На устройствах, работающих в режиме device owner, приложение Kaspersky Endpoint Security для Android может быть удалено только администратором с помощью сброса устройства до заводских настроек.

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 отобразится предложение подтвердить удаление Kaspersky Endpoint Security.

2. Подтвердите удаление приложения.

   Приложение будет удалено с вашего устройства.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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*.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Использование приложения Kaspersky Security для iOS

В этом разделе справки описаны функции и действия, доступные пользователям приложения Kaspersky Security для iOS.

Статьи в этом разделе содержат описание всех параметров, доступных и видимых на мобильных устройствах. Фактический внешний вид и работа приложения зависит от используемой системы удаленного администрирования и от того, как администратор настроил 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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Возможности приложения

Kaspersky Security для iOS обладает следующими основными возможностями.

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 перед открытием, используя облачную службу Kaspersky Security Network. Веб-Фильтр также проверяет сетевую активность приложений на вашем устройстве.

Чтобы Веб-фильтр работал, вы должны разрешить приложению добавлять конфигурацию VPN.

Обнаружение модификации прошивки (jailbreak)

Если приложение Kaspersky Security для iOS обнаруживает модификацию прошивки (jailbreak), то отображает критическое сообщение и информирует вашего администратора о проблеме.

Приложение не может гарантировать безопасность вашего устройства, поскольку модификация прошивки (jailbreak) позволяет обходить средства защиты операционной системы и может вызывать множество проблем, включая:

- уязвимости в безопасности устройства;
- нестабильную работу;
- сбой в работе сервисов Apple;
- возможные сбои и зависания;
- сокращение срока службы батареи;
- невозможность установки обновлений iOS.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Установка приложения

Чтобы установить приложение Kaspersky Security для iOS, выполните следующие действия:

1. Найдите в электронной почте письмо от вашего администратора с приглашением установить приложение Kaspersky Security для iOS из App Store.
2. Перейдите в App Store одним из следующих способов:
   - Если вы открыли письмо на устройстве iOS, на котором хотите установить приложение, нажмите на ссылку в этом письме.
   - Если вы читаете письмо компьютере, отсканируйте QR-код с помощью устройства iOS, на котором вы хотите установить приложение.

   Ссылка в приглашении действительна в течение 24 часов. Если вам не удастся установить приложение вовремя, обратитесь к своему администратору за новым приглашением.
3. Загрузите и установите приложение из App Store, следуя стандартной процедуре установки на платформе iOS.

Приложение Kaspersky Security для iOS будет установлено на вашем устройстве. Чтобы защитить устройство, активируйте приложение.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Активация приложения

Чтобы активировать приложение Kaspersky Security для iOS, выполните следующие действия:

1. Запустите приложение на своем устройстве.
2. Примите соглашения, установив флажки **Лицензионное соглашение** и **Политика конфиденциальности для продуктов и сервисов**.

   Примите необязательное **Положение о Kaspersky Security Network**, чтобы разрешить отправку статистики в Kaspersky Security Network. Это повышает производительность приложения и обеспечивает его бесперебойную работу.
3. Нажмите **Далее**. Приложение подключится к системе удаленного администрирования Kaspersky Security Center и получит информацию о лицензии.
4. Разрешите приложению добавлять конфигурацию VPN. Приложение использует конфигурацию VPN для проверки веб-сайтов на фишинг и защиты вашего устройства от веб-угроз.
5. Разрешите приложению отправлять push-уведомления. Приложение использует уведомления, чтобы информировать вас о проблемах безопасности и статусе вашей лицензии.

Приложение Kaspersky Security для iOS на вашем устройстве будет активировано.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Активация приложения с помощью кода активации

Когда вы устанавливаете приложение Kaspersky Security для iOS на свое устройство, приложение подключается к системе удаленного администрирования Kaspersky Security Center и автоматически получает информацию о лицензии. Если ваше устройство не подключено к Kaspersky Security Center, вы можете ввести код активации вручную. Для получения кода активации обратитесь к администратору.

Активируйте приложение вручную только по указанию администратора.

Чтобы ввести код активации, выполните следующие действия:

1. В сообщении, в котором указано, что приложение не активировано, нажмите **Активировать приложение**.
2. В окне активации введите код активации, предоставленный администратором, и нажмите **Активировать**.

   Если код активации правильный, отображается уведомление об активации приложения, а также дата истечения срока действия лицензии.

Приложение Kaspersky Security для iOS на вашем устройстве будет активировано.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обзор главного окна

Вид главного окна для разных разрешений экрана незначительно отличается.

В главном окне отображаются:

- общий статус защиты вашего устройства;
- сообщения, указывающие на состояние компонентов приложения и проблемы с защитой.

Существует три типа сообщений:

- Выделенные зеленым цветом. Сообщения о состоянии, информирующие вас о том, что защита активна в указанной области.
- Выделенные желтым цветом. Информационные сообщения, уведомляющие вас о событиях, которые могут повлиять на безопасность устройства.
- Выделенные красным цветом. Критические сообщения, информирующие вас о событиях, имеющих критическое значение для безопасности устройства.

Для получения подробной информации вы можете нажать на сообщение.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обновление приложения

Вы можете загрузить последнюю версию приложения Kaspersky Security для iOS из App Store и установить ее на свое устройство, выполнив стандартную процедуру обновления на платформе iOS. Вы также можете включить автоматическое обновление. Дополнительная настройка приложения после обновления не требуется.

Для обновления приложения должны быть выполнены следующие условия:

- у вас должен быть Apple ID;
- устройство должно быть привязано к вашему Apple ID;
- на устройстве должно быть установлено соединение с интернетом.

Чтобы узнать больше о создании Apple ID, привязке вашего устройства к Apple ID или работе с App Store, см. сайт службы поддержки Apple.

Функциональность обновлений (включая обновления антивирусных сигнатур и обновления кодовой базы), а также функциональность KSN будут недоступны в решении на территории США с 12:00 AM по восточному летнему времени (EDT) 10 сентября 2024 года в соответствии с ограничительными мерами.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Удаление приложения

Чтобы удалить приложение Kaspersky Security для iOS, выполните стандартную процедуру удаления на платформе iOS:

1. На главном экране коснитесь и удерживайте значок приложения.
2. Удалите приложение.

Приложение Kaspersky Security для iOS будет удалено с вашего устройства.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Лицензирование программы

Этот раздел содержит информацию об основных понятиях, связанных с лицензированием Kaspersky Security для мобильных устройств.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 файл license.txt, входящий в самораспаковывающийся архив дистрибутива для установки приложения Kaspersky Endpoint Security для Android.
- В разделе **О приложении** в Kaspersky Endpoint Security для Android.
- В разделе **О приложении** → **Соглашения и положения** в Kaspersky Security для iOS.
- В разделе **Дополнительно** → **Принятые лицензионные соглашения** в свойствах Сервера администрирования. Эта функция доступна в Kaspersky Security Center версии 12.1 и более поздней.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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:

- использование приложений на мобильных устройствах в соответствии с условиями Лицензионного соглашения;
- получение технической поддержки.

Список доступных функций 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 и Kaspersky Security для iOS прекращают выполнять большинство функций, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно приобрести коммерческую лицензию.

- *Коммерческая*.

  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 зависимости от приложения доступны следующие компоненты:

  - Приложение Kaspersky Endpoint Security для Android:
    - **Антивирус**. Доступна постоянная защита и антивирусная проверка устройства, но не доступно обновление антивирусных баз.
    - **Анти-Вор**. Доступна только отправка команд на мобильные устройства.
    - **Синхронизация с Сервером администрирования**.

    Приложение Kaspersky Endpoint Security для Android прекращает обмен информацией с Kaspersky Security Network, Google Analytics для Firebase, SafetyNet Attestation, Firebase Performance Monitoring и Crashlytics в случае блокировки ключа "Лабораторией Касперского", по истечении срока действия пробной лицензии и при отсутствии лицензии (код активации удален из групповой политики).

  - Приложение Kaspersky Security для iOS:
    - **Синхронизация с Сервером администрирования**.

Kaspersky Security для iOS прекращает обмен информацией с Kaspersky Security Network, если срок действия пробной лицензии истек или лицензия отсутствует (код активации удален из групповой политики).

Остальные компоненты мобильного приложения 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.

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 окончания ее срока действия, чтобы обеспечить максимальную защиту компьютера от всех угроз безопасности.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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 для Android. Ключ отображается в интерфейсе Kaspersky Security Center и интерфейсе мобильного приложения для Android в виде уникальной буквенно-цифровой последовательности.

  После добавления ключей вы можете заменять их другими.

  > Вы не можете активировать приложение Kaspersky Security для iOS с помощью файла ключа.

- Если ваша организация не использует Kaspersky Security Center, вам необходимо предоставить пользователю код активации. Пользователь вводит этот код активации в мобильном приложении для Android или iOS. Ключ отображается в интерфейсе мобильного приложения в виде уникальной буквенно-цифровой последовательности.

Ключ может быть заблокирован "Лабораторией Касперского", если, например, условия Лицензионного соглашения нарушены. Если ключ заблокирован, мобильное приложение прекращает выполнять все свои функции, кроме синхронизации с Сервером администрирования. Чтобы продолжить использование приложения, вам нужно добавить другой ключ.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О коде активации

Код активации – это уникальная последовательность из двадцати латинских букв и цифр. Вы вводите код активации, чтобы добавить ключ, активирующий приложение Kaspersky Endpoint Security для Android или Kaspersky Security для iOS. 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".

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

О файле ключа

Файл ключа – это файл с расширением key, который вам предоставляет "Лаборатория Касперского". Файл ключа предназначен для добавления ключа, активирующего приложение Kaspersky Endpoint Security для Android.

Вы не можете активировать приложение Kaspersky Security для iOS с помощью файла ключа.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Предоставление данных в Kaspersky Endpoint Security для Android

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 в маркетинговых целях.

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 Kaspersky Security for Mobile (Devices) 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.

Обмен информацией с Kaspersky Security Network

Для повышения уровня постоянной защиты Kaspersky Endpoint Security для Android 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 перед открытием с учетом данных, полученных от KSN. Также приложение определяет категорию веб-сайта для контроля доступа пользователей в интернет на основе списков разрешенных и запрещенных категорий (например, категория "Общение в сети").
- **Контроль приложений.** Приложение определяет категории для ограничения запуска приложений, 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 компонентов Антивирус и Контроль приложений, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать следующую информацию.

Информация о типах данных, передаваемых в "Лаборатории Касперского" при использовании KSN во время работы Веб-Фильтра, доступна в Положении об обработке данных для использования Веб-Фильтра. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

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. Принимая условия этого Положения, вы соглашаетесь передавать перечисленную ниже информацию.

Предоставление данных в рамках Лицензионного соглашения

Если для активации ПО применяется Код активации, с целью проверки правомерности использования ПО Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- формат данных в запросе к инфраструктуре Правообладателя; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; размер содержимого запроса к инфраструктуре Правообладателя; идентификатор протокола; код активации ПО; тип сжатия данных; идентификатор ПО; набор идентификаторов ПО, которое может быть активировано на устройстве пользователя; локализация ПО; полная версия ПО; уникальный идентификатор устройства; дата и время на устройстве пользователя; идентификатор установки ПО (PCID); версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; модель устройства; семейство операционной системы; формат данных в запросе к инфраструктуре Правообладателя; тип контрольной суммы обрабатываемого объекта; заголовок лицензии на использование ПО; идентификатор регионального центра активации; дата и время создания лицензионного ключа ПО; идентификатор лицензии ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; дата и время истечения срока действия лицензии на использование ПО; текущий статус лицензионного ключа ПО; тип используемой лицензии ПО; тип лицензии, с помощью которой активировано ПО; идентификатор ПО, полученный из лицензии.

Для защиты Компьютера от угроз информационной безопасности Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- тип контрольной суммы обрабатываемого объекта; контрольная сумма обрабатываемого объекта; идентификатор компонента ПО;

- идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; название обнаруженной вредоносной программы или легальной программы, которая может быть использована для нанесения вреда устройству или данным пользователя;

- название магазина, из которого приложение было установлено; название пакета приложения; публичный ключ, которым подписан APK-файл; контрольная сумма сертификата, которым подписан APK-файл; временная метка цифрового сертификата;

- полная версия ПО; идентификатор обновления ПО; тип установленного ПО; идентификатор конфигурации; результат действий, выполненных ПО; код ошибки;

- числовые значения, полученные из APK-файла приложения Android в соответствии с определенными математическими правилами и не позволяющие восстановить исходное содержимое файла; эти данные не содержат имен файлов, путей к файлам, адресов, номеров телефонов и другой личной информации пользователей.

Если получение Обновлений выполняется с серверов обновления Правообладателя, то для целей улучшения качества работы механизма обновления Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- идентификатор ПО, полученный из лицензии; полная версия ПО; идентификатор лицензии ПО; тип используемой лицензии ПО; идентификатор установки ПО (PCID); идентификатор запуска обновления ПО; обрабатываемый веб-адрес.

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 для 5 и более узлов, то при использовании KSN Правообладатель будет получать и обрабатывать следующие данные в автоматическом режиме:

- идентификатор сработавшей записи в антивирусных базах ПО; временная метка сработавшей записи в антивирусных базах ПО; тип сработавшей записи в антивирусных базах ПО; дата и время выпуска баз ПО; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; версия пакета обновления ОС; характеристики обнаружения; контрольная сумма (MD5) обрабатываемого объекта; имя обрабатываемого объекта; признак того, что обрабатываемый объект является PE-файлом; контрольная сумма (MD5) маски, по которой была заблокирована веб-служба; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; код типа объекта; заключение ПО по обрабатываемому объекту; путь к обрабатываемому объекту; код каталога файлов; версия компонента ПО; версия отправляемой статистики; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); тип клиента, используемого для обращения к веб-службе; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; IP-адрес (IPv6) веб-службы, на который осуществлялось обращение; веб-адрес источника запроса к веб-службе (referer); обрабатываемый веб-адрес;

- информация о проверяемых объектах (версия приложения, извлеченная из AndroidManifest.xml; решение ПО по приложению; метод, использованный для получения решения ПО по приложению; название пакета установщика магазина; название пакета (package/bundle) из androidmanifest.xml; категория Google SafetyNet; признак того, что SafetyNet включен на устройстве; значение SHA256 в ответе от Google SafetyNet; APK Signature Scheme для APK-сертификата; код версии установленного ПО; серийный номер сертификата, которым подписан APK; название устанавливаемого APK-файла; путь до устанавливаемого APK-файла; компания, выпустившая сертификат, которым подписан APK-файл; публичный ключ, которым подписан APK-файл; контрольная сумма сертификата, которым подписан APK-файл; дата и время истечения сертификата; дата и время выдачи сертификата; версия отправляемой статистики; алгоритм расчета отпечатка цифрового сертификата; хеш MD5 от установленного APK-файла; Хеш MD5 от DEX-файла, расположенного внутри установленного APK-файла; динамические разрешения, которые есть у приложения; версия стороннего ПО; информация о том, является ли приложение SMS-менеджером по умолчанию; информация о том, есть ли у приложения права администратора устройства; признак того, что приложение находится в системном каталоге; информация о том, использует ли приложение специальные возможности (accessibility));

- информация обо всех потенциально вредоносных объектах и действиях (содержимое фрагмента в обрабатываемом объекте; дата и время истечения сертификата; дата и время выдачи сертификата; идентификатор ключа из хранилища ключей, используемого для шифрования; протокол, используемый для передачи данных в KSN; порядковый номер фрагмента в обрабатываемом объекте; данные внутреннего журнала, сформированного антивирусным компонентом ПО для обрабатываемого объекта; наименование эмитента сертификата; публичный ключ сертификата; алгоритм вычисления публичного ключа сертификата; серийный номер сертификата; дата и время подписи объекта; имя и параметры владельца сертификата; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования; дата и время последней модификации обрабатываемого объекта; дата и время создания обрабатываемого объекта; обрабатываемые объекты или их части; описание обрабатываемого объекта, указанное в его свойствах; формат обрабатываемого объекта; тип контрольной суммы обрабатываемого объекта; контрольная сумма (MD5) обрабатываемого объекта; имя обрабатываемого объекта; контрольная сумма (SHA256) обрабатываемого объекта; размер обрабатываемого объекта; название продавца ПО; заключение ПО по обрабатываемому объекту; версия обрабатываемого объекта; источник заключения по обрабатываемому объекту; контрольная сумма обрабатываемого объекта; имя приложения, частью которого является обрабатываемый объект; путь к обрабатываемому объекту; информация о результатах проверки подписи файла; ключ сеанса входа; алгоритм шифрования ключа сеанса входа; время хранения обрабатываемого объекта; алгоритм расчета отпечатка цифрового сертификата);

- тип сборки, например, "user" или "eng"; полное имя продукта; производитель продукта / устройства; разрешена ли установка приложений не из Google Play; статус облачной службы по проверке приложений от Google; статус облачной службы по проверке приложений от Google, устанавливаемых через ADB; текущее название или строка "REL" для публичных сборок; инкрементальный номер сборки; строка версии, отображающаяся у пользователя; название устройства пользователя; идентификатор сборки ПО, отображающийся у пользователя; отпечаток прошивки; идентификатор прошивки; признак рутованности устройства; операционная система; название ПО; тип используемой лицензии ПО;

- информация о качестве работы сервисов KSN (протокол, используемый для передачи данных в KSN; идентификатор службы KSN, к которой обращается ПО; дата и время окончания получения статистик; количество подключений к KSN, взятых из кеша; количество запросов, для которых был найден ответ в локальной базе запросов; количество неуспешных подключений к KSN; количество неуспешных KSN-транзакций; распределение по времени выполнения отмененных запросов к KSN; распределение по времени выполнения неуспешных подключений к KSN; распределение по времени выполнения неуспешных KSN-транзакций; распределение по времени выполнения успешных подключений к KSN; распределение по времени выполнения успешных KSN-транзакций; распределение по времени выполнения успешных запросов к KSN; распределение по времени выполнения запросов к KSN, превысивших ограничение на время ожидания; количество новых подключений к KSN; количество неуспешных запросов к KSN из-за ошибок маршрутизации; количество неуспешных запросов из-за выключенного KSN в параметрах ПО; количество неуспешных запросов к KSN из-за сетевых проблем; количество успешных подключений к KSN; количество успешных KSN-транзакций; количество выполненных 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: хеш MD5 APK-файла; информация о перекрывающем приложении: хеш MD5 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: хеш MD5 APK-файла; информация о перекрытом приложении: хеш MD5 файла classes.dex; информация о перекрытом приложении: имя файла APK; информация о перекрытом приложении: путь к файлу APK без имени файла; информация о перекрытом приложении: название пакета приложения (для перекрытого приложения: если реклама отображается на пустом экране, должно быть значение "launcher"); дата и время перекрытия; информация о перекрывающем приложении: название пакета приложения; ширина перекрытия;

- параметры используемой точки доступа Wi-Fi (тип обнаруженного устройства; настройки протокола DHCP (контрольные суммы локального IPv6-адреса шлюза, DHCP IPv6, DNS1 IPv6, DNS2 IPv6, контрольная сумма длины префикса сети; контрольная сумма локального адреса IPv6); настройки DHCP (контрольные суммы: локального IP-адреса шлюза, DHCP IP, DNS1 IP, DNS2 IP, маски подсети); признак наличия домена DNS; контрольная сумма выданного локального IP-адреса (IPv6); контрольная сумма выданного локального IP-адреса (IPv4); признак работы устройства от электрической сети; тип аутентификации Wi-Fi сети; список доступных Wi-Fi сетей и их параметры; контрольная сумма (MD5 с модификатором) MAC-адреса точки доступа; контрольная сумма (SHA256 с модификатором) MAC-адреса точки доступа; типы соединений, поддерживаемые точкой доступа Wi-Fi; тип шифрования сети Wi-Fi; локальное время начала и конца подключения к сети Wi-Fi; идентификатор сети Wi-Fi, посчитанный по MAC-адресу точки доступа; идентификатор сети Wi-Fi, посчитанный по её названию; идентификатор сети Wi-Fi, посчитанный по её названию и MAC-адресу точки доступа; уровень сигнала сети Wi-Fi; название Wi-Fi сети; набор протоколов аутентификации, поддерживаемых этой конфигурацией; используемый протокол аутентификации при подключении вида WPA-EAP; используемый протокол внутренней аутентификации; набор групповых шифров, поддерживаемых этой конфигурацией; набор протоколов управления ключами, поддерживаемых этой конфигурацией; итоговая категория публичности сети в ПО; итоговая категория безопасности сети в ПО; набор парных шифров для WPA, поддерживаемых этой конфигурацией; набор протоколов безопасности, поддерживаемых этой конфигурацией);

- дата и время установки ПО; дата активации ПО; идентификатор компании партнера, у которого был размещен заказ на покупку лицензии на использование ПО; идентификатор ПО, полученный из лицензии; серийный номер лицензионного ключа ПО; локализация ПО; признак участия в KSN; идентификатор ПО, для которого предназначена лицензия; идентификатор лицензии ПО; идентификатор ОС; разрядность операционной системы.

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:

- информация о приложении: версия, идентификатор, название и идентификатор приложения в сервисе Firebase, уникальный идентификатор установки в сервисе Firebase, название магазина, из которого ПО было получено, время первого запуска ПО на устройстве;
- идентификатор установки приложения на устройство и способ установки на устройство;
- информация о регионе и языковой локализации;
- разрешение экрана устройства;
- информация о получении root -прав пользователем;
- диагностические данные об устройстве от сервиса SafetyNet Attestation;
- признак установки Kaspersky Endpoint Security для Android в качестве службы Специальных возможностей;
- информация о переходах между окнами приложения, продолжительности сессии, начале и окончании сессии работы с экраном, названии экрана;
- информация 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;
- информация о лицензии на приложение, ее наличии, количестве устройств;
- интервалы обновления антивирусных баз и синхронизации с Сервером администрирования;
- информация о консоли администрирования (Kaspersky Security Center или сторонние EMM-системы);
- идентификатор Android ID;
- идентификатор Advertising ID;
- информация о пользователе: возрастная категория и половая принадлежность пользователя, идентификатор страны проживания, список интересов пользователя;

- информация о компьютере, на котором установлено ПО: название производителя компьютера, тип компьютера, модель устройства, версия и информация о языковой локализации ОС, информация о первом запущенном приложении за последнюю неделю и ранее.

  Передача данных в сервис Google Analytics для Firebase осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Google Analytics для 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.

Firebase Performance Monitoring

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Firebase Performance Monitoring для их обработки для заявленных целей:

- уникальный идентификатор установки;
- название пакета приложения;
- версия установленного ПО;
- уровень и статус заряда батареи;
- оператор связи;
- признак работы ПО в фоновом режиме;
- регион;
- IP-адрес;
- код языка устройства;
- информация о радио- и интернет-соединении;
- идентификатор-псевдоним экземпляра ПО;
- ОЗУ и размер диска;
- признак того, что на устройстве выполнена процедура рутинга или джейлбрейка;
- уровень сигнала;
- продолжительность автоматической трассировки;

- информация о сети и сопутствующая информация ответа: код ответа, размер полезной нагрузки в байтах, время отклика;
- описание устройства.

  Передача данных в сервис Firebase Performance Monitoring осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Firebase Performance Monitoring доступна по адресу https://firebase.google.com/support/privacy.

Crashlytics

При использовании ПО следующие данные будут автоматически отправляться на регулярной основе в сервис Crashlytics для их обработки для заявленных целей:

- идентификатор ПО;
- версия установленного ПО;
- признак работы ПО в фоновом режиме;
- архитектура ЦП;
- уникальный идентификатор события;
- дата и время события;
- модель устройства;
- объем полного и используемого дискового пространства;
- название и версия ОС;
- объем полной и используемой оперативной памяти;
- признак того, что на устройстве выполнена процедура рутинга;
- ориентация экрана в момент события;
- производитель продукта / устройства;
- уникальный идентификатор установки;
- версия отправляемой статистики;
- тип исключения ПО;
- текст сообщения об ошибке;
- признак того, что исключение ПО вызвано исключением на вложенном уровне;
- идентификатор потока;
- признак того, что фрейм стал причиной ошибки ПО;
- признак того, что выполнение потока привело к неожиданному завершению работы ПО;

- данные о сигнале, который привел к неожиданному завершению работы ПО: название сигнала, код сигнала, адрес сигнала;
- для каждого фрейма, ассоциированного с потоком, исключением или ошибкой: имя файла фрейма, номер строки файла фрейма, отладочные символы, адрес и смещение в бинарном образе, отображаемое имя библиотеки, содержащей фрейм, тип фрейма, признак того, что фрейм стал причиной ошибки;
- идентификатор ОС;
- идентификатор проблемы, связанной с событием;
- информация о событиях, предшествующих неожиданному завершению работы ПО: идентификатор события, дата и время события, тип события и значение;
- значения регистра ЦП;
- тип события и значение.

  Передача данных в сервис Crashlytics осуществляется по защищенному каналу. Информация об условиях обработки данных в сервисе Crashlytics доступна по адресу https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

Предоставление вышеуказанной информации для обработки в маркетинговых целях является добровольным.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Предоставление данных в Kaspersky Security для iOS

Kaspersky Security для мобильных устройств соответствует Общим нормам защиты данных (GDPR).

Чтобы установить приложение, пользователь устройства должен прочитать и принять условия следующих положений, касающихся обработки персональных данных пользователя:

- Лицензионное соглашение;
- Политика конфиденциальности для продуктов и сервисов.

При желании пользователь может прочитать и принять условия следующего положения:

- Положение о Kaspersky Security Network.

Пользователь может просмотреть условия этих документов в любое время в разделе **О приложении** → **Соглашения и положения** в настройках Kaspersky Security для iOS. Также в этом разделе пользователь может принять или отклонить условия Положения о KSN.

Обмен информацией с Kaspersky Security Network

Для повышения уровня оперативной защиты Kaspersky Security для iOS использует облачную службу Kaspersky Security Network в работе компонента **Веб-Фильтр**. Приложение выполняет проверку веб-ресурсов перед открытием с учетом данных, полученных от KSN.

Информация о типах данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы компонента Веб-Фильтр, приведена в Лицензионном соглашении. Принимая условия Лицензионного соглашения, вы соглашаетесь передавать эту информацию.

Информация о типах статистических данных, передаваемых в "Лабораторию Касперского" при использовании KSN во время работы мобильного приложения Kaspersky Security для iOS, приведена в Положении о Kaspersky Security Network. Принимая условия этого Положения, вы соглашаетесь передавать эту информацию.

Предоставление данных в рамках Лицензионного соглашения

Если для активации ПО применяется Код активации, с целью проверки правомерности использования ПО Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- Формат данных в запросе к инфраструктуре Правообладателя; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; размер содержимого запроса к инфраструктуре Правообладателя; идентификатор протокола; код активации ПО; тип сжатия данных; идентификатор ПО; набор идентификаторов ПО, которое может быть активировано на устройстве пользователя; локализация ПО; полная версия ПО; уникальный идентификатор устройства; дата и время на устройстве пользователя; идентификатор установки ПО (PCID); код активации ПО, используемый в настоящее время; версия ОС, номер сборки ОС, номер обновления ОС, редакция ОС, расширенная информация о редакции ОС; модель устройства; код оператора мобильной связи; семейство операционной системы; идентификатор ПО, полученный из лицензии; список соглашений, отображенных пользователю ПО; тип юридического соглашения, условия которого были приняты пользователем в ходе использования ПО; версия юридического соглашения, условия которого были приняты пользователем в ходе использования ПО; признак принятия пользователем условий юридического соглашения в ходе использования ПО; тип контрольной суммы обрабатываемого объекта; заголовок лицензии на использование ПО; идентификатор регионального центра активации; дата и время создания лицензионного ключа ПО; идентификатор лицензии ПО; идентификатор информационной модели, примененной при предоставлении лицензии на использование ПО; дата и время истечения срока действия лицензии на использование ПО; текущий статус лицензионного ключа ПО; тип используемой лицензии ПО; тип лицензии, с помощью которой активировано ПО; идентификатор ПО, полученный из лицензии.

Правообладатель может также использовать такую информацию для получения статистической информации о распространении и использовании ПО Правообладателя.

Для защиты Компьютера от угроз информационной безопасности Пользователь соглашается периодически предоставлять Правообладателю следующую информацию:

- формат данных в запросе к инфраструктуре Правообладателя; адрес веб-службы, на который осуществлялось обрабатываемое обращение (веб-адрес, IP); номер порта; веб-адрес источника запроса к веб-службе (referrer);

- полная версия ПО; идентификатор обновления ПО; тип установленного ПО; идентификатор ПО; идентификатор конфигурации; результат действий, выполненных ПО; код ошибки;

- обрабатываемый веб-адрес; IP-адрес (IPv4) веб-службы, на который осуществлялось обращение; отпечаток цифрового сертификата проверяемого объекта и алгоритм хеширования; тип сертификата; содержимое обрабатываемого цифрового сертификата.

Предоставление данных в рамках Положения о Kaspersky Security Network

При принятии Положения о KSN, Правообладатель автоматически получает и обрабатывает следующие данные:

- 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;

- дата и время установки ПО; дата активации ПО; локализация ПО; признак участия в KSN; идентификатор ПО, для которого предназначена лицензия; идентификатор лицензии ПО; идентификатор ОС; версия установленной операционной системы на компьютере пользователя; разрядность операционной системы.

Участие в Kaspersky Security Network для обработки статистических данных является добровольным. Вы можете в любой момент отказаться от участия в Kaspersky Security Network.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Обращение в Службу технической поддержки

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Способы получения технической поддержки

Если вы не нашли решения вашей проблемы в документации или других источниках информации о Kaspersky Security для мобильных устройств, обратитесь в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Security для мобильных устройств.

"Лаборатория Касперского" обеспечивает поддержку Kaspersky Security для мобильных устройств в течение его 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:

- Посетить веб-сайт Службы технической поддержки
- Отправить запрос в Службу технической поддержки с портала Kaspersky CompanyAccount

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

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.

Страница Kaspersky Security для мобильных устройств 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 приложений Kaspersky Endpoint Security для Android и Kaspersky Security для iOS вы можете найти информацию о настройке и использовании мобильных приложений.

Обсуждение программ "Лаборатории Касперского" на форуме

Если ваш вопрос не требует срочного ответа, вы можете обсудить его со специалистами "Лаборатории Касперского" и с другими пользователями на нашем Форуме.

На Форуме 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.

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 Private Security Network (KPSN)

Kaspersky Private Security Network – это решение, предоставляющее пользователям устройств с установленными программами "Лаборатории Касперского" доступ к репутационным базам данных Kaspersky Security Network и другим статистическим данным без отправки данных с устройств в Kaspersky Security Network. Kaspersky Private Security Network разработан для корпоративных клиентов, которые не могут участвовать в Kaspersky Security Network по следующим причинам:

- Устройства не подключены к интернету.
- Передача любых данных за пределы страны или корпоративной локальной сети запрещена законом или корпоративными политиками безопасности.

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 можно получить в Kaspersky Security Center. Он нужен, чтобы разблокировать устройство после выполнения команд **Блокирование и Поиск**, **Сирена** или **Тайное фото**, а также при срабатывании самозащиты.

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, блокировка 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.

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.

Устройство в режиме supervised

iOS-устройство, параметры которого контролируются в Apple Configurator – программе для групповой настройки iOS-устройств. Устройство в режиме supervised имеет статус *supervised* в Apple Configurator. При каждом подключении устройства в режиме supervised к компьютеру Apple Configurator проверяет конфигурацию устройства на соответствие заданным эталонным параметрам и при необходимости настраивает ее. Устройство в режиме supervised не может быть синхронизировано с Apple Configurator, установленном на другом компьютере.

Для устройств в режиме supervised в политике Kaspersky Device Management для iOS можно переопределить больше параметров, чем для неконтролируемых устройств. Например, можно настроить HTTP-прокси сервер для контроля интернет-трафика на устройстве в корпоративной сети. По умолчанию все мобильные устройства являются неконтролируемыми.

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 несанкционированного доступа к конфиденциальным данным пользователей.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Информация о стороннем коде

Информацию о стороннем коде можно загрузить и ознакомиться с ней в следующих файлах:

- legal_notices_Android.txt (для приложения Kaspersky Endpoint Security для Android)
- legal_notices_iOS.txt (для приложения Kaspersky Security для iOS)

На мобильных устройствах информация о стороннем коде доступна в разделе **О приложении** мобильных приложений.

Справка для этой версии решения больше не обновляется, поэтому может содержать устаревшую информацию. Актуальная информация о решении доступна в справке Kaspersky Secure Mobility Management 5.0.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

PostScript – зарегистрированный товарный знак или товарный знак Adobe в США и/или других странах.

Apple, Apple Configurator, AirDrop, AirPlay, AirPort, AirPort Express, AirPrint, Aperture, App Store, Apple Music, Apple TV, Apple Watch, Bonjour, Face ID, FaceTime, FileVault, Find My, Handoff, iBooks, iBooks Store, iCal, iCloud, iCloud Keychain, iMessage, iPad, iPadOS, iPhone, iPhoto, iTunes, iTunes Store, iTunes U, Keychain, OS X, Safari, Siri, Spotlight и Touch ID – товарные знаки Apple Inc.

Aruba Networks – товарный знак Aruba Networks, Inc. в США и некоторых других странах.

Словесный товарный знак Bluetooth и лого принадлежат Bluetooth SIG, Inc.

Aironet, Cisco, Cisco AnyConnect, и IOS являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Dell Technologies, Dell, SecurID и другие товарные знаки являются товарными знаками компании Dell Inc или её дочерних компаний.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Gmail, Google Analytics, Google Assistant, Google Chrome, Google Mail, Google Maps, Google Play, Google Safe Browsing, Google SafeSearch, Google Translate, Nexus, SPDY и YouTube – товарные знаки Google LLC.

HTC – товарный знак HTC Corporation.

Huawei, HUAWEI и EMUI являются товарными знаками Huawei Technologies Co., Ltd.

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 и Windows Phone являются товарными знаками группы компаний Microsoft.

MOTOROLA и стилизованный логотип M являются зарегистрированными товарными знаками Motorola Trademark Holdings, LLC.

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.

SonicWALL, Aventail, SonicWALL Mobile Connect – товарные знаки SonicWall, Inc.

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.

AirWatch, VMware и VMware Workspace ONE – товарные знаки VMware, Inc. или зарегистрированные в США и/или других юрисдикциях товарные знаки VMware, Inc.

Mozilla и Firefox являются товарными знаками Mozilla Foundation в США и других странах.

F5 – товарный знак F5 Networks, Inc. в США и в некоторых других странах.